THE INVESTIGATOR'S GUIDE TO COMPUTER CRIME

ABOUT THE AUTHOR

Carl J. Franklin has more than twenty years experience in the criminal justice profession. He spent almost thirteen of those years in a uniform working as a Community Service Officer, Police Officer, and in various roles as investigator and supervisor. He has worked in a uniform position with the University of Oklahoma, Norman, and Oklahoma City police departments. While a police officer, Franklin returned to the University of Oklahoma to complete a Bachelor's of Arts degree in Law Enforcement Administration. He later attended the Oklahoma University College of Law where he completed the Juris Doctor degree and was honored on three occasions with national awards for his writing in the areas of computers and constitutional law. He has also recently completed the Ph.D. in Business with an emphasis in Public Administration.

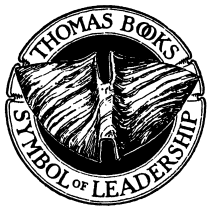
Franklin has also worked with the Oklahoma Court of Criminal Appeals, the Cleveland County District Attorney's Office, and as a private practitioner. He was appointed in three counties as the chief attorney for indigent defense, and maintained an active practice in criminal defense, police civil liability, and related areas.

He is the author of five books, including the *Police Officer's Guide to Civil Liability* (Charles Thomas) and more than forty professional and academic articles. Franklin currently works as an Assistant Professor (Tenure Track) at Southern Utah University where he teaches criminal and constitutional law, criminal procedure, ethics, and related classes.

THE INVESTIGATOR'S GUIDE TO COMPUTER CRIME

By

CARL J. FRANKLIN, J.D., PH.D.



CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

ISBN 0-398-07601-4 (hard)
ISBN 0-398-07602-2 (paper)

Library of Congress Catalog Card Number: 2005050873

With THOMAS BOOKS *careful attention is given to all details of manufacturing and design. It is the Publisher's desire to present books that are satisfactory as to their physical qualities and artistic possibilities and appropriate for their particular use.* THOMAS BOOKS *will be true to those laws of quality that assure a good name and good will.*

Printed in the United States of America
MM-R-3

Library of Congress Cataloging-in-Publication Data

Franklin, Carl J., 1958-
The investigator's guide to computer crime / by Carl J. Franklin.
p. cm.
Includes bibliographical references and index.
ISBN 0-398-07601-4 – ISBN 0-398-07602-2 (pbk.)
1. Computer crimes–Investigation–Handbooks, manuals, etc. I. Title.

HV8079.C65F73 2005
363.25'968–dc22

2005050873

To Christopher, Michael, and Stacey.
You make me very proud.

CONTENTS

Section 2: Specific Computer Crimes

Section 3: The Computer Crime Investigation

Section 4: Search, Seizure, and Digital Evidence

FIGURES

TABLES

THE INVESTIGATOR'S GUIDE TO COMPUTER CRIME

Section 1

ESTABLISHING STANDARDS FOR THE COMPUTER CRIME INVESTIGATION

Chapter 1

THE GROWING TREND OF COMPUTER CRIME

A. INTRODUCTION TO COMPUTER CRIME

In the past half-century we have gone from a world where computers were science fiction to a world where computers are everyday fact. Just thirty years ago the computer that flew with the first astronauts to the moon had less computing power than the computer on the average student's desk today. Computers have grown in popularity, acceptance, and computing power. The average Personal Computer has doubled its computing capacity every eighteen months for more than a decade. Today, we find computers common in almost all parts of our life and there is no reason to believe that usage will decrease in the near future.

Along with the acceptance of computers in our everyday life has emerged a new line of crime revolving around the computer. Just as computers make daily business transactions more efficient they have also made many crimes more efficient. Computers have given us many new advances in our lives and provided great improvement as a whole. This is also true of the criminal element; computers have created contemptible new crimes as well as modernized many of the old ones.

For the law enforcement officer the first major issue is the determination

of how much emphasis to put on the problem. Clearly, computers have become a growing part of our everyday work as criminal investigators, but does that mean they should become a specialization unto themselves? Should departments create a "computer crime" unit similar to our traditional homicide, robbery, and burglary units?

We know that computers have made a substantial impact on our society, but have computer crimes become so significant that they demand special attention? The short answer is that it has not; at least yet. While the number of computer-related crimes has increased over the last two decades the vast majority of police officers rarely are involved in a computer crime. What this means is that while we should be conscious of the increase in computer-related crime, we need not create entire new branches of investigative theory to deal with that crime. For the most part, focused education and training can prepare the majority of police investigators to handle almost any computer crime they encounter.

One should not infer from the above statement that computer crime is not a problem. The fact is that computer crime is on the increase, and there is firm evidence to believe that the growth trend will continue for some time to come. Investigators should also keep in mind the rise in computers as both a tool and potential element of crime. Just as computers have helped the police in becoming more efficient, so too, have they assisted wary criminals in perpetrating a wide variety of crimes. This trend is likely to continue, and for that reason alone police investigators should make themselves better prepared for computer-related crime investigations.

The obvious choice for most police agencies is a combination of upgrading our technology along with an increase of our knowledge so that we become more efficient in our pursuits. Of course, this will vary according to specific needs of the department or the investigative unit. It is clear that a vice unit does not need an advanced computer system when making routine prostitution arrests, but it is equally clear that an investigator will need some computer knowledge if he is to track money transactions stored by pimps on laptop computers. Simply stated, the increased use of computers by traditional criminals significantly increases the need for investigators to be computer competent.

The above example illustrates a crime which is not traditionally considered a computer crime but which does involve the use of a computer. Basic computer knowledge may be all that is needed to conduct this investigation, but what about crimes where the computer is a substantial part of the *modus operandi*? In coming chapters we will examine this issue in much more detail, but for now it is important to recognize that computer crime extends far beyond the original definitions set out by the industry.

Another, and sometimes more pressing issue, which often arises focuses

on the logistics of computer use in both crime and criminal detection. A nagging question facing the police community today is whether police agencies expend significant man-hours and resources preparing for crimes that are often difficult to detect and even more difficult to prosecute? A better way to look at this issue is to ask whether traditional investigative techniques, those that are used in less technologically advanced crimes, are enough to determine who has released the latest virus?

The potential for computer crime is almost limitless. As computers invade more of our everyday lives the need for competent investigators grows. For each of the issues set out above the answers all appear to be relatively the same. In each instance we can find a need for increased knowledge as well as better technology. In other words, to be effective, investigators in today's climate must move ahead both in understanding technology and in their preparedness to investigate computer-related crime.

To better prepare we must focus on training that will upgrade our knowledge and skills. That is the purpose of this book. To begin this task we must first establish some basic guidelines so that all readers will advance significantly in their knowledge and skills. We do this by first establishing basic principles, definitions, and techniques. The first of these is a definition of computers and computer crime.

B. DEFINING COMPUTER AND TECHNOLOGY CRIME

Defining computers and computer-related crime might seem simple on the surface, but therein lays the difficulty of the task. If we define both too broadly then we risk creating a menace that never appears. Define the terms too narrowly and we chance missing the real problem when it comes. In order to hit the proverbial nail on the head we should start with a simple definition, refine it, and then establish a usable working definition that will serve our purposes.

The simplest definition we can use is that "computer crime is any crime involving a computer." Almost immediately one can see that such a simple definition creates critical problems. In our highly mechanized and computerized world to define computer crime so broadly would be to catalog almost any crime as a computer crime. After all, consider the number of appliances in our homes that have some sort of computer system built into them. Today it is hard to buy a microwave, refrigerator, dishwasher, or any other major appliance without having it operate with a *Central Processing Unit* (CPU) of some type.

One of the problems with such a broad definition is that the investigator spends more time defining the crime than investigating it. Imagine for a

moment what would happen if we define computer crime as "any crime involving a processing unit or computer." Every automobile stolen today would now be a computer crime. After all, virtually every car sold has an ignition or emissions system controlled by a computer chip. This creates a false dilemma, and that is what we wish to avoid.

To avoid this type of overgeneralization we must move toward a definition that more clearly defines those crimes that involve a computer. While we might say that any crime involving a computer is a computer crime we are really missing the heart of the issue. A computer crime is much more than the simple presence of a computer in the overall crime. It requires that the computer be a central part of–or at least a significant component of–the crime itself. By adding this element we see that a computer crime is any crime which involves a computer as a central or significant part of the criminal act. In other words, a computer crime is a crime that focuses on the computer as target or uses a computer to perpetrate the crime. Thus, our definition of computer crime now contains three distinct elements. These are:

1. Use of or focus on
2. A computer
3. For the purpose of a criminal act

The above definition certainly provides us with a more sophisticated definition of computer crime, but is it good enough? To answer that let us go back to our example of the automobile. Most will agree that the automobile engine in the twenty-first century is controlled by a sophisticated computer system. Imagine, for a moment, that a would-be bank robber uses a new car as a getaway vehicle. Using the above definition we might argue that we in fact have a computer-related crime. After all, the car was used in the crime in the sense that if provided transportation to and from the bank. In the broadest sense one might argue that since a computer was a central part of the overall control of the automobile it is therefore a central part of the crime of robbery.

Of course, one might immediately wonder why we would spend such time on something that seems so trivial. The reason is simple: defense attorneys. Modern defense attorneys often seek any loophole possible to serve their client's needs. This is a pivotal part of our justice system, and without this ability the "adversarial system" that also helps protect our individual rights would be virtually useless. So, while the ability of the attorney to find such loopholes might serve a greater purpose, the simple fact is that poorly written or administered laws provide such loopholes. In this instance, a computer crime–which is often considered a non-violent crime–could be substituted for the more heinous act of bank robbery.

To combat this type of misuse of the criminal statutes we must carefully define what we are dealing with. The problem in this sense is that while we have defined what a computer crime may be we really haven't defined what constitutes a computer for our purposes. We are using a very broad definition of a computer in this instance. To better identify the true computer crime we not only need a definition of computer crime but also a clear definition of a computer. Without such a definition then we can easily fall back into the dilemma we face with automobiles.

The first step in this practice is to define the terms in the most common methods. To give to the terms the "common meaning" of those terms, we will turn to one of the best known sources of definitions. The *Merriam-Webster Dictionary* (2001) defines the term computer as "a programmable electronic device that can store, retrieve, and process data." This is a very good working definition of a computer and one that we can use to build a better definition of computer crime. We can see, though, that there are already problems with such a definition. After all, the computer-controlled ignition system of a car relies on a unit that can "store, retrieve, and process data."

Working with this simple definition we can now begin to refine what a computer is, at least for the purposes of defining computer crime. At the heart of our definition is the ability of the electronic device to be programmed. This should not be confused with the process of automating a device. For instance, a dishwasher may be automated through the use of mechanical switches and spring-loaded timers. As the timer advances, different wash, rinse, and dry cycles are turned on and off automatically. Simply because electricity is used to operate motors within the machine does not make this a computer system.

On the other hand, if we use an electronic component rather than a spring-loaded timer to give the instructions for turning on and off different cycles, we are getting closer to something which is programmed. In essence, to program a computer means to install instructions that the processing unit interprets and acts upon. Thus, a dishwasher can be computer driven when a programmable electronic device is used.

What then is a programmable electronic device? In defining this term we look first to the core elements of the term itself. First, the device must be programmable. This means the device must be capable of receiving instruction. Again, we must not confuse instruction with automation. For instance, setting a lever so that it falls when a bucket fills with water from a stream may be automated but it is not programmed. To truly be programmable the device must be capable of receiving multiple instructions and having those instructions altered to meet the needs of the system.

Second, the device must be electronic. This alleviates a significant portion of mechanical devices immediately. Some electronic devices might also be

easily excluded. Devices such as switches, tubes, transformers, and similar apparatus may be electronic but they generally serve a single purpose. To be truly programmable the device must be capable of receiving varied instruction and having the instruction change as needed by the system or entered by the user.

For our purposes we can now narrow the definition of computer to *an electronic device capable of being programmed and which can store, retrieve, and process data.* This definition focuses on the central features of the computer as well as the reason for its existence. In this sense we see that a computer can be much more than a device for automation. Now that we have a working definition of computer we can turn back to the task of defining computer crime. By applying our definition of computer we see that we now narrow our definition of computer crime as well. Because a computer, for our purposes, is not merely a device inserted to help control or automate another machine, therefore we have excluded some of the more confusing issues.

To some extent these definitions will become more refined as we explore computers and computer crime in more detail. For now, though, we can get a much better understanding of computer crime by looking at the various statutory definitions that have evolved in the recent past.

C. ESTABLISHING PARAMETERS FOR INVESTIGATING COMPUTER CRIME

In some respects computer crime is very similar to many other crime types we see as investigators. But in many other respects computer crime is much different and requires the investigator to approach the inquiry in an otherwise unconventional fashion. This section focuses briefly on those principles that make computer crime different.

Before investigating computer crime one must have a firm grasp of the computer and the "product" created with it. In recent years the term "cyber" has been tossed about when explaining anything related to computers. Likewise, the term "e-commerce," "e-mail," and "e-security" evolved to help identify otherwise routine transactions which are done through a computer. The need to create new terms and references is our first hint that we are dealing with something quite different.

When dealing with computers it is important to note that we may be dealing with both tangible and intangible properties. The tangible aspect of the computer generally includes the hardware, printouts, floppy disks, and related items. The intangible includes computer code, data, information, and the manipulation of data inside the computer.

Understanding the difference between tangible and intangible helps us to

establish the first real principle or parameter of computer investigation. An investigator must understand fully that by its very nature the computer is both tangible and intangible. For that reason it is quite unlike anything else involved in the typical investigation. On the one hand it is something very easy to see and observe while on the other hand it is something that can be neither seen nor touched. The computer is that thing sitting on all of our desktops, but it is also the work produced by the electrons passing through the process. It has a keyboard, mouse, monitor, and a box where one inserts a floppy disk, but it also has output, input, and calculations at hundreds if not millions of times per second.

Many choose to view the computer as nothing more than a machine. It has individual parts, which by themselves do little or nothing, but when put together in the proper order creates literally a "thinking machine." The "work" of the computer is done at the atomic level. We use the computer to push electrons around inside a slim wafer of silicon. Ask the average person on the street how a computer works and you will likely get a blank stare. Ask them to point out a computer and almost everyone can. The principle is that while we may know what computers are do we really understand how they work?

For the investigator this principle means that we can be dealing with nothing more than a stolen item of property. The stolen computer is no different from the stolen television, stereo or automobile. As such the investigation may be no different from those of any other tangible item. But what about when the investigation is of stolen information? Is stolen information the same as a stolen television? Consider that in many cases the information is not actually taken from the computer, but merely copied or electronically analyzed from another computer. This grows even more complicated when one realizes that the "theft" may occur over great distances and in milliseconds. Is this the same as the investigation of a tangible object?

The investigator must recognize that we are often dealing with a central intangible issue. At its heart, the issues we are dealing with involve electrons that are manipulated by a machine. A computer is nothing more than a complicated electron manipulator, but it is also one that can create, store, and analyze data like no other machine on the planet.

As we will see in Chapter 2, the computer is used to store information, a product without easily defined substance, and manipulate electron representations of that information in order to create new information. What this means is that in dealing with computer crime we are often dealing with something we cannot hold easily in our hands. This is the first criterion we must understand to become a successful investigator: computer crimes may involve tangible and intangible items.

Another important principle is that most computer crime occurs outside

public view. Unlike the bank robbery where the investigator may have a dozen witnesses or more the computer criminal rarely is seen by anyone. In fact, in most instances the computer crime is not detected until some time after it has occurred and there are no direct eyewitnesses to the crime. This often creates unique issues for the investigator since it will certainly affect the external sources of information, such as witnesses, which may be used in the case.

Witnesses that are most likely to be useful when dealing with computer crime are those which typically have secondary or circumstantial information. For instance, a salesman who can verify the sale of a particular brand of computer, hard disk, modem, or other device to a suspect may be useful in later linking the hardware to that person. A witness might also be a technician who installed new phone line, DSL, or other communications link into the house of the suspect. Other witnesses might include the clerk who maintains calling records for the telephone company or otherwise keeps records of connect time for the *Internet Service Provider* (ISP).

Each of these witnesses can contribute useful testimony, but it is rare that we have a true eyewitness unless it is a co-conspirator. Even then the actual witnesses of the crime may be limited. In many cases involving computer espionage or trespass the co-conspirators worked separate from each other. In some instances they were separated by hundreds of miles and communicated only by phone, fax, or e-mail. This may mean that the investigator has to coordinate his efforts over a great distance and even varying time zones.

Another criterion that is often different in computer crime is the nature of the evidence that investigators might expect to find. While the traditional property crime, such as burglary, may leave behind fingerprints and other physical evidence the simple fact is that most computer crimes leave behind much different evidence. In most instances the evidence is of an electronic or digital nature rather than a more tangible one. The computer trespasser does not leave behind shoeprints but may leave behind routing codes.

To further complicate many computer cases the investigator must deal with crimes that occur from a distance. Often referred to as the *distance factor* this element is the physical separation of the perpetrator from the crime target. One of the more important issues that arises from the distance factor is determining jurisdiction for both the investigation and subsequent prosecution. Today's "cyber-criminal" can easily reach across political boundaries with little concern for borders or jurisdictional authority in the case.

This distance factor also creates issues for logistics in the investigation. For instance, in many computer trespass cases the perpetrator may be in one state or even another country while the target computer is somewhere else. For the investigator in the target jurisdiction the problems which arise may include the costs of pursuing a criminal across county, state, or even inter-

national borders.

Distance also compounds the issues when one considers the resources needed to conduct an investigation over a great physical distance. The first problem is the one faced with interviewing witnesses who are several hundred if not several thousand miles away. Add to this the problem one might have in retrieving equipment used by a perpetrator when that equipment is a long distance away and one begins to see how logistics are a problem.

Somewhat related to the distance factor are questions related to time. It is important to remember that many computer crimes are not discovered immediately and in some instances may not be discovered until well after the harm has occurred. As most investigators know the more time that passes between event and investigation the less likely the investigator will be successful. It is also likely that the more time elapsed the more contamination there has been to the electronic evidence.

Each of these factors must be carefully weighed and evaluated by the criminal investigator. Each dictates that the investigator have a specific plan of action and methods of operation when conducting the investigation. As we proceed in this book one should carefully note the various parameters, recommendations, and techniques for conducting the investigation. By establishing these criterions early in the inquiry the investigator increases his or her chances of success.

D. TRENDS IN COMPUTER CRIME

There are three specific trends emerging in the area of computer crime. These are the proliferation of viruses and other sadistic acts through the Internet; the rise in attacks against corporate and government sites for purposes of information theft; and the continued increase in the number of young and often aggressive "hackers."

In recent years there have been a growing number of attacks against computer users at all levels by those who release viruses and similar bugs. While some of the high profile cases have gained media attention the simple fact is that hundreds of viruses are released yearly on the computer world. Sadly, most of these virus attacks are either overlooked by authorities or do not merit investigative effort. One reason that many of these attacks are overlooked is the question of authority in the case. Ultimately the question which drives the trends the most is one of logistics; i.e., at what level and by whom will computer crimes be investigated?

Many would assume that the Federal Bureau of Investigation has ultimate jurisdiction, but the reality is that this agency has very limited authority. The crime must often be either one which arises under the specific federal provi-

sions set forth by Congress or under one of the many "exceptions" that exists in the U.S. Code. The simple fact is that the FBI has neither the manpower nor the logistical ability to investigate every computer crime that occurs.

In the high profile cases that originate inside the borders of the United States, or for cases which begin outside the borders but involve targets inside the country, the Federal Bureau of Investigation has taken a lead in conducting investigations. This is generally because the suspect virus has attacked a government computer system or has caused significant turmoil in the general computer industry. On the other hand, when the virus is merely a "nuisance," such as when it attacks only a small number of targets or is limited in some other way, the FBI often ignores the case and prefers that local law enforcement take the lead. This, as we discussed in our opening paragraphs, creates a problem with logistics as well as jurisdiction.

The "nuisance" virus is one that merrily attacks computers at lower levels in the computer hierarchy. For instance, a well-known bug which hides in Microsoft Word documents has been circulating on the Internet for almost five years but has merited little attention by agencies like the FBI. Millions of dollars in lost time and information has been accumulated, but the virus is easily identified and eradicated with modern virus cleansing software. The question, though, is should the FBI, or another police agency, spend countless man-hours and money to track down the virus creator?

Some would suggest that such investigative acts are fruitless. Where a virus of this type causes little harm to any one individual there is no need to expend vast amounts of time and money looking for the perpetrator. After all, these types of viruses are easily dealt with when one has the proper software. But does that make these type of crimes any less costly overall?

Imagine for a moment what would happen if every business in America lost two hours of work production time because someone sprayed sleeping gas into the work area. Would we spend money investigating that type of crime? And is the loss of work time because of a computer virus any different from the sleeping gas?

The fact is that we must address this issue as computer crime investigators. When a report of criminal vandalism crosses our desk do we investigate or simply file it away for later reference in crime statistics? That is a question for all investigators to answer individually.

The second trend in computer crime deals with increased theft of information and hardware at the corporate and government level. For instance, one report on campus security suggested that less than ten percent of all computers on any given college campus are secure from theft. What this means is that a knowledgeable thief may walk into a number of campuses across the nation and walk out with hardware, software, and even information without even the slightest interruption. Most workers in these environ-

ments simply do not take the time to notice such activity, and when they do they often believe that it is "approved" or otherwise legitimate.

Similar "security" holes exist at many of our largest corporations and government office buildings. In one instance the security services for a major corporation actually helped thieves load stolen computer equipment into their van parked just outside the front door. The security personnel later admitted that they did not ask any questions simply because the perpetrators "looked like they belonged."

Likewise, attacks against corporate and government computer systems are not limited to physical takings. Theft of software and information is increasing as well. High among these thefts is the taking of internal information such as memorandums, personnel files, payroll information, and accounting information. Each theft may be minor by itself, but when one considers the sheer number of such thefts each day it is easy to see how widespread computer-related crime is becoming.

Finally, there has been an alarming increase in the number of young computer criminals in the last twenty years. Computers were initially too expensive for the average person to obtain, but over the years the price (and size) of computers has dropped dramatically. This means that there are more computers than ever in our homes and accessible to our children. In fact, most schools today pride themselves on how early they are exposing children to computers.

A byproduct of the computer savvy child is the growth of computer literate thieves. Children today discuss their latest computer conquest in the halls of our schools, on the playgrounds, and over lunch in the cafeteria.

Of course this doesn't mean that every child exposed to a computer early will turn out to use the computer illegally. But one disturbing trend does seem to be emerging; the lack of instruction on computer etiquette or ethics. In a recent survey of public school systems researchers discovered that out of forty-seven school districts surveyed none had a formal method for presenting information on computer etiquette or ethics. Yet, every district in the survey used computers extensively from the kindergarten through senior grade level.

Clearly, the schools have become a focal point of instruction for computer use, and the number of computers available to almost all school children makes this issue rather important. To better understand how this problem is shaping future computer users we need merely look at the "attitude" of schools toward known computer violations. The best known of these violations are those arising under the civil and criminal laws covering copyright. Today, many school age children have easy access to technologies that allow them to easily copy material protected under the copyright laws. Whether it be with the use of a CD-RW drive or through a "peer to peer" sharing pro-

gram such as Napster, the trend tends to be to ignore the widespread violations that occur every day on campus from grade school through graduate school.

Network and computer systems administrators at these sites often admit that they take little action to prevent such violations. "We are not the police" one systems administrator said when asked about the phenomena. The fact remains that while they are not the police, there already exists a duty to prevent crime on their campus. Yet, many administrators, teachers, and computer professionals seem to ignore or simply not understand that duty when it comes to computer violations, and this appears to have a long-term affect on the children being educated in this environment.

One can easily see that children, like adults, do not always see the similarity between stealing a car and illegally copying a software package. At the same time the intrusion into a computer network is nothing like breaking into a person's house. Or is it? And until we teach our children to see the difference there are many commentators who believe that computer crime will only grow worse.

Chapter 2

THE COMPUTER CRIME INVESTIGATION TEAM

A. WHY DO WE NEED A COMPUTER CRIME INVESTIGATION TEAM?

It is well documented that computer crime is on the rise not only in the U.S. but worldwide. Estimates suggest that computer crime will rise by more than six hundred percent in the next ten years. One reason for this is the speed at which computers are spreading through our society. Today users have access to a vast array of computer products including powerful desktop systems, laptops, and even hand-held computers. Simply stated, we can expect a whirlwind of activity when it comes to potential computer crime.

What this means is that police agencies should begin preparing now for the potential impact that computer crime will have in their jurisdiction. Where yesterday's big crime was the armed robbery of a local bank, tomor-

row's will be the electronic theft through the bank's computer system. And only those departments that have taken the time today to prepare will be ready.

Preparing for computer crime is much more than simply understanding computers. In many ways it is much like investigating a homicide or other major crime. Investigators must be well educated in the best techniques for uncovering vital evidence that may help to solve the case. We would never consider sending an untrained detective into a homicide scene so why consider sending an untrained investigator into a computer crime?

For police administrators the first step in establishing effective policies on computer crimes is to recognize the need. This often means simply evaluating the department, the community, and the potential threat. For instance, according to the National Institute of Justice there are over 600,000 law enforcement officers in this country. What is most surprising about that number is that almost ninety-percent of those officers work for departments with ten or fewer officers. This means that over ninety percent of the police agencies in this country will not have the staff to create a dedicated computer crime investigation team.

Simply stated, even if the police administrator for the average department wanted a full-time, dedicated computer crime squad there would be little need for it. In these departments, those with 10 or fewer officers, there is only a limited demand for full-time computer crime teams. That does not mean, though, that there is not a need for some type of computer crime team. Of course, there are those departments that do have a need for the full-time, dedicated team. These departments often create such teams based on the actual increase in computer-related crimes. These departments include most of the major cities in the U.S. as well as many state and federal agencies.

In both instances the departments have made an evaluation based on their individual needs. Smaller departments simply have different needs from larger departments. The only thing that doesn't change is the need to cover specific tasks in the computer investigation, and that is the focus we shall take in this chapter.

B. WHO SHOULD BE ON THE TEAM

At the outset it is important to note that each department will attack this issue from a different perspective. Creating the perfect investigative team will depend to a large extent on funds, manpower, and need. The model we present in this text is not exclusive nor is it exhaustive in its coverage. It is a plan that has worked well for many departments, and with some modification can work very well in your department.

To create a workable model for the computer crime investigative team we must first establish the basic tasks that may be performed at any crime scene. These include physical search, forensic identification, evidence seizure, interviews, photographs or video, and in some instances sketches. With these tasks in mind we will now look at the individual qualities for each of the people who might fill that role.

1. Case Supervisor

Case supervisors are rarely involved in the actual investigation. They serve a broader, more utilitarian function. In most criminal investigations the case supervisor acts as a "watch dog" mechanism to insure that investigators are performing their job in accordance with both law and policy. The same is true in the computer crime case.

At the outset it is clear that while the case supervisor must have at least a working knowledge of computers and computer crime investigation techniques, the simple fact is that the supervisor does not have to be "the expert" in the area. In many instances the lead investigator may have superior knowledge in some areas of computer crime, but as a rule the case supervisor should have sufficient knowledge to handle routine issues which might arise.

The case supervisor may also serve as a liaison between the investigator and others outside the investigation. This frees the investigator from non-case related matters. These might include any dealing with the press, family of the victim, corporate representatives, or even internal personnel. The investigator is free to investigate and so long as he/she informs the supervisor of the progress. It is then the supervisor's duty to handle all other issues.

In some instances case supervisors also serve as the facilitator for working with outside agencies. For instance, the case supervisor may assist with the forensic science side of the investigation. The supervisor can help move evidence through the system and aid in the effective exchange of information. Likewise, the case supervisor often serves as a conduit between investigators and the prosecution. In these instances the supervisor can help direct the investigation and coordinate it with the appropriate personnel in the other areas of the justice system.

2. Physical Search Team

One of the unique characteristics of the computer crime case is the intangible nature of much of what we deal with. Information, as a commodity, can be easily stored in "cyberspace." This means that there may be very little in the way of a physical scene for the investigator to search.

On the other hand, the computer crime case can involve some of the most volatile and fragile evidence ever encountered in a criminal case. Several million dollars in computer programming can be kept on a single CD-ROM disc. This means that the physical scene, while not large in terms of physical characteristics, can be highly important when it comes to overall value. For that reason it is imperative that the computer crime team have search capabilities to deal with the unpredictable nature of the computer crime evidence.

Most departments offer at least some training on the proper methods of crime scene search. The rudiments of crime scene management dictate that the investigator first secure the scene and then control any access that is attempted. The same can be said for the computer crime scene.

The better choice for crime scene control is to have at least two persons designated as crime scene managers. The job of these persons will vary depending on the size of the scene and the nature of the investigation. We will examine this in more detail in sections to come, but for now it is important that we understand that effective management–and ultimately a winning prosecution–will depend on these two people.

a. Guardian

The first of our crime managers is the "guardian" of the scene. Simply stated, this is the person who controls access to the crime scene itself. In many instances this job is given to a less experienced officer in order to free up the veteran officers for other details. This can be a mistake. If the inexperienced officer does not fully understand the nature of their duty then the crime itself can be contaminated, and in too many cases the whole case jeopardized.

The job of the guardian includes three specific items. First, this person must control access by all persons wishing to enter the crime scene. It does not matter who the person is. If they want to go in or out of the scene they must be controlled by the "guardian." In most instances this simply means that the guardian has knowledge of their arrival or departure. In other instances it may mean that the guardian in fact blocks or otherwise restricts access to these persons.

One example would be the refusal to admit press or other non-investigative personnel. Similarly, the guardian may restrict access to other police personnel, including commanders, who wish to "simply look around." In short, if they are not necessary then they are excluded.

The second job of the guardian is to log the person's name as well as time of arrival or departure. This includes the very first officer on the scene and ends only after the very last officer has left. The easiest way to do this is to prepare a simple written log that notes both the person's name and their time of arrival/departure. Many logs also include a short description of the per-

son's activity or reason for being on the scene. Below is an example of such a log used on a crime scene.

NAME	Time In	Time OUT	Purpose or Activity
Lt. Sam Brownstone	1347	1415	Photographer
Dr. Tim Greene	1422	1754	Systems Analyst
Officer Jon Spencer	1455	1532	Crime lab

The third job of the guardian can also be performed by the second member of the crime scene management team. This is the effective control of activity at the scene. As seasoned investigators already know, a busy crime scene can become a hectic place very quickly. Allowing too many people on the scene can also raise significantly the chance that something will be disturbed or otherwise foiled. To help control this, the guardian or other manager must keep constant watch to insure that there are "no more cooks in the kitchen" than is absolutely necessary.

b. Crime Scene Manager

The second member of crime scene search and management team is the crime scene manager. The reason we do not combine the manager with the guardian is that in many instances the two will have jobs that cannot be done simultaneously. For instance, the job of crime scene management often includes the duty of controlling activity on the scene. On a large or very busy crime scene this can best be accomplished by a dedicated crime scene manager and not someone trying to perform other functions such as controlling access to the scene.

The crime scene manager is responsible for controlling all activity that occurs on the crime scene. In some instances the crime scene manager may also be the case supervisor. When possible this should be avoided since the case manager may have duties away from the crime scene. The crime manager must maintain constant control of the crime scene, and an absent manager is an ineffective manager.

Some of the duties that the crime scene manager must perform is the close supervision of all personnel on the scene. Close supervision means simply watching to insure that other personnel on the scene follow the simple protocols established for effective crime scene management. This includes the need to refrain from handling evidence unless absolutely necessary.

Where a search of any site is needed it is extremely important that the team conducting the search understand both what it is that they are looking

for and how to handle the item when they find it. There are few searches where that is more important than the computer crime search. As we discussed in earlier chapters many of the components of a computer system, including the disk drives, floppies, and other items, are very delicate. If not handled properly then the item may be damaged and crucial evidence lost or tainted. Obviously this means that the crime scene manager must also watch to insure that these precautions are taken.

In some investigations the guardian and the crime scene manager also work as investigators. This is often the case in smaller departments where personnel are at a premium. In such instances it is important that the case manager, who may be the chief or other high ranking supervisor, know and understand who has which duties on the scene. This brings us to the search team itself, and the duties each of these members may have.

c. Lead Investigator

There is some controversy over whether the lead investigator should be involved in the search. The arguments for not using the lead investigator on the search team are many. These include the need for the investigator to concentrate on identifying evidence already uncovered, the need to remain impartial to the search, the need to supervise the search process, and the need to concentrate on interviews or other more valuable tasks.

There are just as many arguments on why the lead investigator should be a part of the search team. These include the need for the investigator to have personal knowledge of where items were found, the ability of searchers to call upon the investigator–as an expert–to avoid mistakes, and the need for the investigator to control the investigation as a whole.

At this point it is not mandatory that we specify the absolute use of the lead investigator but merely bring forth the idea that he/she should be involved. The ultimate decision on whether the investigator will be involved will be made based on a combination of factors including budget, manpower, and need.

d. Search Coordinator

Any search team should include at least one person who will coordinate the search. In instances where a minimal number of search team members are used this is less of an issue. In other instances, such as when searching a warehouse or office suite, the use of multiple searchers demands that tight control of the search site be maintained. This means that someone must be in charge. This is one of the strongest reasons for having the lead investigator involved with the search. The lead investigator can also serve in the role

of search team supervisor and thus complete two tasks at one time.

e. Other Team Members

Other members of the search team should include only those people with at least minimal training in identifying and handling computer components. At the very least this means that the person should be able to identify the items sought (especially when a warrant lists explicit items for the search) and the reason for searching in a particular spot or method. This is important simply because a fouled-up search, one arising from a searcher who had little idea of what they were actually looking for, could taint the entire investigation.

3. Sketch and Photo Team

Surprisingly, many departments have moved away from using sketch and photo teams except when dealing with major crimes. This is a mistake, and it can be a costly one. In many instances the sketch or photo team can be very helpful in more ways than simply documenting the scene for later review in court. For instance, there may be some question as to the exact placement of a particular peripheral used on a computer system. With a good sketch or photo the investigator can immediately identify the item in question and accurately determine the answer to the question.

Anytime evidence is to be seized the investigator should either make a sketch or take a photograph. In more complicated cases this duty is often assigned to a designated "expert" who has received additional training on these duties. The duties of the sketch or photo team member is to document the scene. There are four (4) common methods used for this task. These include:

1. Scaled Drawing
2. Rough Sketch
3. Still Photograph
4. Video

The scaled drawing is carefully created and intended to be very accurate. It often includes detailed descriptions of the measurements, locations, and point of interest in the drawing. The scaled drawing is generally used to depict locations and perspectives for specific evidentiary items.

The rough sketch is the most common method of documenting a scene. Though not as accurate as the scaled drawing it is still intended to accurately portray the scene at the time of its creation. The major differences between

a scaled drawing and a rough sketch is the detail. Many rough sketches may include measurements or comments about the items in the sketch, but they are not intended to be the most accurate representation available. The rough sketch is often used as a quick method for depicting the scene.

Still photographs were once considered too expensive for many cases. Because photography often used film that needed to be specially prepared or developed the costs were often restrictive. The introduction of the instant developing film (such as the Polaroid) allowed some departments to take only a few shots at a time. Costs continued to remain high, though, and many departments simply did not take photographs unless absolutely necessary. This all changed with the introduction of the digital camera and computers.

While traditional photography remains the medium of choice when quality is at a premium, the use of digital cameras brings the costs of single or short-run photo sessions down to almost nothing. A relatively inexpensive camera (less than $200) can be used to snap photos which are then transferred to computers for permanent storage. The relatively low cost of producing a copy of such photos (usually using an inkjet style printer) sacrifices some print quality for cost reduction, but it is a very good trade.

Most crime scenes do not demand the use of video, but on occasion the investigator may wish to use this medium for accurate representation. The advantage of video is that one can easily shoot an entire area in a single take and thus preserve the overall features without using multiple camera still shots. Video is also good to show the actual work on the crime scene. This includes the removal of specific items of evidence as well as the actual processing of objects. Video is especially useful when documenting the methods used to seize a computer or remove a component. Likewise, video can be used to authenticate methods used to secure items such as hard disks and other peripherals.

4. Security and Arrest Team

If the search is to be conducted contemporaneous to the arrest then it is a good idea to have an appointed arrest team present. This frees up the search team to begin the immediate tasks of processing the crime scene while the arrest team secures the suspects. A security team may also help in protecting evidence as well as personnel on the scene.

Common practice is to have the security and arrest team as separate entities. Security teams typically focus on securing the scene while the arrest team focuses on the actual capture. For departments with budget or personnel constraints this team can be combined. One caveat, though, is to make sure that these team members understand their role throughout the process. Arrest team members should be cognizant of potential evidentiary issues, but

only in the sense that they are not to disturb (when possible) the evidence. The evidence processing is actually done by the investigators, techs, or other assigned personnel.

The security or arrest team is an especially important part of any unit, and this is especially so when dealing with dynamic entries. For this reason many security and arrest teams are comprised of members of the tactical or SWAT unit. The term SWAT is not used as much these days, but the idea is to use those officers who have special training or experience in such tactics.

5. Technical Evidence Seizure Team

Because of the highly technical nature of the computer crime investigation it is strongly recommended that only those officers with appropriate training be used for the actual processing. Items such as hard disk, printers, and many other computer components can be easily damaged if not handled properly. More importantly, the savvy computer criminal may even booby-trap the system in some way. This may cause harm to either the investigator or the system when tampered with.

Technical evidence also includes items not normally associated with computers. For instance, in crimes involving computer fraud the technical investigator may need special accounting or other training. Being able to identify evidence associated with such crimes is a special skill. Other crime types, even though also involving a computer, may require similar skills.

6. Interview Team

The use of skillful interrogators is not limited to computer crimes. Simply stated, a competent interrogator can make a big difference in any criminal investigation. This is especially true in computer crimes, and the worthy investigator will have knowledge that makes him or her especially suited to this type of investigation.

As a general rule the interrogator must have the highest levels of competence when it comes to the computer crime. If the interrogator does not know the difference between TCP/IP and CD-ROM then the interrogation will likely go nowhere.

C. WHAT IF WE DON'T HAVE A TEAM?

As indicated in our earliest paragraphs, not all police agencies can afford a full-time computer crime team. Most departments must use officers who have duties elsewhere within the department. This means that the computer

crime unit is often a part of another unit such as property crimes, theft, or fraud. The downside to such units is that most officers will not receive the level of training they probably should have to conduct the best investigation. This does not mean, however, that no effort should be put into the unit, just that officers and commanders must recognize the potential problems before they arise.

If your department cannot justify a full-time unit then they should designate specific officers as computer crime investigators. What this means is that the officer has special training, either through formal college level classes or special seminars, which makes them more qualified than others for the job.

Another alternative is to share officers between multiple departments. For instance, where communities are geographically close the sharing of officers is common for many criminal investigations. The most common example is the multijurisdictional "task force" that is used for narcotics investigations. Similar arrangements can be made for computer crime investigation. The idea is that each department is assigned a particular mission and is responsible for training of specific members.

For those departments that simply do not have the personnel or budgets to manage any unit there remains few choices other than service from other agencies. Fortunately, many state and federal agencies offer assistance to local departments which do not have their own units. The FBI, Secret Service, and U.S. Postal Inspectors are some of the most helpful among the federal ranks. Other federal agencies often have specialty units of their own and are willing to help when federal law allows.

State agencies or larger "neighbor" agencies are often good sources of help as well. In many instances the department will gladly offer help to its smaller neighbors simply as a way to justify their own units. Of course, there are jurisdictional issues and the always present "interdepartmental rivalry" to worry about, but these are often minor issues.

D. WHAT TRAINING AND EDUCATION DO TEAM MEMBERS NEED?

There are two answers to this question. The first, and most expensive, is that you should get as much training and education as you can. Simply stated, computers are changing so rapidly that there is no time to rest for the well-trained investigator. As soon as you learn one thing it is time to move on to the next.

The other answer is really answered best by answering a simple question: how much crime is there? In other words, if your department has yet to face its first computer crime then the amount of training you need is relatively

low. Simply learning the basics may be enough for right now. That way you will at least understand a few of the issues that you will likely face.

On the other hand, if your department is seeing a rise in the number of computer-related crimes then you will want more training and education. Just as we set out in the first paragraph of this section, the more training you can get the better you will be at the job. With that in mind let's now turn to the specifics of training that one might need to be an effective computer crime investigator.

Let's start with college training and then move to vocational, seminar, and on-the-job type training. College-level training has its own rewards. One of the benefits of college level training is that it is easily identified, quantified, and accepted. This is important if an investigator is called to testify at court. After all, a jury is more likely to be impressed by a college degree than a certificate for "x hours" of training. There are some drawbacks, though.

One of the problems with college training is that it takes a long time to finish a degree. If an officer does not already have a degree then it could take several years to complete a degree. Even an associates degree (usually 62 credit hours) take long hours in the classroom to complete, and most officers simply don't have that kind of time to wait. They need the training now.

Another drawback to the college degree is that most computer study programs focus on computer skills and not investigation. There are a few colleges which offer specialized classes in computer security, but at this time there are none which offer degrees in computer crime investigation. What this means is that you will invest your time into training that only partially addresses your interest. While you may be learning a great deal about computers the reality is that only a portion of that education will apply to criminal investigation.

If college is not the right plan then one should consider vocational training. Many of the vocational schools across the country offer computer "technician" programs that prepare the student for specific career paths. For instance, a student can focus on networks, programming, or computer repair. The quality of the training is generally high, but it is important to remember that vocational training is focused on job skills not technical theory. What this means is that while vocational training will help the investigator to gain the skills necessary to perform the job, there is little theory behind the training and this may ultimately affect the investigator's overall capability later.

Seminars, conferences, and similar formalized training provide another path for learning about computers and technology. These are often sponsored by various police agencies around the country or by other law enforcement agencies at all levels. Selected programs are also available at some colleges as are certification programs by many of today's largest computer companies.

It is also important to remember that training does not have to be law enforcement oriented to be valuable. The theory and methods taught in traditional programs can be just as valuable to the investigator. For instance, CISCO–the manufacturer of quality switches and other network appliances–sponsors several "certification" programs around the country. Some are offered through community colleges, vocational schools, and many universities. There are even private vocational schools which provide similar training.

The last form of training is in fact one of the most common. In the broadest sense we could classify this as "on-the-job" training, but in many instances it is anything but such schooling. Many times the person simply has educated themselves using these same methods.

There are hundreds of great books, just like this one, now on the market. There are also dozens of competent journals, magazines, and newsletters that contain valuable information about computers. A person could easily immerse themselves into this material and quickly learn just as much as any computer criminal. In fact, most computer criminals have educated themselves in just this same way.

The problem with this type of informal education is that there are no safety-nets to stop you from learning things the wrong way. This can be a painful experience, and can cost the investigator an important case. If one is persistent, establishes good habits for learning, and is careful to verify everything that is learned then this is a reasonable fashion for educating oneself.

As I conclude this chapter it is important to mention certification and its meaning in the industry. There are several forms of "certification" available for computer experts. The next few paragraphs will explain a few of these.

A+	The A+ Certification is a testing program which certifies the competency of computer service technicians. The A+ test contains situational, traditional, and identification types of questions. The test covers a broad range of hardware and software technologies. This is a valuable certification by itself with excellent job placement opportunities; and it also is a perfect preparation course for the advanced networking certifications.
Network +	Network + is a certification recognized worldwide attesting to the proficiency of its members in all areas of basic networking. Successful candidates are considered by employers to be competent in topologies, media, the OSI model, protocols, TCP/IP, and much more. The certification is valuable in and of itself, and also as preparation for Microsoft MCSE, Cisco CCNA, and Linux. Network + certification confers upon the candidate a skill-set which can be useful in the job market.

MCSE	The MCSE (MICROSOFT CERTIFIED SYSTEMS ENGINEER) credential is one of the most widely recognized technical certifications in the industry–a credential in high demand. By earning the premier MCSE credential, individuals are demonstrating that they have the skills necessary to lead organizations in the successful design, implementation, and administration of the most advanced Microsoft Windows platform and Microsoft server products.
CCNA	The CCNA (Cisco Certified Systems Associate) course covers the important information required to configure Cisco switches and routers in multiprotocol internetworks. Multihands-on labs allow you to perform router and switch configurations on a LAN and WAN network. Perform all basic configuration procedures to build a multirouter, multigroup internetwork that uses LAN and WAN interfaces for the most commonly used routing and routed protocols.
CCNP	The Cisco Certified Network Professional (CCNP) certification indicates advanced or journeyman knowledge of networks. With a CCNP, a network professional can install, configure, and operate LANs, WANs, and dial access services for organizations with networks from 100 to more than 500 nodes, including but not limited to the following protocols: IP, IGRP, IPX, Async Routing, AppleTalk, Extended Access Lists, IP RIP, Route Redistribution, RIP, Route Summarization, OSPF, VLSM, BGP, Serial, Frame Relay, ISDN, ISL, X.25, DDR, PSTN, PPP, VLANs, Ethernet Access Lists, 802.10, FDDI, Transparent and Translational Bridging.

Other certifications include Oracle Database Administrator, Network Systems Technology (UNIX systems), Novel networks, and many others. Each certification meets the requirements or standards of a particular part of the industry. While most investigators will not seek certification it is something to consider. The reason to consider this route, much like obtaining a degree, is to make it easier to establish oneself as an "expert" when it time to testify at trial.

Chapter 3

THE COMPUTER SYSTEM IN THE CRIMINAL ENTERPRISE

A. DETERMINING THE COMPUTER'S ROLE IN THE OFFENSE

One of the first jobs of the criminal investigator is to determine the computer's role in the offense. This is somewhat similar to the task robbery detectives have when determining what weapons, if any, were used to commit the crime. By determining the weapon and its ultimate role, the investigator can begin to piece together the *Modus Operandi.* This will then help the investigator determine who committed the crime.

As we pointed out in earlier sections, just because a computer is part of the overall crime doesn't mean we are dealing with a computer crime. For instance, theft of office equipment might include the theft of a computer itself, but that does not make it a computer crime. On the other hand, theft of information from the computer certainly creates a computer crime. This

is an especially important distinction when one considers the search and seizure issues that might arise in a typical computer crime case.

The first issue for consideration is whether the computer was an integral part of the crime or merely incidental. In making this determination the investigator must look at how the computer was used and to what level the computer was involved in performing criminal acts. If the computer is an integral part of the crime then we may have a true computer crime. On the other hand, if the computer was merely an incidental part of the crime, i.e., just another tool, then we will likely not have a computer crime.

In making this determination the investigator must deduce what actions were taken with the computer. For instance, is the computer a repository of evidence or was it used to actually create the items used in the crime. One example of where the computer is incidental to the offense is where an automobile chop shop uses the computer to store records of customers, product prices, and quantities. Compare this to the counterfeit case where the computer is actually used to create the art, print the masters, and ultimately control the manufacture of fake money orders. In the first scenario the computer is incidental to the offense and in the second it is an integral part of the offense.

One reason it is important to make this distinction is that the computer can play a different role in the same type of crime. Knowing what role the computer played may affect the investigation itself as well as the concentration one places on the computer in question. Such may be the case when we deal with *hackers.* Those who commit illegal computer entry often use their computers both to attack other computer systems and to store stolen files. In this case, the hacker's computer is both a tool and storage device. As such, the computer is both incidental and integral to the crimes.

From a practical standpoint the involvement of a computer in a crime raises several important questions. These include:

1. Does probable cause exist to warrant seizure of the hardware?
2. Does probable cause exist to warrant seizure of the software?
3. Does probable cause exist to warrant seizure of the data?
4. Where will this search be conducted?
5. Is it practical to search the computer system on site, or must the examination be conducted at a field office or laboratory?
6. If investigators remove the system from the premises to conduct the search, must they return the computer system, or copies of the seized data, to its owner/user before trial?
7. Considering the incredible storage capacities of computers, how will investigators search this data in an efficient, timely manner?

Each of these questions is best answered by first defining the role the computer has played in the crime. The less critical the computer was to the criminal act the less likely it will be seized, searched, or even examined.

One method for helping to determine the computer's role in the criminal enterprise is to understand fully the computer and its various components. As an investigator it is important to not only understand the basics of the computer itself but how the computer works. If you are not fully familiar with the computer then take some time to read Appendix A and B at the end of this book.

For the investigator that has knowledge of basic computers the next step is to understand computer forensics. In the following section we will examine the basics of forensic application in the computer crime investigation. There is also additional information concerning evidence and related legal issues in the last part of this book.

B. INTRODUCTION TO COMPUTER FORENSICS

In the last decade the term "forensic" and "forensic science" has undergone significant scrutiny and in some respects a great deal of misunderstanding. Crime dramas on both television and in the theater portray forensic investigators as a modern Sherlock Holmes who works behind a scanning electron microscope one minute and interviews homicide suspects the next. Seasoned investigators know that these portrayals are far from the truth, but there has been a legitimate need to increase forensic understanding for all investigators.

The term forensics comes from the Latin for *public* or *forum*. In the broadest sense the term refers to that which belongs to, is used in, or is suitable to the courts or to public discussion and debate. It also means relating to or dealing with the application of scientific knowledge (as of medicine or chemistry) to legal problems. When it comes to computers the term means the application of computer science techniques and methods to investigate crimes where computers are a central part or have some involvement.

When dealing with the concepts of forensic science, especially as it relates to computers, we must understand that computer misuse falls into two categories. In the first category the computer is used to commit the crime itself. As an example, the transfer of money through electronic means from a secure site which has been hacked to another site directly involves the computer in the criminal act. We would say that the computer is an instrumentality of the crime.

The second category is where the computer is a target of the criminal act. In recent years this category has created a complete genre of specialist under

the umbrella title of *incident response.* Those who work in this area are more concerned with preventing the attack or in the alternative in limiting the effect of an attack once it occurs. Incident response is at its heart crime prevention. The computer crime investigator must certainly understand the basics of this genre of computer forensics, but the meat of the investigation is in the focus on the computer as an instrumentality.

In computer crime investigations the term computer forensics more closely means the preservation, identification, extraction, documentation and interpretation of computer data as it relates to the individual crime. As an example, where the money from one institution is transferred by way of an unauthorized computer access the computer crime investigator will use computer forensics to identify potential egress points, methods of securing relevant financial data, and ultimately the methods used to transfer the money (as a dataset) from one institution to another. In such a case the computer(s) involved in the criminal activity will likely contain traces of electronic evidence which shed light on each of these aspects of the crime.

1. The Methodology of Computer Forensics

The computer crime investigation is not significantly different from other forms of criminal investigations; however, there are some issues that are dramatically different. Just as with most investigations there will be a physical crime scene, but one must remember that in the computer crime case that scene may be actually spread over several physical locations.

For instance, in the example of the electronic transfer of funds the physical scene is spread among the three specific locations where computers are located. The first of these is the suspect's place of operation. Because of the portability of computer systems today that location could be anywhere from the suspect's bedroom to a public café that has Wi-Fi connections available. The second location is that of the bank or other financial institution. The computer for the bank may be at the bank site or at another remote location, especially if the bank uses a Wide-Area Network. The third location is the place of transfer. This may be next door to the original bank, across the country, or even in another country altogether.

Because the physical location can vary so much in any computer crime case the investigator must be able to quickly adjust traditional methods to fit that of a multi-site crime. Likewise, the nature of the electronic intrusion or computer involvement means that the physical nature of the crime is much different from that of a traditional crime involving tangible items. Computer evidence may certainly include tangible items such as a notepad kept near the computer to house notes on suspect activity, but the reality is that in most computer crime cases the investigator will be dealing with intangible forms

of evidence such as files, datasets, and related items.

Because of the nature of the computer crime, and the evidence most closely associated with it, the methods of computer forensics are a bit different. There are three basic methodologies consistent with computer crime investigations. These are:

1. Methods to seize or recover the computer evidence without damage or alteration.
2. Methods to authenticate the seized or recovered evidence.
3. Methods for analysis of data or evidence seized or recovered.

In later chapters of this text we will examine all three of these methods in greater detail, but for now we must establish a few basic concepts that are very important in each computer crime investigation. The first of these concepts is that of evidence handling. Just as with any traditional crime the methods for handling evidence are normally under very close scrutiny by the courts. Because of this the methods must be well established so that they meet the practical and legal requirements of the legal system.

At the top of the list when dealing with any investigation is the act of securing the crime scene or specific evidence in question. This act is complicated, though, by the nature of the computer and the evidence likely produced. As an example, in a case of electronic stalking the victim may receive a series of disturbing email communications which threaten her life or safety. The initial investigator, usually a uniformed officer assigned to respond to the initial call, will likely view the messages on the victim's computer. To protect this evidence should the officer seize the computer itself or simply make a printed copy of the message?

This type of question has no easy answer; however, there are some basic methods that can be used to protect the potential evidence. The first of these is documentation, and this is where the responding officer plays a vital role in the investigation itself. The officer must document that the message in fact existed on the victim's computer. The first method of documentation is the police report, and when making the report the officer should endeavor to include as much detail as possible. This includes the information on computer type, location, and method for viewing the message in question.

Officers may also choose to photograph or in some other way document the existence of the message on the victim's computer. The use of digital cameras has certainly found favor for police departments simply because they are easy to use, do not require printing of the photograph, and can be quickly viewed on the camera itself or on another computer. In such a case the officer would simply take a series of photographs showing the victim's computer, the message, and if possible the victim with the computer.

2. Establishing Policy and Procedures for Computer Cases

In any investigation there is a basic set of requirements the investigator must follow in order to insure a successful investigation. These requirements are generally set forth as part of the department policy and procedure. In most instances these requirements include the identification and preservation of evidence, formulation of leads, searches, analysis, and decisions as to criminal charges.

Many of the standard practices found in other investigations easily apply in computer crime cases, but there are exceptions. For instance, when dealing with the collection and preservation of computer evidence the investigator often finds that the evidence in question is intangible by its very nature.

There are a number of different methods for securing computer data, and for each method there are an equal number of options within the method. Because there are so many methods, and because there are so many different ways to conduct any part of the investigation, it is generally accepted that the policy or procedures within the department be somewhat flexible. The flexibility allows investigators to adapt to the given circumstances while still maintaining the basics of policy or procedure.

While flexibility allows investigators to use discretion it also creates a potential legal issue at any computer-related trial. This is especially important when we consider the potential evidentiary questions that may arise when dealing with potential policy issues. The courts are slowly establishing standards and new grounds for the treatment of computer related evidence, especially when it deals with any type of digital recreation or seizure, and each of these new methods of treatment carries with it potential legal ramifications which may affect later computer crime investigations.

One of the most important considerations is that of the "chain of custody" and the need to seize the computer system itself. A computer system is much more than the individual components, and for that reason the choices of which components, if not the entire system, to seize create individual issues of proper procedure. For example, in a computer fraud case the investigator would likely seize the data on the suspect's hard drive, but would they also need to seize the hard drive itself? Likewise, in a case where the computer system is used to scan a government check into the system, where it is then altered using high powered graphical editing software, and later printed on a high-quality color laser printer, the question is one of which component is proper to seize.

There are many other issues which will arise, and for that reason it is important that we establish some basic parameters for creating policy. The following list are minimal items which should be considered when creating a new policy on computer seizure or investigation:

1. The nature of the case.
2. The evidence necessary to secure a conviction.
3. The likelihood of damage or loss of evidence if not seized.
4. The volatile nature of data or other evidence being seized.
5. The storage and protection of the evidence.
6. The physical nature of the computer or storage devices.
7. The capability of the investigative team.
8. The potential need for outside experts or assistance.
9. The Fourth Amendment and related issues that may arise.
10. Accepted practices within law enforcement.

C. THE MODUS OPERANDI OF COMPUTER CRIME: MOTIVE AND TECHNOLOGY

As with all crimes, the criminal's *modus operandi (MO)* reflects their methods, plan, or system for completing the criminal act. Criminologists have long held that the *MO* is comprised of learned behaviors that evolve and develop over time. The *MO* can be refined as an offender becomes more experienced, sophisticated, and confident.[1] It can also deteriorate over time through loss of skill, mental capacity, or through the use of mind-altering substances.[2]

What this means to the criminal investigator is that the *MO* in computer crime is just as important as it is in many other crimes. Especially important are the aspects of motive and technology. In most computer crimes these two issues rise to the top when assessing the *MO* because they often are the most obvious when measuring the crime itself.

In understanding the concept of *MO* we will focus first on the topic of motive. In recent years the number of computer attacks have fallen into one of three broad categories:

1. Revenge,
2. Theft, and
3. Trespass.

Revenge is the act of taking retribution against one who is seen as an evildoer. Revenge might come from an ex-employee, disgruntled customer, or in some cases spurned suitor. In these instances the motive is generally no different from that seen in other revenge oriented crimes such as vandalism. The attack is made more as a means of doing damage than a way of gaining an advantage.

Attacks oriented toward theft tend to take two forms. First is the theft of

hardware or software, which is very similar to other theft crimes. In these cases the object of the attack is the computer system or the software that runs on it. Typically the *MO* is similar to other forms of theft including many property crimes such as larceny or burglary. The perpetrator must establish a means of gaining access to the hardware or software and then a method for removing it from the location.

The second form of theft attack focuses on the information stored or manipulated by the computer. This includes theft of trade secret, financial reports, market sensitive proprietary information, and customer information. Other types of information theft include the thievery of process technology, human resource information, and security data. In these cases the *MO* is to gain access to the information often through stealth, obtain the material necessary by copying or viewing, and making an escape without leaving behind signs of entry.

The last item under motive covers trespass. In this category we find the newest type of criminals: computer hackers. From the outset it is important to note that not all computer trespass is done by a hacker. As we will see in later chapters, hackers are the group of computer criminals who are most notorious for their intrusions, but are far from the leading candidates for the greatest actual loss to victims. In fact, in many instances the loss from hackers is minimal when compared to the time and effort expended to prevent their intrusions.

Hackers are not the only computer trespassers, though. To help us understand this we first define computer trespass as simply the unauthorized invasion of a computer system. These crimes occur both on site and from thousands of miles away depending on the system and the ability of the intruder. In each instance the primary goal is the intrusion into the system. Under the latest criminal law dealing with this problem we see computer intrusion treated as a separate crime from computer theft. It is important to note that in many instances the investigator may be dealing with a combination crime of both computer intrusion and computer theft.

In each of the above instances the *MO* is very important to the investigation. Just as with traditional crimes, the investigator uses the particular *MO* to help understand the crime. The *MO* can help determine motive as well as help to narrow the number of suspects in a given case. That is also why the investigator must consider technology when evaluating the *MO*.

Computer crime does not require the latest and greatest in high technology before a perpetrator can be successful. In fact, many forms of computer crime are completed with computers that are no more sophisticated than those found in the average home. The key to technology is determining that the minimal technology is available to the perpetrator during the times the crime was committed.

In some respects one might find that motive and technology also blend to create a hybrid for *MO*. This hybrid is a direct outgrowth of the recent work done by psychologists, criminologists, and criminalists in the areas of profiling. For instance, some acts of computer crime are directly linked to behavior pathways and responses seen in other forms of crime such as rape, battery, or theft. For that reason it is important that the investigator be grounded in the concepts of profiling as well as psychological forensics.

One study that appears to have some application to this topic comes from Nicholas Groth, an American clinical psychologist. Groth's study focused on both victims and offenders from rape. He specifically looked at the behaviors that satisfy emotional needs, and for our purposes it appears that there are similarities between crime types of this nature. Groth theorized that rape–as well as other crimes–often satisfies complex emotional needs sometimes unrelated to the act itself. In this sense, the act is committed not to obtain the object of the act (sexual relation in a rape case and electronic intrusion in a computer trespass case) but to satisfy some emotional need.

Groth's work is important because it helps us establish behavior typologies that can be applied in many similar situations. Specifically, the Federal Bureau of Investigation (FBI) and the National Center for the Analysis of Violent Crime (NCAVC) modified Groth's work to establish certain profiles and psychological criteria that could be used in later crimes.[3] Similar work has produced other typologies that may be applied to other crimes.

Borrowing from Groth's work and applying similar typologies to computer crime it is possible to establish specific criteria for "profiling" or labeling computer crimes and their actors. In the following sections we will examine a few of those profiles.

1. Entitlement

This category of computer criminal acts to establish his dominance over or right to a particular item. For instance, when we deal with software piracy we find that individuals not typically prone to criminal acts do a great deal of the theft. In some instances these individuals see themselves as "entitled" to the software in question. In many cases the person claims that they intended to buy the software, eventually, but that they needed to evaluate it fully before committing to the purchase.

Similar examples of an entitlement typology are those trespassers who are "merely browsing" another computer system. Though these persons often gain access only after defeating complicated security systems they don't see themselves as wrongdoers but merely curious "explorers." The intruder claims that since there was no harm there can be no foul. They tend to ignore the fact that they were not invited into the system in the first place and

instead see themselves as having a special entitlement to such cyber-trespassing.

2. Compensatory

This group is often most closely aligned with those typologies arising under theft and deceit crimes. Actions are often taken for no other purpose than to net the perpetrator some financial or other advantage. Compensatory crimes appear to focus on a specific goal, but as with other crimes of this nature (such as shoplifting) the crime is sometimes one of opportunity rather than specific design.

We further divide this classification by recognizing that some compensatory crime is committed with specific intent or with a grand design. Other crimes in this category fall under the heading of "crimes of opportunity" or "crimes of impulse." The investigator must be cautious as to which category they place the particular act in since both tend to have a bit different personality typology.

For instance, a perpetrator who finds himself connected to a network not commonly accessed and with privileges not normally granted to the casual user may commit the compensatory crime but only because it "was there." In interviews with these type of offenders criminologist often find that they had no set plan to commit the act in question but merely "stumbled upon" the crime and took advantage of a "good thing."[4]

On the other hand, some forms of compensatory crime are well planned. The perpetrator knows the target and sets about committing the acts with purpose and design. For instance, where the perpetrator seeks to gain a business advantage by reading confidential memorandums, payroll account numbers, or other valuable data there is often a period of planning followed by specific acts to further the criminal enterprise.

While both instances of compensatory crime may be similar in result there is clearly a big difference in the type of work that went into the acts. These differences can not only affect the results of the crime but also the MO and digital evidence investigators have to work with.

3. Anger or Retaliatory

As discussed in the introductory comments to this section there are some computer crimes that arise from anger or the need to retaliate against a perceived evildoer. On the surface this is one of the easier typologies to work with, but the savvy investigator knows not to immediately choose the easiest path when concluding the investigation.

The Anger or Retaliatory act is often done to correct perceived wrongs.

The perceived wrong may be an accumulation of several minor wrongs or a single incident. An example of this type of crime is the current employee who commits the act not for a single instance of wrongdoing by the employer but for the perception of "long-term" wrongs committed over time. This may include the failure to provide meaningful recognition for a difficult task done well. It may also include the perception that management (or owners) refuse to award appropriate raises in salary. In these cases a single event is often insufficient, but taken over several years the employee may build a desire to "strike back."

The retaliatory crime easily includes theft of hardware, software, or information. This crime may also include intentional damage or destruction of tangible and intangible components of the computer system. The focus tends to be on damage in either the traditional sense or in the less tangible manner. In other words, the retaliatory crime might involve physical damage to a computer system or simply the erasure of important data from the network.

The investigator must recognize that the initial wrong for which retaliation is needed may not exist outside the mind of the suspect. It is the perception of the perpetrator that is important. If the perpetrator feels that he or she has grounds for retaliation then that is all that is needed.

The main goal of the offender is to service the cumulative aggression. They are retaliating against the target for wrongs real or imagined and their aggression can manifest itself through any number of means. These may include abusive epithets, targeted slurs, and even violent behavior.

It is imperative that the investigators not confuse retaliatory behavior with sadistic behavior. Just because a computer system is attacked (hacked) with damaging results is not enough to assume that it is the work of a disgruntled employee. Sometimes the act may in fact be that of a vandalizing rogue simply looking for something to trash. To distinguish the two the investigator should evaluate carefully all the evidence that may present itself over time, and therein lies the secret to a successful investigation.

4. Anger Excitation

These are crimes that are done for the sheer pleasure of destroying something. For instance, the youth that intentionally throws rocks at the large picture window seeks to destroy the window not because of some financial need but instead for the sheer thrill of watching the window shatter. Most in society simply shake their heads in wonderment as to what could have driven the youth to such senseless destruction, but the wary investigator is less casual. The reason, as criminologist often find, is that the youth was merely seeking excitement, and that is a very specific *MO*.

For the computer crime investigator this same excitement is often the goal of the hacker or other cyber-criminal. For example, in a recent case several high school students gained access to a local hospital database in their hometown. Their goal was not financial gain but merely the thrill of intruding into a computer system that was a simple phone call away. Once inside the computer system, though, the group found themselves seeking higher levels of excitation.

In understanding this act investigators often liken it to the neighborhood group that breaks into a known vacant house. The homeowners are usually away for a short period of time and the house is left unguarded. The group, knowing that the house is vacant for the time being, breaks in initially for the thrill of the entry. Once inside, though, they often turn to theft or vandalism as the need for higher levels of excitation grows.

In the past there has been a great deal of effort put into the clear definition of the anger excitation typology. Some have suggested that these acts are done primarily as a release of sexual dysfunction or for purposes of sexual gratification.[5] The primary motivation for the behavior is sexual, however the sexual expression for the offender is a manifested physical–or in the case of computers, digital–aggression.

Another analysis suggests that this typology is motivated by emotional needs unrelated to sexual desire or dysfunction. The perpetrator is not necessarily satisfied by purely profit-motivated behavior but may instead be motivated by other more internal needs. One recent study suggests that emotional and physical abuse early in childhood may lead some to seek release under this typology.[6]

Still other studies suggest that computer perpetrators act out much like "thrill seekers" in other endeavors. The better comparison, when defining in this realm, is the use of "danger junkies" or those who engage in "extreme sports." Many computer intruders are not sports-minded individuals, and for this reason the thrill associated with computer crime is equal to that received by the sports enthusiast.[7]

From the investigative standpoint the need to identify a perpetrator typology focuses on the *MO* much more than the academic identification. By understanding the basic motivators the investigator can more quickly define the potential suspects in any given crime. This allows investigators to also formulate patterns evidenced by other forms of evidence, especially when dealing with digital evidence. This is also significant as one understands the growing trends of computer crime.

ENDNOTES

1. *Practical Homicide Investigation,* 3rd Edition, Geberth, V., CRC Press, (1996).
2. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis,* Turvey, B., Academic Press, (1999).
3. *Practical Aspects of Rape Investigation: A Multidisciplinary Approach,* Burgess, A. and Hazelwood, R. (eds), CRC Press, (1995).
4. Franklin, *Striking While the Iron's Hot: A Look at Crime of Convenience in the Computer Marketplace,* Midwestern Association of Forensic Computing Annual Meeting, Fall 2000.
5. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis,* Turvey, B., Academic Press, (1999).
6. *Id.*
7. *Abnormal Psychology and Modern Life,* by Robert C. Carson, James Neal Butcher, Susan Mineka; ISBN: 0321034309; 11th edition.

Chapter 4

THE COMPUTER CRIME LAB

A. INTRODUCTION

To this point we have concentrated on establishing the basic principles that will be used for later computer crime investigations. These have included an understanding of computer crime, the perpetrator, and of the various components of the computer itself. It is now time to turn our attention to another subject that most investigators will need to understand before they begin investigating computer crimes.

A majority of police agencies in the United States do not have a dedicated crime laboratory. It is unlikely that these departments will build a dedicated computer crime facility either. Unlike the traditional crime lab, the computer lab is relatively inexpensive and can be maintained in a reasonably small space. Of course, there are huge laboratories dedicated to forensic computing, but for the most part a moderately well-stocked electronics

workbench is all that is needed to handle most computer investigations.

With that in mind we can cover the basics of a computer crime lab. What the typical investigator will need is a simple workspace that meets minimum standards for working with computers. In this chapter we will focus on those standards and on the equipment needed to start such a laboratory. It is important to keep in mind that an emphasis is placed on both costs and on reasonable expectations. In order to do this we will focus on the equipment most needed and stay away from the more advanced, and always more expensive, equipment found in the larger labs.

Before building any computer laboratory it is important that the investigator first acknowledge the need for a specialized work area. This typically means that the computer crime lab should be separate from labs used in other forensic duties. This is especially important when we deal with the issues of computer data storage in later sections of this chapter. Because disk drives often have moving parts that travel within millimeters of each other, and at speeds up to 10,000 revolutions per minute or more, it is important to maintain a clean work environment with controls against outside contamination.

There are three basic components that make up the sophisticated computer crime laboratory. These include (1) ample workspace, (2) the right tools, and (3) reasonable precautions to protect cleanliness. We will begin with an examination of the workspace. We then examine the issues of tools, both basic and advanced, and finish with a discussion of the common issues associated with storage devices.

B. THE WORK SPACE

The perfect laboratory for any forensic endeavor is large, well lit, and has ample room for performing any necessary task. Of course, the task in question will often dictate the amount of space that is required. For computer crimes this means room enough to examine computer hardware without significant risk of harm to the equipment or contamination from other sources. As a general rule, the workspace itself should be large enough to house the equipment and the items being examined.

Setting an exact size for the lab is very difficult. A desktop can be big enough for a single computer; that is until the investigator starts working on the contents of the computer case. As anyone who has worked on a computer knows, once the case is open the amount of space available for work significantly shrinks. For that reason, it is recommended that the computer crime lab have a workstation large enough to hold a computer case, motherboard, CPU, SIMMs, power supply, and three disk drives. Something

roughly the size of an executive desk should suffice.

The simple fact is that the more room the investigator has the more he can accomplish, and for that reason it is often necessary that at least two work areas be available. For instance, if investigators are working on a computer's hard disk drive there may be room needed to open the PC itself, remove the drive, and then move the drive to a separate–uncontaminated–work area nearby. What this means is that the computer lab may need to be big enough to house at least two "desk-size" workstations. Of course, this will depend, to a large extent, on the budget and need of the department.

One must also remember that the typical computer system is composed of several parts including the main computer case, monitor, printers, and upwards of a half-dozen peripherals connected to the machine. The investigator may not need to remove the internal components from the PC's case, but instead merely need enough to recreate the computer's setup at the crime scene. Again, space is important, but will be determined by other factors that may be outside the investigator's control. For that reason it is necessary to establish at least some minimum standards that will easily apply to even the smallest workspace.

The first standard that is to be attached to the workspace is access. Like all forensic activities it is imperative that investigators maintain constant control over the area and the work performed. Questions of contamination are just as important in computer crime cases as they are in homicides. What this means is that even if a temporary area is set up for the computer crime lab the first job of the investigator is to insure that the area can be secured.

When the maximum space is not available then any clean space that can be maintained separately may be used. This will help us to establish the second standard for our computer crime lab. Like most forensic workspaces, the computer laboratory must be free from external contamination or clutter. This often means that the laboratory must be maintained in a room apart from other work areas. The preference is given to a room where access is easily controlled as well. In the best environment only those technicians, investigators, and others who have absolute need to access the room will be allowed to enter. This cuts down on potential contamination as well as keeps the lab free from questions of security.

A common practice is to house the computer lab in the same area as other forensic labs. This can be done, so long as the computer area is free from contamination from the other work in the labs. Of course this standard is also applied whether one is working on DNA, blood, or fiber evidence. A clean work area that is controlled for contamination–both human and environmental–is a common standard among all forensic sites.

Work surfaces are also important considerations when preparing the crime lab. Though one will rarely work with liquids it is still preferable to have a

non-porous material for the top of the workbench. One reason for this is that the non-porous material often means a smoother work area and one that creates less friction. Friction can create static electricity, and any kind of electrical charge can be dangerous to computer parts. Wooden desktops do make good bench tops, but the preferred material is often plastic or a similar non-conductive material. Something that hinders electrical buildup should be chosen rather than a material that may cause static electricity.

Workbenches should be easily accessible to all that work in the laboratory. This is especially important considering today's requirements for work areas that meet the standards for handicapped or physically challenged workers. In many cases laboratory workspaces are often set at much higher levels than the traditional desk, and this is obviously a consideration when designing a laboratory that might be accessed by workers in wheelchairs.

The height of the workbench is also a concern when working with electrical equipment and especially when working with computers. Because the computer crime case can take on so many different forms there is no single workbench design that works best for all cases. If the investigator is working on data retrieval through software then a traditional computer desk might be sufficient. On the other hand, if the investigator is working on the hardware side of the computer crime then a traditional electronics workbench may be preferred.

There should also be consideration given to comfort while at the workstation. Ergonomically correct placement can ease muscle or joint tensions and help workers perform at higher levels of efficiency. One must remember that the typical computer crime investigation may take hours of steady work to access a hidden or damaged file containing incriminating evidence. The computer technician who is uncomfortable may perform at a lower level of efficiency than one who is properly outfitted.

Ventilation in the work area is a factor often overlooked by designers. One problem with ventilation is that it allows dust and other external particles to invade the work area. Major manufacturers of storage components such as hard disks or optical scanners know the value of a well-ventilated work area that is still free from airborne contaminants. They provide their workers with superb ventilation systems that help control dust and other particles while allowing for the circulation of fresh air at a rate that is conducive to the worker. The same focus should be given on the ventilation system for any computer crime lab. The last thing that an investigator needs is ruined data disk because excessive dust particles invaded the work site.

A final consideration for the design of any work area is the issue of lighting. Fluorescent lighting is preferred in many office environments but is not always the best for the laboratory setting. This is especially true when dealing with computer monitors. It is also important when considering the type

of material that will be handled during the investigation.

One concern is that harsh lighting makes reading certain computer monitors more difficult. Just as with the physical layout of the work area, special attention should be given to ease of use when it comes to lighting. Harsh lighting means workers are more prone to visual fatigue. This can harm an ongoing investigation and raise the risk of error.

To combat harsh lighting it is recommended that moderate lighting be installed overhead with individually controlled lights installed at each workstation. Lights that can be easily adjusted should be chosen instead of fixed focus lights. Adjustment for brightness, intensity, depth, and coverage–the area the light actually covers on the desktop–should all be taken into consideration. Different investigations may require different light. For instance, a broadly lit area is ideal when working on a large object, but when dealing with small items such as disk drives a more narrow focus of the light beam may be desired. By providing adjustable lighting the investigator makes the most of his work environment.

Small flashlights are also common in computer crime labs and portable kits. These lights allow the investigator to illuminate hard to reach areas such as the nooks behind drive connectors or SIMM bays. Anyone who has lost a small screw inside a typical PC case knows the value of a flashlight.

C. BASIC EQUIPMENT NEEDS

We briefly touched on equipment in the above section as we discussed the physical setup of the computer crime lab. We now turn to the additional equipment that will be needed not only at the computer crime lab but also in a transportable tool kit. We will begin with the computer toolkit.

1. The Computer Toolkit

The modern personal computer is typically a sum of its parts. That is, the computer is made up of several independent parts that can be installed or removed separate from other parts. The computer is very much like an automobile in this sense. Just as the tires can be removed from the car separate from the motor itself, so too, can the hard drive be removed from the motherboard in a personal computer. What this means to the investigator is that it is important that the person working on the computer have the right tools for the job. One would certainly not try to remove the tires of a car with a small Phillips screwdriver, but that same tool would be very necessary when working on the carburetor. The same concept applies in computers.

The basic computer toolkit can be assembled from individual tools or pur-

chased as a unit at most computer retailers. Kits which are commercially available commonly cost less than twenty dollars ($20). Most kits include a selection of screwdrivers, tweezers, nut driver, and a simple chip extractor. Figures 4-1 and 4-2 depict two common toolkits in the price range. Both toolkits contain basic tools for working on most computers, and the major difference is in specialty items such as chip extractor, needle nose pliers, and *Torx* tips.

Before going into detail on the individual tools it is important to point out that any tool made from or containing metal should be demagnetized. Magnetic fields can easily damage computer chips, drives, and other parts. More importantly, it is imperative that investigators recognize the danger any magnetic field can pose for the computer disk (both hard and floppy). Even the magnet used to power the common car speaker is enough to damage the data stored on an older floppy disk. Manufacturers of computer toolkits recognize this and specifically make their products to be safe with computers.

Toolkits like those in Figures 4-1 and 4-2 can be purchased at most computer and business supply stores. More expensive and much more sophisticated kits can also be purchased, but the choice on what tools and how large the kit will depend on the needs of the individual user. For the entry level investigator, or one who does not do a lot of computer investigations, these

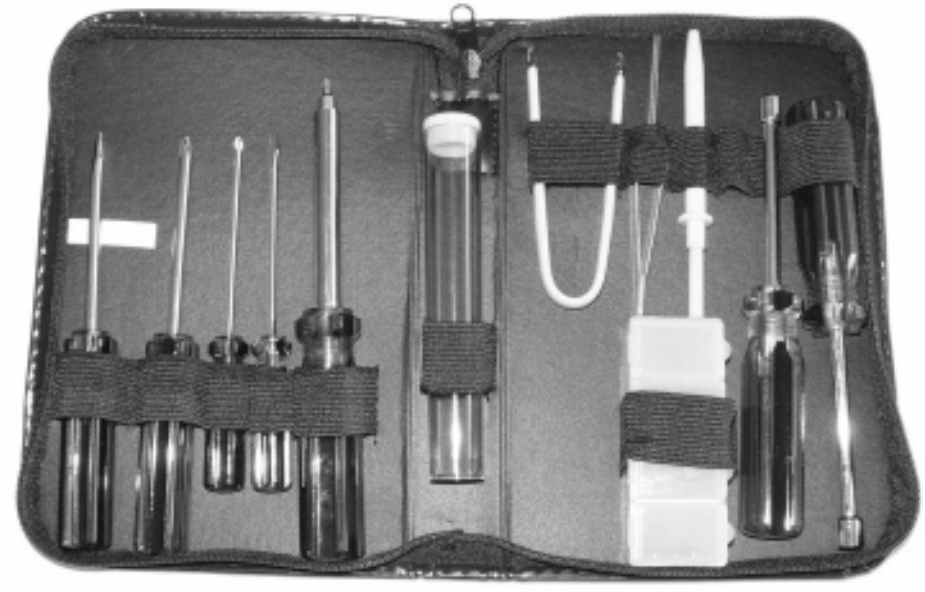


Figure 4-1. Toolkit with chip extractor.

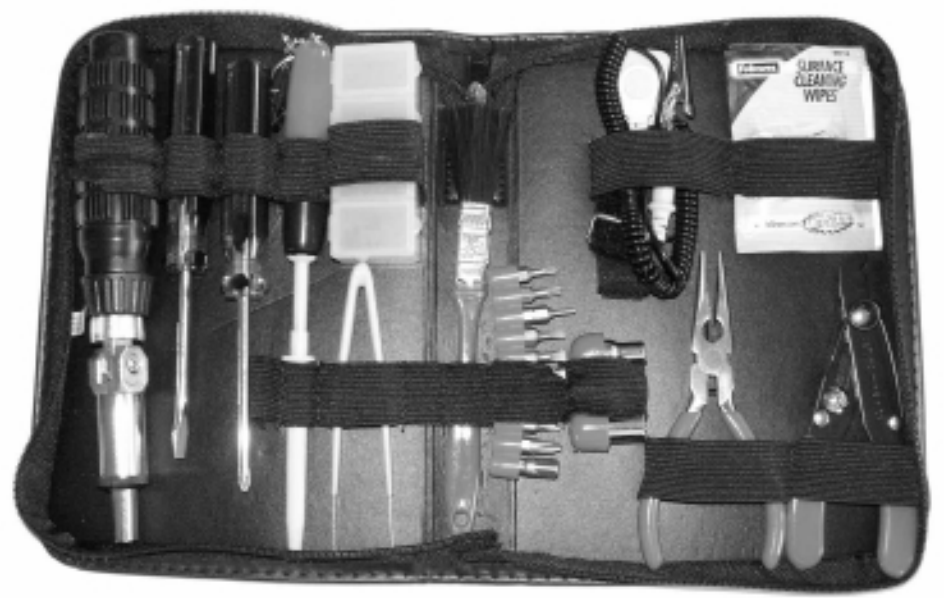


Figure 4-2. Toolkit with anti-static strap and pliers.

simple kits are perfect. There are two items worth noting that may affect the kit choice as well as tool use. A common practice among defense attorneys is to question the investigator about the toolkit used. Common questions focus on the specific tools used, their intended purpose, and their likelihood of causing damage or contamination to evidence involved in the computer crime case.

Before beginning any work on a computer the investigator should have an antistatic bracelet (Figure 4-3) which is worn to prevent the buildup of static electricity. The bracelet, which is often known as a *grounding strap,* helps shield the computer from static built up by the investigator. The human body is literally a dynamo when it comes to electricity, and this devise helps to protect both user and system. To make things worse, the clothes we wear, especially with many of today's synthetic fibers, promote static electricity. It is important to consider the potential static electricity buildup that can occur with certain fibers or articles of clothing. By using the antistatic wrist bracelet, which is connected to the technician and then to the computer, the user can dramatically lower the risk of damage caused by electric discharge.

Having given fair warning on the hazards of static electricity and magnetism, it is time to turn back to the basic computer toolkit. At the heart of the computer toolkit are screwdrivers. At least four different screwdrivers are recommended. These should include a 1/8th inch and 3/16th inch flat head as well as the #0 and a #1 Phillips-head screwdriver. These will fit most pop-

Figure 4-3. Anti-static wrist strap.

ular screws used in today's computers. More advanced kits will include other screwdrivers, and one of the more common specialty additions are "jeweler's screwdrivers."

Jeweler's screwdrivers (Figure 4-4) take their name from the common use of these small tools in the jewelry and watch repair industry. They are now routinely included in many hobby and electronics toolkits as well. The typical set, much like those pictured in Figure 4-4, include an assortment of flat and Phillips head screwdrivers that fit very small screws.

Many computers also use nuts or small bolts to hold parts together. In some instances the parts may have slotted heads and can be manipulated with a screwdriver. In other instances it is better to use a nut driver since the hexagonal head provides better grip; especially in confined areas such as around disk drives or the motherboard. The two most popular sizes are the 1/4 and 3/16-inch nut drivers.

Manufacturers of computer toolkits have recently begun adding other tools to their kits to help meet the expanding needs of consumers. One of the popular additions is the Torx(brand screwdriver and bit set (Figure 4-5). The Torx(system uses specially designed bits to help reach computer compo-

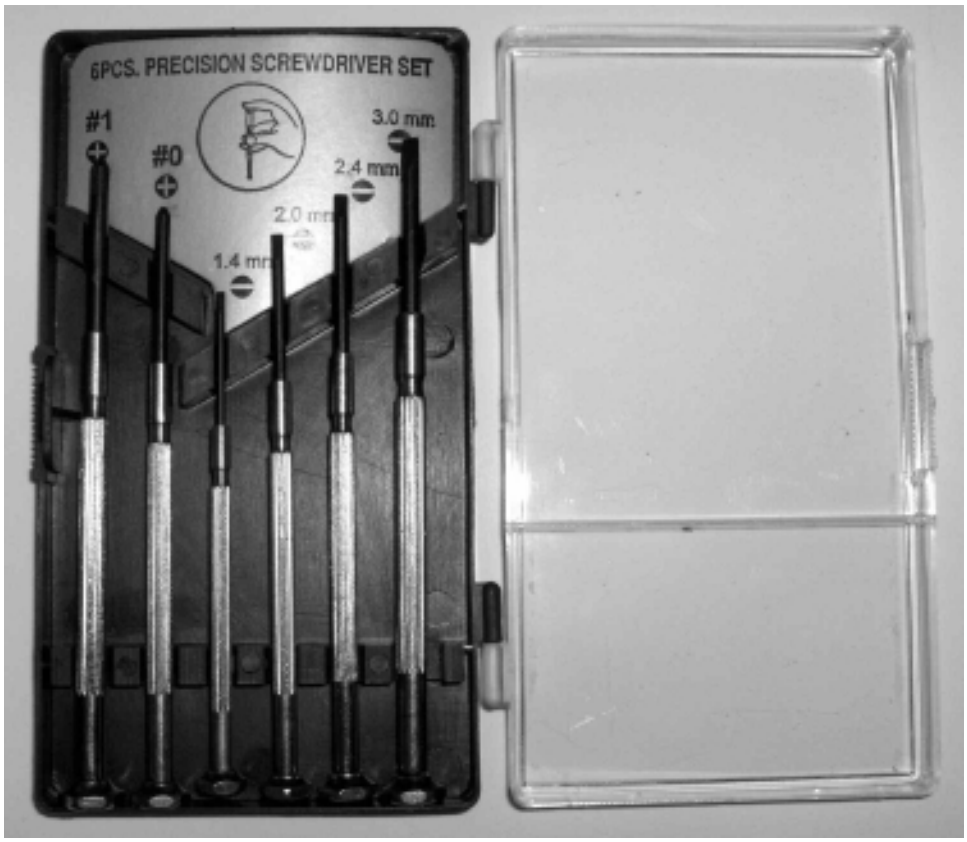


Figure 4-4. Jewelers screwdrivers.

nents and has grown tremendously in popularity in the past few years.

Kits also include small tweezers, clamps, and other gripping devices. In Figure 4-6 we see a pair of tweezers and a chip extraction tool which are both covered in plastic to lessen the potential for static electrical shock. Similar tools can be seen in the two kits pictured in Figures 4-1 and 4-2.

While on the subject of retrieval, many investigators–not to mention computer repair experts–often stock their toolkits with hemostat or similar tools. Most investigators are familiar with these precision gripping or clamping tools since they are often used to hold marijuana cigarettes. Hobbyist, computer repair personnel, and criminal investigators also use these medical tools for general purpose duty.

The better kits also include a specially designed tool commonly called a "chip extractor" (Figure 4-6). This device, which looks like a mutant set of tweezers, is used to grip the outer edges of the integrated chip. The tool allows the user to apply even pressure when pulling the chip from its receiver. As most users know, the IC often has tiny metal legs that are inserted into specially designed areas of the motherboard or other device. These legs are easily bent, and if crooked will cause poor connections or ultimately a fail-

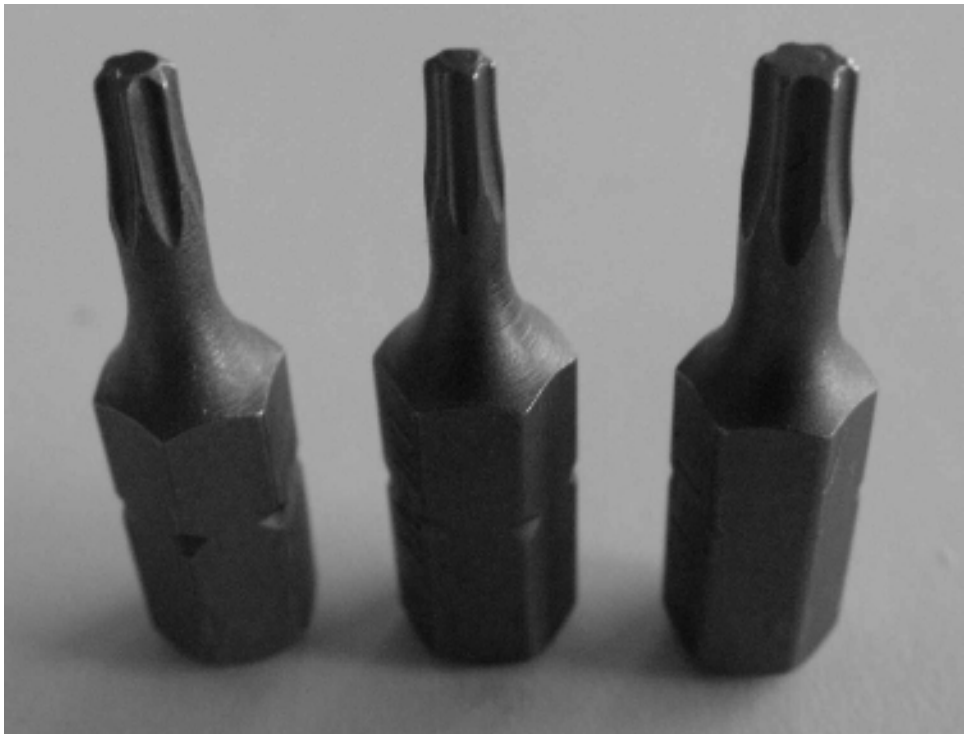


Figure 4-5. Torx type nut/screw driver tips.

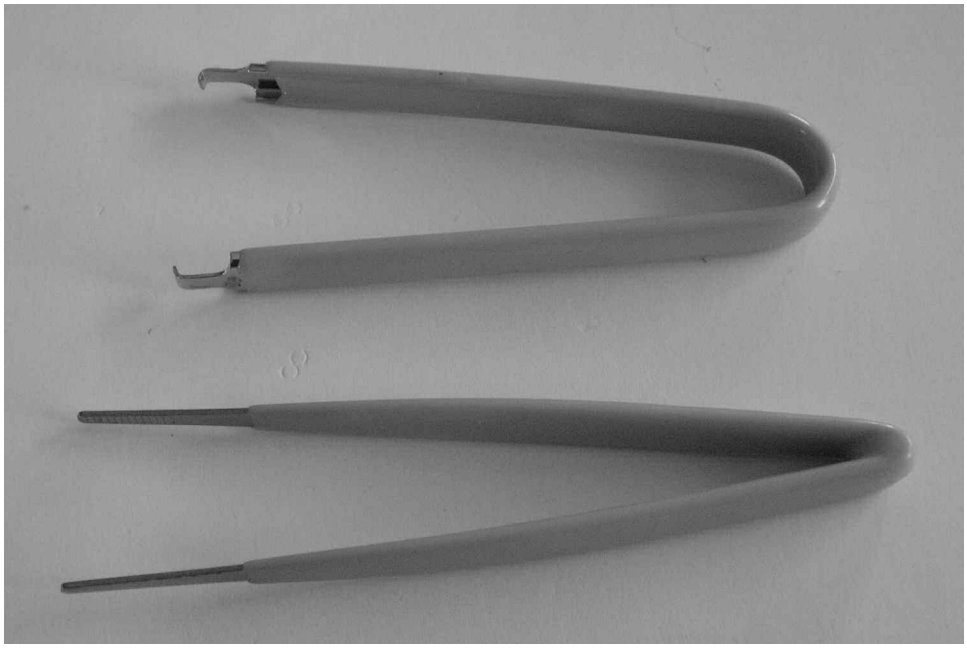


Figure 4-6. Chip Extractor and tweezers.

ure in the system. The chip extractor helps avoid such problems by allowing the user to insert and remove the chip in a simple motion.

With an increasing number of computer cases and components being manufactured in the Far East it is a good idea to also have metric tools available as well. The 7mm nut is the most common in many computer cases today. Investigators can purchase a small nut driver or ratchet set with sockets (3mm through 11mm) for less than five dollars ($5.00). Larger sockets are uncommon in most commercially manufactured computer products, but that doesn't mean a computer hacker who prefers "homemade" parts won't resort to such odd sizes. For that reason is also a good idea to have larger metric sockets available for those special occasions.

Professional grade toolkits are available from electronic and computer supply stores. These kits cost much more than the smaller kits discussed to this point. Average price of a professional quality electro-mechanical toolkit is over nine hundred ($900) dollars. These kits often come in specialized cases and include a wide variety of general and special tools for the job at hand.

As one moves toward a better prepared toolkit it is important to include wire cutters, pliers and wrenches. At least two sizes of wire cutters should be included. The first should be of sufficient size to cut power cables and simi-

lar size wires. The "lineman's pliers" are often preferred for this task. These heavy-duty cutters will easily cut through most computer power cables. They will also handle the task of cutting through extension cords, most household wiring, and some of the smaller commercial size wiring.

Because the typical computer contains nothing smaller than 22-gauge and usually nothing larger than 10 gauge wire there is a need for a smaller set of cutters in the toolkit. The most popular choice is the combination wire-cutter and wire-stripper found at tool and hardware stores. These cutters can be purchased separately or as part of a larger set of tools. In fact, these cutters are so popular they are often found in auto and appliance repair shops.

Less dainty tools found in many kits include a small claw hammer, nail extractor, and sharp knife. The additional tools found in such kits are not so much for the individual computer parts as they are for other items associated with the computer. In one case both the claw hammer and pry bar were used to retrieve an external *SCSI disk array* from inside a homemade cabinet. The user had obviously feared someone gaining access to the disk drives and had literally welded them inside the steel frame of the cabinet. The larger tools were needed to pry open the cabinet and then remove a steel strap welded across the top of the disk case.

In the opening section of this chapter the availability of a flashlight was discussed. In reality, at least two flashlights should be made available to investigators. The first light is a powerful full-size light much like those used by police officers in the field. The standard police flashlight is often bright enough to illuminate a larger area, such as the inside of a dark room, but still maneuverable enough to use inside a computer case. The only drawback to such a large light is that it is not easily manipulated in tight areas such as around drive bays.

For more confined spaces it is recommended that a much smaller flashlight be used. A good example is the traditional "penlight" which is readily available at most major retail outlets. In the last few years many field officers have begun carrying small flashlights on their duty belts as well. These lights generally work well in tight places and are often very durable. The light is used primarily to look in small nooks or in other areas that a larger light will not fit.

No computer crime toolkit is complete without plenty of extension cords and connectors. At least three lengths of extension cords should be available. One cord should be at least twenty-five (25) feet, a second should be at least ten (10) feet, and the third should be no longer than three (3) feet. Some investigators even prefer to stock at least three of the smaller cords (along with the two longer ones) because they always seem to be needed.

Extension cords should provide safe delivery of electricity as well. The cords should not be frayed and must be capable of delivering a constant sup-

ply of power. Older cords, especially those that have had heavy usage, tend to lose some of their quality. These cords can cause electrical spikes and shifts in power that may endanger the computer or cause other unforeseen problems.

While on the topic of surges and spikes it is imperative that the kit or laboratory have access to quality surge protectors. A quality product may have multiple outlets and take the place of an extension cord. Most protectors include a short cord with three-prong grounded plug, and offer plenty of protection for normal use.

Connectors and adapters are also important to investigators, especially those working in the field. The last thing an investigator wants to do is bring the investigation to a halt while someone runs to the hardware store for an extra adapter. While most buildings (including homes) built in the last decade have outlets with the three-prong grounded connection, the investigator should never assume that all sites will be equipped that way. That is why it is important to have at least five (5) three-prong adapters available.

Another strongly recommended adapter is the wall outlet adapter. These typically allow the user to convert a single two-opening outlet into a six or eight plug unit. While this is not recommended for long-term use, especially in older buildings that may not be wired for such use, there is the occasional short-term need that outweighs the concerns for long-term use. Of course, one can easily use the surge protector discussed above for such outlets as well.

A final concern when working in both the laboratory and in the field is the availability of computer power cables. Investigators may come across a computer system which has had its power cable removed by the culprit. This is an inexpensive–yet effective–way to control access to the computer. After all, if the computer cannot be turned on, the user has no need to worry about who may be browsing through unprotected files. Since many of today's PCs use a similar style power cable it is a good idea to include at least one spare in any computer crime kit. These cables can be purchased from most computer supply stores.

2. Evidence Seizure Tools

Along with the tools mentioned above the investigator should also have available the more traditional tools for seizing and marking evidence. Many departments create their own evidence kits and there are several brands available commercially. A typical kit contains just about everything an investigator needs to secure a crime scene as well as contain, mark and seal the evidence. These kits typically cost less than two-hundred dollars ($200) and can be purchased through most police supply stores.

Marking an item of evidence is often necessary for later identification. One method that does not leave any permanent mark is the use of an adhesive label. Many commercially manufactured labels are available at most police supply stores. Pre-printed labels can be customized to include the name of the department along with an area for pertinent investigative data. Other labels are more generic and may include only an area for basic information such as officer's name, department, case number, and short description of the item in question.

In recent years many labels are made using "tamper resistant" materials. For instance, one of the more popular brands is *Tamper Guard Evidence Tape,* which is tear resistant and uses strong glue that resists attempts to peel the label away. Other brands use paper that is very delicate and resists being removed in one piece.

Another popular method includes pre-cut areas on the label that prevent the label from being removed in one piece. These methods allow investigators to seal a container or mark a piece of evidence with some assurance that any effort to alter the label (or evidence) will result in destruction (partial or whole) of the label.

One drawback to the labels made especially for investigative work is the price. To avoid such costs some departments choose to use more generic labels. One of the more popular is the standard file label found in any office supply store. These labels are relatively inexpensive and are often blank. Investigators can write the information needed on the label. Such labels come in varying sizes from the small file label (5/16th x 2 inch) to the full size (8.5 x 11 inch) sheet.

Another common marking method is the use of "tie-on" tags. Usually made of a heavy stock paper or cardboard with a wire or string tie connector, these tags are used to mark large items. Tags are especially useful for marking items such as monitors, printers, and other peripherals. Police supply retailers have several types to choose from, and investigators can also use tags normally associated with retail outlets.

Wire bread ties are also used quite often in computer crime kits. These ties make it easy to control the many electrical cables and wires that are common with computer systems. Manufacturers of such products sell ties in lots or as continuous feed units that can be cut by the investigator to a specific length. Investigators can find these products available in many retail outlets such as office supply and general merchandise stores. Another good source for labels, ties, and other marking products are the many grocery and restaurant supply companies in most major cities.

While on the topic of keeping items together for identification, it is often necessary to carry a selection of rubber bands in the investigative kit. Rubber bands are useful when trying to control loose wires, small parts, and other

items. Most office supply stores have a wide assortment of rubber bands including the largest bands used to bundle magazines, newspapers, and other large items.

No forensics kit would be complete without gloves. Both rubber and cloth gloves should be included in any kit. Each glove is used to handle specific types of evidence. For instance, the rubber glove is preferred when handling items that are greasy or otherwise dirty. This includes items that have been dusted for fingerprints.

Cloth gloves, usually made of cotton to cut down on the chance for creating static electricity, are preferred when handling delicate parts for an extended period of time. The cotton glove allows the investigator to work for long periods of time without the discomfort caused by sweating hands, which often comes when hands are confined in a rubber glove. The cloth gloves allow the investigator to avoid contamination while allowing a greater feel for the item being examined. Gloves also help stop the deposit of body oils, dirt, and other particles from human contact.

3. Storage Containers

Storage containers are almost always needed in a computer investigation. Not only are containers handy for holding wires, disks, and other items found around computers, they can also be used to store larger items that are susceptible to external contamination. There are several types of containers that are commonly found in any forensic kit, and in this section we will discuss the most common.

One of the more common methods for storing items is the brown paper bag. These bags come in a variety of sizes and can be used for extended period of times with little deterioration to the bag or contents. Items that do not need to be free from airborne contaminants work well in the brown paper bag. The bags are easy to use, easy to seal, and make handling lightweight items convenient.

One concern that must be raised when using the traditional brown paper bag is potential contamination to small parts. Because the paper bag is often made of coarse material which has a tendency to fray there is a chance that contaminants can accumulate in computer parts. For instance, the paper "fuzz" that is common with bags found at grocery stores can easily build up in the drive head of a computer disk drive. Such contaminants can ruin the drive and ultimately affect the investigation if the investigator is not careful.

If a bag is preferred but there is fear of contamination from the paper-type bag then the investigator should consider using the plastic bag. Like the paper bag, plastic bags are common and can be purchased at many retail outlets. Office, grocery, and other supply stores carry an assortment of plastic

bags. It is important to remember, though, that a plastic bag will "seal" the item when the bag is sealed. In other words, if the item being stored needs airflow to be properly stored, then the plastic bag may be a poor choice. It is also important to remember that plastic bags, like plastic containers, will seal in other contaminants or corrosives such as water, dirt, and other items.

It is worth noting that while plastic bags are sometimes cheaper than other containers there is a higher risk of static electricity. This is especially true when working with certain synthetic fibers or electrical components. Investigators should be extremely cautious when considering which type of bag or container to use. The wrong bag may be cheap to buy, but the cost to an investigation may be much higher when the bag causes damage to the evidence.

If a bag is too thin or awkward for the job then the investigator will likely use a storage receptacle such as a box or plastic container. Paper or cardboard boxes are preferred for the same reason that paper bags are favored. In some instances a cardboard box is less expensive, provides better protection, and is easier to handle than any other container.

One should remember as well that cardboard boxes are often very different from their paper bag cousins. Most computers today are shipped in cardboard boxes, and the key is to use a box that is made of higher quality material than the cheapest brands. It is important that the investigator choose the right box for the job.

Certain fiber boxes may also work. In recent years there has been a movement by container manufacturers to introduce boxes made from natural products other than wood. For instance, straw and hemp-based products have surfaced in some areas of the country. These products are often as strong as paper (wood-based) products and last just as long. The only caveat worth mentioning is actually the repeat of earlier warnings. The investigator must carefully consider what is being stored in the box, where it is being stored, and how much contamination may occur with such storage.

For long-term storage few containers can match the dependability of plastic boxes or bottles. Plastic has a very high strength to weight ratio. Plastic also allows investigators to store items that may soil other containers because of oil or lubricants. The investigator should be cautious when choosing plastic or synthetic containers, though. Some may raise the risk of static electricity and this should always be a concern when dealing with delicate computer components.

In some instances it may also be worthwhile to keep packing material handy. Styrofoam peanuts or other packing materials can often help shield sensitive electronic components from damage during transit. One of the best forms of packing material is shredded paper, but one should be careful of using shredded newspaper. The ink on the newspaper can rub off onto seized

items and taint them.

Investigators should be especially careful when using any of these materials. For instance, the popular Styrofoam peanuts used in packing may actually "shed" small particles when they are handled or buffeted by heavier items. Obviously this is not a major concern when dealing with a box of books, but when one packs computer disks, disk drives, and other equipment there is a substantial risk of contamination which may later cause severe problems.

4. Computer-Oriented Items

Tools and evidence material are not the only things that go into a good forensics toolkit for computers. The investigator should also have some very specific items for the use with a computer. The first of these is a collection of small batteries used to power the storage for CMOS information. CMOS stands for *Complementary Metal-Oxide Semiconductor.* This is a type of chip that requires little power to operate and is often used in today's computers to store basic information needed by a computer at startup. In the modern computer a battery-powered CMOS memory and clock chip is used to store and maintain the clock setting and system configuration information. Since the investigator may need this information later it is important that the battery not be allowed to lose its power.

Other batteries might also be useful. Some peripherals and even plug-in devices use batteries like the AAA, AA, and 9-volt size. The recent trend toward wireless mice, keyboards, and other input devices means that an investigator should be prepared for any contingency. The well-stocked kit will include at least one battery used to power the CMOS chip, four to six AAA and AA batteries, and at least one 9-volt battery.

Floppy disks, disk containers, sleeves, and labels are a must as well. The investigator should not rely on the offender to provide proper storage or protective containers. The computer kit should include several disk jackets for both 3.5 inch and the older 5.25 inch disk. Though the larger "floppy disk" are not used in many computers today there are a surprising number of older machines with these disk drives still around.

Tyvek or cardboard sleeves are commonly used to store some media, and this is especially useful for the 5.25 inch disks used in older systems. The tyvek sleeve is also used for CD, DVD, and similar products. Paper sleeves are also common, and can be purchased at most office and computer stores. Another solution is to use "disk pages" which can be easily kept in a traditional three-ring binder.

For storing more than one disk or CD at a time it is recommended that the investigator use disk containers. Containers hold from one to several hun-

dred disks, CDs, or DVDs. For CD and DVD storage a "jewel case" is often preferred when storing a single disk. Multiple cases can also be kept in larger containers made specifically for that purpose. Likewise, a CD in a jewel case can be kept easily in almost any box or container that is wide enough to store the CD safely.

The investigator should also have several blank (pre-formatted) disks available as well. It is extremely important that these disks be new. Do **NOT** use a disk that has been used in any other fashion before. Information that might be seized from a computer and stored on a used disk is open for attack by the defense. It is similar to putting evidence from a rape in a used rape kit. While the kit may have been "clean" there is still an appearance of impropriety, and it is simply not worth the chance of contaminating an otherwise valid seizure.

The growing use of CD-ROM drives and the CD-RW drive suggests that investigators also have blank CDs available. Both CD-R (write once, read many) and CD-RW (write many, read many) disks should be kept separate. While most write software will not write to an already completed CD-R it is possible to harm or even erase valuable data with a simple tweak of the software.

D. ENHANCED AND SPECIALTY EQUIPMENT

It is important to note that there is no standard computer investigation kit. To this point we have examined the more common items which might be found in a well-prepared kit, but it is now time to turn to those items which are not required but may be a good idea to include.

One must remember that most of today's computer storage solutions use magnetic media to store data. A magnetic field is used to write and erase the data. This factor is not overlooked by some of the better computer criminals. Those who wish to keep material "safe" will often set up magnetic fields around vital entry and exit areas.

In one recent investigation the culprit installed a relatively powerful electromagnet around his front door. The magnet caused no harm to those entering or exiting the home, but anyone carrying a computer disk ran a high risk that the information on the disk would be affected. The idea was that by setting up a strong magnetic field between the criminal's computer and the doorway there is a likelihood that any data taken from the computer via disk will be erased or irretrievably altered before the investigator can get out the door. Sounds like something from a strange science fiction movie, but it is a reality of life for the computer investigator.

1. Magnetometer and Magnetic Compass

In order to detect such fields some investigators use a magnetometer. The magnetometer is a device used to detect magnetic fields. Prices vary greatly depending on the quality of the device and the intensity of the field in question. In essence the magnetometer detects the field and depending on its quality will even pinpoint the origin or display the intensity of the field for the investigator.

A magnetic compass will work in the same fashion. While the simple compass won't generally tell the investigator how strong the field is it is possible to gauge field strength–at least how widespread the field is–by evaluating the reaction of the compass needle. As the magnetic compass gets closer to the source of the magnetic field the needle will react more strongly. Of course, the cheap magnetic compass is really not the best replacement for a magnetometer, but it is at least better than nothing.

As with many investigative kits the department may wish to include one or more cameras. Both video and still cameras are a good addition to any investigative kit. Photographs help investigators to recreate a scene and are often valuable in understanding the relationship between items. The instant camera like the Polaroid brand is used extensively as are 35mm SLR (single lens reflex) and the newer digital cameras. When using the SLR the investigator should have film that will allow shots in low light as well as in artificial or indoor lighting. A tripod is also a good idea as are flash, flash attachments, and a selection of lens for varying shot types.

Video is also rising in popularity. Today digital video is very popular and the investigator can get a combination still and action digital video camera for well under one-thousand ($1000.00) dollars.

2. Portable Computer System

A laptop or portable computer is a great tool to include in the forensics kit. Preference is given to the laptop with both a 3.5-inch floppy and CD drive. An external drive may also be used. The computer should have ample RAM as well as plenty of room on the hard disk drive. While most data retrieved from a suspect computer will likely be stored on a floppy or CD there are times when it will first be transferred to a neutral laptop or other portable computer system.

One reason for including the laptop is to avoid problems with computers that may have been booby-trapped. Use of passwords and advanced programming techniques are commonly used by computer criminals to protect sensitive data. The wrong key combination can easily start a "self-destruct" program already loaded on the subject computer. One way to avoid this type

of problem is to load the suspect data onto another computer or storage disks.

In some instances a more powerful computer may be needed. For instance, some laptops cannot be used very well as a server. It may be necessary to establish a small Local Area Network for the transfer of data from one computer to the other. A more robust computer like a desktop may already be fitted for such work.

This secondary system should also include a portable printer, paper, and the necessary items needed to support such a system. This includes extra cables, such as null-modem cables, parallel and serial cables, and other connecting devices.

3. Software

Even if the target computer is using the latest Operating System (OS) the investigator should have several versions of the OS available. In fact, the preference is to keep at least two copies of the last five versions of the software available. This means that for the Windows OS the investigator should not only have Windows 2000 but should have Windows ME, Windows '98 (SR1 and SR2), Windows '95, and Windows 3.1. The same applies for the Macintosh OS. Mac OS 10 backward through 5 should be available.

While most of today's computers do not use the venerable MS-DOS it is a good idea to have a copy available at the lab and in the toolkit. Some of the file recovery techniques discussed later in this book use DOS routines to find and protect data stored on a computer. Also, some computer criminals prefer working in the older versions of the various operating systems since they are often the most well known and easiest to manipulate. A good computer crime kit will include the following OS:

1. DOS 3.3 through DOS 6.2
2. Linux 4.0 through 7.0 (Redhat appears to be the most popular)
3. BeOS, and
4. OS/2

Along with the operating systems the kit should also contain some quality utility programs. Some of the better choices include Norton, McAfee, Fastback Plus, and Safeback. Other utility programs include Laplink (with a cable), an ASCII editor and a graphics editor or viewer program like VPIC.

Finally, the kit should include various programs for accessing file types. The first of these are the "zipped" or compressed files. These include PkZip, PkArc, LHArc, Gzip, and similar routines used to compress data. As a general rule the computer should also have a good word processor, spreadsheet,

and database with the latest routines for converting data from one file type to another.

Some other items that you may want to purchase include the following:

- SCSI cables and active terminators
- parallel and serial cables
- coaxial, category 5, and related cables
- printer ribbon, inkjet, and laser printer supplies
- power strips, uninterruptible power supply, and power cables
- compact and floppy disk (at least 50 of each)
- labels for disk
- a permanent marker
- Jazz or Zip (100 & 250 megabyte) disk
- Manila folders, envelopes, and related items
- lockable storage containers
- printer paper

The investigator should also have appropriate manuals for reference material. This would include the operating manual for the investigators computer system, a reference book for all of the operating systems available to the investigator, and reference material for software being used by the investigator. A good reference text to have handy is *Upgrading and Repairing PCs,* Fifth Edition or higher, by Scott Mueller. This book is normally used by intermediate to expert technicians, but is also a great reference text for investigators.

Many computer labs will also have reference text for specific software. This includes operating systems such as Microsoft Windows, Unix, and Apple. This also includes reference text for specific hardware items such as motherboards, modems, sound and video cards, and other I/O cards.

One of the common tactics used by attackers is to make small applets, commonly known as Trojans, which attack the command systems of the computer. This approach originally was adopted for Unix systems, but has become increasingly popular for Windows and Apple systems. Such tactics often inject hybrid commands into dynamically linked libraries (DLL) which affects normal behavior of Windows programs. To combat this tactic investigators should also include backup DLL files along with appropriate system and command files. In many instances these files are maintained on a floppy disk drive or on a CD-ROM drive. Of course, this assumes that either the floppy or CD-ROM drive of the target computer is working.

The software response kit should also include software that the investigator knows is trusted and pristine. This software should include a clean version of DOS, or other operating system, as well as the appropriate DLLs, system files, and trusted binary files. These files or programs should allow the

investigator to change the time/date stamps on files residing on the target hard drive.

In addition to trusted files the software should include bootable floppy and CD-ROM disk. Other software that is recommended includes *Safebak, EnCase, Diskpro,* or similar software. These packages, commonly called forensic software, are used to recreate exact copies of computer files for later processing. *Quickview* and *Handyvue,* or similar software, allows the user to view nearly all file types found on today's computer. What these programs allow you to do is to view files even when you do not have the appropriate program to create or edit the file.

4. Electronic Specialty Equipment

Before getting into this highly specialized area of equipment it is first important to point out that only the best prepared labs or field kits include most of the equipment in this section. There are two reasons for this: (1) The equipment can be very expensive, and (2) the equipment is not for just anyone to use. What this means is that the equipment is to be used by someone who has both a working knowledge of the equipment's operation and a knowledge of how to safely use the equipment around computers. After all, the last thing an investigator wants to do is explain to the local prosecutor why the data was lost when the wrong setting was used on a multimeter or other testing device. With that in mind, we start with some of the more basic equipment found in many electronic and computer shops.

The first piece of electronic equipment is the voltmeter. This is both the simplest and most common piece of equipment on the workbench today. The meter is used to measure voltage. Direct measurements can be made, and this can help investigators determine that the equipment in question is receiving the proper charge. One reason a voltmeter might be used is to insure that drives or other devices are working as designed.

With the development and widespread use of semiconductors we have seen a growing list of meter-oriented electronic equipment. All of these devices are designed and intended to measure various levels of electronic activity in a given device. The precise manufacturer of semiconductors has led to a whole new set of "standards" for such meters. Most significant of these is the *Zener* diode, which when manufactured to close tolerances, so as to be temperature and current independent, do not lose their reference value as readily as the older systems. This has led to the development of better equipment.

Where the voltmeter was the staple of any early electronics shop other equipment has been designed and added over the years. Today, many electronics workbenches include a "do it all" piece of equipment commonly

called the "multimeter." In essence, the multimeter combines the common voltmeter with measuring devices for such functions as ac/dc voltage, ac/dc current, resistance, temperature, frequency, capacitance, diode and continuity.

The Multilog multimeter is a fine example of this type of meter. Selling for around three-hundred dollars ($300) this unit allows electronic hobbyist and professional alike to measure a wide range of electronic conditions. Data can be easily viewed on the LCD display, and use of such a device is accepted throughout the industry.

When working with network connections investigators may need to certify that the connection meets accepted standards. One reason for this is to avoid later defense claims that the connections caused inaccurate collection problems due to bad connections or faulty systems. One method for verifying such connections is the use of electronic testing equipment designed specifically for network applications.

Cable systems tested by older analog cable scanners may not guarantee cabling performance when high-speed networks are installed. Not only does an instrument like the DSP 200 Cable analyzer allow you to certify links with accuracy, insuring the highest level of confidence, but its unique "Fault Info" feature shows exactly where any failures may be. The diagnostics are displayed in a graphic representation and in plain language on a bright backlit display. Whether poor workmanship, a bad patch cord or improper cabling is to blame, this device allows the investigator to discover how reliable any link in a high-speed network will be.

Chapter 5

EXPERT ASSISTANCE

Obviously not every investigator is going to know everything there is to know about a computer system or the methods for using it. Investigators must be relatively knowledgeable, but more importantly must be able to at least recognize when they need help. When the need arises then it is important that the investigator have a plan of attack. That means they should know of local experts, as well as some national or regional ones, to help with the more complicated computer problems that might arise. In the coming pages we will explore the basic need and use of experts in the computer crime case.

A. DETERMINING THAT AN EXPERT IS NEEDED

The first significant step in using an expert is making the decision to actually use one. Surprisingly there are many investigators who simply will not ask for help. Too often they stumble their way through an investigation, often

causing more harm than good, and when they do finally decide to get help it may be too late. To avoid these problems the investigator must be willing to admit that he needs help.

The first step in determining whether an expert is needed is the process of self-evaluation. The investigator must be willing to effectively rate his own abilities and computer knowledge. Skill must also be rated, so that the investigator has a clearer understanding of where he will need help. As an example, an investigator who is knowledgeable about basic computer components may be overmatched in a case dealing with complicated network issues. In this instance the investigator who is able to evaluate his personal abilities will be a better asset to the case by recognizing the need for help in the area of network technology.

When making such an evaluation the investigator should consider four specific areas. First, the investigator must clearly define his understanding of the particular technology issues in question. As in the example above, an investigator may have sufficient practical knowledge in one or more areas, but if the question at hand is in another area then the investigator's ability may be impractical.

Second, the investigator must rate his competence in a given area. On the surface this may appear to be similar to that of understanding, but in practical terms they are much different. I will use myself in this example. I have a marvelous understanding of how an internal combustion engine works, but I have the mechanical ability of a dry sponge. In other words, my understanding may be sufficient but my competence (ability to perform) is very limited. As such, I often call an expert when it comes to the repair of my own vehicle. As an investigator if I had a similar dilemma when dealing with technology I would clearly need an expert for some of the issues I might face.

Third, the logistical ability of the department must be evaluated to determine the capability for handling the particular case. This includes an evaluation of laboratory facilities, manpower, and budget. A perfect example of this type of case would be one involving the retrieval of data from a hard disk drive. If the department does not have the forensic computing equipment (hardware and software) needed for such a delicate task then the investigator would likely need to call upon an outside expert for assistance. This is especially true when dealing with a sophisticated suspect; i.e., one who has likely booby-trapped the hard disk to corrupt the files if unauthorized access is attempted.

The fourth criterion is a bit more difficult to fully apply. In this element the investigator must evaluate the logistics of using an expert. What this means is that the investigator must look at those external factors (those outside the investigation) which affect the ability to use an expert. Chief among these are costs, availability, and related details.

The logistics of costs is a constant issue for both private and public investigators. Few investigators have an unlimited budget in any case. This means that the costs of the expert may hamper the ability to use that expert. This will vary greatly depending on the expert, the task, and the overall issue in question. For instance, if the question is one involving data retrieval then the expert may be someone with the right equipment. Recovering data from a damaged hard drive does not require high levels of education, but merely the right tool with the right knowledge of how to operate it. On the other hand, if the expert is called upon to decipher a complicated algorithm–such as those used in encryption–then the level of training, experience, or education might mean the expert's cost rises significantly. All of these factors now come into play when choosing the expert in a given case.

Somewhat related to cost is that of availability. The first issue of availability is physical in nature. Is the expert physically able to join the investigation? In this instance the question of availability might mean that the cost to secure this expert's assistance is cost prohibitive. For example, flying an expert in from Germany will certainly raise the issue of availability to a new level.

Availability also includes the work side of the equation. Is the expert available to work on the case during the time allotted? It is not uncommon for experts, especially those with highly sought-after skills, to be engaged in other work which prevents them from taking new cases. In such a case the availability question is one that may be well outside the control of the investigator, regardless of how much funds are available to pay for assistance.

Once the investigator has rated those areas set out above it is time to fully evaluate the case itself. Investigators should determine, to the extent possible, the knowledge that the suspect may have as it relates to the given issues of the case. Much of this evaluation is subjective and often inaccurate simply because the officers never have enough information. The secret is to find enough to rate the suspect so that a proper expert may be used. Sadly, since most suspects try not to leave such clues behind this task is often the most difficult to do.

The focus of this evaluation is on the suspect's behavior, relationship, and specific modus operandi of the case. Many officers use a checklist for such evaluations, and a sample of such a checklist (Table 5-1) is provided below. This form has been adapted from similar forms used to rate suspects in information theft investigations. As such, it is essential that one remember that this form is used to rate a potential computer criminal in a specific type of case. More detailed forms, and those fitting other case types, are discussed in later sections of this book.

The last factor evaluated in this form is part of the overall MO of a given suspect. In evaluating this level of sophistication the investigator is also eval-

Table 5-1. Sample Checklist.

Municipal Police Department 1234 Main Street Anytown, USA 99999	
Computer Suspect Rating Sheet	
Rating Scale: 3 - Suspect displays above average knowledge or ability 2 - Suspect displays average or ordinary knowledge or ability 1 - Suspect displays knowledge or ability below average 0- Suspect displays little or no knowledge or ability	
☐ 3 ☐ 2 ☐ 1 ☐ 0	Location of information taken; i.e., did suspect know where the information was stored in the system or systems?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Access to information; was suspect able to easily access information or systems in question?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Use of OS during access; did suspect use any special OS tools to access areas where information was stored?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Chance of detection or capture; did suspect display knowledge or understanding of monitoring or security systems?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Contact points or points of entry; did suspect easily negotiate either or both?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Collateral trespass; did suspect commit any trespass to other areas not associated with the target acquisition?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Errors or omissions; do logs show suspect committed errors or omitted information during trespass?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Use of other tools; did suspect use other hardware or software to access system or information?
☐ 3 ☐ 2 ☐ 1 ☐ 0	Knowledge of overall system architecture.
☐ 3 ☐ 2 ☐ 1 ☐ 0	Prior knowledge of information; did suspect display any knowledge of the information they were seeking.
☐ 3 ☐ 2 ☐ 1 ☐ 0	Use of specialized equipment or methods.

uating the potential need for expert assistance. As such, the investigator should consider the type of computer involved, what operating system it uses, and whether the information sought can be accessed by, or is controlled by, a computer literate target.

By evaluating these first few issues the investigator is providing a realistic view of the overall case. To see how this might work in a case let us imagine for a moment that the investigator is very knowledgeable in PCs but lacks

substantive knowledge in the area of mainframe computers. The suspect, on the other hand, is very savvy in the working of both mainframe computers as well as UNIX systems. If the investigation involves a UNIX system then the investigator, who may be an expert in other areas, must recognize the need for help.

Answering these questions is key simply because no expert can be expert on all systems. Mainframes, for example, are made by various companies (e.g., IBM, DEC, Cray) and often run unique, proprietary operating systems. Even the PC market offers significantly different hardware/software configurations. Although the most common desktop computer is an IBM or IBM-compatible system, it runs a range of operating systems including DOS (with or without Windows), OS/2, and UNIX. Apple Computers are also popular and run their own unique operating system. In this sense, the investigator may be very knowledgeable in the PC system using Windows, but the culprit's use of Unix now takes the case to a new level.

A detailed evaluation of the suspect is also helpful in determining the potential troubles one might have in future legs of the investigation. A computer literate suspect may attempt to frustrate the investigation by using tricks known to specific groups but not to others. For instance, a group of college-age "hackers" may know several routines or tactics that an experienced officer may not know. Likewise, codes or phrases used to pass information may be easy for a person coming from a particular background to understand, but someone a few years older or maybe educated in a different part of the country would not understand it. The expert might, and if the investigator has made a thorough analysis of the case then such need may be immediately recognized.

In sum, since computer experts cannot possibly be expert on all systems, it is important to have the correct expert on the scene. Knowing the type of computer to be searched, and the type of operating system being used, will allow the appropriate expert to be selected. This, in turn, will streamline the search process, since the expert may be familiar with the software and file structures on the target machine.

B. FINDING EXPERTS

To determine what type of expert will be needed, investigators should get as much information about the targeted system as possible. Sources like undercover investigators, informants, former employees, or mail covers can provide information about the system at the search site. Once the computer systems and software involved have been identified, an appropriate expert can be found from either the federal, state, or private sector. Ultimately, the

expert must use sound scientific techniques to examine any computer evidence.

1. Federal Sources

The best place to find an expert may be in the investigating agency itself. Many federal and state investigative agencies have experienced people on staff who can quickly help when the need arises. If the investigating agency lacks an expert in the particular system to be in question then other agencies may be able to assist.

The trick, of course, is to find the expert while conducting an already complicated investigation. For that reason it is recommended that investigators begin immediately to gather names, contact numbers, and relevant information from those who may serve as expert. By developing this list of contacts the investigator builds a database of experts which may be easy to reach and even easier to use. The secret is not to wait until an investigation begins, but instead gather names and contact information now so that time is not wasted later.

Most of the federal agencies that routinely execute search warrants for computer evidence have analysts at central laboratories or field experts who can search the seized computer evidence. Many of them will also work on evidence from other federal or state agencies as time permits. It is important to call early to get specific instructions for handling the evidence, and these experts can provide other technical assistance as well. For example, there are many kinds of software (both government and private) which will help process evidence, break passwords, decrypt files, recover hidden or deleted data, or assist investigators in other important ways. Because these utilities are constantly changing, it is important to consult with experts who have them and know how to use them.

When beginning your trek into the area of experts it is necessary to also understand how these federal or state agencies work. Each agency organizes its computer experts differently. For example, the *Computer Analysis and Response Team* (CART) is a specialized team within the central FBI Laboratory in Washington, D.C. This team examines various types of computer evidence for FBI investigators nationwide. They will also handle requests from other federal, state, and local agencies as time or budget permit.

The Internal Revenue Service (IRS) also maintains a full-time cadre of experts. Unlike the FBI, the IRS experts are decentralized and work out of various field offices around the country. *One of the more well known of these IRS groups is the* Seized Computer Evidence Recovery (SCER) unit. These agents generally work in controlled labs in most major cities, but the decentralized

nature of the unit means that one will have to do more legwork to get to know who does what in the agency. Almost every IRS District has at least one SCER Specialist, and many have two, so local investigators should start with their local offices.

The Drug Enforcement Administration's (DEA) forensic computer experts are also experienced in all phases of computer operations related to criminal cases, including data retrieval from damaged media and decryption. Other federal agencies that use computer experts include the *Electronic Crimes Special Agent Program* (ECSAP) with the United States Secret Service. The Secret Service maintains at least twenty special investigators who are members of the team. These investigators are assigned to field offices on a regional basis and are trained in the area of computer investigations and computer forensics.

There are also state sources that have similar duties and functions. Unfortunately space does not allow a detailed discussion of each of the individual state agencies. In many instances investigators at the state and local level have a greater command of which agencies serve their area than could be covered in a book of this nature.

2. Private Experts

When a federal or state expert is not available some departments are forced to turn to private experts. As a general rule it is good practice to clarify with the private expert their role in the investigation and to protect the department with a strict contract that sets forth that role. The contract should also set forth a specific non-disclosure clause that prevents the expert from revealing, without permission of the department, any information which is discovered in the course of the expert's work with the department.

There is also some concern when a private expert, sometimes called a police agent, is used to secure, serve, or administer a search warrant. Where the expert will be used the investigator should provide notice to the issuing magistrate and make note in the affidavit of the expert's qualifications. The issuing magistrate should know why an expert is needed and what his role will be during the search. Investigators must carefully monitor the expert to insure that he does not exceed the limits described in the search warrant.

Because most private experts are not familiar with the judicial system it is unlikely that the expert will know how to execute a search warrant, protect chain-of-custody, or resolve search issues that may affect the evidence's admissibility at trial. Thus, a private expert should be paired with an experienced agent every step of the way.

a. Professional Computer Organizations

Many professional computer organizations have members who are experts in a wide variety of hardware and software. For instance, there are more than two-dozen certification organizations around the country today. Certification in a particular topic is a good way to find an expert. For instance, if one needed a generalist, an expert who could identify computer hardware and make basic repairs or alterations, then one would likely use an "A+" certified individual. An expert in software applications might easily be one with MCSE certification. Virtually every aspect of computer science has a corresponding group or certification forum.

Other forms of certification include that done by specific manufacturers or vendors. For instance, the Microsoft Corporation certifies individuals in a wide variety of issues involving Microsoft products. One of the better known certification is the Microsoft Certified Systems Engineer (MCSE). Microsoft Certified Systems Engineer candidates are required to pass seven exams testing the knowledge in areas of operating systems, system design, and business implementation. The examination is provided by Microsoft and given at testing centers around the country. These centers also maintain a list of people who have passed the certification. There are other Microsoft exams available in such areas as Office (MOUS), Database design and use, and certification in specific software packages.

Other manufacturers such as Novel, Cisco, and many others also offer certification for their products. If an expert is needed in one of these areas it may be helpful to find a person certified by the particular manufacturer or vendor. In most instances the investigator need merely call the manufacturer and ask for a list of certified persons in their area.

If the investigator is not familiar with these organizations then he may get information on such entities from other agencies or private individuals. Computer experts from the government are a good source for finding a private expert since many have gone through the same certification programs. Likewise, searching the Internet with one of the many popular "search engines" will reveal a great deal of information about computer certification.

Another good source in private industry are local companies that service the items in question. For instance, if you needed an expert on Western Digital hard disk drives then one might look for a Western Digital service center. If no one at the center is willing to help, or they don't fit the need in another way, then they can probably point you in the right direction.

Another source, but not necessarily a good source, is the local computer users group. Many are affiliated with the local library, college, or other civic organization. These groups are generally made up of various professional and amateur computer users who share a common interest. There are many

groups which focus on specific software packages, programming languages, or other computer areas. While most of the members of a computer user group are far from being experts they are at least a good source for finding an expert.

b. Colleges and Universities

In other areas of Forensic Science the universities and colleges around the nation tend to be good sources for expert assistance. All professors at these institutions typically hold at least a masters degree in their subject area and a majority will possess the doctorate. When dealing with high-tech crimes involving rare kinds of hardware or software the college and university may be the best bet for finding an expert. The academic environment attracts problem-solvers who may have skills and research contacts unavailable in law enforcement.

One point worth mentioning when dealing with this level is that there is a big difference between the expert who teaches and the one who sells his product as a commodity. Many college and university professors provide consulting on the side which means they will help with a problem but not be readily available for courtroom work. Others provide both levels of services and are willing participants as "expert witnesses" in courts. As a general rule the investigator must keep in mind the ultimate reason for using the expert. The expert is hired to assist with the investigation, and for that reason the expert's qualifications must meet the needs of the investigation as well as those established by the courts.

What all this means is that there is often a difference in capability between someone who gets paid to explain things and one that can actually do those things. Let me give you a perfect example. In a recent case, the expert hired had impressive academic credentials but almost no practical experience in the area being examined. In other words, this alleged expert had read a lot about the problem but had never really solved the problem in the field. This is much like calling someone who has read a book on homicides an expert detective. The fact remains that experience and capability are more important than just good entries on a résumé.

Because college level professors are good at teaching, or at least should be good at teaching, they make great expert witnesses. They are effective communicators, but not always effective problem solvers. If the investigator needs a special problem solved then the college professor may still be a good choice, but be sure to get one with practical ability not just verbal.

c. Computer and Telecommunications Industry Personnel

In some cases, the very best expert may come from a vendor or service provider, particularly when the case involves mainframes, networks, or unusual systems. Many companies such as IBM and Data General employ experts solely to assist various law enforcement agencies on search warrants. If your community has one of these companies then this is a great place to find the expert you need.

Other industries, such as the local telephone company, television station, and school district may have staff who qualify as well. The key is to expand your search so that you include all potential experts in a given area. That way you have a choice of who to use and can usually be assured of higher quality work.

d. The Victim as Expert

Finally, in some circumstances, an expert from the victim organization may be the best choice, especially if the hardware configuration or software applications are unique to that organization. Investigators and prosecutors must, of course, be sensitive to potential claims of bias by the defense when the victim is used as the expert. Many relevant issues, such as estimates of loss, may pose a considerable gray area. Even if the victim-expert is completely dispassionate and neutral in her evaluation, her affiliation with and loyalty to the victim organization may create a bias issue later at trial.

C. WHAT THE EXPERTS CAN DO FOR YOUR INVESTIGATION

Investigators and prosecutors who anticipate searching and seizing computers should include a computer expert in the planning team as early as possible. Experts can help immeasurably in anticipating the technical aspects of the search. This not only makes the search smoother, it is important information for designing the scope of the warrant. In particular, if investigators can give the expert any information about the target's specific computer system, the expert may be better able to predict which items can be searched at the scene, which must be seized for later analysis, and which may be left behind.

One should also remember that if the computer system is unusual or complex the technical expert can be invaluable help at the scene during the search. This is particularly true when evidence resides on computer networks, backup tapes, or in custom-tailored systems. The evidence will be

safest in the hands of an expert who has experience dealing with that type of system.

Experts can also help with the analysis of electronic and other components. Most forensic computer examiners will perform at least the following: (1) make the equipment operate properly; (2) retrieve information; (3) unblock "deleted" or "erased" data storage devices; (4) bypass or defeat passwords; (5) decipher encrypted data; and (6) detect the presence of known viruses.

Section 2

SPECIFIC COMPUTER CRIMES

Chapter 6

HARDWARE AND SOFTWARE CRIMES

A. INTRODUCTION

In most cases involving computers there is a significant likelihood that hardware will be a central issue in the case. Knowing what hardware is involved, how it is involved, and what to do with it once known is an important matter. In this section we will examine some of the issues that face an investigator when hardware is an issue in the computer crime.

Before beginning the individual sections of this chapter it is important that investigators understand the relationship that hardware has to all things related to computer crime. In the earliest sections of this book we focused on defining the computer crime, and a central focus of that definition relied on the use of hardware. We also spent a significant amount of time identifying and describing specific hardware in today's PC. The investigator must have at least a general understanding of these areas before he or she begins any investigation, and without this knowledge the investigation will likely stall.

With that in mind, it is time to focus on the computer as a part of the criminal act, and we will start with the issues of classifying the hardware based on its involvement.

B. CLASSIFYING HARDWARE INVOLVEMENT

Depending on the facts of the case, the involvement of the computer hardware will generally fall into one of three broad categories:

1. the hardware is contraband;
2. the hardware is an instrumentality of the offense; or
3. the hardware constitutes evidence of an offense.

In each of these instances the investigator will take specific steps to protect the hardware and any potential evidentiary value that might be gained from the hardware. The biggest difference is in the treatment of the hardware within the case itself. As we will quickly see the issue is one of what an investigator may do with the hardware in question. To better understand these three areas let us break them down into their individual issues.

1. Hardware as Contraband

The term contraband is generally used to refer to any item, whether tangible or intangible, which is unlawful to produce or possess. We include both tangible and intangible items to help us deal with both hardware and software. In a more specific usage the term refers to goods exported from or imported into a country against its laws. The term "Derivative Contraband" is also used to describe items of this nature, and specifically refers to items of property not otherwise illegal but subject to forfeiture according to the use to which they are put.[1]

When investigating computer crime the term contraband applies when the computer, software, or peripheral is illegal to possess. The easiest example for us to use is a computer containing electronic components which are imported illegally. This might include an illegally manufactured CPU. In this example the CPU design is protected under patent law, and the unauthorized copying/manufacturing of that CPU design can result in criminal prosecution. Typically CPU pirates copy the design then manufacture less expensive versions of the original design, and in many instances this is done outside the borders of the United States. The CPU is then "imported" for sale in the American market.

Computer software may also be contraband in the same sense as hard-

ware. While hardware is often protected by patent, software is more commonly protected through copyright. The criminal provisions of copyright proscribe the unauthorized copying of any software. A large market for pirated software exists, and not all of it comes packaged in a tangible form. For instance, the epidemic copying and distribution of software using "peer to peer" technologies such as Napster, Gnutella, and KaZaa demonstrate how easily software can be pirated. To avoid criminal prosecution some pirates operate outside the borders of the United States, and any importation of pirated software creates a contraband issue.

2. Hardware as an Instrumentality of an Offense

In identifying hardware as an instrumentality of an offense it is first necessary to understand a few basic theories behind the law of evidence. As a general rule, one can define evidence as any item (whether tangible or intangible) presented in court for the purpose of proving or disproving a question under inquiry. Traditionally evidence included tangible items such as documents, weapons, photographs, and many other items. Evidence also included intangible things such as testimony, audio or video, and related items.

The use of *direct evidence* is often preferred in any given case, and computer crimes are no different. Direct evidence is any item that stands on its own to prove an alleged fact. The use of eyewitness testimony is an example of an intangible form of direct evidence. We cannot hold or physically manipulate the testimony, and the transcript of the testimony is not itself evidence, so we say that the testimony is intangible only in the sense that it cannot be physically held. The spoken words take an intangible form, but are still considered as direct evidence.

Tangible items may also be direct evidence. As an example, if a victim is shot by a robbery suspect then the recovered bullet is a form of tangible evidence which is also direct. It is a direct link between the criminal act and the criminal. We do not need an eyewitness to verify the shooting since the presence of a bullet in the victim's body is enough.

When exploring the issue of the computer as an instrumentality of the crime it is important to remember that the computer is an inanimate object. As such, the computer cannot commit a criminal act. The term "instrumentality of the crime" is used to explain that the computer was an important part of the crime, but not necessarily the criminal act itself. Thus, the printer connected to the computer system may in fact be an instrumentality of the crime of counterfeit.

The computer, and those peripherals connected to it, is no different than any other tool used in a criminal act. Like a gun it is virtually harmless by itself. Someone must use it before it can cause harm. And like a gun, when

the computer is not the central focus of the criminal act then it may or may not be seized. Only when the computer plays a central role in the criminal act would we consider it to be an instrumentality of the crime.[2]

The point of the instrumentality theory is to distinguish goods having a "close enough relationship to the offense" from those incidentally related to it.[3] Like many items used to perpetrate a criminal act, the computer may be seized when it is used in the actual crime. In the example above the computer and printer are used to print phony documents such as checks, identification cards, or even money. In such an instance the computer is considered to be an instrumentality of the crime because of its direct involvement with the criminal act. In this case, though, the computer is not ordinarily considered as direct evidence of the crime, and this is often where many lay persons get confused.

In many instances the instrumentality of the crime is seized not only because it is evidence but because it can be used in continued criminal acts. In such instances the item will not be released, even upon conclusion of the case. It is also important to remember that the item may be seized under more than one of the theories discussed. This is especially true when the computer is both evidence of a crime and an instrumentality of the crime. The computer may be seized as an instrument of the crime but may also be held as evidence in the trial that follows. In such cases, the investigator may need to establish each of the reasons the computer was seized. Recognizing when a computer is seized for multiple purposes can help avoid confusion later.

Once the investigator has his reason for seizing the computer he must determine what part of the computer system is to be seized. This will vary from case to case depending on the needs of the investigator and the type of equipment involved. In some cases the investigator may take only the hard disk drive while in other cases the investigator will seize all of the components of the computer system. This is where the understanding of the rules of evidence and that of instrumentality of a crime are useful.

The Federal Rules of Criminal Procedure authorize officers to seize a computer when it is an Instrumentality of the Crime. Specifically, the Federal Rule of Criminal Procedure[4] authorizes warrants to seize the instrumentalities of crime, and these have been traditionally identified as "property designed or intended for use or which is or has been used as the means of committing a criminal offense."[5] The justification for such seizure focuses on the need to prevent use of the item to commit future crimes.

An instrumentality of the crime is often defined as "any machinery, weapon, instrument, or other tangible object that has played a significant role in a crime."[6] An example would be the sophisticated scale used in narcotics trafficking. The scale is used to carefully measure the narcotics, and as such

is proof of the narcotics sale. Few casual users have any need for a sophisticated scale, and investigators of such crimes are quick to identify the presence of such scales as a contributory connection to the criminal act.

In the narcotics scale example the item in question is said to have an "innocent character," and this places some additional obligation on the investigators to prove its use in the criminal act. The courts have held that even where the object in question is innocent in character, courts will assess its role in the crime to determine whether it was an instrumentality.[7]

Not every article that plays some part in the commission of the alleged crime is a means of committing it. An important question asked by the courts and investigators alike is whether the crime alleged could have been committed without the article seized. The courts tend to look at the totality of the circumstances in answering this question.

Before the Supreme Court's decision in *Warden v. Hayden,* courts held that property subject to seizure included instrumentalities but did not include mere evidence.[8] In practice, however, judges were reluctant to suppress useful pieces of evidence at trial, preferring instead to interpret the term "instrumentality" broadly enough to encompass items of evidentiary value. The specific question is whether the item in question connected the defendant to the alleged criminal act.[9] The Court also held that the Fourth Amendment principally protected privacy rights, not property rights. Thus, the amendment secured "the same protection of privacy whether the search is for 'mere evidence' or for fruits, instrumentalities or contraband."[10]

Although items that are evidence of crime may now be seized along with instrumentalities, fruits, and contraband, this historical perspective is important in understanding why some early decisions may have categorized evidentiary items as instrumentalities. Moreover, the distinction between "an instrumentality" and "mere evidence" remains critical in computer crime cases because it may determine the government's ability to seize hardware. If a computer and all its peripherals are instrumentalities of a crime, the warrant should authorize the seizure of these items. But if we are seeking the computer only for the documentary purposes or for the components (mere evidence) it contains, it may be more difficult to justify the seizure or retention of hardware.

3. Hardware as Evidence

In 1972, the Federal Rules of Criminal Procedure[11] were amended to authorize seizing "mere evidence" of a crime. In relevant part, the Rule now states: "A warrant may be issued under this rule to search for and seize any property that constitutes evidence of the commission of a criminal offense. . . ."[12]

A physical item is evidence if it will aid in apprehending or convicting a

person who has committed a crime. This does not mean that the evidence will have to be presented at trial or even be admissible at trial. In this instance we are talking about evidence which the investigator may use to prepare or further his case.

The test applied by most courts is whether the evidence in question would be reasonably seized by another officer under the same circumstances. This is a form of the now famous "reasonable man" test where the court views the investigator's actions as compared to what a reasonable man (or in this instance, a reasonable officer) under similar circumstances would do.[13]

Of course, simply because an item is "evidence of a crime" does not mean that other restrictions may not apply. Law enforcement officials should be aware of other limits imposed by the Constitution, statutes, and regulations upon the seizure of evidence. Where other standards limit or exclude the seizure the officer may not simply rely on the federal rule. This is one reason that the officer must be intimately familiar with the rules of criminal procedure for his jurisdiction. One should not assume that a legal action in the federal system will necessarily be legal in an individual state court.

C. THEFT OF HARDWARE OR SOFTWARE

1. Tracing Stolen Computers and Components

Tracing stolen computers or computer components is often a difficult task. Many of the individual parts that make up a computer system do not have a unique number or other identifier, but that does not mean that they cannot be traced. For the computer crime investigator the task of tracing stolen computer components involves a great deal of legwork to become familiar with the various components and their means of identification. That is why we spent so much time in the beginning of this book identifying and examining basic computer hardware.

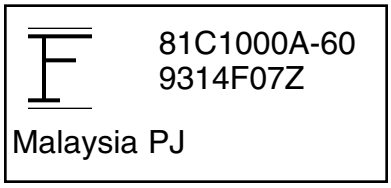
The majority of computer components have some type of marking or identification feature. This typically includes a serial or part number which is commonly marked either directly on the component or on a sticker attached to the component. We begin this section with some of the smaller, and often more difficult parts, to both identify and trace.

a. Identifying Integrated Circuits

Identifying marks on ICs vary from manufacturer to manufacturer. In order to make a proper identification of any IC the investigator must be able to recognize at least three out of four identifying marks. These include:

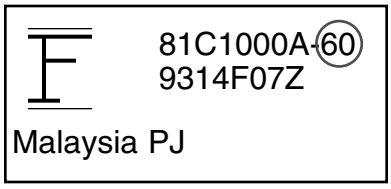
1. The Manufacturer's Logo
2. The "serial" number or "ID" code
3. Chip assembly mark
4. Data code

Most IC manufacturers mark their product in some way with a logo or other company identifier. The example below provides an artist rendition of the common marking method used by many chip manufacturers. The upper left corner contains a stylized "F" which indicates that the manufacturer of this particular chip is Fujitsu. Just below the manufacturer's logo is the assembly plant identifier; in this case indicating the chip was manufactured in Malaysia. To the right of the logo are two numbers. The top number is the part number and below that number is the date code.

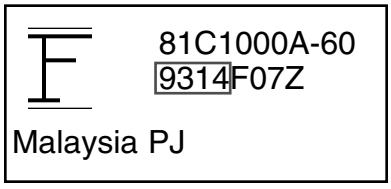


In the example above there is no real serial number for this chip. There is, however, a series of identifying marks which can work together to help the investigator identify the chip. Starting with the logo the investigator can begin to trace a specific chip to the manufacturer, manufacturing plant, and even date when the specific item was made.

The identifying marks and numbers often have very specific meaning beyond that of a serial number. In this example, the top number along the right-hand side is used to determine the type of chip in question. It is imperative that investigators either learn how to identify chips or have appropriate reference material available to make such identifications. In this example the chip in question can be easily identified as a 60 nanosecond memory chip. Fujitsu typically marks their chips so that the last two digits of the part number (circled in the pictured below) represent the speed of the chip.



We can also identify the year and week in which the chip was manufactured. Staying with the Fujitsu example we can use their markings to determine that the chip was made in 1993 during the fourteenth week of the physical year. A box has been drawn around the numbers that make this identification possible. Again, it is important that the investigator understand the marking scheme in question. In this instance, the remaining numbers help identify the batch number of that particular production run, and armed with information a investigator could begin to trace the route of the chip from manufacturer through normal retail routes.



One reason date codes are important is that they help identify the chip in relation to other chips of the same grouping. For instance, it is common for ICs to be stolen in quantity simply because they are so easy to smuggle out of a plant or warehouse. A few hundred chips will fit effortlessly inside a man's coat pocket, and few would notice unless they were earnestly looking for something.

Understanding this and other identifying methods will greatly help the investigator when dealing with bulk crimes as well as those of individual chips. For instance, if the investigator finds several chips from the same manufacturer and same batch in one isolated location there is a greater chance that the thief, or some conspirator of the original thief, has "dumped" the stolen items in the area. In other words, the thief has disposed of the stolen merchandise through the various sources, including traditional fencing operations, which are available. In this sense, computer component thieves, like their non-cyber counterparts, tend to stick with patterns that they are familiar with and this is a plus for investigators.

Investigators should also note that some distributors and OEMs (Original Equipment Manufacturers) are assigned date codes or other identifiers by their suppliers. This means that the chips sold to that customer are marked with a unique date code placed only on those chips. This further helps identify one chip over another since the unique date code is always assigned to a specific customer. This means that someone not authorized to have such a chip will have little excuse or alibi.

The obvious first step in investigating any computer crime is to obtain the marking methods of the manufacturer. There is a catch to this, though. In

many instances the chip manufacturer may mark the product in a specific fashion only to have that chip remarked by the next level user or marketer. For instance, the Fujitsu company manufacturers several types of ICs including memory chips, and these chips may be purchased for resale by an OEM. In this instance, the marking on the Fujitsu chip might easily be modified, erased, or simply covered over by the new identifier for the OEM. That is why it is important that the investigator obtain all the information about any identifying marks from all who have had a hand in the development/manufacturing process.

Figure 6-1 shows a chip mounted on a printed circuit board. As one can quickly see this chip is a permanent part of this board, and can only be

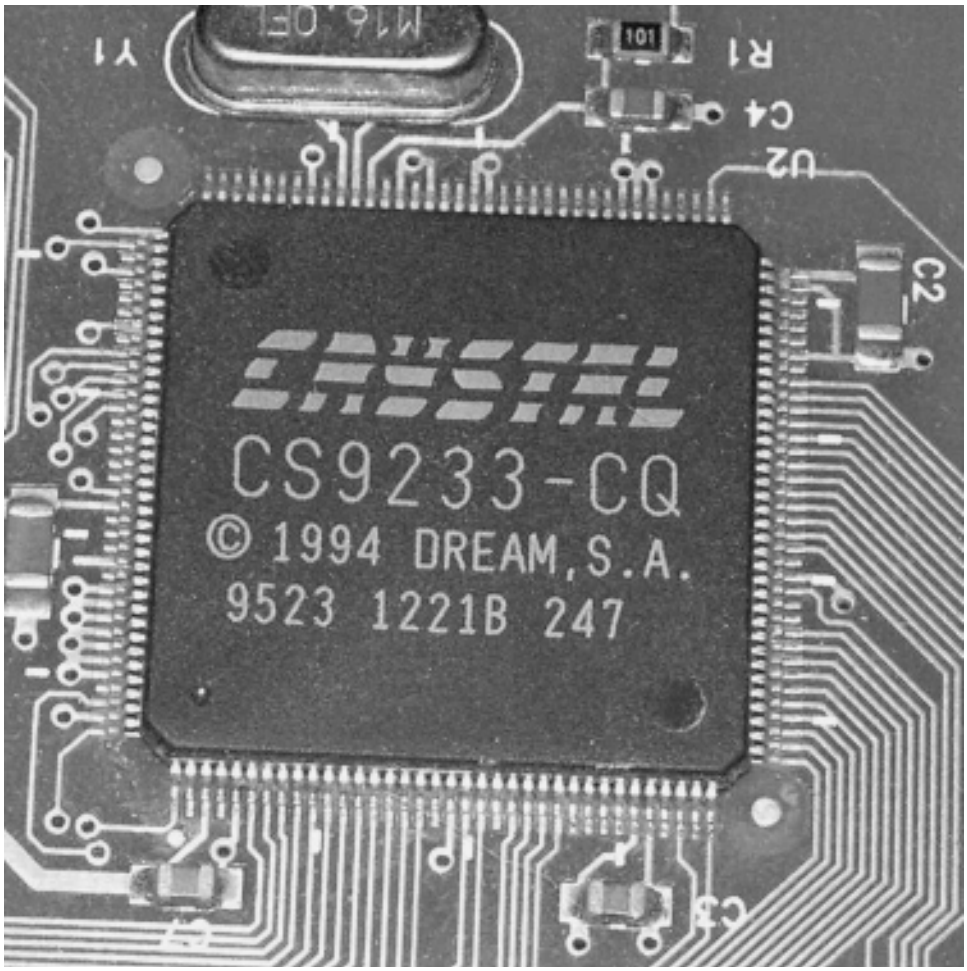


Figure 6-1. Integrated chip.

removed by snipping the connecting wires seen around the edges or by removing the solder that holds the wires in place. For the investigator this may be very important in helping to determine which chips were mounted by the OEM and which by the suspect.

This figure is also a good example of the identifying marks that might be seen on an individual chip placed on a motherboard. Here the copyright date is clearly identified (next to the (c) symbol) as well as the manufacturers identifying numbers. Investigators may be able to use the identifiers from this chip along with those from other chips mounted on the same board. In some instances the motherboard, or other printed circuit board, may also bear some markings, and this increases the opportunity for identification.

In the Figure 6-2 we see several components on a *daughtercard*. The card is a sound card from an older PC and is used to show the type of configuration normal for such pieces. The photograph depicts the main integrated chip with its clear marking. In this example not only can the identifying numbers of the chip be seen but the various identifying numbers of the circuit board as well. Investigators can use the numbers on this chip, along with information from the board, to help identify the chip, board, manufacturers, and even distributors.

After locating the chip identified above, one should also be able to quickly identify other chips or components with markings. Each of these contains important information which an investigator can use to help track possible

Figure 6-2. Linksys Ethernet card.

stolen goods. In short, an investigator need not identify each IC or other components so much for what it is as for what information it might tell us. In other words, an investigator who is not sure whether the wafer-like chip he has identified is a memory chip or CPU must at least be able to identify identifying marks to help make later identification.

When it comes to tracking computer components the combination of various chips, cards, and other components can help investigators determine the validity of a given system. For instance, most manufacturers track their products even when used as part of a larger item. This is especially true when dealing with computers. Thus, stolen Network Interface Cards (NIC) may turn up in otherwise legitimate computers. The investigator must identify not only the computer case, which may have it's own series of identifying numbers, but also those components inside the computer case which may be easily traceable as well. With that in mind we can now turn to the process of identifying larger components inside a computer system.

b. Computer Motherboards and Add-On Cards

As mentioned in the material above, many of the components and parts found inside a computer carry identifying marks or numbers. The same is true for the larger components such as motherboards. Like many of the items we have discussed to this point, the motherboard will vary greatly according to the manufacturer, type, and ultimately consumer need. What this means is that while many motherboards share similar characteristics, especially in matters such as size and access points, the actual marking or identification of motherboards will vary greatly from one manufacturer to the next.

There are three basic points of identification that can be used to help investigators identify a motherboard. These are: the size of the board, the general layout, and the placement of markings. Beginning with size it is important to recognize that the size of a motherboard is controlled by the manufacturer as well as the layout of the case it is to be fitted within. A manufacturer obviously needs enough room to efficiently install all of the components that are necessary on a board, and this fact affects the size the most. Similarly, the size of the computer case will affect not only the layout of the motherboard but also the size.

Figure 6-3 depicts a standard "mid-tower" type case with the motherboard mounted in the proper position. On the left side, connected to the "front wall" of the case, can be seen the speaker and below that the cage for disk drives. On the lower left one can see the power supply with a tangle of wires running toward the front. These wires carry the power to the various components of the system, including the motherboard. Investigators should be especially careful when handling these wires.

Many computer manufacturers use stickers when marking products. The sticker typically includes the routing numbers which identify the manufacturer as well as the board type. The reason a stick-on identifier is used has more to do with OEM convenience than with later identification of possibly stolen parts. The OEM typically purchases the motherboard from a Pacific Rim manufacturing plant, removes the sticker in question, and can easily mark the motherboard with the manufacturer's own label. Of course this makes later identification and prosecution harder, but it does help the OEM keep costs down which in turn helps make consumers happier.

This brings us to an interesting issue when it comes to identification; when is a number an identifying number and when is it for another purpose? Because there is no clear standard for all computer components this question is almost impossible to answer. Without knowledge of each manufacturers marking methods, codes, and those of all other providers in the industry it would be impossible to say which are valid and which are not. For our purposes, though, we can be sure that certain marking standards are followed, and it is these that we must concentrate on as effective investigators. Go back to the earlier chapters in this text to again view the various components and

Figure 6-3. Mid-tower case with power supply and motherboard.

parts we have discussed. Take a few moments to determine which parts have identifying numbers and which do not.

One should also take some time to examine parts firsthand. If you do not have a computer that is already taken apart it is fairly simple to open the case on the daily used computer at home. Make sure the computer is unplugged and that there is plenty of room to work in. Once the case is removed be careful not to unplug any of the connectors inside or jostle the individual parts. Simply use a small flashlight, if necessary, to see all the numbers or other identifying marks inside the computer system.

c. Cases and Peripherals

Markings on the case, just like markings on all other electronic parts, vary greatly from manufacturer to manufacturer. One reason for this is the nature of the computer marketplace. The computer industry, much like many other industries around the world, does not rely on localized manufacturing or distribution. A computer manufacturer today is more likely to buy individual parts from around the world than have them all made locally. What this

Figure 6-4. Mid-tower case with identification label.

means is that the case may have been made in China, the motherboard in India, and the processors in the United States. All of these parts are then brought together in Canada where they are combined to make a single computer unit. This unit is then sold in various countries, sometimes with only minor changes between the various models. Of course, this process will vary from one manufacturer, wholesaler, or even retailer to another.

Another fact that often affects identification of computer components is the trend of consumers to build their own systems. Today's PC has been refined to a point that the average hobbyist can easily build a powerful computer system at home by simply buying the parts online. Not only do major resellers enjoy the ability to buy directly from the manufacturers but the hobby-consumer in electronics has benefited from this practice for decades.

When it comes to cases and peripherals the chances that a consumer or reseller will alter the original manufacturer's identifier is high. Today a hobby-consumer can easily buy new "metalicized" stickers which mimic those used by major manufacturers. For instance, the "Intel Inside" sticker used on many computer cases to advertise the use of the Intel processor is now readily available to consumers. Likewise, ready made stickers or those made on the consumer's own printer allow hobbyist to create computer systems which are very personalized. This may greatly affect the investigation and cause some confusion among those investigators not fully prepared for such conduct.

Other identification can be found on the case. Unfortunately, it is common for various stickers, including those used for quality assurance, to be added to the back of cases and this may make later identification much harder.

2. Tracing Stolen Software

The illegal copying of software is a crime. It is a form of electronic piracy that has impacted the software industry at all levels. The theft of software can occur through the taking of core computer code, often done at the programming level, or by the widespread delivery of illegal copies of commercially available software. The theft of software is such big business today that even traditional organized crime has found a way to become involved.

Tracing stolen software is as simple as verifying the purchase or license to an individual user. All commercially available software is packaged with a license agreement, and possession of the legitimate license typically proves right of ownership. Tracing can also be as complicated as tracking delivery methods over the internet or through any of the peer-to-peer systems that allow quick exchange of electronic materials. In many instances the software license is also transferred, when available electronically, as well as encryption or software "key" systems.

According to the Business Software Alliance, a non-profit organization devoted to combating software piracy, the losses for computer software theft exceed $13 billion in lost revenue annually. That also means there is an estimated loss of more than $5.3 billion in lost wages and another $2 billion in lost tax revenue.

For the computer crime investigator the theft of software is often considered a non-issue since most theft occurs at the corporate level. Municipal police agencies will simply not be involved in the widespread investigation of software at this level because there is rarely a report to them. Software taken by a company, usually through the illegal sharing of otherwise legally obtained software, is not easily identified nor traced. This has begun to change, though, as more software manufacturers turn to higher levels of protection for their software.

If called upon to investigate potential software theft the investigator will likely begin with the most basic tasks of identifying the software itself. All software manufactured commercially today uses a system of identification, and for the Windows user this is normally found by accessing the information under the "Help" menu.

Located along the top toolbar on most Windows software the "Help" menu typically includes a section known as "About." As an example, if one is using the popular Microsoft Word application software for word processing then the "About" section is located under "Help" and is labeled, "About Microsoft Word." By clicking on this item a new window will open where the investigator can find two very important pieces of information.

The piece of information is the "licensed to" entry, which will generally have the name of the person who has registered the software. Many software manufacturers allow users to register the software, and upon registration the manufacturer will now have record of the properly licensed person or company. If the investigator finds that the licensed to section does not match the actual user or owner then a red flag should go up in the investigation.

The second piece of information is the product identification number. Most software today now has a product identification number associated with it. This number may be a unique identifier for that particular version or software item. In some instances the identifier is given when the software is loaded from the CD or other location. It may also be issued by the manufacturer when the software is registered. In the latter instance the registration can take place online (and the registration ID passed through that connection) or by other means such as telephone or even traditional mail.

Software manufacturers have also begun using other forms of verification or authenticity. One such practice is the Certificate of Authenticity, which is very popular with Microsoft and Windows based products. A "Certificate of Authority" (COA) is a label to help identify genuine Microsoft software. It

includes advanced anticounterfeiting features to help verify the authenticity of the software acquired. The COA is often provided on a separate form of documentation within the software package. The most common form is the COA card, which contains a description of the product along with a unique identifying number.

For products that come preloaded on the computer system, especially products such as the operating system, the COA label is typically affixed to the PC chassis or case. It is important that the COA not be removed since this is used to identify the software with that particular machine. In most instances the COA will also include the Product Key needed in the event the operating system needs to be reinstalled.

Another identifier that has become popular in the last few years is the holographic image that is affixed to either the CD or other material included with legitimate software. Because holographs are difficult to make without the proper machinery the missing holographic image on a copied CD is a sure sign of potential software piracy.

ENDNOTES

1. *Kane v. McDaniel,* 407 F.Supp. 1239, 1242 (D.C.Ky 1975)
2. *United States v. Real Property Located in El Dorado County,* 59 F.3d 974, 982 (CA9 1995)).
3. *Austin v. United States,* 509 U.S. 602, 628, 125 L. Ed. 2d 488, 113 S. Ct. 2801 (SCALIA, J., concurring in part and concurring in judgment).
4. Federal Rule of Criminal Procedure 41(b)(3)
5. *United States v. Boyette,* 299 F.2d 92, 98 (4th Cir.)(Sobeloff, C.J., dissenting), cert. denied, 369 U.S. 844 (1962).
6. *United States v. Viera,* 569 F. Supp. 1419, 1428 (S.D.N.Y. 1983).
7. *United States v. Markis,* 352 F.2d 860, 864-65 (2d Cir. 1965)(telephone used to take bets by operators of illegal wagering business was an instrumentality because it was integral to the criminal enterprise), vacated without opinion, 387 U.S. 425 (1967), with United States v. Stern, 225 F. Supp. 187, 192 (S.D.N.Y. 1964)(Rolodex file was not instrumentality where it contained names of individuals involved in tax fraud scheme).
8. For an excellent discussion of this topic see 3 Wright & Miller, Federal Practice and Procedure: Criminal 2d § 664 (1982).
9. See, *United States v. Robinson,* 287 F. Supp. 245 (N.D. Ind. 1968)(upholding the seizure of several items, all of which connected the defendant to the murder of a federal narcotics agent, as "instrumentalities" of the crime and not "mere evidence." Items included a pair of shoes, a shirt, a jacket, handkerchiefs, spent shell casings, and wet washcloths).
10. *Warden v. Hayden,* 387 U.S. at 306, 307.
11. Federal Rules of Criminal Procedure 41(b).

12. Id.
13. *See Andresen v. Maryland,* 427 U.S. 463, 483 (1976)(holding that the "trained special investigator reasonably could have believed" the seized evidence could be used to show criminal intent); *United States v. Truitt,* 521 F.2d 1174, 1176-78 (6th Cir. 1975)(holding that a reasonably cautious police officer could have believed under the circumstances that a sawed-off shotgun, although legal if registered, was incriminating evidence).

Chapter 7

THEFT OF INFORMATION

A. INTRODUCTION

In today's modern society information has become almost as valuable as gold. Some of the most important information is that available on the Internet or the thousands of computer systems around the world. One can easily imagine the monetary loss that would be suffered by corporations, government, finance, and other entities if the law did not protect information.

For the information thief the amount of material available in today's society is almost too much to pass up. In the last two decades we have seen a tremendous increase in information theft not only in the U.S. but also around the world. Trade secrets, financial information, and customer data are the most common pieces of information to be stolen. Among these, materials from scientific and technological inventories tend to be the leading targets.

At one time information theft from corporations was the domain of private investigative services. Few corporations, both large and small, were interested in making their loss known publicly, and in many instances the theft was investigated and prosecuted privately. That attitude has changed in the last

decade, though, as the magnitude of the problem has grown. Where it was once thought that a civil suit against the perpetrator was enough to offset any loss there is clear incentive now to include criminal sanctions as well.

One reason for this change has been society's overall change in the way we view corporations. Less than fifty years ago a company fought hard to protect its image, and allegations of theft or misappropriation of trade secret were enough to cause severe penalty to many corporations. Things have changed over the years, and in today's market the mere allegation of a wrongdoing, even if it is criminal, is not enough to tarnish the already smudged reputation of many of our largest corporations. Theft of trade secret or customer lists is nothing new anymore. In the "dog eat dog" world of today's business a mere allegation is often seen as just so much free advertising.

Lois Mock and Dennis Rosenblum evidence the increase in corporate theft in the 1988 study prepared for the National Institute of Justice and titled, *A Study of Trade Secret Theft in High Technology Industries.* In the study the authors point out that at least thirty-eight (38%) percent of companies now report that they have been victims of information theft. Some estimates now place that figure at closer to sixty (60%) percent.

In a similar report, completed in 1998, researchers found that a significant number of companies, forty-three (43%) percent, consider information theft to be an "ongoing part" of their business or trade. In other words, these businessmen and women believe that information theft is just another part of the business itself. The use of "corporate spies" to obtain information is now a part of everyday business in some industries. In 2001 a survey of graduate business students revealed that a whopping seventy-four percent (74%) expect to see corporate spying in the largest industries.[1]

One should also remember that the attitude toward information theft is not restricted to corporate boardrooms. Today's consumers also believe that information theft is a natural part of a competitive market. For instance, one surveyed consumer suggested that in a competitive market it is natural for the competition to look for "any means necessary" to beat their rivals. This may even include the theft of secret ingredients to a famous cookie or the pilfering of a potent customer database.

While there appears to be a cogent change in attitude at the corporate and private level there has been an equal change in attitude in the way our government views information theft. Many state legislative bodies have now taken significant steps in protecting information. Where information theft was once considered a minor problem, today's legislatures now recognize the impact such theft has on our society–not to mention our economy–and they have created new and unique ways to deal with the problem. In the past ten years almost every state legislature has addressed the issue of information

theft in some form or other.

The Congress of the United States has not been slow to react either. At least seven significant bills have come before Congress in just the last decade. Each of these bills, many of which have passed to become law, address specific issues and provide explicit penalties for violation of the acts.

Sadly, while the priority for investigation and prosecution of information theft has risen among legislative bodies the financial support needed to carry out such tasks seems to have lagged behind. Many legislative bodies have created impressive criminal sanctions for information-related crimes, but they seem to have ignored the need to appropriate funds to pursue such investigations. From a law enforcement standpoint this is much like the local municipal council creating a law against speeding but then forgetting to give police a vehicle to chase speeders when they break the new law.

Until legislative bodies provide the manpower and financial support necessary to address the problems addressed in this chapter it will be up to law enforcement to determine the priority which they will give to information theft. With that in mind we will begin this chapter with a brief look at the issues of information theft and the needs for conducting a successful investigation.

B. PRIORITIZING THE INVESTIGATION

At the outset it is important to note that information theft cases can consume great deals of investigative time and money. In many instances the theft itself may be of intangible material such as a database file or financial figures. The lucky investigator will find a clearly marked notebook with the information inside, but this is the exception and not the rule. In most cases the investigator is not searching for the tangible but is instead hunting for something that exists only when a stream of electrons pass through a silicon chip.

For the typical criminal investigator each day is filled with decisions on which case to focus on and which to leave alone. In most police agencies time, money, and manpower simply do not allow for extensive investigations into every crime that is reported. With information theft the problem is the same, and as with other crimes the investigator quickly develops a system for prioritizing the cases he or she will work on that day.

At the top of the list for determining the priority of a case is the overall impact the case may have on the victim or society. Obviously crimes with a significant monetary loss will get higher priority than crimes with smaller money value. The big issue, though, is how do you determine the monetary value of information?

Unlike the theft of tangible goods, information theft can literally threaten a company's overall ability to make a profit or survive in a competitive market. Imagine for a moment the impact the theft of Coca-Cola's® secret formula might have on the company if the recipe were revealed on the Internet. The company would begin losing money almost immediately and would continue to lose money until its untimely closure due to lack of profits. After all, who would pay for a bottle of Coke when one could easily mix the same thing at home?

While the above example may seem extreme on the surface the reality is that information can be very valuable even when it does not have an outward appearance of such. The theft of a competitor's customer database is another example of an information crime that may seem trivial at first glance. Consider, though, how much financial loss might occur if a competitor knew the buying habits of the company's customers? If armed with the right information, a competitor could easily market his or her own products to the exclusion of the victim's business.

As an investigator the first duty in prioritizing the case is to determine the true value of the information. This is best done by looking not at the information but instead at the potential impact the loss of information might have on the victim. In making this determination it is helpful for the investigator to understand how information might be regarded and protected. To help us in understanding this we will focus on the three most common levels of protected information: Trade Secret, Proprietary, and Confidential information.

1. Trade Secret

In many states the term "trade secret" is defined by statutory provision; thus, the definition may vary from state to state. There are, however, a few simple elements that all trade secret definitions seem to have, and those are the elements we shall use to define the term.

One of the best definitions of trade secret comes from the courts. In a Washington case the court defined trade secret as, "[a]ny formula, pattern, machine or process of manufacturing used in one's business which may give the user an opportunity to obtain an advantage over its competitors."[2]

In this sense we can see that the formula for Coca-Cola is certainly a trade secret. It clearly gives the company an advantage over its competitors. If the competitor knew the exact formula then they may simply make their own version of the cola and deprive Coca-Cola of its profits. While many cola companies have tried to duplicate the formula–and some have come close enough to build a significant market of their own–the fact remains that without the true formula there is only one Coke.

Immediately one may be asking what is the difference between a trade

secret and a patent. The answer is not altogether complicated, although it is complicated in its application, and comes down simply to the question of prior disclosure. To receive protection under the patent laws the inventor (or other owner of the process, formula, etc.) must fully disclose the product's design, formula, or other details. In other words, Coca-Cola would have to voluntarily disclose the formula for Coke in order to receive protection under patent law. Obviously the downside to this protection scheme is the need to disclose the formula.

There is another negative side effect to patent. As a general rule the patent is enforceable for a set period of time, and once that time period has elapsed there is no protection. This means the owner of the process has protection from infringement for only as long as the law allows. Once this time period has run then the process, formula, etc., is open to immediate copy. What this means is that for companies like Coca-Cola the secret formula is protected for a limited time, and once that time has elapsed then others may be free to copy or recreate the formula at will. Obviously, for a company like Coca-Cola the secret to longevity lies not in patent but in trade secret.

With trade secret the owner of the secret can maintain legal protection so long as the secret is maintained. There is no time limit on the protection. This means that the owner must hold the "plan or process, tool, mechanism or compound" as a secret in order to maintain legal rights. A general disclosure will void the trade secret protection. The owner can disclose only to those employees who must know in order to perform their duties, and in many instances the employees may know only a portion of the overall recipe, formula, or process.

Where all or part of the trade secret is revealed, through any fashion, the owner carries a burden of proving that that the disclosure was not intentional. If the disclosure were intentional then the trade secret may be lost. If unintentional, and especially if the trade secret is obtained through deceit, fraud, or outright theft, then the owner has certain rights of protection.

The first step in obtaining this protection is to seek an injunction against the offender and those to whom the offender has disclosed the information. For instance, if John, an employee of Coca-Cola, were to obtain the entire recipe for the product he might be able to disclose such to Pepsi. Coca-Cola would then seek an injunction against John, to preclude him from further disclosing the recipe, as well as Pepsi®. If Coca-Cola is quick enough with their legal action, and assuming the court grants the injunction in time, then there may be no or only minor damage from the disclosure.

In instances where the secret revealed causes injury the victim may seek damages in court. To recover, the owner must prove that the idea or information was held in strict secrecy and that others obtained it through fraud, deceit or by other unfair means. This is often where the investigator comes

into the picture. It will be the investigator who provides proof of such misdeed.

2. Proprietary Information

Proprietary information is very similar to trade secret. In fact, the two are often used together to explain the relationship between the owner and the information maintained in the secret. As a general rule, proprietary refers to the ownership of knowledge or information by a particular person. That *person* may be a flesh and blood type or a legal entity such as a corporation. Thus, the trade secret–the recipe itself–is proprietary property in the sense that Coca-Cola owns it.

Protection of proprietary information is often an extension of contract law rather than trade secret or patent law. Staying for a moment with our example of the Coca-Cola formula we can see that incoming chemists or other employees who might be exposed to the secret will be bound to the secret through a contract calling for the recognition of proprietary information. These clauses, often called simply "non-disclosure clauses," create a legally enforceable agreement between the owner of the secret and the person to whom it is disclosed.

Proprietary information is a common part of the computer industry. For instance, the foundation code for a particular operating system may be held both in trade secret and as proprietary information. Often called the "Keystone Code" this material is protected by both types of legal stratagem.

In applying this material it is important to remember that the computer software industry is a relatively small and close-knit group. In the earliest days of the personal computer many of the pioneers in the industry worked with each other at one point or another. It is clear that two of the major players in the personal computer industry, Apple® and Microsoft®, once had a close relationship. While the two companies were competitors on one aspect of the market they were also partners in other areas.

In the eighties the two companies worked closely on several projects that later caused a severe split between the businesses. The Xerox® Corporation had developed an interface system for their office copiers that used a graphical environment for user interface. Dubbed the *Graphical User Interface* the system allowed non-experienced workers to use the copier with little or no training. A user simply pointed to icons on the copier's LCD (Liquid Crystal Display) screen in order to enter instructions for the copier.

Apple first obtained portions of this interface and introduced it in their Lisa line of computers. Aimed at the small to mid-size business market the Lisa relied on a Graphical User Interface (GUI) to make many routine computer operations easier for users. Instead of typing in a command from the

keyboard the user used a peripheral–later dubbed the mouse–to guide a small arrow over the screen and point at an icon representing the task desired.

Though the Lisa never won much of the overall market it was successful in the sense that it revealed a market for GUI-based computers. Apple followed the Lisa with the Macintosh computer. By late 1984 the "Mac" was gaining popularity with its GUI-based operating system. The Mac was marketed to users who wanted an easier method for operating their computers. Instead of typing in textual commands the GUI interface allowed the user to simply point and click their way through work. It was a successful campaign; so much so that the founder of Microsoft seized upon the popularity to create his own version of the GUI-based operating system.

Bill Gates quickly formed an alliance with a major Japanese electronics manufacturer to put his new *Windows* operating system on their machines. The Windows OS also used a GUI interface not wholly unlike that found on the Apple Mac and Lisa. The computers were already less expensive than the computer being sold by IBM and the other major PC manufacturers. This created an instant market for Windows; a market that allowed Microsoft to establish very quickly a broad user base from which they could merchandize their companion application software packages.

Apple, who had earlier entered a contract with Microsoft for the development of software for the Mac, soon filed suit alleging that Microsoft, among other things, appropriated GUI technology while under contract with Apple. Apple claimed ownership rights to the GUI system and claimed it was proprietary property. Microsoft countered by claiming, both in and out of court, that Xerox had actually given the technology to both Apple and Microsoft as part of other deals. As such, Apple had no proprietary interest.

Both Apple and Microsoft received, at least in part, their GUI systems from Xerox. Xerox, either from a lack of interest or simply as part of a charitable relationship, "gave" the algorithm to both companies, and neither Apple nor Microsoft had a superior right in claiming ownership of that original technology. In order to gain such protection the companies would have to show either original ownership or at least a grant of ownership/rights through contract. Neither did, nor could, and as such had only limited ability to protect their product.

On the other hand, changes that each made to the original computer code, changes that would arguably be "new code," may have been protected, but that was reserved for another lawsuit and another court. In a surprising turn to this saga Microsoft actually bought stock in Apple and the two companies eventually entered into other partnership agreements during the decade of the nineties.

3. Confidential Information

If we were to establish a hierarchy of protection then we would place trade secret and proprietary information at the top of the list. Below both of these, and some distance behind at that, would be confidential information. In its simplest definition confidential information merits only a portion of the protections that either trade secret or proprietary information share.

Confidential information is that information that is crucial to business practice but is not so invaluable that the organization could not run without it. In some instances we might say that confidential information is similar to the veiled information we encounter with trade secret, but not as powerful in its protection as that found with proprietary information. For instance, the information on employee salaries is often considered confidential information. The information is certainly important to a company but is not so important that if it were leaked it would cause significant injury.

In many respects the law does not protect confidential information but instead provides protection of the information through other means such as contract or other binding relationship. One example of this method is the "non-disclosure" clause found in many of today's top executive contracts. The marketing, supply, manufacturing or any other information obtained by that person while in the employ of the company is protected by the contractual language. The contract specifically prevents the person from disclosing the information, and if such disclosure is undertaken then the company would have specific legal rights available.

Confidential information might also be protected by ethical standard within a given industry. For instance, an attorney working for one law firm may switch to a different firm but may not disclose certain information obtained while in the employee of the first firm. The information the employee has about the first firm may well be confidential and is subject to certain ethical restrictions. As a general rule, though, the disclosure of such information is not criminal nor is it punishable by criminal sanction.

From a practical standpoint the issue of confidential information arises under a criminal investigation as part of a larger electronic trespass case. In many instances the intrusion into the computer system is the crime and the information obtained by that intrusion is minimally related only as necessary to show the attack itself. For the criminal investigator this is a significant difference since the higher level protections may have some other sanction attached to them not normally found with confidential information.

All in all the prioritizing of the information theft case will depend, to a large extent, on the type of information that was taken. For that reason it is important that the investigator understand not only the legal differences between these information types but also the pragmatic differences.

C. THE VALUE OF INFORMATION

One of the more interesting aspects of information theft is the vague value we often place on information. After all, information that has no value can hardly be worth the effort of conducting an investigation. Simply stated, if there is no relevant statute covering computer intrusion or trespass then there may be little to investigate when the information has no value. What we may have instead is nothing more than an electronic nuisance rather than a crime. To better understand this concept let us look at a few examples of information that may have no intrinsic value.

Baseball fans often collect statistics on their favorite players or team. That information is certainly interesting to the fan, but has little value outside of the world of baseball. For instance, George Herman Ruth, better known as "The Babe" or "The Sultan of Swat," stood six feet and two inches tall. While most fans know him as a hitter the reality is that Babe Ruth also pitched early in his career. In fact, he pitched a total of one thousand two hundred and twenty-one (1221) innings between 1914 and 1933.

Of course, to the fan of baseball those facts are interesting and have some value (especially if you are involved in a game of baseball trivia). To the rest of the world, though, the information on Babe Ruth is of little value. The interesting thing about such information, though, is that it is exactly the type that might be kept on a computer system. It is conceivable that a "hacker" might access those same files by way of an external connection and there by "steal" the information. The question then is whether there is some value to the information or do we simply have a computer trespass case?

Chances are that no one will bother with an investigation into such a theft. Why? Because the information is readily available in many other sources and is not worthy of such high level protection. In fact, I obtained the information easily enough in my copy of *Total Baseball: The Official Encyclopedia of Major League Baseball,* 5th edition. Dozens (if not hundreds) of similar books are available. Likewise, I can replace the information with a few keystrokes and a trip to some of my favorite baseball trivia sites on the Internet. Simply stated, the information is readily available and easily obtained through many means short of criminal action.

This brings us to the question of what level of emphasis should the police put on this "theft?" Clearly there was an intrusion of the computer system. The information was also taken. This is the typical information theft case, and therein lies the big issue. How much time, effort, and investigative prowess should be expended on a case of this type?

In answering this question it is important to recognize that the value of information comes from the manner in which the information is kept and the degree to which it is available from other sources. The first issue for us to

understand here is that the information must have some intrinsic value. Intrinsic value is that natural or peculiar value that the information has itself. One should quickly recognize that the number of innings that Babe Ruth pitched has a very minimal intrinsic value. On the other hand, the formula for unlocking the genetic combination for male pattern baldness would have a much higher value.

In measuring the intrinsic value one must first look at the value the information has to the owner of the information. Again, using the Babe Ruth analogy we see that the knowledge of baseball can be very valuable to someone who is engaged in a trivia contest. On the other hand, the number of innings pitched has little value to most people even if they were to know the information. Thus, having the information and having valuable information are two very different things.

We can also measure intrinsic value by looking at the issue as it relates to other people. The scorekeeper with the Boston baseball club, where Ruth played his early years, probably saw little value in keeping track of Babe's innings pitched. While Babe Ruth was certainly a good pitcher it was not his pitching that made him famous. It was his ability to hit the baseball that earned him his real fame, and even that was more closely associated with his time spent in New York than in Boston. Yet, the information has some intrinsic value even it didn't mean much to the scorekeeper at the time.

As information is accumulated it may gather value as society uses it. In this case the value of the statistic on Ruth's pitching is more a curiosity than a real accomplishment. Yet, it gives us a picture of the whole player, not just the hitter. It also has value when it is put in perspective with other pieces of information, and as society views that information it may deem the value appropriate even when no real intrinsic value seems clear. Thus, such information is always included in any treatise on the history of baseball or on the Babe himself. In this sense we might easily argue that the information has intrinsic value, but the actual monetary value is the difficult issue.

Getting back to our issues of information theft we must now focus on the issue of disclosure in determining value to information. Clearly, information that is highly secretive will have a higher value while still a secret than if it would once disclosed. If, for instance, a scientist were to discover the proper genetic combination for stopping male pattern baldness then we could say this information has very high value. Whether the information need be patented or protected through other means is immaterial at this point since it is still relatively fresh as a discovery and still nothing more than a secret. The disclosure of such information, especially if it occurs prior to any implementation of other protections such as patent, would certainly affect the value of the information.

Another factor that may substantially affect the value of information is

time. The passage of time between theft and disclosure may affect the value in many different ways. Staying with the male pattern baldness analogy we can see that the theft of the information has little impact if the scientist is able to obtain a patent before the information is released. Thus, the theft would be valid but the overall value of the information taken is lessened by the new protections offered under the patent laws. In other words, the information is now disclosed as part of the patent application itself but then is protected from use by others simply by nature of the patent law.

Likewise, certain time-sensitive information may have value only for a set time. In such a case the rightful owner may intend to disclose the information but wishes to conceal it for a short period of time for financial gain or other reasons. The theft of that information might carry some reward all its own, but such reward would be lost if the information becomes stale or is in some other way tainted by time.

Another issue that is often overlooked when determining value is the development costs of the information. This is much easier to determine with some items than with others. As an example, if a scientist has worked for three months on a particular formula to make more bubbles in shampoo then the value of the information can be increased by the costs of the scientist's salary and related expenses.

On the other hand, some information may be of relatively low value even though someone has worked on it for an extended period of time. Development costs must be considered in relation to other value issues. Likewise, the value placed on a project in development may vary greatly depending on who has worked on it. Clearly, the value inherent with a project created by a high-priced consulting firm is much higher than the value of an item created by a hobbyist working in his spare time.

When considering value the investigator must also consider the whole rather than the individual parts of the item(s) taken. This is especially important where no state law exists to punish the theft of information but law does exist to punish the taking of a tangible thing. If the thief has taken the container of the information, such as a hard or floppy disk drive, then he/she may be punished for that theft. The theft of a floppy disk, however, would be a misdemeanor in most states since the actual disk has a minimal value (under $1, usually). The value of the information on that property may have a much higher value, and in such a case investigators may need to consider this intangible value along with that of the disk.

Finally, the easiest way to establish a value on information is through a "market value" analysis. What would the information bring on the open market? When dealing with theft of information there is traditionally a three-tiered test for making such a determination:

1. What value would a competitor place on the information?
2. What revenue or other loss has the victim suffered?
3. What value did the thief place on the information?

In the first tier the investigator looks simply at what would the open market pay for such information. In some instances this will be easy to identify because the information has a ready market with willing buyers. Other instances may be more difficult because the information is unique or simply has a narrow market. Of course one of the easiest ways to assess this value is simply to find out what a worthy buyer would pay for the information in question. If this is readily available then the value is easily established, but in some instances the value is not so easy to find.

From a practical and legal standpoint it is a good idea to use someone from the field in question to make the appraisal. In some instances there are professional appraisers who can readily set a value on any item in question, but in other instances the investigator may need to use someone who is not normally used as an appraiser. When this is the case the investigator should educate himself on the field in question and on the persons who might be called upon to make such an appraisal.

Sometimes the first tier is the only level to which an investigator must look to determine a value. In other instances the ready market value is not immediately available or cannot be easily determined. In these instances the investigator may use the second tier of the test to help make an estimate of market value.

In considering this tier we must evaluate the total impact the loss might have on the victim. For instance, many companies go to great lengths to gather information on consumers in their area. A competitor can save a great deal of time and gain some unfair advantage if he were able to steal that data. The loss to the victim is twofold: (1) the loss of information that took effort, time, and probably money to accumulate; and (2) the loss of potential customer revenue. In this sense the loss to the victim can be calculated using both areas.

As with our first tier, it may be necessary to involve someone from the field in question when making a market loss determination. While criminal investigators are expected to know a lot about many different areas it would simply be unreasonable to expect them to know everything about every field of endeavor known to man. Information can be very valuable to one person or one group but not to others. Thus, it is important to use someone knowledgeable in that particular field in order to insure the best estimate of loss.

Of course, one must not overlook the value that a thief may place on a particular item himself. That value may be much different from the value the victim or even a worthy buyer may place on the item. For instance, the loss

of certain data may be more important than the actual distribution of that same data. Imagine how important the loss of the Coca-Cola formula might be to one of Coke's competitors who already have a strong following. Coke drinkers who found themselves without their favorite beverage might easily switch to Pepsi simply because Coke can no longer make its magical elixir. Certainly to Coke the value of the lost formula is high, but to Pepsi it might be even higher.

D. IDENTIFYING THE STOLEN INFORMATION

One of the earliest problems an investigator will have with an information theft case is the need to identify the exact information stolen. It is not enough to simply show that an intrusion into the computer system has occurred. The investigator must show that the intrusion lead to some form of taking or there can be no theft charge.

In understanding this it is important to first remember that all criminal acts contain elements which must be met. For theft the general elements are the (1) taking of property, (2) asportation or carrying away, and (3) intent to deprive the owner. In states where information theft is a separate crime from other forms of theft these elements may be expanded or altered. For our purposes, though, we will stick with these basic elements as we discuss the theft aspect of computer crime.

The first step in determining what was taken is to determine the means of access. To this end the investigator must have a working knowledge of computer systems and the methods in which they are used. By understanding the way in which information is accessed in a computer system the investigator will have a better chance of determining what was intruded upon and what was likely taken from that area.

The question of access is no different for the computer crime investigator than it would be for a burglary detective. The means of access is important for two reasons. First, it helps us establish a pattern or modus operandi. Second, it helps us narrow potential suspects by recognizing abilities or shortcomings of each suspect. Just as physical limitations of a suspect might help narrow the field in a burglary case so too can technology limitations help limit selection of computer crime suspect.

One should not assume that a limitation on access completely absolves a suspect from involvement with the crime. In the more profitable information theft cases there is a great likelihood that multiple parties worked together to accomplish the unlawful goal. It can certainly help, but limitations on the means of access should not be used as the sole criteria for inclusion or exclusion of any suspect.

As pointed out in our earlier sections the theft of information often deals with the intangible side of computers and technology. The theft of a floppy disk, or other piece of hardware, which contains the information is the easiest for us to understand. It is in fact the same as the theft of any other piece of tangible property. The big difference may come in the value placed on that item. Is this a theft of the tangible container or a theft of the information it holds?

In cases where a tangible object is taken along with the information the investigator should be careful not to separate the two too quickly. As mentioned above, the value of a floppy disk may mean the theft is a misdemeanor where the theft of information may have much more value. For that reason, the investigator should consider both items together and until forced by a court to do otherwise should treat the theft as a single event.

The value of the container, the prosecutor must argue, is enhanced by the contents. Thus, the value of the "property" taken is in direct proportion to the value of the tangible container as well as the contents of that container. Even if the contents are nothing more than zeros and ones there is still a value which can be placed on the container and the contents of the container. The federal system, as well as various state courts, has adopted this concept as early as 1966. The courts have quickly recognized the value of information and allowed investigators–as well as prosecutors–the latitude to seek a remedy in accordance with that value. The key is to establish the value in a clear and convincing manner.

ENDNOTES

1. Franklin, D.K., "Business Ethics in the New Millennium: Something to Talk About Around the Watercooler," Kansas Wesleyan University, October 2001.
2. 278 N.W.2d 81, 89–90.
3. See *United States v. Battone,* 365 F.2d 389 (2d Cir. 1966) and *United States v. Greenwald,* 479 F.2d 320 (6th Cir. 1973).

Chapter 8

CYBERSTALKING

A. What is Cyberstalking?
B. Nature and Extent of Cyberstalking
C. Offline vs. Online Stalking–A Comparison
D. Evidence that Cyberstalking is a Growing Problem
E. Current Efforts to Address Cyberstalking
F. Jurisdictional and Statutory Limitations
G. Anonymity on the Internet
H. Law Enforcement Response
I. Industry Efforts
J. Victims and support organizations
K. Cyberstalking Laws

There is little debate that both computers and the Internet have brought about tremendous changes in our society. More and more users are now turning to the Internet and related electronic forums for social interaction. It is estimated that more than sixty million Americans use the Internet each day, and many of these are online for social interaction. One of the fastest growing and most popular social areas on the Internet is the chat room.

Chat rooms are very similar to public gathering places where people meet to talk. One big difference is that the chat room exists only in "cyberspace" and the people in the chat room are often hundreds or even thousands of miles apart. One would think, given the great distance of separation, that there would be some protection from potential crime. Sadly, the opposite is proving truer each day as chat room visitors are faced with new crimes found only on the electronic frontier.

A crime which is relatively new to both society in general and computer users as a whole is cyberstalking. Most investigators are now familiar with the

term stalking, and is really nothing more than a short step to identify cyberstalking as a crime. In the broadest terms, cyberstalking is the unrestricted contact, either personal or electronic, between the stalker (criminal) and the victim. A typical case involves the incessant contact with the victim by the stalker. This can be accomplished either in person, by telephone, or by other electronic means.

Less than twenty years ago the nation knew little about the criminal sanctions we now call *stalking*. In the past, if no easily identifiable threat was made then most law enforcement agencies took little or no action. A stalker was seen to have the freedom to come and go just as easily as the victim. This meant that victims were often followed and even contacted while in public areas. Stalkers also made telephone calls to the victim with little or no concern for the criminal law. Over time the problems became so pronounced that many state legislatures found it necessary to create new criminal laws which made stalking a felony.

By the mid-eighties the courts and legislative bodies began to take action against these social terrorists. New laws designed to curb stalking actions were soon created, and states like California, New York, and Florida led the way. Soon, most states had similar laws since stalking was not limited to television, movie, or other stars. Stalking was a very real problem and there were soon very real answers.

Now, in the new millennium, we find ourselves on the information superhighway with all new opportunities for stalking. Unfortunately, many of the attributes of this technology–low cost, ease of use, and anonymous nature, among others–make it an attractive medium for fraudulent scams, child sexual exploitation, and increasingly, a new concern known as "cyberstalking."

At the outset it is important to note that cyberstalking, much like it's face-to-face counterpart, has received mixed responses from law enforcement. The nature and extent of the cyberstalking problem is difficult to quantify. In addition, while some law enforcement agencies are responding aggressively, others are not fully aware of the problem and lack the expertise and resources to pursue cyberstalking cases. Similarly, while some Internet Service Providers (ISPs) have taken affirmative steps to crack down on cyberstalking, others have not. There is a great deal more that industry itself can and should do to empower individuals to protect themselves against cyberstalking, but for our purposes we will focus on the investigator's response to cyberstalking.

A. WHAT IS CYBERSTALKING?

The term cyberstalking is a creation of the last decade. It is a new phe-

nomena that has roots in more traditional forms of harassment and stalking. While there is no single definition for cyberstalking there are a few well-known elements that help us to identify it. These include the use of the Internet, e-mail, or other electronic communications devices to stalk or harass another person.

Because cyberstalking is a relatively new form of crime there has been some confusion on where it should be placed as a crime. It is not generally to be a crime of violence, though it can certainly lead to such crimes. For that reason we find that many states now place cyberstalking within the realm of traditional forms of harassment or as a whole new form of crime. In the broadest sense stalking generally involves harassing or threatening behavior that an individual engages in repeatedly. An example would be the continued following of a person and may include unwanted visits to the person's home, place of business, or known gathering places. Stalking also involves continual messages on the phone, in writing, and through other sources such as mutual friends. In extreme cases the stalker actually intrudes on the victim's private property and may even cause physical damage to the property or harm the victim.

The current array of laws in this country varies greatly as to the actual elements necessary to charge a person with stalking. In some instances the law requires that the perpetrator make a credible threat of violence against the victim. Simply being in the same location at the same time is not enough. Neither is an occasional telephone call, letter, or message. These stalking laws have similar elements to assault in that a "reasonable apprehension" must exist in order to sustain a charge.

Other laws require less of the suspect. These statutes, often called annoyance or nuisance statutes, include elements of minimal contact. Frequent appearance by a suspect at otherwise unrelated venues, such as the same movies, restaurants, etc., may be enough to sustain a claim of stalking. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking or violence and should be treated seriously.

For the investigator it is important to first note that statutes that require a "credible threat" to the victim create unique problems for prosecution. Because cyberstalking does not generally involve the initial physical stalking associated with the more traditional crime there is less likelihood that the acts will be seen a true threat. This is certainly cause for concern for the investigator simply because there is a very short leap from acts carried forth online and those carried out in person.

As most investigators know, stalkers do not commonly threaten their victims overtly or in person. The stalker may instead engage in conduct that, when taken in context, would cause a reasonable person to fear violence. In

the context of cyberstalking, a credible threat requirement would be even more problematic because the stalker, sometimes unbeknownst to the victim, may be located a great distance away and, therefore, the threat might not be considered credible.

One of the more credible stalking laws available today is found in the United States Code. Commonly known as the "federal interstate stalking statute,"[1] this statute prohibits conduct that places a person in "reasonable fear of death or bodily injury." The statute, much like many common statutes on assault, does not require an actual physical intrusion but merely an apprehension of such. The emphasis, of course, is on the "reasonable fear" element, and in this sense the measurement is of a reasonable person under the same circumstances.

B. NATURE AND EXTENT OF CYBERSTALKING

Stalkers have been around since man lived in small villages, and the nature of stalking has simply changed from the traditional physical approach to an electronic one when we talk about cyberstalking. While stalking is an existing problem the reality is that new technology makes cyberstalking something completely new and different. Although online harassment and threats can take many forms, cyberstalking shares important characteristics with off-line stalking. Many stalkers–online or off–are motivated by a desire to exert control over their victims and engage in behavior which is very similar regardless of the method used.

As with off-line stalking, the available evidence (which is largely anecdotal) suggests that the majority of cyberstalkers are men and the majority of their victims are women. There appears to be a growing trend in the other direction, though. Recent reports tend to support the proposition that cyberstalking is gaining popularity among women. One reason for this is the fact that many more women are now using the Internet and computers than before. As the number of online users increases so does the percentage of women.

A similar trend appears to be rising among homosexual men and women. Same sex cyberstalking is becoming much more prominent as the Internet offers an abundance of opportunity for sexual encounters. Leading the way in this area are homosexual chat rooms as well as other online avenues for sexual contact.

In many cases, the cyberstalker and the victim had a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship. This is similar to the off-line version in that the victim and stalker often know each other, and in some instances have in fact been very intimate

in the past.

It is noteworthy that cyberstalking does differ from off-line stalking in this one key area. While there are cases of stalking by a stranger in the off-line world there appear to be few cases of such action in the cyberworld. As a general rule there must be some connection between the cyberstalker and the victim. It is difficult for the cyberstalker to find a true "anonymous" victim in places such as chat rooms, news groups, or other areas. The reason for this is simple: the victim has made some public display of themselves in order for the stalker to find them.

What this means is that in the cyberstalker case the victim has taken the initial action of entering the chat room or other public forum. Those who enter but remain anonymous, often called "lurkers," do not become victims since the cyberstalker has little means for identifying them. It is only because the lurker reveals him or herself, and actively participates in the group, that the cyberstalker has knowledge of them at all.

For instance, in one well-known case a criminal justice professor was chosen as a victim simply because of comments he had made on an online forum. Had the professor remained anonymous then the cyberstalker would not have identified him and may not have even known the professor was in the group. When the professor commented on topics being discussed on the group the cyberstalker chose his target. Fortunately, the cyberstalker used his real name and other identifying information so that it was easy for investigators to track him down.

The choice of a victim by a stalker is often classified by the relationship between victim and stalker. In the first category we find relationships which are clear and in many instances were considered to be "close." This includes the stalking of an ex-lover, fiancé, spouse, or other person who was once close to the stalker. The stalker and victim both know each other and in many instances have had a long-term relationship.

The second category arises from perceived relationships. These are the typical "star" or "celebrity" stalking cases. In these cases the stalker believes there is, or will be, a relationship with the victim. In many instances this perceived relationship might be very dramatic and quite fanciful. The perpetrator may even go so far as to identify him or herself with the victim; i.e., claim to be a spouse, lover, or significant other.

It is important to remember that not all perceived relationships fit a specific pattern. The perceived relationship might arise from an actual encounter or past relationship. One example is where the stalker knows the victim from casual contact such as at a local coffee shop or other public gathering place. In such cases the victim may not know the stalker on a personal level, and in some instances may not even know the stalker at all. The perceived relationship, however, is developed in the stalker's mind and is

enough to start the proceedings.

The third category of stalking is one that has seen tremendous growth in the last decade. These are the cases where the stalker and victim have only a casual relationship. This includes the cases such as the cyberstalking of the professor discussed above. In that case the relationship was virtually nonexistent in a real world sense. The only relationship was common membership in a given communication forum. That may be enough to start the acts in question.

One area where we see this arises in public forums on the Internet. People join these forums to discuss topics of similar interest with others. For instance, there are a number of forums available for those who have an interest in photography. While many of the forums are lawful there are some members who are there for less than legitimate purposes. An otherwise innocent member may find themselves the victim of cyberstalking simply because they joined a forum that included someone capable of these type of acts. These are certainly very casual relationships indeed.

It is important that one recognize the difference between true stalking and other forms of aggressive–and often offensive–communication. In many forums, such as newsgroups, the use of abusive language toward other group members is often tolerated. One member may post information that another finds offensive or simply disagreeable. Instead of discussing the issues in a reasonable fashion they choose instead to "flame" the other member. A flame occurs when one or more members of a social group post offensive, insulting, and even abusive material about another member.

In most instances the parties will hurl "flames" at each other for days, weeks, and even months. In fact, on one well-known newsgroup two members have had an ongoing flame war for more than five years. The parties, both of whom claim to be professionals in "real life," have disagreed over the most trivial matters and now are locked in a written battle that seems to have no end in sight. Neither will back down from their position nor will they leave the group. Each also claims that it is the others "fault." What makes it more interesting is that the two have never spoken or even met; yet, they continue this long-distance battle of wits simply because they choose to be a member of the given group.

These situations also lead to the misuse of communication devices such as e-mail. They are not, however, to be considered as true cyberstalking. As one can quickly see, these type of situations are in fact very similar to the continuing neighborhood disputes that police find themselves in the middle of all too often. There is no easy answer (other than to tell both parties to shut up), and the police tend to be stuck with the situation as much as anyone else. In such a case the only stalking being done is at worst mutual and at best lopsided.

Receiving a flame, and even sending one, does not necessarily exclude one from stalking. A flame war can quickly turn to a stalking case when one of the parties withdraws. In most cases the flame war dies a natural death when one party leaves the discussion or simply refuses to participate. When the second party then takes the flame war to a more personal level we may have a stalking case. In such an instance the insults leave the public forum and begin showing up in the private mailbox. Certainly the original cause of the abusive attack was the original flame war, but once that has been stopped any continued attack may be considered harassment or even stalking.

While in most instances we see at least a minimal connection between stalker and victim there are a few instances where no connection can be made. It should be noted, though, that there are very few true stalking cases by total strangers; i.e., where neither the victim nor the perpetrator knew each other before the case began.

One of the unintended side effects of our now well-connected society is the greater risk of information abuse. Today there is an enormous amount of personal information available through the Internet, and even the most amateur computer user can find out information with just a few keystrokes. For the cyberstalker this means an unprecedented access to the victim's vital information.

The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information.

The ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. Put another way, we know that a potential stalker is often unwilling or unable to confront a victim in person, but in the cyberstalking case there is often little hesitation about sending harassing or threatening electronic communications to a victim. Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence.

C. OFF-LINE VS. ONLINE STALKING–A COMPARISON

There are a number of similarities between off-line and online stalking. The first of these continues to be the domination of stalking cases by men against women. In most instances we find a greater number of men as perpetrators and women as victims. At this time there does not appear to be a likelihood of change in this area. Even the increase already seen in the num-

ber of women involved in cyberstalking is marginal compared to the number of men.

Acquaintance between the parties is also common in both types of case. Though the intimacy or nature of the acquaintance may be quite different there remains the fact that the victim and stalker often know each other. The most common relationship is that of the spurned suitor, spouse, or other close companion. Next are the disgruntled friends and business contacts. Next come the casual contacts. In the online world these are generally the people who mingle at electronic forums such as newsgroups and chat rooms.

One of the greatest similarities between off-line and online stalking is the need of the perpetrator to control the victim. From a psychological standpoint this need is not wholly unlike the power or domination factor we see in many rape cases. The incidents are less about an individual issue and more about the ability to dominate or control the other person.

When it comes to differences the first, and probably largest, difference is that presented by geographical distance. Obviously the off-line stalking must occur within a reasonable proximity to the victim; i.e., the stalker must be near the victim to actually carry through with the actions in question. For the online stalker, though, there is often a considerable distance between the two parties. The parties may be tens, hundreds, and even thousands of miles from each other, but this does not lessen the psychological impact such a case may have on a victim.

An interesting twist to the cyberstalker theme is the use of third parties to further the harassment or contact. For instance, a stalker can easily encourage others to participate in a "flame war" against the victim even though the victim has no intention of engaging in such activity. By using the victim's identifiers or something close enough to them to appear to be the victim, the cyberstalker encourages others to join in. The best example of this is to join a public forum as the victim and then post offensive remarks. Others on the forum, believing the remarks are coming from the victim, will lash out in retaliation for what they perceive as inappropriate remarks.

Such tactics also include the use of e-mail to harass the victim. In some instances this is the equivalent of sending unwanted pizzas to the victim's door. An off-line stalker might call the local pizza shop and order a dozen or more pizzas to be delivered to the victim's house. The victim is of course chastised by the delivery driver and in the end the harassment is done by a third party. In the cyberworld similar tactics such as signing a victim up for unwanted e-mail advice or services creates harassment that can be just as harmful.

One of the big issues with online harassment is that it tends to lower the social barriers we normally face in our day-to-day life. For instance, most people will not openly curse at someone they confront in a public place. It

would be embarrassing to call someone a "dirty rotten scoundrel" (or worse) while at a restaurant. But remove the parties from the physical location, put a keyboard instead of a person in front of them, and watch the insults begin to fly. The lack of social barriers means the stalker is now free to say practically anything they desire.

The Internet and other communications technologies also provide new avenues for stalkers to pursue their victims. A cyberstalker may send repeated, threatening or harassing messages by the simple push of a button. In one test students were asked to send a single message to others participating in the study as many times as they could in one minute. The record was ninety-seven messages sent by a single student in a sixty-second time period. The message was simply copied time and again by a simple e-mail macro that had been written by students in the class. The result, however, was the virtual cramming of the e-mailbox of the intended victim. Single minutes worth of work by cyberstalker resulted in ten minutes of clean-up for the victim.

More sophisticated cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal. California law enforcement authorities say they have encountered situations where a victim repeatedly receives the message "187" over and over again. The numbers "187" represent the section of the California Penal Code for murder; thus, the sender was sending a clear threat to the victim even though the perpetrator was not near his computer for most of the day.

In the first successful prosecution under California's new cyberstalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards. The perpetrator posed as the victim while online. The perpetrator then posted messages which appeared to be from the victim. The messages told of the victim's alleged fantasy to be raped. The perpetrator also posted the victim's name, address, and telephone number. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault.

In another case, a local prosecutor's office in Massachusetts charged a man with the equivalent of cyberstalking after he used anonymous "remailers" to send messages to his victim. In this case the defendant engaged in a systematic pattern of harassment of a coworker aimed at extorting sexual favors from the victim. The stalker threatened to disclose past sexual activities to the victim's husband if she did not consent to sex with him.

At the University of San Diego an honors student terrorized five female

university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day, before the perpetrator was stopped. The graduate student, who entered a guilty plea, told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In fact, the victims had never met him.

The anonymity of the Internet also provides new opportunities for would-be cyberstalkers. A cyberstalker's true identity can be concealed by using different ISPs or by adopting different screen names. As we have seen, more experienced stalkers can use anonymous "remailers" that make it all-but-impossible to determine the true identity of the source of an e-mail or other electronic communication. A number of law enforcement agencies report they currently are confronting cyberstalking cases involving the use of anonymous remailers.

D. EVIDENCE THAT CYBERSTALKING IS A GROWING PROBLEM

There is currently no comprehensive, nationwide database showing the statistics for cases of cyberstalking. In fact, most evidence that is available is anecdotal and relies heavily on a system of self-reporting. Thankfully, some ISPs have made their own records available for researchers and from these sources we are able to draw some reasonable inferences.

Some of the more readily accessible data indicates that stalking in general is on the rise. One report, which has addressed the problem, is known as *Stalking in America: Findings from the National Violence Against Women Survey.* This report defines stalking as "instances where the victim felt a high level of fear."[2] According to the report, among adults in America one out of every twelve women (8.2 million) and one out of every forty-five men (2 million) have been stalked at some time in their lives. The report further reveals that one percent of all women and 0.4 percent of all men were stalked during the preceding 12 months.

It is estimated that in the United States there are more than 100 million adults and 18 million children with access to the Internet. Assuming the proportion of cyberstalking victims is even a fraction of the proportion of persons who have been the victims of off-line stalking within the preceding 12 months, there may be potentially tens or even hundreds of thousands of victims of recent cyberstalking incidents in the United States.

Anecdotal evidence from law enforcement agencies indicates that cyberstalking is a serious–and growing–problem as well. At the federal level, hundreds of matters have been referred (usually by the FBI) to the U.S.

Attorney's Offices for possible action. Still other instances are referred to state and local authorities when no federal jurisdiction is involved.

Local officials have reported an increase in cases as well. For example, the Los Angeles District Attorney's Office estimates that e-mail or other electronic communications were a factor in approximately twenty percent (20%) of the roughly 600 cases handled by its Stalking and Threat Assessment Unit. The Manhattan District Attorney's Office also estimates that about twenty percent (20%) of the cases handled by their sex crimes unit involve cyberstalking. Similarly, the Computer Investigations and Technology Unit of the New York City Police Department estimates that almost forty percent (40%) of the caseload in the unit involves electronic threats and harassment.

The issue is not restricted to just large cities either. Many local law enforcement agencies are beginning to see cases of cyberstalking even in the most rural settings across America. This is easy to understand since the Internet connects all points of the country equally. A user in rural Kansas is just as capable of accessing a newsgroup or chat room as the most sophisticated user in New York or Los Angeles.

One of the more interesting research projects to touch on this issue comes from the University of Cincinnati. Researchers surveyed more than 4,400 randomly selected women attending two- and four-year institutions of higher education. The study focused on sexual victimization of college women. Researchers defined a stalking incident in a very broad sense. According to the report, a stalking incident was as any case in which a respondent answered positively when asked if someone had "repeatedly followed you, watched you, phoned, written, e-mailed, or communicated with you in other ways that seemed obsessive and made you afraid or concerned for your safety."

The study found that 581 women (13.1% of respondents) were stalked. In some cases the respondent was actually stalked more than once and this led researchers to report a total of 696 incidents of stalking. Of these 696 stalking incidents, 166 (24.7%) involved e-mail. Such statistics suggest that at least twenty-five percent (25%) of stalking incidents among college women could be classified as involving cyberstalking.[3]

E. CURRENT EFFORTS TO ADDRESS CYBERSTALKING

Stalking as a whole is a relatively new brand of criminal law. The first true stalking law was enacted by the state of California in 1990 following the death of a popular young actress which was linked to her stalker. In less than a decade a majority of states have enacted some form of stalking law, but most are woefully inadequate to address the actions which arise with computers. For that reason many legislative bodies have begun to rewrite their

original stalking statutes or supplement them with new computer-oriented laws.

Just as the law itself is new so too are the means for addressing the issue within law enforcement. Less than five percent of police agencies in the United States have a formal training program for computer-related crime. Of those agencies that do, most do not fully address the issues presented by the cyberstalking case.

Fortunately, most departments are now recognizing the need for training in the area of stalking as a general act. This does help when it comes to cyberstalking, but it may not be enough. While some agencies are developing the expertise and resources to investigate and prosecute traditional stalking cases only a handful of agencies throughout the country have focused attention or resources specifically on the cyberstalking problem.

In addressing the issues of cyberstalking we can draw many inferences from what we have already learned in the now traditional off-line case. The first is that there is a clear disparity in the activity level among law enforcement agencies across the country. This is due, in large part, to the same problems that cause similar disparity for other crimes as well. Namely, budget, manpower, and logistics issues prevent some department from being able to fully address any perceived problem.

Another issue that often arises is the inability of victims to report the crime. Cyberstalking, like rape and other crimes of this nature, appears to be underreported in all jurisdictions. One reason for this is that many victims are not aware of laws that might protect them. They simply do not know that a law exists that might stop someone from sending them harassing or threatening messages.

Victims may also find themselves afraid to report such an incident for fear of ridicule. In one such instance the alleged victim reported the incident to local law enforcement whose first step was to telephone the perpetrator. The law enforcement officer told the perpetrator to stop the harassment, but acknowledged that there was little he could do about it. The perpetrator then used this information to perpetrate further harassment of the victim.

What made matters worse was the involvement of third parties when the perpetrator posted this information to the original newsgroup. The victim stopped her own activity in the newsgroup rather than push the issues further with law enforcement. According to the victim the perpetrator continued to send harassing e-mail for over six months after she left the group, and she stated that she would never again contact law enforcement for assistance with a problem of this nature.

Most law enforcement agencies have not had the training to recognize the serious nature of cyberstalking and to investigate such offenses. In the example above the officer in question did not know the extent to which he could

legally push the case. The perpetrator was in another state and the officer was unsure of how to apply his own state's law to someone across state lines.

In other cases the victims have been told that because there was no physical threat made there was no law broken. Victims are often told to simply wait until the perpetrator confronts them in person and that without such a confrontation there is nothing law enforcement can do. In other cases law enforcement officers tell the victim to simply to turn off their computers or stop frequenting the public forums where the stalker is known to be.

Another indication that many law enforcement agencies underestimate the magnitude of the cyberstalking problem is the wide disparity in reported cases in different jurisdictions across the country. For example, one state attorney general's office in a Midwestern state indicated that it received approximately one inquiry a week regarding cyberstalking cases and that it is aware of approximately a dozen prosecutions last year alone. In contrast, the state attorney general's offices in neighboring states indicated they have never received an inquiry into this type of behavior. Certainly one can expect some disparity between states or regions; however, such disparity may be easily explained based on population size, density, and overall technology use. In these cases, though, the issues of population and technology appear to be very similar. From this one might easily draw the conclusion that the report rate may in fact be due to other factors.

F. JURISDICTIONAL AND STATUTORY LIMITATIONS

Many state and local law enforcement agencies have expressed frustration imposed by jurisdictional limitations. In many instances, the cyberstalker may be located in a different city or state than the victim. This creates a true investigative problem when local authorities must now go outside their own geographical jurisdiction to investigate an alleged crime. Such inter-jurisdictional investigations come with latent problems such as inter-agency cooperation.

Even if a law enforcement agency is willing to pursue a case across state lines, it may be difficult to obtain assistance from out-of-state agencies when the conduct is limited to harassing e-mail messages and no actual violence has occurred. A number of matters have been referred to the FBI and/or U.S. Attorney's offices because the victim and suspect were located in different states. In most instances, according to FBI sources, the jurisdictional limitations create almost unworkable barriers for local law enforcement. It is not that local law enforcement is unwilling to conduct an investigation but merely that they are unable to sustain such an investigation across state lines.

The lack of adequate statutory authority can also limit law enforcement's

response to cyberstalking incidents. At least 16 states have stalking statutes that explicitly cover electronic communications,[4] and cyberstalking may be covered under general stalking statutes in other states. It may not, however, meet the statutory definition of stalking in the remainder. In many cases, cyberstalking will involve threats to kill, kidnap, or injure the person, reputation, or property of another, either on or off-line and, as such, may be prosecuted under other federal or state laws that do not relate directly to stalking.

Finally, federal law may limit the ability of law enforcement agencies to track down stalkers and other criminals in cyberspace. In particular, the Cable Communications Policy Act of 1984 (CCPA) prohibits the disclosure of cable subscriber records to law enforcement agencies without a court order and advance notice to the subscriber. See 47 U.S.C. 551(c), (h). As more and more individuals turn to cable companies as their ISPs, the CCPA is posing a significant obstacle to the investigation of cybercrimes, including cyberstalking.

While it may be appropriate to prohibit the indiscriminate disclosure of cable records to law enforcement agencies, the better approach would be to harmonize federal law by providing law enforcement access to cable subscriber records under the same privacy safeguards that currently govern law enforcement access to records of electronic mail subscribers under 18 U.S.C. 2703. Similar legislation could be easily passed through both the House and Senate, and law enforcement would find the restrictions carefully offset by the procedural safeguards for privacy.

G. ANONYMITY ON THE INTERNET

In our earlier discussions the term "remailer" was used to refer to a service in which e-mail is sent without need to disclose the true user. These services are growing in number on the Internet and present a special problem of anonymity to law enforcement.

On the one hand anonymity provides important benefits by protecting the privacy of Internet users. Women prefer, and are encouraged, to use remailers or non-gender-oriented identifiers simply as a means of avoiding unwanted contact. To allow this segment of the population such access and not another certainly creates a legal dilemma, but the issue actually runs much deeper than that.

Cyberstalkers and other cybercriminals exploit the anonymity available on the Internet to avoid accountability for their conduct. Such individuals can literally say and do almost anything without fear of immediate prosecution. In fact, for the investigator who seeks to prosecute someone using a remailer or other anonymous system the chances of catching the criminal are

dramatically reduced.

Anonymous services on the Internet come in one of two forms. First, a host of "free electronic mailbox" services are available to users who require anonymity. Services such as Geocities, Yahoo, Hotmail, and many others provide an unlimited supply of such services, and most are at no cost to the user. In most instances the provider does not even require the use of a real name, merely another verifiable e-mail address. Thus, a wary user can establish multiple personalities on the Internet merely by "ping-ponging" his identity between various services.

For the few providers that do provide some form of protection up front there is often a way around the service requirements. For instance, if one does not have an instantly identifiable e-mail address (not one from another free service) then the site requires another form of guarantee. In most instances this can be accomplished by simply pre-paying for a limited service contract. The culprit simply pays with a money order (no name, address, etc. is required on these methods) and an account is established without question. As long as payment is received in advance by the ISP, the service is provided to the unknown account holder.

The second form comprises mail servers that purposefully strip identifying information and transport headers from electronic mail. By forwarding mails through several of these services serially, a stalker can remove all signs of his real identity from the original message. The presence of both such services makes it relatively simple to send anonymous communications, while making it difficult for victims, providers, and law enforcement to identify the person or persons responsible for transmitting harassing or threatening communications over the Internet.

H. LAW ENFORCEMENT RESPONSE

To this point the focuses response of law enforcement has been in those cities where Internet usage is growing dramatically. Larger metropolitan areas, such as Los Angeles and New York, have seen numerous incidents of cyberstalking and have created specialized units available to investigate and prosecute these cases. The Los Angeles Police Department developed the Stalking and Threat Assessment Team. This team combines special sections of the police department and district attorney's office to ensure properly trained investigators and prosecutors are available when cyberstalking cases arise. In addition, this specialized unit is given proper resources, such as adequate computer hardware and advanced training, which is essential in investigating and prosecuting these technical cases.

The New York City Police Department created a similar unit known as the Computer Investigation and Technology Unit. This unit provides regular training for police officers and prosecutors regarding the intricacies of cyberstalking investigations and prosecutions. The training includes understanding how chat rooms operate, how to obtain and preserve electronic evidence, and how to draft search warrants and subpoenas.

The key to success in any program of this type is proper training. Personnel must also have a strong interest in computers and a willingness to spend long hours at often-mundane tasks. One of the critical steps is learning how to trace communications sent over computers and the Internet. Traditional law enforcement techniques for surveillance, investigation, and evidence gathering require modification for use on computer networks and often require the use of unfamiliar legal processes.

Law enforcement at all levels must be properly trained to use network investigative techniques and legal process while protecting the privacy of legitimate users of the Internet. These techniques are similar to those used in investigating other types of computer crime. Just as a burglar might leave fingerprints at the scene of a crime, a cyberstalker can leave an "electronic trail" on the web that properly trained law enforcement can follow back to the source. Thus, technological proficiency among both investigators and prosecutors is essential.

While there are numerous efforts at the federal and state levels to focus on high technology crimes the reality is that most do not focus on cyberstalking as a primary concern. They may certainly include some form of investigative service, but few departments have the necessary expertise in computers and the Internet to assist in the investigation of cyberstalking when it arises. Because of this most agencies now turn to the FBI or other large agencies for assistance, and of this course places a higher level of use on each of these departments.

Some states have also established specialty units to assist local law enforcement. State police or investigative bureaus act in support of local law enforcement and are often able to set up a relatively effective crime lab at the scene if necessary. As with the federal agencies the emphasis is not on cyberstalking but instead on the overall use of technology to commit crimes.

A critical step in combating cyberstalking comes by understanding stalking in general. In many instances, cyberstalking is simply another phase in an overall stalking pattern, or it is regular stalking behavior using new, high-technology tools. Thus, strategies and techniques that have been developed to combat stalking in general often can be adapted to cyberstalking situations.

I. INDUSTRY EFFORTS

The computer industry, especially that associated with the Internet and electronic communication, have made efforts to combat abusive electronic communications overall. These efforts have increased over time, and from an industry standpoint have actually been very fruitful. One of the most common forms of abuse response is the establishment of an "abuse hotline" by most ISPs. Typically the ISP will setup a special e-mail address to which reports of abuse, including cyberstalking, may be forwarded. The most common e-mail address is "abuse@[domain name]" as in "abuse@aol.com." Another common address used for complaints or inquiry is "webmaster@[domain name]." An example might be webmaster@msn.com.

Many providers also include powerful provisions in their use agreement with customers. Such provisions specifically prohibit abusive or harassing conduct through their service and provide that violations of the policy will result in termination of the account. In some instances a cyberstalker will bounce from one ISP to another as he is reported for each new incident of abuse. Sadly, some ISPs do little to control their users and the language is more of a self-protection clause than a true enforcement tool.

One must note, though, that the reality is that the industry practices have been more in line with assisting customers in avoiding annoying online behavior rather than stopping the behavior. In fact, most of the efforts have been toward reducing the number of unwanted commercial solicitations (SPAM) rather than preventing true online stalking.

Unfortunately, most ISPs simply do not inform their customers about what steps, if any, the ISP has taken to follow-up on their customer's complaint. These problems are made worse by hard-to-locate complaint procedures, vague policies about what does and does not constitute prohibited harassment, and inadequate follow-up on complaints.

Fortunately, one area where the computer industry has made significant advances is in providing education and information to users. This information is primarily focused on protecting children and consumers on the Internet, but it has also been very helpful in cyberstalking cases. For example, since 1996, the Internet Alliance, one of the key Internet industry groups, has worked with the Federal Trade Commission and government agencies on Project OPEN (Online Public Education Network). Project OPEN provides information about fraud, parental controls, and protecting privacy.

Other similar industry efforts have recently been announced to address other aspects of computer-related crime. The Department of Justice and the Information Technology Association of America (ITAA) announced the Cybercitizen Partnership in March 1999. This partnership is intended to

boost cooperation between industry and government, expand public awareness of computer crime issues among children and adolescents, and provide resources for government to draw upon in addressing computer crime.

J. CYBERSTALKING LAWS

Less than one-third of the states have antistalking laws that explicitly cover stalking via the Internet, e-mail, pagers, or other electronic communications. Some states, such as California, have amended existing stalking statute to cover cyberstalking, but the trend has been slow in spreading.

At the federal level the law provides a number of important tools that are available to combat cyberstalking. Under 18 U.S.C. 875(c), it is a federal crime, punishable by up to five years in prison and a fine of up to $250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Section 875(c) applies to any communication actually transmitted in interstate or foreign commerce–thus it includes threats transmitted in interstate or foreign commerce via the telephone, e-mail, beepers, or the Internet.

Although 18 U.S.C. 875 is an important tool, it is not an all-purpose anti-cyberstalking statute. First, it applies only to communications of actual threats. Thus, it would not apply in a situation where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat). Also, it is not clear that it would apply to situations where a person harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person.

Certain forms of cyberstalking also may be prosecuted under 47 U.S.C. 223. One provision of this statute makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number.(10) The statute also requires that the perpetrator not reveal his or her name. See 47 U.S.C. 223(a)(1)(C). Although this statute is broader than 18 U.S.C. 875–in that it covers both threats and harassment–Section 223 applies only to direct communications between the perpetrator and the victim.

In 1996 Congress passed the *Interstate Stalking Act,*[5] which makes it a crime for any person to travel across state lines with the intent to injure or harass another person. This statute certainly addresses at least the physical part of stalking, but the downside is that it requires the person to physically travel across state lines in order to be subject to penalty. Critics have suggested that the act should be expanded to include any communication made across state lines as well.

ENDNOTES

1. 18 U.S.C. section 2261A
2. "Stalking in America: Findings from the National Violence Against Women Survey," U.S. Department of Justice, Office of Justice Programs, and Department of Health and Human Services, Center for Disease Control and Prevention, April 1998 (available at www.usdoj.gov/ojp).
3. Fisher, B. S., F. T. Cullen, J. Belknap, and M. G. Turner, "Being Pursued: Stalking Victimization in a National Study of College Women." (From a forthcoming report on sexual violence against college women funded by the US Department of Justice, National Institute of Justice).
4. These states are Alabama, Alaska, Arizona, California, Connecticut, Delaware, Hawaii, Illinois, Indiana, Maine, Massachusetts, Michigan, New Hampshire, New York, Oklahoma, and Wyoming. Arkansas and Maryland have enacted statutes that cover harassment via electronic communications outside their stalking statutes.
5. 18 U.S.C. 2261A

Chapter 9

IDENTITY THEFT

A. THE NATURE OF THE PROBLEM

Until a few years ago few outside of law enforcement had ever heard the term "Identity theft." Today, with the focus from the media and the access to instant information, there are few who have not heard of the crime. Fortunately, for law enforcement today's identity theft problem is merely an electronic extension of some very old crimes. This means that many of the basic techniques for identifying and apprehending identity theft suspects still apply. In this chapter we will examine a few of those techniques, as well as some new methods being used across the country.

At its root identity theft is the taking of basic information from the victim and then using that information to obtain cash or merchandise under cover of the new identity. While some might call this the "crime of the new millennium," the fact remains that identity theft only works when information is readily available. As we begin to understand this we can first look at one of the oldest and most profitable identity theft tricks around: stealing routing numbers from a check.

Most investigators who have worked questionable document cases know that there are unique numbers assigned to each bank, branch, account, and

account holder. Even the individual check has a unique number, and when a thief has access to that information they may be able to obtain cash from the account without a legitimate check. The trick is finding out how to get that information, and one of the best methods is to simply steal the checkbook, purse, or other container with the checks in it. Another common practice is the theft of checks or bank statements from the mailbox or other delivery location.

The major attraction of identity theft is the anonymity that accompanies the act. Unlike crimes such as robbery–where the suspect is typically seen and potentially identifiable by the victim–the crime of identity theft is committed under cover or through anonymous attack. The act of stealing the identity is accomplished through a variety of means, and the impact upon the victim can be devastating. The anonymity factor not only adds to the difficulty in investigating the crime but also in the impact felt by the victim.

At its heart identity theft is simply the theft of identity information such as a name, date of birth, Social Security number (SSN), or a credit card number. The mundane activities of a typical consumer during the course of a regular day may provide tremendous opportunities for an identity thief. Simple acts such as purchasing gasoline, meals, clothes, or tickets to an athletic event offer opportunity. Likewise each time we rent a car, a video, or make a transaction using any credit or debit card we increase the chances of identity theft. Any activity in which identity information is shared or made available to others creates an opportunity for identity theft.

It is estimated that identity theft has become the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society.[1] The last decade has seen significant increases in the crime, and much of this is due to the changing nature of how we conduct personal business. Identity theft is not limited to just online or computer-related crimes. The Social Security Administration reported a substantial increase in the number of allegations, and since 1999 that number has grown at a surprising rate.[2] The widespread use of SSNs as identifiers has reduced their security and increased the likelihood that they will be the object of identity theft.

The expansion and popularity of the Internet to effect commercial transactions has increased the opportunities to commit crimes involving identity theft. Today many consumers conduct transactions from online banking to purchase of birthday gifts online. Each of these transactions requires the consumer to enter valuable information including credit card number, date of birth, and even social security number. Each time information is entered into the computer or other electronic connection the risk of identity theft increases.

Identity theft has become enough of a problem that several federal, state, and local agencies now place it at the top of their white collar crime lists. It

is a significant part of the general investigations conducted by different federal agencies,[3] and many of these agencies have reported continually rising reports of crime. A number of studies and reports have focused on the issue of identity theft and they have found that methods used to obtain identity information ranged from basic street theft to sopisticated, organized crime schemes involving the use of computerized databases.

Investigators have found that not only is the electronic connection a source for obtaining identity information but other sources are being developed as well. One form of theft occurs when suspects wait in public areas to see the credit card numbers of people making transactions at ATMs, phones, and other sales devices which use non-cash methods for transactions. In some instances employees of prominent retailers and outlets are bribed to obtain otherwise secure information given to merchant and online sources.

To help get a better perspective on the breadth of identity crime one need merely look at the arrests and investigation statistics in the last decade. As an example, since 1995 more than 93 percent of arrests made by the U.S. Secret Service Financial Crimes Division involved identity theft. By 1997 estimates placed identity thefts at 94 percent of total financial crimes arrests. Just a decade ago the Secret Service estimated actual losses to individuals and financial institutions from identity theft at $442 million. That number rose to almost $750 million by 1997, and by the middle of 2004 that figure has easily topped $1.2 billion.

These increases are not limited to Secret Service investigations either. In fiscal year 1995 the Social Security Administration reported a sharp increase in fraud investigations. Since then the agency has seen a 400 percent increase in misuse and fraud associated with identity theft. Similar increases have been seen by the United States Postal Service investigations units. According to Postal Inspectors the number of investigations involving identity theft has risen by more than 500 percent in the last decade.

Increased concern with identity theft is not limited to public entities or law enforcement. Private companies at all levels report increased losses from computer and identity-related crime. One industry that has seen a significant impact is the credit reporting. The largest reporting agencies including Trans Union Corporation, TRW, and Equifax have reported significant numbers of cases in the last few years. In its annual reports Trans Union Corporation maintains that over 65 percent of inquiries to its fraud department involved identity fraud. What makes this significant is that this is an average increase of more than 600 percent from the last decade. In some instances the increase has been from 3,000 a month in 1992 to over 43,000 a month in 1997.

Similar increases in activity have been reported by the nation's largest credit card companies as well. Both VISA U.S.A., Inc., and MasterCard

International, Inc. report an overall increase in fraud losses, and the issues of identity theft account for millions of dollars in loss each year. In one report financial company MasterCard reported that identity fraud and related crimes now account for as much as 96 percent of their total fraud losses as reported by members.

While the sheer volume of cases as well as monetary loss is staggering the more far-reaching issue is that of victim impact. Most victims of identity theft do not realize they have become victims until they attempt to obtain financing on a home, vehicle, or other major purchase. Because consumers do not keep track of their respective credit or the patterns of activity related to their accounts they often miss the fact that they are being targeted until it is too late.

In many instances consumers can help protect themselves by taking simple precautions such as checking their credit score regularly. They can also monitor credit card activity by using online banking or access points. Of course these activities in themselves become another source of potential fraud or misuse. For that reason consumers should become more wary of potential scams and fraud attempts. They must also become better educated in how their credit or credit scores are being used. For the criminal investigator the task of educating the public easily falls under the same call for service seen in burglary and other crime watch systems. Computer fraud and identity theft is merely an extension of the education services provided for other crime types.

Identity theft can also bring with it a great deal of financial and emotional grief. Not only may the victim become a consumer victim in the credit industry but they may feel "invaded" or "violated" by the offender. One of the most commonly reported feelings is that very similar to the feeling experienced by burglary or home invasion victims. The ability to strike the victim in such a personal way has long lasting and often deep effects on much more than the credit score.

B. HOW DOES IDENTITY THEFT OCCUR?

There are as many different ways for identity theft to occur as there are ways it identify someone. The most common methods are often the easiest. One of the most common is the simple sharing of personal information in a careless fashion. One example is the person who gives their personal identifying information to another without first verifying that the person is who they claim to be. For example, in one study an estimated 18 percent of those surveyed said they would give their checking account information to someone who would call them at their home.[4] In the worst cases the consumer

admitted that they would likely give credit card information, including card number and security codes, to any person who called and properly identified their bank. In a similar study respondents admitted that they would give out vital information about credit card and checking accounts to someone who simply identified themselves as "from your bank."

As mentioned in the introductory section, a popular form of identity theft occurs when the victim uses a public phone or point of sale. Commonly referred to as "shoulder surfing," the identity suspect merely watches from a spot behind the victim so that they can see credit card, check, or other important numbers as the victim shops or uses the item in question. This is a common practice at locations where large numbers of people gather and where there is a continuing source of consumers. Malls, airports, theaters, and other public areas are the most common locales.

Shoulder surfing is accomplished in a number of ways including the simplest act of memorizing a credit card number spotted over the shoulder. With the increased use of cell phones with wireless (Bluetooth) connections the suspect can wear a small earpiece with built in microphone. As the suspect spots the credit card or other number he may simply repeat numbers as if he were talking on the phone or even in a way where few would notice that he was saying much of anything.

Other forms of identity theft occur through intentional acts including the taking of purses, wallets, mail, and even the interception of electronic "wireless" communication. The interception of wireless communication has become so easy that some thieves simply use their laptop computer with wireless network cards to cruise neighborhoods looking for open connections. The victim is usually inside the home working at the computer while the thief remains outside intercepting every keystroke or message being sent. In the worst case scenarios thieves have also used wireless connections to actually gain access to the victim's hard drive, which is where financial data is commonly stored.

Thieves also work outside the home when they steal the victim's mail, go through their garbage or recycling bin, and even intercept pizza or delivery orders hoping to gain credit card or other information.

The action does not stop at the home, though, as thieves turn to other locations for opportunities to steal valuable information. Medical facilities, businesses, public sites, and many other locations present opportunities as well. "Dumpster diving" is a common practice where a thief will go into garbage cans, large dumpsters, or recycling bins to obtain identity information.

A number of merchants still use the paper-based credit system, and these systems provide a wealth of data on the carbon or extra copy of a credit transaction. Similar information can be obtained from debit card receipts, bank statements, medical records such as prescription labels, or other

records that bear a name, address, or telephone number. Even fast-food restaurants now take credit or debit cards, and these are rapidly becoming a new source of identity harvesting.

One activity that continues to net amazing results is the theft of pre-approved credit card solictations which are commonly sent through the mail. In many instances the actual credit card is included in the solicitation, and consumers who want the card must activate it either with a phone call or online. Thieves who acquire the card, either directly or by purchasing it from other thieves, can activate the card with a single phone call, and once activated offenders will quickly charge the card to its maximum limit before the consumer ever knows what has happened.

Once thieves have identified information such as name, date of birth, social security number, etc., they need merely start applying for credit cards on their own. They can set up a drop box or use another address for the delivery of new credit cards. A consumer with good credit can quickly find that dozens of credit cards they never requested have been activated by thieves with basic personal information. By the time the consumer finds out what has occurred the thieves have destroyed his credit and run up a bill in the tens if not hundreds of thousands of dollars.

C. INVESTIGATING THE IDENTITY THEFT CASE

Like most criminal investigations where the suspect is initially unknown, the investigation of identity theft can be very difficult. Investigators typically put in two hundred or more hours in a single case, even when they have some basic leads. These investigations are not only labor intensive but they demand a high level of coordination. In most instances the investigator is assigned dozens or even hundreds of cases, and each case will have its own unique nature. Tracking all the details for the individual cases can be very tough, and investigators must develop a good system to track and identify potential leads.

The lucky investigator will notice an immediate pattern in the case, and this can be a significant break. Perpetrators usually victimize multiple victims in several jurisdictions, though, and this can make it more difficult to see such patterns. Investigators may easily work a large number of cases before they begin to see a sign of a pattern. This is also complicated by the fact that most victims do not realize they have been victimized until weeks or months after the crime has been committed. Likewise, victims often provide little assistance to law enforcement simply because they have little information to provide.

One can clearly see that identity theft has become one of the fastest-growing financial crimes in America and perhaps the fastest-growing crime of any kind in our society. The difficulties of investigating the traditional fraud, theft, or computer crime are exacerbated by the fact that an identity thief can hit without most victims knowing the crime has occurred. This means that most identity offenders are seldom caught, and because of this the crime itself continues to see a steady increase.

One of the best tactics taken by law enforcement in recent years has been the expansion of training at all levels. For instance, the federal government has sponsored numerous training sessions, conferences, and learning opportunities for investigators at all levels. For the investigator who is new to this type of investigation one of the first steps in becoming proficient is to find and attend such training.

Another positive step has been the creation and continuance of the various multijurisdictional task forces that call on local, state, and federal law enforcement to work together. Multiagency task forces have proven successful in investigating and prosecuting identity theft at virtually all levels. The top advantage to such a task force is the ability of agencies to pool resources and information to combat regional and even national crimes. In recent years private industry has joined with government agencies to help spread the message as well as coordinate information. This has allowed investigators in both public and private sectors to improve overall effectiveness.

Because identity cases involving large numbers of victims present unique challenges there is a concerted effort to improve communication between agencies and investigators. Communication is necessary to obtain fundamental investigative information, including loss and restitution information. In complex cases, it is imperative to devise a system for communication with the victims at the outset of the case. The investigator should work with victim/witness units to identify the best communication system for the case. The investigator should also work with the various administrators to develop a link where victims and investigators can exchange information.

Some departments have also created web-based systems that allow victims and investigators to exchange information. This tool has been especially good for keeping victims up to date on their individual cases, though at times it may seem like nothing is really happening. One advantage is that victims can file supplemental reports or provide additional information much easier than the formal methods used in the past. As most investigators know, a victim will often recall information days or even weeks after an event. The quick exchange of information is vital, and this two-way system allows victims to feel more a part of the investigation. It also allows investigators a way to communicate with victims much easier.

D. FEDERAL CRIMINAL LAWS FOR IDENTITY THEFT

The different states have all begun significant revisions of their laws governing identity theft. Some states simply had no law and others have merged or altered existing theft laws. The most far reaching law, though, has arisen at the federal level, and for that reason we will explore the federal system as we examine the legal issues of identity theft.

Federal law falls into two very broad categories. On the one hand are those criminal laws that focus on the theft aspect and seek relatively stiff punishment for identity theft cases. The other type of laws are those that seek to limit or in some way lessen the impact of identity theft on the victim. Both laws serve an important purpose in the system, but they also create a dramatically different way to approach the same problem.

One of the primary identity theft statutes is found in 18 U.S.C. § 1028(a)(7) and was enacted on October 30, 1998, as part of the Identity Theft and Assumption Detterence Act (Identity Theft Act). Prior to this act identity theft was addressed in part by 18 U.S.C. § 1028, and the coverage was fairly narrow. The statute actually only addressed a small part of the larger crime by focusing on the fraudulent creation, use, or transfter of identification *documents,* and not the theft or criminal use of the underlying personal *information.* This meant that the taking of the information (identity) was allowed so long as the document itself remained in place. Clearly, under such a statutory sceheme the clever identity thief would concentrate on means of taking the information without actually taking the document containing the information. This meant the crimes such as shoulder surfing were rarely prosecuted unless some physical taking had taken place.

With the creation of the Identity Theft Act the fraud connected with the taking of the information is now considered a crime. Under § 1028(a)(7) fraud in connection with the unlawful theft and misuse of personal identifying information, regardless of whether the information appears or is used in documents, is now a crime when the suspect, "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. . . ."

The new act also strenghtened the penalty provisions of § 1028(b) by extending its coverage and applying more stringent penalties for identity thefts involving property of value. Section 1028(b)(1)(D) provides for a term of imprisonment of not more than fifteen years when an individual commits an offense that involves the transfer or use of one or more means of identification if, as a result of the offense, anything of value aggregating $1,000 or more during any one year period is obtained. If the value is less than the

$1,000 amount then § 1028(b)(2)(B) provides for imprisonment of not more than three years. The Identity Theft Act also addes language which provides that attempts or conspiracies to violate the statute are subject to the same penalties as those prescribed for substantive offenses under § 1028.

As one can quickly see, the changes to the act now brought focus on the acts of stealing the information not just the document containing the informaiton. This made the prosecution of shoulder surfing cases much clearer, and it also allowed for a much higher level of protection to the individual consumer. Other parts of the act make additional changes such as that found in § 1028(b)(3) which provides that if the offense is committed to facilitate a drug trafficking crime, or in connection with a crime of violence, or is committed by a person previously convicted of identity theft, the individual is subject to a term of imprisonment of not more than twenty years. The Identity Theft Act also added § 1028(b)(5) which provides for the forfeiture of any personal property used or intended to be used to commite the offense.

Other areas of the act makes changes in the definitions of terms or acts associated with identity crime. For instance, under § 1028(d)(1) the definition of "document-making implement" has been enhanced to include computers and software specifically configured or primarily used for making identity documents. This is a very important addition since computers are rapidly becoming a significant part of the identity theft trade. It is important to note that the Identity Theft Act is intended to cover a variety of individual identification information systems that may be developed in the future and utilized to commit identity theft crimes.

The Identity Theft Act also directed the United States Sentencing Commission to review and amend the Sentencing Guidelines to provide appropriate penalties for each offense under Section 1028. The Sentencing Commission responded to this directive by adding U.S.S.G. §2F1.1(b)(5) which provides the following:

(5) If the offense involved–
  (A) the possession or use of any device-making equipment;
    - the production or trafficking of any unauthorized access device or counterfeit access device; or
    - the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification; or
    - the possession of [five] or more means of identification that unlawfully were produced from another means of identification or obtained by the use of another means of identification.

These new guidelines take into consideration the fact that identity theft is

a serious offense, and an important part of the changes has been the removal or modification of past monetary thresholds. In the past, when dealing with most fraud offenses, the loss would have to be more then $70,000.00 for the resulting offense to be punishable at such a high level. Under the new guidelines the Sentencing Commission acknowledged that the economic harm from identity theft is difficult to quantify, and that whatever the identifiable loss, offenders should be held accountable. Today identity theft offenses generally merit a two-level increase in sentencing because they often involve more than minimal planning or a scheme to defraud more than one victim. The sentencing guidelines also provide for two to four-level upward organizational role adjustments when multiple defendants are involved.[5]

The Identity Theft Act also directed the Federal Trade Commission (FTC) to establish a procedure to acknowledge receipt of complaints from victims of identity theft, to provide educational materials to these victims, and to refer the complaints to appropriate entities. The FTC responded by creating a web site which allows consumers to log complaints, access educational materials, and access a central database for information. The web site can be found at www.consumer.gov/idtheft. The FTC also created a hotline which consumers can use for the same purposes; that number is 1-877-ID THEFT.

When received the identity theft complaint is entered into *Consumer Sentinel,* a secure, on-line database available to law enforcement. The FTC has become a primary referral point for victims of identity theft as well as a prime partner with local law enforcement in combating identity theft.

Identity theft has also been addressed in other areas of federal criminal law. Because identity theft is often committed to facilitate other crimes there is a significant chance that the acts will be addressed by other legislation. For instance, identification fraud (18 U.S.C. §1028(a)(1) - (6)), credit card fraud (18 U.S.C. §1029), computer fraud (18 U.S.C. §1030), mail fraud (18 U.S.C. §1344), mail theft (18 U.S.C. §1708), and immigration document fraud (18 U.S.C. §1546) all include specific language which addresses issues associated with identity theft.

When it comes to cases involving computer fraud a central theme is to address the use of the computer to facilitate the theft of identity information. Computer fraud may also be the primary vehicle to obtain identity information when the offender obtains unauthorized access to another computer or web site to obtain such information. These acts might result in the offender being charged with both identity theft under 18 U.S.C. §1028(a)(7) and computer fraud under 18 U.S.C. §1030(a)(4). It is also worth noting that not only does specific criminal law address the acts but the federal sentencing guidelines also address the punishment. Specifically, section 2F1.1(c)(1) of the guidelines provides minimum sentence, notwithstanding any other adjust-

ment, of a six-month term of imprisonment if a defendant is convicted of computer fraud under 18 U.S.C. § 1030(a)(4).

E. EXEMPLARY FEDERAL CASES

A number of federal cases allow us to see the application of the new laws to specific cases, and the study of some of these cases will help to better understand the issues that likely arise. One case worth noting arose in California and involved prosecution under 18 U.S.C. § 1028(a)(7). In this particular case the defendant obtained the private bank account information for policyholders from an insurance company. Using the private information the suspect was able to deposit over $764,000 in counterfeit bank drafts and withdraw funds from accounts of policyholders. The suspect was sentenced to a twenty-seven month term 0f imprisonment.[6]

In another case the offenders obtained names and social security numbers of high-ranking military officers from an Internet web site. They then used the information to apply on-line for credit cards and other instruments in the names of their victims. One culprit was sentenced to a thirty-three-month term of imprisonment and $160,910.87 in restitution while the second defendant received a sentence of forty-one months and $126,298.79 in restitution.[7]

Identity theft has also been involved in a number of other crimes including drug trafficking. In one case coming from the Oregon federal courts seven defendants were convicted and sentenced to imprisonment for their roles in a heroin/methamphetamine trafficking organization which used stolen identities to further the drug crimes. The defendant entered the United States illegally from Mexico and later obtained social security numbers of other persons. Using these social security numbers the defendants obtain temporary employment and identification documents, which were then used to facilitate the distribution of heroin and methamphetamine. In obtaining employment, the defendants used false alien registration receipt cards, in addition to the fraudulently obtained social security numbers, and these acts are criminal in their right.

Some of the defendants also used the fraudulently obtained SSNs to obtain earned income credits on tax returns fraudulently filed with the Internal Revenue Service. Some relatives of narcotics traffickers were arrested in possession of false documents and were charged with possessing false alien registration receipt cards and with using the fraudulently obtained SSNs to obtain employment. A total of twenty-seven defendants have been convicted in the case to date, fifteen federally and twelve at the state level.[8]

F. STATE CRIMINAL LAWS

While most states now have laws prohibiting the theft of identity information there is some significant differences. Listing each state and the individual criminal law would leave little room for anything else, and for that reason this text will restrict comments to those laws that share similar characteristics or present a unique approach. Before beginning the review of specific state laws it is important to note that even where no explicit identity theft laws do not exist the practices may be prohibited under other state laws.

A number of states already include specific laws designed to address identity theft. The following table provides a list of current states and laws:

State:	**Citation:**
Arizona	Ariz. Rev. Stat. §13-2008
Arkansas	Ark. Code Ann. § 5-37-227
California	Cal. Penal Code § 530.5
Colorado	2000 Colo. Legis. Serv. ch 159 (May 19, 2000)
Connecticut	1999 Conn. Acts 99-99
Delaware	Del. Code Ann. titl 11, § 854
Florida	Fla. Stat. Ann. §817.568
Georgia	Ga. Code Ann. § 16-9-121 to 16-9-127
Idaho	Idaho Code § 18-3126
Illinois	720 Ill Comp. Stat. 5/16G
Indiana	Ind. Code §35-43-5-4 (2000)
Iowa	Iowa Code § 715A.8)
Kansas	Kan. Stat. Ann. § 21-4018
Kentucky	Ky. ev. Stat. Ann. § 514-160
Louisiana	La. ev. Stat. Ann. §67.16
Maine	Me. Rev. Stat. Ann. titl. 17-A, § 354-2A
Maryland	Md. Ann. Code art. 27, § 231
Massachusetts	Mass. Gen. Laws ch. 266, § 37E
Minnesota	Minn. Stat. Ann. § 609.527
Mississippi	Miss. Code Ann. §97-19-85
Missouri	Mo. Rev. Stat. § 570-223
Nebraska	Neb. Rev. Stat. § 28-101
Nevada	Nev. ev. Stat. §205.465
New Hampshire	N.H. Rev. Stat. Ann. § 638:26
New Jersey	N.J. Stat. Ann. § 2C:21-17
North Carolina	N.C. Gen. Stat. §14-113.20
North Dakota	N.D. Cent. Code § 12.1-23-11
Ohio	Ohio Rev. Code Ann. 2913.49

Oklahoma	Okla. Stat. tit. 21, §1533.1
Oregon	Or. Rev. Stat. § 165.800
Pennsylvania	Pa. Cons. Stat. Ann. § 420
Rhode Island	R.I. Gen. Laws § 11-49.1-1
South Carolina	S.C. Code Ann. § 16-13-500
South Dakota	S.D. Codified Laws 20
Tennessee	Tenn. Code Ann. § 39-14-150
Texas	Tex. Penal Code Ann. § 35.51
Utah	Utah Code Ann. § 76-6-1101-1104
Virginia	Va. Code Ann. § 61-3-54
Wisconsin	Wis. Stat. §943-201
Wyoming	Wyo. Stat. Ann. § 6-3-901

G. STEPS TO HELP THE VICTIM OF IDENTITY THEFT

One of the most common problems with the identity theft case is the need to assist the victim to recreate accounts or information needed in the investigation. By assisting the victim to recover from the identity theft the investigator can often gain important information on how the identity was stolen and how the thieves have used it to their advantage. The first step is to have the victim create a log of all conversations, including dates, names, and telephone numbers.

The log will serve several purposes. For the victim the log will help to recreate or explain any time spent and expenses incurred. This is important in the event restitution can be obtained in a civil or criminal judgment against the thief. The log will also help in refreshing the victim's memory of any conversations and should be confirmed in writing or for any exchanges where the information in question may have been compromised.

The victim should also contact the fraud departments of each of the three major credit bureaus (Equifax, Experian, and Trans Union). Of course the victim will want to inform the representative of each as to the identity theft but it is also a good place to start the act of recreating accounts and expenses. A "fraud alert" will be placed on the victim's file, as well as a statement asking that creditors call the victim before opening any new accounts. This will, of course, likely alert the suspects to the fact that the victim now has notice of the actions, but it will also help the investigator to begin the task of gathering all the relevant dates, times, locations which will help establish an MO.

Copies of credit reports from the credit bureaus should also be ordered.

The reports should be reviewed carefully to identify unauthorized accounts or unauthorized changes to existing accounts. The investigator should also be careful to note any "inquiries" made from companies that opened fraudulent accounts. The consumer will want to make a request to remove the "inquiries" from the report, but the investigator will need information to help further establish the MO or pattern.

A request should also be made for the credit bureaus to notify those who have received a credit report in the last six months and alert them to the disputed and erroneous information. The victim should request a new copy of the reports after a few months, to verify that the requested changes have been made, and to ensure no new fraudulent activity has occurred.

The victim should contact the security or fraud departments for any creditors of accounts in which fraudulent activity occurred. This should also be done by the investigator, and if possible separate reports should be obtained. Creditors may include businesses, credit card companies, telephone companies and other utilities, and banks and other lenders. All conversations should be confirmed with written correspondence. It is particularly important to notify credit card companies in writing because it is required by the consumer protection laws.

This victim will likely close all accounts that have been tampered with, but before this is done the investigator must get current balances and a list of all transactions during the suspect time period. The investigator should also insure that the creditor or account source understand that the accounts are subject to the provisions of a criminal investigation, and the company should take normal precautions to protect the potential evidentiary value of the account.

Some situations may requie additional action by the victim such as in cases where the mail has been stolen. In such a case the investigator will be working closely with federal officials from the United States Postal Service, and the sharing of information may be a vital link to identifying the interstate or regional group responsible.

If financial information has been obtained, the financial entity (the bank, brokerage firm, credit union, credit card company, etc.) should be contacted, the fraudently affected accounts closed, and new accounts opened with new PINs and passwords, including affected ATM cards. Payment should be stopped on any stolen checks, and banks or credit unions should be asked to request the appropriate check verification service to notify retailers not to accept the checks.

Three check verification companies that accept reports of check fraud directly from consumers are: Telecheck: 1–800–710–9898; International Check Services: 1–800–631–9656; and Equifax: 1–800–437–5120. If investments or securities may have been affected, brokers should be notified and

the victim should file a complaint with the Securities and Exchange Commission (SEC). A complaint can be filed with the SEC at the SEC Enforcement Complaint Center, 450 Fifth Street, NW, Washington, D.C. 20549–0202; its web site www.sec.gov, e-mail enforcement@sec.gov, or fax 202-942-9570.

If someone is using a victim's SSN to apply for a job or to work, it should be reported to the Social Security Administration (SSA). The victim should first visit the SSA's web site at www.ssa.gov, read the Guidelines for Reporting Fraud, Waste, Abuse and Mismanagement, and then call the SSA Fraud Hotline at 1–800–269–0271, and file a report at SSA Fraud Hotline, P.O. Box 17768, Baltimore MD 21235, fax 410–597–0118 or e-mail oig.hotline@ssa.gov.

The victim should also call the SSA at 1–800–772–1213 to verify the accuracy of earnings reported under the SSN and to request a copy of the victim's Social Security Personal Earnings and Benefit Estimate Statement. The Statement should reveal earnings posted to the victim's SSN by the identity thief. If an SSN has been fraudulently used, the Internal Revenue Service (IRS) Taxpayer Advocates Office should be contacted. The fraudulent use of an SSN might result in what appears to be an underreporting of a victim's taxable income and an attempt by the IRS to collect taxes on the underreported income. The IRS Taxpayer Advocates Office can be contacted at 1–877–777–4778 or www.treas.gov/irs/ci.

If someone has fraudulently obtained a driver's license or photographic identification card in a victim's name through an office of a DMV, the local DMV should be contacted and a fraud alert should be placed in the license. Likewise, if someone has stolen any other identification document, the entity responsible for creating the document should be contacted and informed of the theft. If a passport has been lost or stolen, the United States State Department should be contacted at Passport Services, Correspondence Branch, 1111 19th Street, NW, Suite 510 Washington, DC 20036, or www.travel.state.gov/passport_services.html.

In rare instances, an identity thief may create a criminal record under a victim's name by providing the identity when arrested. Victims of this type of problem should contact the FBI and initiate a request that the victim's name be cleared, and retain an attorney to resolve the problem as procedures for clearing one's name may vary by jurisdiction.

ENDNOTES

1. *Identity Theft: Is There Another You? Joint hearing before the House Subcomms. on Telecommunications, Trade and Consumer Protection, and on Finance and Hazardous*

Materials, of the Comm. on Commerce, 106th Cong. 16 (1999) (testimony of Rep. John B. Shadegg).

2. In fiscal year 1999 alone, the Social Security Administration (SSA) Office of Inspector General (OIG) Fraud Hotline received approximately 62,000 allegations involving SSN misuse.
3. *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited,* published in support of the Identity Theft and Assumption Deterrence Act, the General Accounting Office (GAO).
4. *How Easy the Hook: A Study of Consumer Practices in Distributing Identifying Data by Telephone,* C. Franklin, Western and Pacific Association of Criminal Justice Educators, Spring 2005.
5. United States Sentencing Guidelines § 3B1.1
6. *United States v. Anthony Jerome Johnson,* CR 99-926 (C.D.Ca. Jan. 31, 2000).
7. *United States v. Lamar Christian,* CR 00-3-1 (D. Del. Aug. 9, 2000); *United States v. Ronald Nevison Stevens,* CR00-3-2 (D.Del. Aug. 9, 2000).
8. *United States v. Jose Manuel Acevez Diaz,* Cr 00-60038-01-HO (D.Or. Aug. 10, 2000); *United States v. Pedro Amaral Avila,* CR 00-609-44-01-HO (D.Or. Nov. 7, 2000); *United States v. Jose Arevalo Sanchez,* CR 00-60040-01-HO (D.Or. Nov. 21, 2000); *United States v. Maria Mersedes Calderon,* CR 00-60046-01-HO (D.Or. May 10, 2000); *United States v. Victor Manueal Carrillo,* CR 00-60045-01-HO (D.Or. Oct. 24, 2000); *United States v. Alfonso Flores Ramirez,* CR 00-60035-01-HO (D.Or. Nov. 7, 2000); *United States v. Javier Hernandez Lopez,* CR 00-60038-01-HO (D.Or. Aug. 10, 2000); *United States v. Ranulfo Salgado,* CR 00-60039-01-HO (D.Or. Jan. 18, 2001); *United States v. Angel Sanchez,* CR 00-60080-01-HO (D.Or. Aug. 31, 2000); *United States v. Cresencio Sanchez,* CR00-60143-01-HO (D.Or. Dec. 13, 2000); *United States v. Piedad Sanchez,* CR 00-60141-01-HO (D.Or. Jan. 9, 2001); *United States v. Noel Sanchez Gomez,* CR 00-60034-01-HO (D.Or. Dec. 12, 2000); *United States v. Kelly Wayne Talbot,* CR 00-60001-HO (D.Or. Dec. 31, 2000); *United States v. Jose Venegas Guerrero,* CR 00-60037-01-HO (D.Or. Nov. 21, 2000); *State of Oregon v. Fred Harold Davis,* Case No. 006276FE (Jackson County Dec. 13, 2000); *State of Oregon v. Pablo Macias Ponce,* Case No. 004317MI (Jackson County Sept. 13, 2000); *State of Oregon v. Raul Navarro Guiterrez,* Case No. 005257FE (Jackson County Nov. 8, 2000); *State of Oregon v. Miranda Mae Byrne,* Case No. 004363FE (Jackson County Jan. 9, 2001); *State of Oregon v. James Tracy Campbell,* Case No. 002376FE (Jackson County Aug. 25, 2000); *State of Oregon v. Michael Scott Gilhousen,* Case No. 002225FE (Jackson County Nov. 7, 2000); *State of Oregon v. Robert Dean Golden,* Case No. 002726FE (Jackson County Oct. 18, 2000); *State of Oregon v. Annetta Lynn Kelley,* Case No. 002377FE (Jackson County July 24, 2000); *State of Oregon v. Gerald Jerome King,* Case No. 003594FE (Jackson County Oct. 31, 2000); *State of Oregon v. Micah John Right,* Case No. 002374FE (Jackson County Sept. 7, 2000); and *State of Oregon v. Todd Ivan Williams,* Case No. 004533FE (Jackson County Jan. 12, 2001).

Section 3

THE COMPUTER CRIME INVESTIGATION

Chapter 10

INITIAL ASSESSMENT AND RESPONSE TO THE COMPUTER CRIME

Every effective investigation begins with planning that took place long before the crime occurred. What this means is that the competent investigator begins preparing for the potential crime even before the crime has been committed. The first step, as we discussed earlier in this text, is to educate oneself about computers and the issues that arise in a computer crime case. The next step is to create a protocol for assessing and investigating that case. In this section we will examine the issues that arise with the initial assessment of the computer crime case.

A. INCIDENT NOTIFICATION AND RESPONSE PROTOCOL

Most police agencies today have clear policy and procedure for dealing with reports of crime. Police dispatch units follow standard practices for identifying the caller, the nature of the call, the need for response, and the appropriate assignment of police personnel. These practices have developed over the last fifty or more years of law enforcement, and for most crimes these are perfectly acceptable practices. Problems arise, though, when one realizes that computer crime is a relatively new phenomenon, and the very nature of the computer dictates that new policy and procedure be implemented.

In examining this issue let us begin with the initial report of a computer crime. By the very nature of the criminal act itself we see that there can be a very different set of circumstances for even the same type of crime. For instance, it is clear that a homicide, regardless of how long the person has been dead, is a top priority call. Police officers are normally dispatched with due diligence to the scene of a death. A burglary, on the other hand, may demand a much different approach from the department. If the burglary is "in progress" then officers are dispatched immediately. If the burglary is hours (or days) old then the response is much different. Officers are generally sent as time and manpower allows. This same concept holds true for computers, but there are added issues that must be addressed.

One of the first issues to emerge in any computer crime case is the possibility of contamination. Because of this it should also be one of the first items to be addressed by the protocol. It is important to remember that contamination of a computer crime scene can be both tangible and intangible. An example of tangible contamination is the removal of a floppy disk drive from a target computer's disk bay. For instance, the perpetrator has copied information from the computer and left behind one of the disk used in the information theft. Removal of that disk, much like the removal of or touching of a knife at a homicide scene, can substantially contaminate the evidence.

Intangible contamination is also a strong concern. Imagine that the perpetrator has not left a disk behind but has instead left behind log-in codes that might be easily traced by detectives. These codes are stored temporarily in one of the files on the computer system but can be easily lost when another user logs onto the system. If the machine is not protected, and measures are not taken at the initial stages, then there is a chance for electronic contamination when the next user logs on.

There are many other issues that arise as well, and each of them can be easily addressed if the department's initial assessment and response protocol is an effective one. The first step is to make sure that those who work in dispatch, records, or other areas where reports can be made have proper training and know the protocol.

Because the conventions applied in normal call receipt gave us a good foundation for building an appropriate computer response protocol, we will begin there. Over time many departments have developed their own standards or follow industry standards for handling calls. One of the most common practices is the use of a checklist by dispatchers when taking a call. For departments which use a checklist or similar system for logging incoming reports a simple system can be added to prompt dispatchers as to the right questions to ask as well as the correct response for a potential criminal report.

One of the better methods to use is known as an "Incident Notification Checklist." Many departments, especially those using computer aided dispatch (CAD) systems, already use such checklist. The standard checklist begins with some basic information such as caller's identification (name, address, phone, etc.) and a statement of the crime reported. This often includes basic information such as time of incident, location, potential witnesses, and other material. Figure 10-1 shows an initial incident checklist as it might appear on a CAD screen.

In this example the first tasks in the protocol is to have the dispatcher, or other person taking the initial call, enter the preliminary information just as they would for any other call. The CAD system in this example requires dispatchers to enter basic information including the caller's ID, phone, etc., and then turns to the incident. Once the nature of the crime is entered then additional questions appear that will prompt the dispatcher to seek further information. In this example the code for "computer crime" was listed as "*99" and when the dispatcher entered this code the checklist for the computer crime is incorporated.

What this allows the department to do is to begin gathering information about the crime immediately. A few moments of the dispatcher's time can merit a great deal of information that may be useful to responding units and will certainly be useful to investigators later. Figure 10-2 is a representation of the "*99" screen.

Advanced systems may further prompt the dispatcher as each of the ques-

Date:
Time:
Reporting Party:
    Name:
    Address:
    Telephone:
Incident location:
    Address:
    Description:
Nature of Incident:
When was incident detected:
How was incident detected:
Who detected incident:

Figure 10-1.

tions are completed. For instance, if the answer to the question "Is the computer still on" is in the affirmative then the dispatcher may receive a prompt telling the person to leave the system on. Other specific instructions may also be included, and these will vary greatly from department to department simply because of the protocol each department adopts.

In a few departments dispatchers are also given instructions on what actions to take to secure the scene. This typically requires special training or supervision. In those instances, though, the first steps are to protect the system from further intrusion/damage and to secure any potential evidence. This is a tough task, though, and one not always best handled by telephone. It may be enough to simply instruct the caller to "not touch anything" or to "keep others away from the system" rather then try to give complicated instructions over the phone.

When dealing with a computer network the initial response protocol may be a bit trickier. With the popularity of the "always on" type of network, such as those connecting users via DSL, satellite, cable or other connection to the Internet, there is an increased potential for contamination. The dispatcher certainly does not want to instruct the caller to disconnect the computer from the network. After all, if the caller is unfamiliar or untrained with this type of system he or she could cause damage to both the system and the potential evidence. There are, however, some basic information that the dispatcher

Is activity/incident still taking place:
Can the scene be secured now:
What hardware is involved:
Is the computer on a network:
Is the computer or system still turned on:
Does anyone have immediate access to the system:
Is there any danger to people in the area:
What physical security is present:
What is the name of the person responsible for the computer system:
Has there been a denial of service:
Has there been vandalism or damage:
Are there logs available:
    If yes, can they be safely protected from contamination?
Additional Information provided by caller.

Figure 10-2.

may be able to secure through the use of a proper protocol.

It is important that one remember that the initial assessment of the computer crime will likely come through the dispatcher or other person taking the initial call. The next step is generally taken by the responding officer, which is usually a uniformed officer in most municipal, county, and state agencies. The procedures for dealing with the initial issues that arise when one first arrives on scene can be very demanding. For that reason it is often necessary to provide at least a minimum level of training to the line level officer who may be called upon to secure a potential computer crime scene.

B. THE INITIAL CONTACT

Just as with the dispatcher, it is important that the department have a clear policy for the initial investigative response. Where the department is a municipal, county, or state agency that uses uniformed police officers it is imperative that these officers have a clear understanding of what actions to take when confronted with a potential computer crime. This means that a clear policy, with appropriate procedures, be adopted by the administration and enforced by the department's supervisory teams.

Education plays a vital role in this step as well. Not only should the investigator be educated in the science of computers but the average police officer should have at least a modicum of knowledge as well. This begins with a clear understanding of the nature of computer crime itself. The officers must understand that computer crime, unlike any other crime type, may involve evidence that cannot be seen, held, or even easily identified. They must understand that some of the evidence may be either electrons or magnetic signatures which are very fragile.

For departments that require line officers to conduct the initial investigation it is crucial that the officer understand the basics of a computer system. Many cases have been tainted simply because a police officer who was first on the scene did not realize that all the data in the RAM is lost when the computer is turned off. That data may be the key to the whole investigation, and there is no method known to modern computer science for recovering data erased from a RAM chip when the power is cut.

If an officer is not educated in the basic responses of dealing with a computer crime then it is best to simply limit their job to securing the scene. Of course this means that no one, even the officer, disturb or alter the computer system in question. This includes the movement of the mouse, removal of disks from the floppy drive bay, or even adjusting the volume on the speakers attached to a multimedia machine. Any actions, under the right conditions, may result in loss of evidence or other valuable material.

If the officer is knowledgeable of computers, and can effectively judge the extent to which the computer is compromised or damaged, then the officer should take appropriate action to protect the system from further harm. The better practice, though, is to secure the computer in the most reasonable fashion and then allow the investigators to take any action that is needed only after the computer system is safe.

C. EVALUATING THE INITIAL SCENE

To this point we have focused on the human aspects of computer crime, but it is now time to look at the physical side of the case. We begin with the initial survey of the crime scene, and like most crimes we first require that the scene be secured. Just as we have discussed a protocol for the initial human response to the crime we must also recognize that there is typically a specific set of rules for securing a crime scene.

There is little need to vary from the standard practices taken by most departments when securing a scene. The first step is generally to secure life or render aid to those who are injured. Of course computer crimes don't often have injured persons in the area of the crime scene, but there are those cases that may be out of the ordinary. As such, the first duty of the responding officers is to render aid to those who have been hurt or may be hurt.

The second duty is to protect those at the scene from potential harm. Again, there has been few cases where a computer crime suspect is also a violent criminal, but there are always exceptions to the rule. Potential harm may also include harm to property. It is important that the initial officer take immediate action to protect both life and property. These practices are not unlike those applied to any crime scene and for that reason it is not necessary to cover them in great detail.

D. THE INITIAL INTERVIEW

The initial interviews in a computer crime case are very similar to those conducted in most major crimes. There are generally three categories of people who are interviewed. The first are the reporting parties. These are persons who reported the crime but have limited knowledge of the actual crime itself. For instance, a user may attempt to log onto a computer in a common area of the company. When that user attempts to log on they instead receive a message that states; "You have been hacked." That user has little knowledge of what has occurred other than what the screen displays and the fact that they were denied log-on capability. These persons are generally inter-

viewed initially for the little information they have and there is often no need for a follow-up.

The second category is likely the most important and is commonly known as the "end user." This may be the computer owner, the system administrator, or simply the person who has been assigned that computer on the system. In a commercial setting there are typically assigned computers to certain users, and these people fall under the category of end user.

The end user is important because they are the people who have the most contact with the computer on a regular basis. In many instances these people have a working knowledge of their computer but are not "computer professionals." They have valuable information that the investigator will need, but they are not the people who will be able to adequately describe the crime or the methods of acquisition. In a non-commercial setting the end user is usually the computer owner as well, but may also be another family member, friend, or visitor to the computer site.

The third category can be the most important of those to be interviewed, especially when dealing with a network or commercial system. This category is broadly labeled the computer manager. This includes the network administrator, system technician, department manager, and others who have the duty of monitoring the computer system. For crimes such as intrusion, information theft, and similar incidents the computer manager is the person who will have access to system files and logs.

There is no set priority for interviewing any of the people from each of these three categories. Obviously, the first category of persons may be the first to be interviewed, and this may start with the initial response protocol. That is one of the reasons departments are encouraged to develop this protocol. What is said by that initial reporting party may ultimately shed some light on the whole case, but if no protocol is in place–or if it is not followed–then this potential evidence is lost.

Certainly one might argue that the third category is the most important simply because it is the most knowledgeable about the computer system itself. Of course, this will depend in large part on what event we are investigating and the involvement of the second category in the overall crime. For instance, the end user may be the most important interview simply because they are the next best thing to an "eye witness." In short, the investigator must use a great deal of judgment when deciding which of these people will receive the most attention or interviews. Each is a potential reservoir of information, but the investigator has no clear guideline to tell him which of these is the right source for the information needed.

Regardless of which category is being interviewed, it is important that the interviewer discover three very important pieces of information. First, the investigator must establish relatively quickly the expertise of the particular

person. This may be important later when examining the crime itself. For instance, if the reporting part is also the primary computer user, one would expect a certain level of familiarity with the computer system in question. When that person displays either too little or too much knowledge, the investigator may need to pay more attention to the story of this person.

The investigator must also establish quickly what involvement the person has with the computer or computer system in question. Obviously, a reporting party need not have a great deal to do with the individual computer, and the investigator who establishes this quickly can be more precise in the type of questions to ask this person. Likewise, a computer manager may be in charge of a dozen or more computers on a single network, but not have daily contiguity with the individual computer. Again, this may affect the overall interview process for that particular person, and by establishing this fact early the investigator may focus their investigation in an appropriate fashion.

The third piece of information to be obtained up front is the person's involvement in the crime itself. Is this person a witness, suspect, or victim? Or do they have some other involvement that narrows the need for an interview? One can quickly understand that a potential victim will be treated much differently from a potential suspect. The investigator who can narrow that field accordingly can conduct more effective interviews, and will ultimately produce more evidence or explanations.

Experienced investigators know that everyone is a suspect until proven otherwise. The cardinal rule of investigating any crime is to rule no one out until enough facts are uncovered to clear him or her from suspicion. With this in mind most investigators use a standard method for conducting all interviews. The method is simple, ask questions and don't suggest answers.

This method may sound oversimplistic, but the fact is that more investigations are slowed because an investigator assumed he knew the answer when he in fact did not. By suggesting an answer, often in the form of a question, the investigator is in fact leading the interviewee to a specific answer. For instance, an investigator might say, "You didn't see anything, I suppose." This is not a question, but in fact is a suggestion that the person did not see anything useful. Many witnesses will willingly take such a suggestion even though they might have seen some small item that could be useful. Because the investigator has suggested that they did not see anything, the witness admits they did not see anything. Had the investigator asked the question another way they might have gotten a much different answer.

"What did you see?" It is a simple and easy to understand question. The problem is that many investigators allow impatience or inexperience to cloud their ability. They know that people tend to meander through the tale as they are telling their version of what happened. To avoid all those irrelevant details the investigator tries to steer the interview in a direction that

might be more helpful. The fact is that such tactics often produce very little that helps and often just encourages the witness to shut up.

A skillful investigator will know when to move the witness to or away from a given topic. The open-ended question will give the interviewee a chance to explain in their own words, and the investigator can gently nudge them in the right direction.

Once an investigator has made an initial assessment of the suspected incident it is time to move to a higher level within the investigation. In most instances this means conducting detailed interviews or interrogations of all that may be involved. Depending on the particular circumstances or needs, the focus of each interview and interrogation is on gathering enough information to begin building an effective case. One of the first steps in doing this is to secure the log files from the computer, and this often takes cooperation from the system administrator, manager, or end-user.

If the log files have not been secured from the network administrator then it is important to do so as early in the investigation as possible. This prevents potential contamination as well as a chance for someone outside the investigation to destroy the files. Of course, one of the primary concerns is minimal disruption to the network system or other users, and the investigator must take this into consideration when requesting such logs. As a general rule the investigator secures a copy of the log files or obtains the original file leaving a copy behind for others to use.

To gain access to the log files, or other system files, the investigator must be especially careful not to disclose too much information to the system administrator or end-user. It is important to remember that the end-user may in fact become a suspect, as might the administrator or manager, and the key is to obtain cooperation without tainting the investigation.

If log files are examined using common system utilities, and the administrator has access and opportunity to alter these files, then viable evidence may be destroyed. For that reason it is imperative that the investigator, or his designate, closely monitor the initial work of the system administrator. This means keeping track of the person during the investigation as well as his actions around the computer system. If possible, access or use of the system should be limited to only those tasks necessary to maintain the system.

When conducting this early stage of the investigation it is likely that a suspect or potential material witness will be tipped by the investigator's actions. There is this chance in every investigation, and so all investigators must use caution and good sense when conducting any interview or interrogation. As such, the interview in the computer crime is not much different from the interview in any other crime. There are, however, some concerns when interviewing the system administrator or other person closely associated with the target computer system.

Because the system administrator can be of so much help, especially at the initial stages of the investigation, it is important that the investigator seek out the administrator as quickly as possible. Simply stated, many suspected incidents may be classified as non-incidents after a discussion with the system administrator or primary user. This is especially true when the detection of the potential crime arises from an inspection of firewall logs or other logs. Under these circumstances the system administrator can often provide information that will either confirm the suspicions or otherwise clarify the nature of the incident.

In the initial interview with the system administrator the investigator must quickly gather usable information while still maintaining investigative integrity. Sample questions and topics that should be addressed include the following:

- Have you noticed any recent unusual activity?
- How many people have administrative access to the system?
- What applications provide remote access on the system?
- What is the log-in procedure for accessing the system?
- What other logs are maintained?
- What is the network or system topology?
- What security for precautions are currently taken on the system?
- Has any user, especially those who do not normally make such requests, asked for special access privileges?
- Has any user requested anything unusual?

Chapter 11

APPLYING FORENSIC SCIENCE TO COMPUTERS

In the broadest sense forensic science is the application of science to legal issues. Forensic science applies the knowledge and technology of science for the definition and enforcement of laws. We may also define forensic science as the application of science to both criminal and civil laws that are enforced by police and criminal investigators in the criminal justice system. At the heart of this definition is the application of scientific principle and practices to legal issues. For the investigator it is imperative that they understand how forensic science is used in proving criminal cases involving computers.

If information on a computer is evidence and the investigators know what they are looking for, it might be possible to collect the evidence needed quite quickly. Swift searches are necessary in exigent circumstances; e.g., when there is a fear that another crime is about to be committed or a perpetrator is getting away. If the information is evidence but the investigators do not know what they are looking for, either a lengthy search of the computers involved will be required, or it might make sense to collect everything and search it later in a controlled environment.

In any case, the investigators must be able to prove the authenticity and integrity of the evidence collected. This means that the investigator must be

able to show:

1. That the evidence is what it is said to be,
2. That the evidence came from where it is said to have come from, and
3. That the evidence has not been altered or contaminated in any way.

This can be particularly difficult when dealing with digital evidence because it is so easily changed. The simple act of turning a computer on or off can change or destroy evidence. Therefore, it is important to be methodical, well organized, and familiar with the technology involved before beginning the computer crime investigation.

This chapter describes various methodical approaches for dealing with digital evidence. The theories and methods discussed herein apply equally to all systems. We will also discuss the application of these methods to digital evidence on different parts of computer networks.

It is crucial to understand how to deal with an individual computer as a source of evidence before venturing into the complicated domain of digital evidence on computer networks. Individual computers are a fundamental part of computer networks, and the majority of digital evidence on a network is either stored on or passing through individual computers. In short, this chapter provides the necessary foundations for understanding not only how to obtain digital evidence from a single computer but also how to obtain it from an individual computer connected to a network.

A. FORENSIC SCIENCE TECHNIQUES

In any computer investigation it is important to understand the method that will be employed for evidence collection. Like most criminal investigations the computer crime case will involve the use of forensic science to help gather evidence. The forensic sciences have long been accepted in the court system simply because they portray events accurately. The proven methods of forensic science make the investigation much easier to verify than other forms of evidentiary gathering as well.

In understanding the application of forensic science methodology, the investigator must understand the simple rules of science itself. The first rule is that an item is not declared accurate until it has met a test for reliability. As an example, chemists using forensic science methods often testify in court to the presence of a given drug, such as cocaine, and not necessarily to the quality of the drug. Because drug investigators know that cocaine and many other drugs are often diluted or mixed with other compounds, the focus is on locating the illegal substance and not quantifying the other items.

We can carry this concept into the world of computer crime in many different ways. For instance, computer log files are created routinely and contain information about acts and events made at specific times and by terminals. This will not, however, always identify the exact user of the computer terminal. As such, the forensic computer investigator must be able to identify the use of the computer, the location where the log-in was made, and the methods of logging in. The presence of a user, identified by their user name and password, may be a part of a greater combination of information such as time, date, etc.

For the investigator using forensic techniques the question is, how reliable is that information? Just as the forensic chemist must test to check for the presence of a given compound or element so too must the forensic computer investigator. In fact, some computer-generated information has been seen as so reliable that it has been accepted as direct evidence. In most cases, though, the computer-generated evidence is typically seen as circumstantial evidence which is then weighed for reliability by the trier of fact.

Scientific techniques can also be used to discern minor details that would escape the naked eye. This is an especially important part of any investigation. Additionally, using the scientific method to generate and verify hypotheses can lead investigators to suspects and additional evidence. From the forensic science perspective, there are several key aspects to processing and examining evidence. These include:

1. Recognition of potential evidence,
2. Preservation, collection and documentation,
3. Classification, comparison and individualization; and
4. Reconstruction.

As digital evidence is found, it should be collected, documented, preserved, classified, compared with other samples, and individualized. The evidence can be used to reconstruct the crime. Gaps in the resulting reconstruction often lead to additional evidence, at which point the cycle begins again, resulting in an increasingly clearer picture of the criminal act as a whole. Since each stage of this evidence processing cycle is key to this text, they are covered separately in more depth.

B. RECOGNITION OF DIGITAL EVIDENCE

Recognition of digital evidence is a two-fold process. First, investigators must be able to recognize the hardware (e.g., computers, floppy disks, network cables, etc.) that contains digital information. Second, investigators

must be able to distinguish between the irrelevant information and the digital data that can establish that a crime has been committed. Likewise, the investigator should be able to distinguish evidence which links the crime to the perpetrator or evidence which links the crime to the victim.

To get a better idea of how this works let us examine one of the more famous cases which used forensic science to prove guilt. In this example it might be easy enough to claim that a bloody glove was found in a suspect's home, but is there an additional level to prove other than simply claiming an item existed. In other words, when guilt or innocence hangs in the balance, the proof that evidence is authentic and has not been tampered with becomes essential. If the evidence cannot be readily identified then there is some question as to authenticity.

In the United States we find methods for such proof in the various rules of criminal procedure. At the federal level this includes the Federal Rules of Evidence. Each state has its own set of specific rules for proving authenticity of an item. In fact, these rules are adopted in most westernized court systems. For instance, in the United Kingdom the courts rely on the Police and Criminal Evidence Act. Similar rules are found in other countries outside Great Britain and the United States.

In each country, state, or jurisdiction where evidence is used to prove guilt, the procedures often require that the offering party prove the validity of the evidence in question. This is where the principles of science, and more specifically forensic science, come into play. Using the standards set forth by the scientific method the investigator can actually prove, often beyond a reasonable doubt, the existence of a given fact or relevant evidence.

In an earlier section we spent a great of time defining what computer crime is and what a computer is. The reason for that, as stated earlier, is that there are many computerized products that can hold digital evidence. These include telephones, personal digital assistants, palmtops, and many other devices. It is imperative that the investigator be able to distinguish between these devices, and others that are more "computer-like" so that he can verify the existence of specific evidence.

Other hardware that may contain digital evidence includes the various hand-held devices, laptops, desktops, larger servers and mainframes. There are also many forms of storage media including compact disks, floppy disks, magnetic tapes, zip and jazz disks. In addition, wires, cables, and the air can carry digital evidence that, with the proper tools, can be picked out of the ether and stored for future examination.

Exposure to different kinds of computing environments is essential to develop expertise in dealing with digital evidence. Local organizations (especially local computer science departments and Internet Service Providers) may provide a tour of their facilities. Visits can be made to local computer

stores, university computer labs, and Internet cafes. Whenever possible, the computer investigator must educate himself as to any new hardware that has reached the market. In doing so the investigator will be better prepared to identify the hardware when encountered.

Different cybercrimes result in different types of digital evidence. For example, cyberstalkers often use e-mail to harass their victims, computer crackers sometimes inadvertently leave evidence of their activities in log files, and child pornographers sometimes have digitized images stored on their computers. Additionally, operating systems and computer programs store digital evidence in a variety of places. Clearly the ability to recognize digital evidence depends on an investigator's familiarity with the type of crime that was committed and the operating system(s) and computer program(s) that are involved. Thus, the first step in recognizing digital evidence is the ability to recognize where and how such evidence may be stored, transferred, or manipulated.

C. COLLECTING AND PRESERVING HARDWARE AND DIGITAL EVIDENCE

Once recognized, digital evidence must be preserved in its original state. Remember that the law requires that evidence be authentic and unaltered. It is not enough that the evidence presented is "similar to" the evidence in the computer. It must, in fact, be the evidence. To better understand this simply think about how a court might respond if an officer were to appear with a broken test-tube which once contained the suspect's blood. "The blood is all gone, judge, but we drew blood from someone who is very similar to the suspect." How long would it take a judge to throw that case out?

With that in mind the immediate question focuses on the methods for preserving the digital evidence in question. Fortunately, the courts have given investigators some latitude in this area; especially when one considers the delicate nature of digital evidence. For that reason we can find exceptions in the rules of evidence that would allow us a printout or duplicate of digital evidence. The key is the ability to authenticate the original and certify the nature of the examined alternative.

A major aspect of preserving digital evidence is collecting it in a way that does not alter it. Special tools and techniques are available to preserve and protect the evidence. Making a copy of the file may be one of the many ways to accomplish such a mission. Others include the use of printouts, back-up disks, transmitted or copied files, and many other techniques.

Printouts and papers that could be associated with the computer should be collected. Printouts can contain information that has been changed or delet-

ed from the computer. Notes and scraps of paper that could contain dial-up phone numbers, account information, e-mail addresses, etc. should also be collected. Although it is often overlooked, the garbage often contains very useful evidence. A well-known forensic scientist once joked that whenever he returns home after his family has gone to bed, he does not bother waking his wife to learn what happened during the day, he just checks the garbage.

When a computer is to be moved, spare floppy disks should be put in the disk drives to prevent the drives from being broken in transit. Evidence tape should be put around the main components of the computer and across the floppy drives. Taping the computer will not only help to preserve the chain of evidence, it will also warn people not to use the computer. Whenever possible, investigators should write the date and their initials on each piece of evidence.

Any hardware and storage media collected must be preserved carefully. Computers and storage media are quite delicate and must be protected from dirt, fluids, humidity impact, excessive heat and cold, strong magnetic fields, and static electricity. According to the U.S. Federal Guidelines for Searching and Seizing Computers safe ranges for most magnetic media are 50–90 degrees Fahrenheit and 20–80 percent humidity.

There are many anecdotes about computer experts who religiously backed up important information carefully but then destroyed the back-ups by inadvertently exposing them to (or storing them in) unsuitable conditions. Leaving disks in a hot car, a damp warehouse or near a strong magnetic field can result in complete loss of data, so be careful.

When dealing with digital evidence (information as contraband, instrumentality or evidence) the focus is on the contents of the computer as opposed to the hardware. There are two options when collecting digital evidence from a computer: copying everything, or just copying the information needed.

If there is plenty of time and uncertainty about what is being sought but a computer is suspected to contain key evidence, it makes sense to copy the entire contents of the computer and examine it carefully at leisure. However, if a quick lead is needed, as is often the case when computers are involved, or only a small portion of the digital evidence on a computer is of interest, it is more practical to search the computer immediately and just take the information required.

When collecting the entire contents of a computer, the general concept is the same in most situations:

1. all related evidence should be taken Out of RAM;
2. the computer should be shut down;
3. the computer should be booted using another operating system that

bypasses the existing one and does not change data on the hard drive(s);
4. a copy of the digital evidence from the hard drive(s) should be made.

When collecting the entire contents of a computer, a bitstream copy of the digital evidence is usually desirable. In short, a bitstream copy copies what is in slack space and unallocated space, whereas a regular copy does not.

There is one empirical law of digital evidence collection that should always be remembered: If you only make one copy of digital evidence, that evidence will be damaged or completely lost. In other words, make a back-up of the back-up. Or, like grandma always said, "It is better to be safe than sorry."

It is imperative that digital evidence is saved on completely clean disks or write-once media like compact disks. If digital evidence is copied on a disk that already has data on it, that old data could remain in the slack space, commingling with and polluting the evidence. Whether all available digital evidence or just a portion is collected, the task is to get the evidence from the computer with the least amount of alteration.

If the focus of the investigation is only on a small selection of the information stored on a computer the "just take what you need approach" is an alternative to seizing all of the hardware or seizing all of the digital evidence on a computer. This approach has the advantage of being easier, faster, less expensive and less risky than shutting down a computer, rebooting it and making full bitstream copies.

When an investigator encounters a computer there will be several alternatives depending on the computer's condition, the operating system, and the storage devices encountered. If, for instance, the investigator finds the computer off upon arrival at the scene then the first question is whether to seize the computer and turn it on at the lab or leave it in place to search. As a general rule it is preferred that the computer be searched in place unless a warrant specifically authorizes its removal. The warrant, or exigent circumstances leading to a search without a warrant, may only authorize a search for data and not necessarily a seizure of the computer system itself. For that reason we recommend that the investigator who has obtained a warrant also obtain permission to remove the computer to the crime lab for further examination and search.

If the computer is running when first encountered the investigator should first insure that the system is not "bobby-trapped" in some way. Many users will set their computer system up so that when it is breached by an unauthorized user there will be an automatic shutdown of the system. The user may also have rigged the system to dump or destroy material on the storage media unless the new user accesses the material using a specific method.

The investigator must also focus on obtaining the information currently in

RAM. For example, if investigators notice a suspect at a computer typing a warning e-mail message to an accomplice, that message might only be stored in RAM and could be lost if the computer is unplugged. To get evidence out of RAM, all open programs must be closed and if any of them prompt to save, they should be saved to a clean floppy disk. This will prevent the program from writing over existing evidence on the hard drive, leaving both the old version and the new one intact.

The next issue is the shutdown question. Should the computer be shut down or should the search begin immediately? Much like our problems with a computer that is already off upon arrival we have a situation where the answer depends on what type of warrant or authority the investigator has. If a decision is made to shut down the computer then it is absolutely imperative that before turning it on again the computer's operating system should be bypassed to avoid corrupting evidence. Again, some users are sophisticated enough as to set up the computer with a complicated password or other protection system. Bypassing this system, usually part of the boot-up routine, allows investigators to protect the data on the system.

Personal computers store their operating system on the hard drive, and this operating system can be bypassed using a boot disk. An investigator who does not know how to make a boot disk should refer to the operating system instructions for the particular system in question. After booting the computer, digital evidence can be copied to disks or tapes. As discussed at several points in this book it is important that those disks or tapes not be used. They must be new and completely cleaned of data and viruses. Whenever possible, digital evidence should be saved on storage media that can only be written to once, like compact disks. However, it is not always possible to use a writable compact disk drive so investigators should practice using different back-up devices to collect digital evidence.

Be aware that most tape and disk drives require specialized drivers that must be loaded in addition to the operating system so investigators should do some research and preparation before using a drive to collect evidence in an actual investigation. If there is a concern that a certain tape or disk drive will not work with a specific computer, test the device on an identical or very similar system before proceeding.

As mentioned earlier, if there is a suspicion that the slack space on a disk contains important digital evidence, a bitstream copy of the data should be made. There are a growing number of products that make the process of collecting and documenting digital evidence easier and faster. These instructions apply to machines running Microsoft DOS, Windows, and Windows NT. Windows NT machines that have FAT 32 partitions (as opposed to NTFS partitions) may be treated slightly different, but investigators should make themselves aware of these differences prior to attempting any seizure

techniques.

It is important to note that NTFS partitions offer additional security on a Windows NT machine by restricting access to data on the disk. The restrictions that NTFS imposes can make it more difficult to gain access to all of the data on a hard drive, and for that reason we will treat this issue separately.

As mentioned, Windows NT has a higher degree of security that can make it more difficult to collect digital evidence. Windows NT enables a number of individuals to use a computer without having access to each other's files. This is achieved by creating separate password protected accounts for each individual who uses the computer. This added protection can interfere with evidence collection.

Fortunately, it is possible to bypass the restrictions that Windows NT attempts to enforce. Some investigators use a boot disk that contains an operating system called Linux to bypass Windows NT and give them access to the entire contents of the hard drive(s) on a computer. Alternately, a boot disk containing DOS data collection software and operating system can be used to bypass Windows NT. In many instances by simply bypassing NT the investigator can access the hard disk with little or no concern for loss of data.

There is one caveat: it is possible to configure Windows NT to prevent booting from another disk–in which case more advanced methods will be needed to gain access to the digital evidence on the computer. In those instances it is important that the investigator be familiar with NT and be familiar with the methods for circumventing this protection scheme.

D. CLASSIFICATION AND COMPARISON OF DIGITAL EVIDENCE

Classifying digital evidence is the process of finding characteristics that can be used to describe it in general terms and distinguish it from similar specimens. An item is classified when it can be placed into a class of items with similar characteristics. For example, firearms are classified according to caliber and rifling characteristics and shoes are classified according to their size and pattern.

Most individuals are familiar with e-mail messages and will be able to say, "This is an e-mail message" the moment they see one. With training, investigators can classify e-mail even more precisely–determining what application was used to create it. Similarly, graphics created using computers are similar to each other in many ways, forming a class, and there are different types of graphics files (e.g., JPG, GIF, TIFF) making it possible to be specific when classifying them.

The importance of classifying digital evidence is often overlooked because

it cannot be directly associated with a specific individual or computer. However, classifying digital evidence is useful when reconstructing a crime because it provides additional, reliable details. The value of classifying physical evidence lies in its ability to provide corroboration of events with data that are, as nearly as possible, free of human error and bias. It is the thread that binds together other investigative findings that are more dependent on human judgments and, therefore, more prone to human failings.

There are many kinds of digital evidence that most individuals are unfamiliar with and will have difficulty classifying. For example, there is a class of computer programs called scanners that computer crackers use to probe a computer for information and vulnerabilities. There are many different types of scanners and few people have seen every kind. Therefore, it is often necessary to closely examine a piece of digital evidence and compare it with other samples before one can say, "This is a scanner" with any degree of certainty.

Also, if digital evidence has been damaged in some way, it might not be immediately obvious whether it was a computer graphic, a program, or some other type of digital data. Comparison is key when examining digital evidence. In addition to revealing class characteristics, comparing a piece of digital evidence with a control specimen can highlight unique aspects of the digital evidence (individualizing characteristics). Some individualizing characteristics are created at random–like a flaw in a particular piece of computer equipment that was used to digitize child pornography. Other individualizing characteristics are created purposefully for later identification (e.g. an identification number associated with a computer). These individualizing characteristics of a piece of digital evidence can be used to link cases, generate suspects and associate a crime with a specific computer.

In understanding this we can see how classification has helped investigators in the past to solve computer crimes. For instance, in 1999 the Melissa virus hit the Internet. Melissa traveled in a Microsoft Word document that was attached to an e-mail message. This virus propagated so quickly that it overloaded many e-mail servers, and forced several large organizations to shut down their e-mail servers to prevent further damage.

Richard Smith, president of *Phar Lap Software* tracked down the individual who created the virus. Smith used a feature of Microsoft Office 97 to verify that the suspect's computer was used to create the virus. Any files created using Microsoft Office 97 contain a hidden line with a unique number identifying the computer that was used to create the file. The suspect had not considered such an identifying mark and through his ability to classify the data Smith was able to trace it as well.

Of course, creating a unique signature on every piece of data we create raises several interesting issues related to privacy. While investigators caught

a glimpse of a hopeful future in which catching criminals was facilitated by the very tools that criminals use there were those who claimed that such high-tech branding was just another form of corporate oppression. Of course this is a debate for other times so we will move back to the topic at hand.

Digital evidence can be classified, compared and individualized in several ways:

1. **Contents**–investigators use the contents of an e-mail message to classify it and to determine which computer it came from. Also, swap files and slack space contain a random assortment of fragments of digital data that can often be classified and individualized.
2. **Function**–investigators examine how a program functions to classify it and sometimes individualize it. For example, a program that surreptitiously transfers valuable information from an unsuspecting computer to a remote location is classified as a Trojan horse program. These programs are individualized by the remote location to which it transmits data.
3. **Characteristics**–file names, message digests, and date stamps can be helpful in classifying and individualizing digital evidence.

Although the process of classifying, comparing and individualizing evidence can be tedious, it is extremely important to examine digital evidence in minute detail. The smallest clue can often have significant bearing on a case. Also, it is crucial to be able to describe accurately and completely your evidence when called upon to do so in a court of law. Any lack of understanding could damage an investigator's testimony, particularly if the minutiae turn out to be important. Although it can be tedious to study each piece of digital evidence carefully, it is far better to be bored with the evidence than to be stuck with no evidence at all.

Chapter 12

TRACKING THE OFFENDER

Just a few years ago the thought of tracking a criminal across an electronic matrix was the stuff of science fiction. Then came the internet and just about every business and individual in North America was linked through their computer. With the popularity of wireless connectivity growing each day more and more people are now connected through their cell phone. Tracking a computer criminal requires an expanding base of knowledge for almost every police officer.

The first issue to address is the concept of computer connectivity and true network tracking. At the outset it is important to note that computer connectivity, network systems, and the expanding opportunities for connection through cell phones and other wireless devices is worthy of several volumes of investigative texts all to its own. For the purposes of this treatise we will

restrict the material to those basic ideas and applications that the average investigator is likely to encounter. We begin our discussion of tracking the offender with some background on the use of the TCP/IP system and basic computer network operations.

A. BASIC NETWORK SYSTEMS

A network is a collection of individual computers linked together in one of many different patterns. The most common network is the Local Area Network (LAN) which is a system of interlinked computers within relatively close proximity to each other. For instance, many business connect computers for shipping, accounting, inventory, warehouse, and management together. This system allows users to track products or inventory and to easily communicate together.

Individual networks can be linked to other networks. In some instances multiple individual networks are linked so that users at remote locations can have access to each others' data as well as communicate more efficiently. These networks, often referred to as *Wide Area Networks* (WAN), allow the network environment to expand, and large systems of interconnected networks are commonly called *intranets.* An intranet is a large system that typically remains connected to only a limited number of smaller networks.

Ultimately, a user may connect the individual computer or small network to the *Internet,* which is the largest network system in the world. The *Internet*–not to be confused with an *internet*–consists of multiple independent networks connected through a major system of *backbone networks.* Each backbone provides direct links to other backbones within the system, and by connecting to a single backbone the user now has access to millions of other computers and networks.

To make all this connection work the computer industry has adopted standards or protocols. The most common protocol used in the network system is known as the TCP/IP, which stands for *Transmission Control Protocol* (TCP) and *Internet Protocol* (IP). Early network developers realized very quickly that true connectivity, the ability to connect independent or individual computers together, would rely on a clearly defined protocol, and the TCP/IP is accepted worldwide. For the investigator, understanding the basics of the TCP/IP is the first step to a successful track and investigation.

Initial development of the procedures began in the 1960s and has continued on a steady pace since that time. With the introduction of the Internet the protocols grew in power and capability. To be most effective the protocols were specifically designed so that they would not be hardware dependent. In other words, they are designed so that they will work equally well

whether we are using a Mac, Windows, UNIX, or just about any other operating system or computer. There is one key, and that is all hardware and software must comply with the standards in order to work at the peak of efficiency. That is also where we might find our first computer issue for both modus operandi and computer crime typology.

For our purposes it is important to know that the system works primarily through the Open Systems Interconnection (OSI), which is a seven-layer Network Reference model. A model developed by ISO (International Organization for Standardization) to allow computer systems made by different vendors to communicate with each other. The goal of OSI is to create a worldwide open systems networking environment where all systems can interconnect. Most communications protocols today are based on the OSI model. The OSI model defines a framework for communications which has seven layers:

1. Physical layer
2. Data link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

Control is passed from one layer to the next. A communication begins with the application layer and then proceeds through each layer as required for the specific tasks. As an example, a user opening an application and typing a request would begin the process with the application layer. The communication is then passed through each of the seven layers down to the physical layer which is the actual transmission of bits. On the receiving end control passes back up the hierarchy.

While the traditional criminal investigator need not necessarily know the seven layers, or even how they work, it is important to understand that they are a part of the larger system. More advanced investigators will certainly want to understand the system in some detail, especially if they intend to investigate more than one crime or related incidents. It is also important to note that use of the layers requires knowledge from certain skill sets, and this may be another item worth considering as one compiles the facts. A computer criminal that manipulates or in some way uses the OSI to hide, or in the alternative enhance, his efforts has certainly left a unique calling card.

Both internal (Local Area Networks) and external (internet) networks rely on the seven-layer model, and many network-oriented tasks must meet those standards of application. This is also important since it means as a computer

forensic investigator you must understand the differing levels of hierarchy or services that are being used. To get a better understanding of this we can utilize an example where email is used to access data across the network.

B. THE BASICS OF TRACKING

Tracking of the computer criminal can be one of the most involved and difficult tasks any investigator can face. An investigator working a burglary case may have physical evidence such as fingerprints to help track a suspect. With the computer crime case physical evidence is a rare commodity, and investigators are often left to track the suspect in an electronic environment rather than a physical one. That does not mean, though, that a computer criminal will not leave evidence of their misadventure behind. The opposite is quite true, and for the investigator knowledgeable in the type of electronic evidence left, the track can be just as effective as any other criminal investigation.

Because most computer crimes now occur through the use of some sort of network, it is important that the investigator understand the basics of network technology. That is why the first part of this chapter focused on that topic. We will also use this basic information to set the foundations of computer crime tracking, and for our purposes the most common forms of tracking will arise with email or network connection.

Each time an email message is sent or received it involves no less than three different addresses. Each address in the email is contained within a different network (OSI) layer. In addition, every network interface card has a unique hardware address burned into it at the factory. This address is called the *MAC,* which stands for *media access control.* By knowing this address all of the devices on a network segment (such as a LAN) can quickly identify any other device.

We can think of a network interface as a small mail box designed to look for mail (or data) sent to that address. Each individual device not only knows its own label but can identify the labels of other devices on the local network. This is done through use of the MAC address incorporated within the dataset on the network. Think of it like a unique street address on a box being sent via United States Postal Service. When the postal truck comes by the house the address is recognized and the mail box opens to receive the box. In computer terms these are called packets, and each packet contains the address or MAC for that particular network segment.

The MAC address is certainly useful in determining which piece of hardware on the network will receive the packet. It is also useful to the investigator since it is the final address needed to pinpoint the specific computer that

sent out or received the packet in question. In other words, if the investigator knows the MAC then the individual computer is also known. Unfortunately, the MAC is likely the last piece of information the investigator will use in most tracks, so we must also understand the larger system of communication.

Because there can be hundreds if not thousands of hardware MAC addresses on a small closed network, the use of MAC address alone is very limited. When we expand the network, especially by linking to the Internet, the number of potential MAC addresses increases exponentially so that the sheer number makes the use of MAC alone ill advisable.

1. The IP Address

Simply stated, it would be impossible for every device to know the address of every other device on the entire Internet. There is a system that does allow these addresses to be set into an easily defined locator system, though. This system is known as the IP address, and it is usually written as a series of four numbers separated by dots. Each of the numbers has a value of 0–255, and an IP address will look something like this: 192.168.152.245.

The system also uses a set of reserved numbers for IP addresses. As a rule, IP addresses that end with 0 denote a network address. Network administrators can set "private addresses" on the internal network by using the last series such as 192.168.0.0 to 192.168.255.255. Note that this is specifically being set up for an internal (closed) loop network, so the IP addresses above cannot be accessed from outside sources. The reason we must point this out is that once connected to outside sources, such as the Internet, we would find that this range of addresses is likely assigned to somewhere very different from where we thought.

What this means is that as you begin the investigation you may find yourself with different IP addresses from different sources. Be careful not to confuse a single IP address with either a closed system or the broader Internet itself. You will likely want to use one of the many lookup services available to track the IP address, and you will certainly want to use it only in the context that it exists with other identifiers.

Each Internet address contains two distinct parts, the network and host. The network portion is unique among all the networks interconnected on the system while the host section is unique among all the devices using the same network portion. What this means is that an IP address from the broader Internet—or other interconnected network system—will have an IP address which identifies the address within that system. If we close the network system then we can usually use network IP addresses which might otherwise already be in use. So long as that closed system remains closed we can assign

them as necessary, but once open they will conflict with those already assigned on the broader or open network.

What this boils down to is that within a small network the IP itself may identify the individual computer. For example, if in a LAN the IP address is set for each computer then the knowledge of the individual IP address –usually obtained by looking at the packet addresses–will lead us to the right computer. This breaks down, though, when the network expands. Inside the LAN the IP address may have specific meaning, but because the LAN itself is connected to a larger network that IP address may be useless.

2. The Internet Service Provider and Whois

When connecting to the larger network the point of connection becomes its own IP address. Thus, a single computer user on a home PC may connect to the *Internet Service Provider* (ISP) as part of that enclosed system. The ISP is linked to a larger connection, or to a backbone within the Internet, and the ISPs link has its own IP address. In this way, the larger Internet identifies the individual IP of the ISP, which is used for sending packets to and from the Internet. When the home user sends a file then the packet has the initial IP of the user, but when it is ready to send over the larger Internet the ISP's system will alter the packet to include the ISP's address. Thus, the IP for the single user is no longer valid since it has been replaced or altered in the protocol for identification (routing) to the ISP instead. It is only within the ISP's network that the original IP address applies.

While on the topic of IP addresses it is worthwhile to note that all IP addresses used on the Internet are logged and maintained by various organizations around the world. If you are working within the United States these addresses are maintained by the *American Registry for Internet Numbers* (ARIN), which has a lookup service commonly referred to as the "whois" directory. One can find the registry online at http://www.arin.net.

Use of the ARIN lookup service takes some practice, and queries should be well formulated in order to increase the ability to find the right address. The ARIN database contains resource records, which contain network (IP address) and autonomous system numbers. The ARIN database does not contain U.S. Military, investigative agency, and addresses outside of the United States. For addresses outside the United States one must use one of the other lookup systems which can be easily located using a traditional search engine. Simply look for "whois" or "IP address lookup" to find the services around the world.

Coming back to the unique nature of each address we can note that the use of a network and host numbering system allows the various routers, gateways, and connectors in the larger networks to move packets along the net-

work. Like the NIC, each router or gateway has its own MAC, and depending on the location with the network system may have its own identifiers within the larger framework.

3. The Route Through the System

An oddity of the system is that there is no single route between any set of computers. The Internet is so vast, and there are so many different routes that can be taken trough the system, that the protocols seek efficiency through a system of varying routing sequences. In other words, unlike a mail truck on a normal street the router may not always choose to use the most expedient route to a given address. Where the mail delivery system tends to send the truck around the route in a well-defined pattern, even if there is no mail for a single address on that route, the router works in a much different fashion.

As a message is created and sent from the individual computer it will be passed along to the "next available" point along the many paths of the network. The focus is on activity and not relative distance along the network pathway. This is because the electronic messages travel at near light speed along the wires or wireless connections. The amount of time "wasted" by going through an open–but distant–part of the system is negligible compared to that wasted while waiting for a closer part of the system to open up.

What this means is that each message is passed along the network according to open segments. This is very unconventional since it means that we will not find an easily defined loop in any message system. When a router receives a packet it will note the IP address, and the router will then send the packet either to the appropriate address within that network or onto another router in the larger system. We can think of it this way–if a letter is sent from New York City to Cedar City, Utah, the address will include the name of the person intended, their house number with street, the city, state, and a zip code. If the postal system were a router the first stop the letter makes would be the originating post office.

The originating post office would identify the letter as being sent outside of its network (not staying in New York) and would forward the letter to the next stop along the way. Instead of looking for the most direct route, though, the system will simply look for the next available point in the system. In such a system the letter would not go from New York to Kansas City to Utah which may be the most logical in terms of direct link. Instead, if the Kansas City station is busy the New York station would send the packet to whichever stop is not busy.

New York may find it is Los Angeles that is actually open, and instead of waiting for Kansas City to open the message goes all the way across country

literally missing the stop in Utah along the way. Again, speed is determined not by how fast the message can travel down a given set of wires but by how fast the next router can send the message along to the right stop.

At each stop the router for that office would determine where to send the letter next. If the letter is destined for a final stop not on that part of the system, the letter is forwarded again. Eventually it stops at a router or gateway which does have a direct connection to the intended network address, and at that time it would leave the main Internet and enter a smaller internet. Again, each stop along the way simply looks to see if the message is intended within that internet, and if not, it is sent along to the next station. If it is, it will be dropped into the next level of the network system.

As one can quickly see, this system typically means that no two messages sent from the same address to the same destination will go along the same path. Each message takes a path according to the protocol, and that protocol is designed to speed the delivery based on open or readiness rather than direct links.

Routers base their decision on where to forward a packet on current conditions of the network–is there traffic along a given path as compared to another–and on their programmed instructions. Thus, if a packet is being sent through a planned route with instructions being given at each stop for a specific new route, the letter will travel a known route. Otherwise, each router in the system will simply pass the letter along to the next router, which then determines whether it stays in that network or goes on to another.

4. Assigning Addresses

The network part of an Internet address is assigned by the Internet Assigned Numbers Authority (IANA; http://www.iana.org). By using these assigned numbers the routers can know which place to send the packet based on network address alone. Once the packet gets to that network hub the host address is needed. All hosts addresses are assigned by the network owner, and the packet is then routed internally from the host's router to the specific address. The common address is that which is assigned to an Internet Service Provider (ISP) and within the ISP's network are the various customer addresses. In this sense the original message is sent to the host (ISP) address, and once there is routed by the host to the individual customer's address.

A computer which uses the same IP address is said to have a *static address.* A static address–also known as a dedicated address–remains the same and never changes. Most large companies or service providers use a static address, as do most ISPs. If the user is not going to move or make changes the static address is a good idea. If the user is mobile, though, a static address will not work since the movement of the computer means that connections

to the network will change.

For computers that do not need a static IP address we use what is known as *dynamic* IP. This means that the address is assigned by the host when the computer connects and it will change every time the computer logs in. Each time the computer registers itself on a network a protocol called the *Dynamic Host Configuration Protocol* (DHCP) assigns it an IP address from those available. Most, if not all, ISPs use DHCP to assign addresses to their customers. The downside of this trend, at least from an investigator's perspective, is that DHCP addresses change so quickly and are much harder to trace.

Understanding how the IP address works we can now move back to the question of the MAC address. Remember, in some instances the IP address may not be permanently assigned to the suspect's computer. These dynamic addresses will certainly lead you to the network, but once at the network portal the rest of the job may fall back onto the MAC address. In other words, the sequence of the IP address may lead you to the ISP's doorstep but not the suspect's. To get the rest of the way you must identify the potential address locations, including those within the LAN segment. It is also important to remember that even inside the LAN the MAC address is not used in the formal sense. The MAC address is actually used at the hardware layer, so when a process or application "up stream" or "up the stack" specifies another device on a network segment by IP address, it has to be translated into a MAC address.

To make these conversions the system uses the *Address Resolution Protocol* (ARP). The ARP runs in the background, invisible to most users, and is essential to the operation of the network itself. The ARP is a method for finding a host's *Ethernet* address from its Internet address. An ARP request is sent to the network, naming the IP address; then the machine with that IP address returns its physical address so it can receive the transmission. On a typical LAN the various computers are rather busy communicating with each other even when the computer user is not intending such exchanges. The computers, along with routers, etc., compare usage, routing information, network conditions, and often simply communicate as a way of verifying that someone else is out there.

This constant exchange of information on the open network connection means that the potential suspect is always susceptible to capture even when they are not performing the criminal acts. In other words, if you have the IP address, can track to the network, and can then use the MAC within the network you can locate the proper computer even if they are using a dynamic IP so long as the device that sent the packet with the suspect address connected. These devices, by their very nature, confirm the existence of each other, and this makes them rather easy to eventually track down.

C. THE DOMAIN NAME SERVICE (DNS)

Most readers have likely used the Internet or a network system at some point. We are very familiar with the use of different computer software to access the network. The most common form of software is the *Web Browser.* This is a program such as Mosaic, Netscape, Internet Explorer, and others that is used to view pages on the World Wide Web. When we use the browser the common interface for the user is to type in a web address, and these normally use plain language rather than the true IP address.

The plain language web address typically has three important parts. The first part (prefix) is the identification for the protocol being used in the communication sequence. The term "HTTP" is often seen, and this stands for *Hypertext Transport Protocol,* which is the primary language used on web pages. There are other protocol identifiers that are used as well, and these include "FTP"–File Transport Protocol–and a secure version of the HTTP which is designated as HTTPS.

The second is the domain identifier, and this is the name of the service. We typically see the domain name preceded by the "www" identifier, which tells us that this is a location on the World Wide Web. It is useful to note that in recent years some domains have been created which do not need the "www" part in the name, and most browsers today will assume that "www" is intended if left off by the user.

The last part of the web address is part of the *top-level-domain* identifier, and this tells the user where the domain fits within the system. The most common is the "com" designation, which means the site is commercial in nature. Other identifiers include "org," for organization, and "edu," which stands for education. New identifiers have been added as well, and these include: biz, tv, info, and others.

The Internet Assigned Numbers Authority (IANA) currently classifies top-level domains into three types:

1. *Country code top-level domains*–used by a country or a dependent territory
2. *Generic top-level domain* (gTLD)–used (at least in theory) by a particular class of organizations (for example, com for commercial organizations)
3. *Infrastructure top-level domain*–the top-level domain arpa is the only one currently being used.

While this system certainly makes the addresses human readable the reality is that computers refer to each other in code using numbers of other designators. Fortunately, the computer industry has established as part of their protocols the ability to list and cross-list domain names and address identifiers. This means that a human does not have to memorize a series of num-

bers but can use words and human readable forms instead. This all comes together using a system known as the *Domain Name Service* (DNS).

D. USING THE DNS IN THE TRACK

The DNS is a global database which can be accessed from any point on the Internet. It provides investigators the mapping techniques that allow the conversion of the human readable name (www.suu.edu) to the corresponding numeric IP address. As an example, if I were looking for the IP address of my employer (Southern Utah University) then I would look up the human readable Internet address (www.suu.edu) to find the IP address of: 134.250.2.3.

There are many services today that provide this type of look-up service, and one of these is Network Solutions (www.networksolutions.com). Users access the database online, and by entering the human readable form the system tells you the name of the server, the IP address, the registrant, and the contact person.

Finding the owner or contact for each domain is an important part of the investigation since it gives you at least someone to contact in the search. The owner of each domain is responsible for placing all host names and corresponding IP addresses on a name server so that outsiders can resolve their names. Most name servers also support *reverse look-ups,* which is the process of providing the human-readable domain name that corresponds to a specific numeric IP address.

It is important to note that while the domain registrant is responsible ultimately for the domain that does not mean they are always the responsible party for the particular criminal act in question. Many ISPs are domain registrants, and they provide, as a part of their service to the customer, an ability to create a home page or use the domain registrant's computer for access to the Internet. In such a case what the investigator will find is the IP or DNS registers to one part, but it may be the customer of that party who actually committed the offense in question. For that reason having the IP or DNS does not close the door on a suspect, but like most forms of circumstantial evidence can certainly be use to link the suspect to the crime in question.

A domain name usually consists of two or more parts (technically *labels*), separated by dots. The rightmost label conveys the top-level domain as described in the preceeding paragraphs. One of the first steps for tacking any data sent is to identify this identifier. By knowing the type of domain (.com, .edu. etc.) we can already begin to narrow our search or track.

The label to the left specifies a subdivision or subdomain of the domain above it. Note that "subdomain" expresses relative dependence, not absolute

dependence: for example, iacp.org is the domaina and subdomain of the International Assocation of Chief's of Police. The identifier "iacp" comprises a subdomain of the "org" domain. It is also possible for the IACP to form a subdomain of the domain iacp.org. In theory, this subdivision can go down to 127 levels deep, and each label can contain up to 63 characters, as long as the whole domain name does not exceed a total length of 255 characters.

As noted above, the leftmost part of the domain name expresses the hostname. The rest of the domain name simply specifies a way of building a logical path to the information required; the hostname is the actual target system name for which an IP address is desired. Staying with our IACP example we would find that the domain name www.iacp.org has the hostname "www."

The DNS also consists of a hierarchical set of DNS servers. Each domain or subdomain has one or more authoritative DNS servers that publish information about that domain and the name servers of any domains "beneath" it. The hierarchy of authoritative DNS servers matches the hierarchy of domains. At the top of the hierarchy stand the root servers: the servers to query when looking up (resolving) a top-level domain name.

1. Recursion

We can get a better understanding of this system by working through what is known as a recursion. In this example we need to find the IP address of www.iacp.org. The first step is knowing where to find the root servers; administrators of recursive DNS servers manually specify (and periodically update) a file called the root hints zone which specifies the IP addresses of these servers.

The process starts by the recursor asking one of the root servers–for example, the server with the IP address "198.41.0.4"–the question "what is the IP address for www.iacp.org?" The root server replies with a delegation, meaning roughly: "I don't know the IP address of www.iacp.org, but I *do* know that the DNS server at 204.74.112.1 has information on the org domain."

It is important to pause at this point to make sure that we understand that any domain inquiry such as this is completed in the background and not easily observed by the user. There is a tremendous effort to make the use of the Internet and networking in general more "user friendly." As such, some of the items discussed are not easily accessible, nor are they something a true amateur would understand. With that in mind we can move back to the process of tracing or recursing.

The local DNS recursor then asks that DNS server (i.e., 204.74.112.1) the same question it had previously put to the root servers, i.e., "what is the IP address for www.iacp.org?" It gets a similar reply–essentially, "I don't know

the address of www.wikipedia.org, but I *do* know that the DNS server at 207.142.131.234 has information on the iacp.org domain."

Finally the request goes to this third DNS server (207.142.131.234), which replies with the required IP address. This process utilizes what is commonly referred to as *recursive searching*. To the average user recursive searching makes no sense, but to the computer science industry it is a great way to find something without actually knowing where to look. As we see in this demonstration, each step did not necessarily produce our needed information, but it did provide us with a way of searching elsewhere.

We can think of recursive searching along the same lines as almost any criminal investigation. Rarely do we have a true "who-done-it" crime that allows us to immediately find our suspect. As a rule, the investigator must make several inquiries with each leading to a new lead or potential information point. Taken alone, each of these inquiries may not seem like much when it comes to identifying the true suspect. When taken together, though, the questioning of one witness often leads to another, and this compilation method is much like recursive searching.

Reading the example above, one might reasonably wonder: "how does the DNS server 204.74.112.1 know what IP address to give out for the iacp.org domain?" In the first step of the process we noted that a DNS recursor has the IP addresses of the root servers more-or-less hard-coded. Equally, the name servers that are authoritative for the Top-Level Domains are not changed or altered normally. This means that once a domain or IP address is inserted into the system it will likely remain there for an extended period of time. And each inquiry along the various routes will add to the ability of the recursive search method in finding it.

As part of the process of registering a domain name (and at any time thereafter), a registrant provides the registry with the name servers that will be authoritative for that domain name; therefore, when registering iacp.org, that domain is associated with the name servers for the ".org" registry. Consequentially, in the example above, when the server identified by DNS receives a request, the DNS server scans its list of domains, locates iacp.org, and returns the name servers associated with that domain.

Usually, name servers appear listed by name, rather than by IP address. This generates another string of DNS requests to resolve the name of the name server. When an IP address of a name server has a registration at the parent zone, network programmers call this a glue record. By using these links and connections the investigator begins the track simply by having the DNS or IP address.

2. Other Addresses

There are other methods for identifying the potential suspect, and one of the address protocols that has become more prominent is the Application Address. The *Application Address* (AA) is another layer in the model, and services components such as email, web browsing, ICQ, and Internet Relay Chat (IRC).

One example of the AA as used in the investigation is found when someone uses email. The email message contains a two-part address that includes both a mailbox and a domain. The typical email address looks something like this: The first part of the address (cfranklin) contains the mailbox and the part following the ampersand (@) is the domain. This convention is part of the AA and can be a simple way track. Of course, this assumes the suspect has not masked or hidden the true email address which is a common trick today. We will see in later sections a bit more on how to track these addresses.

We have already been using another of the common AA when we used the human readable Internet addresses above. These are actually known as the URL, or Universal Resource Locators. These are used by web browsers to locate web pages and Internet links. Like the email, the URL contains specific information on domain, user, and the type of communication protocol. As discussed above, the most common is the Hypertext Transfer Protocol (http) which is seen before many URLs.

E. WHY ARE ADDRESSES IMPORTANT

For the investigator the address may be the method for tracking the offender. It is much like the address of a home or business. If we know the address of a counterfeiter then we can go to that address to seize the equipment and arrest the offender. While we cannot use a computer address to actually arrest the offender we can at least use it to trace him or her to a server location.

In cases such as child pornography the address is very important. Not only can we find the stored pornographic material in many instances but we can find the location where the suspect is accessing the Internet. Because most pornographers cannot afford their own direct connection to the Internet they are forced to use an ISP. The address of the ISP will link us to the offender, and in most instances the ISP is ready to cooperate in order to keep their site open.

Another reason addresses are important is that they will show the methods used by the computer suspect to commit the acts in question. For

instance, in mail scams–such as the current bank fraud scams hitting the email systems–the DNS, URL, or IP addresses are normally faked or run through various cover addresses. It usually takes awhile, but even with simple programs such as ping or Trace-route the investigator can find a surprising number of links back to the suspect. Knowing those addresses, how they are created, and how they are used in the larger system is a key to being able to track the suspect.

F. THE ART OF THE TRACK

Now that we have covered the basics of how the Internet and most network systems work it is time to move on to the actual investigative tools used today. By understanding the basic internet applications protocols we can better understand how the system works. We can also better identify, and later testify about, the potential criminal.

The first of the systems to understand is that used in the common email. Programs such as Outlook, Notes, Eudora, and other email programs are considered to be "client applications," which means that the software is intended to work as a client of the network server. Today most email programs actually interact with two different servers in that they deal with one server for outgoing mail and another server for incoming mail. To read mail the program uses one of the three different protocols:

- Post Office Protocol (POP)
- Internet Mail Access Protocol (IMAP)
- Microsoft's Mail API (MAPI)

While the specific protocol being used to gather incoming mail is usually immaterial it is important that the investigator at least know what the three are in case there are questions by the defense. One might think of this knowledge much like that possessed by a good robbery detective. The detective does not have to be a certified gunsmith to know the difference between the Smith & Wesson and a Colt. Knowing that they are different is often enough, and when necessary can help establish at least a level of competency as well as evidence.

One important distinction worth noting is that POP users have an option when viewing email. The email is stored on the network server and the user has the option of downloading a copy of the message, leaving the original on the server, or downloading the copy and deleting the original. Thus, the POP user has an option of storing the email on the network server, which means there are traceable messages on that server, or deleting it so that only the

copy on the user's computer remains.

One reason there is a difference between the download programs is that some prefer to leave the copies on the network server for easier backup. The best example is mail coming into a corporate server. This email, usually related to the corporate business, can be backed up all at once, with copies of all mailboxes being stored in a central location. In this way the loss of data from a user's computer will not necessarily jeopardize the copy on the corporate server. For the investigator this is an important piece of information about mail systems since it means that even if the suspect has deleted the message there is likely a backup somewhere within the corporate information system.

While incoming mail has specific routines and tracking systems associated with it we should also note that outgoing mail has its own methods. Outgoing mail generally uses a completely different protocol from incoming. The protocol is known as *Simple Mail Transfer Protocol* (SMTP), and unlike protocols for incoming mail SMTP does not require any authentication. We can think of SMTP along the same lines as the local post box on the corner. Anyone can drop mail in without need for authentication or registration.

One of the first tricks any hacker learns is how to manually send an email message by "telneting" to port 25, which is the SMTP port, on a domain server. This is relatively simple, and allows the hacker to tweak or alter the headers to the email message. This generally means that the hacker can alter or fake the origination and return addresses. For more information on how to use the port 25 hack turn to Appendix D.

The more current versions of SMTP have identified problems with this type of access and there have been some significant changes that will help the investigator. One of these is the use of IP address tracking by the SMTP server. Each time a server connects the SMTP protocol allows the connecting server's IP address to be logged. Because of this the investigator could legitimately track even an anonymous email message by simply tracking the IP addresses of each server as they log in to each other.

Service providers have also caught onto the trick used by *spammers*–those who send unsolicited commercial email–to use their systems as a "free relay station. Many ISPs now limit the SMTP access their servers allow to only those IP addresses that are known as valid. This is usually accomplished by simply limiting the range of IP addresses.

It is also noteworthy that many of the *anonymous remailing* services now provide the originators IP address as part of the mail message header. While the "anonymous" part of the service remains true–the receiver won't have the real email address of the sender–the inclusion of the IP address certainly helps to track the sender.

G. TRACKING THE MAIL TRAIL

The first investigative step in tracking anyone using email is to obtain the actual email header. To do this one must first know what type of email reader is being used and how it handles the header. Most *email clients* now hide the header since most users do not need the information from it. The mail reader may simply show the sender's email address–if one is listed–and maybe the time/date the message was sent. There is much more to the header than that, though, and the investigator must know how to get to it.

If the user has Microsoft *Outlook Express* as the mail client then the mail header can be displayed with some simple changes. Go to "file" and click the "properties" button. A dialog box will appear, and the message header information will be in that box. There should be a tab for "General" and "Details." Using both tabs allows the user to see the message header. A similar method is used in other programs, and in most instances the message may look something like this:

X-Original-To: cfranklin@infowest.com
Delivered-To: cfranklin@infowest.com
Return-Path: doc_cj_cf@yahoo.com
Received: from psmtp.com (exprod5mx120.postini.com [64.18.0.34])
by mailbox.infowest.com (Postfix) with SMTP id BAA42CB5B17
for <cfranklin@infowest.com>; Sun, 23 Jan 2005 16:38:37 -0700 (MST)
Received: from source ([206.190.38.49]) by exprod5mx120.postini.com ([64.18.4.10]) with SMTP;
Sun, 23 Jan 2005 15:38:37 PST
Received: (qmail 13711 invoked by uid 60001); 23 Jan 2005 23:38:37 -0000
Comment: DomainKeys? See http://antispam.yahoo.com/domainkeys
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=s1024; d=yahoo.com;
Message-ID: <20050123233837.13709.qmail@web50208.mail.yahoo.com>
Received: from [209.33.192.117] by web50208.mail.yahoo.com via HTTP; Sun, 23 Jan 2005 15:38:36 PST
Date: Sun, 23 Jan 2005 15:38:36 -0800 (PST)
From: Elbert Davis <doc_cj_cf@yahoo.com>
Subject: Test Message for Book
To: cfranklin@infowest.com
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
X-UIDL: a4619e3e871fda8c19c7b848c7ff2535

Clearly the header contains a great deal of information which may appear to be more gibberish than useful information. By knowing what we are look-

ing at, though, the investigator can gain some useful information from just the message header. In this example we can see that the message was intended for and sent to the author's personal mail address. It was also sent using a readily available mail service through the www.yahoo.com domain, which is identified from the text, *Return-Path:* doc_cj_cf@yahoo.com.

What is also important is that we see that the message went through several different servers, and each time the label "Received" was added by the new server. Each server identification helps us to see where the message has been and can ultimately be used to help track this message. It is not just the header that can be used, but as we will see in later sections it is also the logs at the server sites that become important. Sadly, each of the individual servers could be bogus, and one of the toughest jobs for the computer crime investigator is running down all of the potential servers as one tracks the message to its original source.

The good thing is that even if the server name is bogus you will have the IP address that the user was assigned. By using the IP address the investigator can also contact the ISP or company where the message "bounced" or originated. Even if they will not disclose the IP address immediately you can request that they save the logs so that when you return with the warrant it will be available. Most ISPs and companies will cooperate relatively quickly, though.

Even when you cannot obtain the original email from the victim's computer it is possible to get enough from the header to be useful. The first mistake a novice investigator makes is to simply have the victim forward the message, and this is not good enough. To succeed it is important to give the victim very specific instructions on the right way to send the mail. The first instruction is to remind the victim not to destroy or delete the message. It should be left in place or moved to a secure folder on the client.

The next step is to have the victim send you an email with the original as an attachment. It is important to note that forwarding replaces the suspect's information with that of the victim, so you will get the body of the message but the header will be worthless. Simply have the message saved and then a copy of the saved message sent as an attachment. This should preserve the full message header for you to use in the investigation.

H. SMTP SERVER LOGS

The final item to address in this section on tracking is the SMTP server log. All email servers have the ability to maintain logging information. In practice the server log is actually a better source of details than the message header, and the investigator should determine as soon as possible whether

the logs will be needed. If they are needed the first step in preserving them is to gain cooperation from the ISP or other server host.

Accessing the logs is best handled by the network administrator. While some investigators may be knowledgeable in what the logs are and even how to retrieve them the fact remains that the network or server administrator is the person most likely capable of retrieving the logs without potential harm or disruption. That does not mean that the investigator should simply make a request and forget it. Unless the administrator is trusted, and capable of testifying capably under oath later about the log contents, then the investigator should be present when logs are seized.

As part of the investigative task the issue of chain of custody becomes very tricky when dealing with logs. Remember that the printed log is a representation of the log content and not the actual log itself. While some courts will allow the introduction of such printed material there is generally a question of validity and chain of custody that will arise. To protect the validity issue the investigator should be prepared to testify as to how the logs were maintained, accessed, obtained, and whether they are still intact or available in their natural format.

It is also important to remember that logs from each server may be needed to verify the tracking itself. If the email has bounced through five servers on the way to the victim's computer then the logs of each of these servers is material. Just like the chain of custody linkage the server logs links can help show the trail from perpetrator to victim.

Section 4

SEARCH, SEIZURE, AND DIGITAL EVIDENCE

Chapter 13

COMPUTER-RELATED EVIDENCE

A. TYPES OF COMPUTER RELATED EVIDENCE

The ultimate goal of all investigations is to obtain evidence admissible in court. In order to accomplish this mission all investigators must understand both the legal and technical issues associated with evidence. In this chapter we will focus on the most common evidentiary issues present in computer crime cases. Where appropriate we will use the Federal Rules of Evidence as a guide and to help explain specific issues. One should note that these rules are similar to those adopted in the individual states and there are often only minor differences between the rules. Officers should carefully check the rules for their specific jurisdiction to insure that the standards set forth in this text match those of their home jurisdiction.

1. Direct and Circumstantial Evidence

For the most part computer-related evidence is no different than evidence

obtained in any given case. As a general rule evidence falls into two broad categories; to wit: Direct and Circumstantial Evidence. The broadest definition of these two types of evidence is often the best to work with when defining new standards for computer crimes.

Direct evidence is that evidence which tends to prove a fact based on the existence of the fact itself. It evidence which proves existence of a fact in issue without inference or presumption.[1] In short, direct evidence is that which tends to prove a fact without inference or proof of another fact. The most common form of direct evidence is the "eyewitness." An eyewitness is one who directly sees the events in question and can testify to the facts from recall, without the benefit of other facts or evidence.

Circumstantial evidence is the evidence which tends to prove a fact by the existence of another fact. In some instances circumstantial evidence is often referred to as indirect evidence. The term indirect means that the evidence does not prove the fact in and of itself. Proof is provided not through the individual piece of evidence in question, but by the external existence of other evidence or facts. In many ways circumstantial evidence requires the trier of fact to draw an inference of proof by the existence of those other facts.[2]

2. Applying Direct and Circumstantial Evidence

Now that we have the broad definition down it is time to examine these two types of evidence from a perspective that should make them easier to understand. One of the best examples of how Direct and Circumstantial evidence apply is an analogy used by many attorneys to explain the difference to juries. All that is required is a bit of knowledge about the actions of young boys.

In this example one must put themselves in the position of being responsible for a 3 or 4-year-old boy. As any parent can attest, when things grow quiet it is time to check on the boy, and in this case we find the lad standing in the kitchen near the counter. A chair has been pulled to the counter where the open cookie jar sits. As you enter the room you notice that the boy also has cookie crumbs on his cheeks and a half-eaten partially in his mouth. Has this boy eaten a cookie?

The answer is an emphatic, Yes! We have clear (direct) evidence of his involvement. Not only do we see the open cookie jar, the chair beside the counter, and the crumbs on his face, but we also see the evidence of a partially eaten cookie shoved halfway into his open mouth. There is little doubt that this boy has eaten a cookie. This is a direct evidence of the fact.

Now let us imagine that instead of finding the boy with a cookie in his mouth we find instead a boy with nothing more than cookie crumbs on his cherubic face. We still have the open cookie jar, the chair beside the count-

er, and the evidence of cookie on the boy. What we do not have, though, is the direct evidence of his having eaten the cookie itself. The cookie, for all practical purposes, is gone; with the exception of the residue on the cheeks. Has this boy eaten a cookie?

Much like before it seems clear that the boy has eaten a cookie, but in this instance the existence of the fact (eating the cookie) is made clear only because of the existence of the other facts. Without these other facts (circumstantial evidence) we would not be able to conclusively say that a cookie has been pilfered.

What we have in the second scenario is circumstantial evidence. This is evidence which proves a fact by the existence of other facts. In this case we prove the stolen cookie by the presence of facts such as the cookie crumbs around the mouth, the chair placed near the counter, and the open cookie jar. Each of these facts tends to prove the fact of the taking.

The investigator must understand that in our courts the weight given to direct or circumstantial evidence is often a question for the jury. Obviously, some direct evidence would weigh more in the scales of justice than some circumstantial evidence. The ultimate question is, given the weight according to the juror's perception, whether the evidence tends to prove the fact or not. Thus, in the typical case the prosecutor presents a mixture of direct and circumstantial evidence that may be used to prove the ultimate allegations of criminal conduct.

That brings us back to the question at hand: what type of computer-related evidence will we deal with in a case? Obviously the first answer is that we will deal with both circumstantial and direct evidence. The investigator must be able to expand his view of evidence beyond that which clearly proves a fact and include all evidence which may prove the fact even through the existence of other facts.

It can be especially confusing to think about digital proof because legal analysts have tended to treat "computer evidence" as if it were its own separate evidentiary category. Of course, in some very practical ways electronic evidence is unique if only because it is not common in our criminal courts. It may also be seen as unique to investigators and jurors alike because electronic evidence is created, altered, stored, copied, and moved with unprecedented ease. This is the intangible element of computer crime evidence. Unlike a gun, knife, or other tangible item of evidence most digital evidence cannot be held or examined easily by jurors.

B. THE BEST EVIDENCE RULE

The key to identifying this potential evidence lies not in the tangible or

intangible but in the application of very traditional evidentiary standards. Computer-related evidence must pass the established admissibility tests faced by all direct and circumstantial evidence. We begin with one of the more confusing evidence issues: the best evidence rule.

The term best evidence is used in many circumstances under the law, but is generally applied when dealing with copies or reproductions of evidence. One of the most common circumstances where the rule is applied is in cases using documents or copies documents. The best evidence rule provides that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required. . . ."[3]

In the computer realm this issue arises when we deal with copies of electronic evidence. For instance, when investigators seize a computer they might make archival copies of the files on the hard disk drive. These reproductions are, in most instances, exact duplicates of the original file. From an evidentiary standpoint, though, there are issues of alteration that may be raised and the primary question is whether the duplicate is good enough or must we actually present the file on the original hard disk?

In answering this question the courts often turn to an analysis focused on the issue of reliability. A primary question is whether the offered evidence, even though a copy, reliable for what it contains? If the answer is yes, the evidence may be admitted. If the answer is no, or there is a significant question as to reliability, the best evidence rule might require the use of the original.

Some of the earliest issues of this type arose from business records. Many businesses kept copies of records such as receipts and other documents. The original was given to a customer and a copy, usually a carbon copy, was kept in the business file. Later, when questions of best evidence arose, the business owner merely pointed to specific exceptions in the law for support of the records. Many of the early decisions arising in computer cases, and the records or copies kept on computers, focused on these same principles. Specifically, the rules required the prosecutor to show that the record was made at or near the time by, or from information transmitted by a person with knowledge.

An issue that arises frequently focuses on the nature of the computer evidence. While we can easily manipulate and identify the copy of an original document it is much harder to fathom the copy of an electronic file. Altering a physical document is something we can easily understand and for most jurors it is something that can be readily identified. Jurors are more willing to accept a copy of a document as the best evidence when it is easily authenticated, but the very nature of computer files often becomes the issue rather than the reproduction.

On the surface one might argue that all computer-related evidence must be authenticated. Such a rule of thumb would certainly do the investigator

good in the long run since there would be less debate on the material than for material not easily authenticated. But is that truly what the law requires? To better understand that we must look to specifics in the law itself, and for that we will turn to the Federal Rules of Evidence.

Before applying the rule it is important to note that the rule does not stand alone. The application of the best evidence rule is not contingent on the rule itself but on the application of the rule in conjunction with other rules. The impact of best evidence rule is softened considerably by its reference to other rules and the need to meet so many standards. What this means is that the application of the rule is not a simple matter of applying specific language in the rule, but is instead an application wound through the words of other rules and many court cases interpreting the rule.

The biggest issue when dealing with best evidence is the definition of "original." Under the Federal Rules of Evidence two separate provisions give the term an expansive meaning when it comes to electronic documents. Section 1000(1) defines "writings and recordings" to expressly include magnetic, mechanical, or electronic methods of "setting down" letters, words, numbers, or their equivalents. Applying this rule to the computer means that when someone creates a document on a computer hard drive, for example, the electronic data stored on that drive is an admissible writing. The question now is in what form the evidence must be offered.

The most obvious choice is to produce the "document" itself to the court by bringing forth the hard drive and displaying the contents with a monitor. But that somewhat cumbersome process is not the only choice. In telling us what constitutes an "original" writing or recording, the Federal Rules of Evidence, Rule 1001(3) states that "[i]f data [is] stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" What this means, from a practical standpoint, is that so long as the copied file is accurate, paper printouts from electronic storage devices qualify as "originals" under the rule. It also appears that other means of displaying–such as overhead projection, LCD projection, etc.–might also be admissible.

While this relaxed standard appears to help when it comes to presenting computer generated files in court there are some additional provisions that help as well. Section 1003 provides that "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."

This appears to take care of the problem of archival copies of files taken from a computer hard disk. Unless authenticity or some unfairness is at issue, courts may freely admit duplicate electronic documents. "Duplicate" as defined in the rules, means "a counterpart produced by the same impression

as the original . . . by mechanical or electronic re-recording . . . or by other equivalent techniques which accurately reproduce (sic) the original."

Many investigative agencies analyze data evidence from exact electronic copies (called "bit-stream" copies) made with commercial or custom-made software. So long as the copies have been properly made and maintained, it appears that the Federal Rules allow judges to accept these copies as readily as the originals. This also means that expert opinions, those of investigators especially, may be based on the copies of the files and not always on the original file itself.

Of course, the obvious reason we would deal with the copy rather than the original is safety. Analyzing and manipulating an original file puts that file in jeopardy. Investigators often rely on the use of copies rather than the original. What this means is that even while the common law best evidence rule appears to be alive and kicking it has been substantially abbreviated by the rules of evidence. Questions of admissibility turn not on whether the data before a court is on a hard-drive, duplicate floppy disk, or a printout, but instead on whether the original data is authentic and whether any copies offered are accurate.

C. AUTHENTICATING ELECTRONIC DOCUMENTS

While the task of authenticating a document in court often rests with the trial lawyer, the reality is that the investigator must do the leg work. For that reason it is important that investigators understand what is necessary in order to authenticate a document in court. To this end there is some guidance under the Federal Rules of Evidence, and investigators should become intimately familiar with those standards as well as the standards for their own jurisdiction. As mentioned earlier, state standards may vary from those of the federal rules, but in many instances the standards simply do not exist at the state level because computer crime has not risen to a level to require such nuances. With that in mind we turn again to the Federal Rules to help us understand the intricacy of authentication.

When it comes to authenticating, Rule 901(a) states that the "matter in question is what its proponent claims." In other words, when the attorney presents the material (copy or reproduction) there is a general assumption that the material is what it is claimed to be. To that end, though, there are specific issues which must be addressed and rule 901(b) provides ten illustrations of how this is best done.

1. Distinctive Evidence

One of the most common methods for authenticating evidence is to show the item's identity through some distinctive characteristic or quality. The authentication requirement of rule 901(a) is satisfied if an item is "distinctive" in its "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."

One of the most common practices under this rule is the authentication of the document through a witness with knowledge of the document. For instance, photographs are often taken of crime scenes and then introduced at trial. The rule does not require the authentication through the photographer but instead allows the authentication through a witness who has knowledge of the scene. Thus, the authenticating question might be whether a particular photo is "a fair and accurate representation" of the scene. So long as the witness authenticating the photograph has knowledge of the scene they can say whether such is the case or not.

The practice in federal court is to use this method to authenticate different types of evidence which may now be digitally created, stored, and reproduced. For example, attorneys offering evidence obtained through a reproduced computer file may offer the authentication through an investigator "with knowledge" of the file and its contents. The primary question for such a witness might be, "Is this a fair and accurate representation of the original computer file?" If the answer is in the affirmative, thus authenticating the copy, then the court may allow the copy.

Where this type of authentication becomes a problem is in the modern age of computer-generated prints and digital photography. For instance, in a recent seminar on computer crime the instructor first displayed a rather gruesome photograph of a dead body. Blood on the chest indicated that the victim had been stabbed and the presence of a knife on the floor tended to support the finding. "But wait." The instructor warned. And with a few quick keystrokes, a few artful swipes of the mouse, and a little touch-up work the wounds on the chest were gone. The knife was replaced with a gun, and a new bullet wound appeared in the temple. Someone not knowing what the original picture looked like might easily mistake the "touch-up" work for an original scene. To make things even more convincing the gun was now in the hand of the "victim" and our homicide was now a suicide. Case closed.

The fact that the original picture was digital made the authentication even more difficult. At this point digital photography is still not as good as film photography. And where a medium grade digital camera was used to create a *bitmap* photograph, the ability to alter the scene increases dramatically. Most of the investigators in attendance had trouble finding the original wounds or the knife even though they had watched the instructor make the

changes. How, then, is a photograph such as this authenticated?

This is where the issue of "distinctive characteristics" alone is not enough. The true issue will be the veracity of the witness who is authenticating the document. The question for both judge and jury will be the witness's ability and veracity in observing and recalling the original person, photo, scene, or document with which he compares the in-court version. It is not enough that a document could be altered. The issue will be whether the authenticating witness is independently sure from observing the document that it is in fact a "fair and accurate representation" of the original.

One issue that investigators and trial attorneys alike must be cognizant of is the question of whether the distinctive characteristics must be also relevant. Take for example a witness who can remember the font used in a note but not the content. Is the authentication by remembering the font enough when the note in question actually states something different from the original? Perhaps judges will find themselves admitting digital photographs and documents based on distinctive characteristics if a witness with knowledge can identify and authenticate the item in all relevant detail. But that, of course, requires a judge to know in advance which details will be relevant to the case and which are insignificant.

If the characteristic that makes the item distinctive is not the same one that makes it relevant, judges might and should be wary about admitting digital evidence merely because it is distinctive. After all, the relevant issue in our homicide to suicide example was the nature of the death. A witness who remembers distinctive characteristics about the victim's clothes or the room's dimensions might miss altogether the relevant evidence as to the swap of a gun for a knife. Such a witness could certainly authenticate that this is the place where the death took place, but are they also then authenticating the nature of the death?

For the trial attorney the issue turns to one of asking the right questions. If the witness authenticates a document or other evidence on its characteristics then certainly someone needs to verify that the characteristics are relevant to the legal issues at hand. Without such additional authentication there is a likelihood that otherwise inadmissible evidence is allowed simply because it was "authenticated."

2. Chain of Custody

The term chain of custody refers to the link between those persons who seized the evidence and the route it has taken to the courthouse for presentation at trial. The links in this chain may include the initial officer on the scene, the investigator, the crime lab technician, and the evidence room attendant. At each stage the person accessing the evidence will be held

accountable for its condition and any alterations, tests, or other work done with it.

When prosecutors present evidence to a court, they must be ready to show that the evidence they offer is the same as that seized by the investigators and if it has changed why or how. Chain of evidence does not mean that a piece of evidence can not be tested or altered. It simply means that we can account for all who have had contact with the evidence. It means that we can account for the condition of the evidence and authenticate that it is in substantially the same condition as when seized.

When dealing with the chain of evidence the first rule for investigators is to document clearly all who have had contact with the evidence. This is traditionally done with a pen and paper log kept with the evidence or maintained by an "evidence officer." As we have seen in other chapters the evidence officer on a crime scene is responsible for logging all evidence, seized and otherwise, and securing that which is taken.

Regardless of how many people have handled the evidence the evidence log is used to document those having access. Typically this log is also used to maintain comments on any testing or changes made to the evidence. As a general rule today's investigative agencies use a hand-to-hand chain of evidence to guarantee accountability. Whether it be a pen and paper log or a series of electronic entries on a computer the investigator must show that the evidence has been maintained in a strong chain of custody.

D. ELECTRONIC PROCESSING OF EVIDENCE

When data goes into computers, there are many methods and forms for getting it out. To the extent that computers simply store information for later retrieval, a data printout may qualify as an original document under Federal Rules of Evidence 1001(3). Where the computer has merely acted as a technological file cabinet, advocates must be ready to authenticate the in-court version of the document as genuine, but the evidentiary issues (at least those connected to the computer) do not pertain to the substance or content of the document.

One of the issues common to the processing of electronic evidence is the method or manner used. For this reason investigators will need to log the methods used for storage as well as those used for processing the data on the system. If the computer, its operating system, and its applications software have been reorganized in order to obtain relevant information then this processing should be logged as well. The concept is that the alteration of file structure may in some way affect the ultimate structure of the content.

One of the best methods for processing this type of evidence is to main-

tain a log of all file structures. Where possible, a hard copy–usually a printed copy–is maintained each time the computer system is accessed. By comparing, calculating, evaluating, re-grouping, or selectively retrieving the material the log is used to verify the content of the system. One might think of this in much the same way as we would if authenticating a photograph. If a photograph is altered then the person altering is responsible for explaining such alteration. It does not mean that a photograph cannot be altered, it just means that we must account for the alteration.

The fact that the computer system has changed in some way does not make the resulting product inadmissible, but it does require another analytical step. The computer processing itself may in fact create a new file structure or other document. For instance, many word processing documents created in Microsoft Word have a "version" file associated with them. This addendum logs the number of times the file has been accessed and how many times it has been modified. The simple change in that number, though probably not relevant to the file content, may create an evidentiary issue which is avoided by keeping a simple log.

Because computers process data in many different ways by running programs, which can be commercially or privately written, there is always the underlying issue of how was that particular data accessed or evaluated. Any of these programs can contain logical errors, called "bugs," which could significantly affect the accuracy of the computer process. And even if there is no error in the code, a technician may run the program in a way that creates a false result.

For example, a particular computer search program may be "case sensitive," which means that the upper- and lower-case versions of any given letter are not interchangeable. If an author working in WordPerfect (a popular word-processing program), searches a document for the word "Evidence," the computer will not find the word "evidence," because the letter "e" was not capitalized. What does it mean, then, when the computer reports that the word was "not found"? Under what circumstances should a computer's conclusion be admissible in court? This is an issue often answered in the rules of hearsay.

E. CREATION OF EVIDENCE FROM COMPUTERS

Along with the logging of computer access the investigator must also be prepared to document the methods used in computer manipulation. As we will see in a moment, the use of a computer to access, analyze, and sometimes manipulate data creates many issues related to hearsay. For the moment, though, we will concentrate on the issues of creating evidence using

a computer.

The manipulation or creation of evidence using a computer is a relatively new issue for the courts. To this point there are few cases which specifically set out rules as to how such manipulation will be tested. To better understand this issue let us examine a typical case where manipulation or the actual methods of using the computer might be a factor.

Everyone who obtains income from work or other methods has an obligation to pay taxes when appropriate and to file a tax return. The enforcement of these provisions generally falls to the Internal Revenue Service. In this scenario a taxpayer is being investigated for "failure to file" tax returns or pay taxes owed. An obvious part of the overall evidence is the showing that no tax return was found with the IRS.

Prior to the computerization of the IRS the typical tax case was a question of searching physical records for a copy of a return. A clerk or other employee was assigned the task of finding the return in the IRS's filing system. When no return was found the clerk would report the fact to the agent who then reported it to the federal prosecutor. In limited cases the clerk might be called to testify that he conducted the search, but in most instances the testimony of the agent was simply allowed. This, as we will see, is an exception to the hearsay rule. But what happens when that search is of a computer system? For instance, the taxpayer alleges to have filed electronically but the IRS computer does not have a record of such return.

The hearsay rule allows the absence of a public record to be shown by testimony "that diligent search failed to disclose the record. . . ." A question raised in this type of case, though, is whether the testimony is of an actual finding or merely a negative report? Will the negative computer report suffice, or should the technician who ran the search testify? Must the technician explain not only what keystrokes he entered to conduct the search, but also establish the error-free logic of the program he used? Must he know not only that the program searches for both lower-and upper-case versions of the taxpayer's name, but also exactly how it accomplishes that task?

While the absence of a record is often admitted in evidence, prosecutors can expect that as attorneys become more computer-literate, defense counsel will raise new challenges in this area. Indeed, the accuracy or inaccuracy of the IRS's negative report rests on many different components, including the reliability (both human and technical) of the computer process. And for that reason the investigator using a computer for evidence analysis or creation must be especially wary of the methods at hand.

Certainly, the mathematical validity of any program is a question of fact. As we discussed in our introductory chapters computers are tools to manipulate electrons which are in fact representations of real life problems. Are those manipulations valid and do they in fact prove what they suggest.

Similarly, the methods and safeguards involved in executing the program must also be fair ground for analysis and challenge. While it would clearly be both unnecessary and burdensome to prove every step of a computer process in every case, courts must be ready to look behind these processes when the facts warrant. What this means for the investigator is that proper documentation and records must be maintained to insure that the processes are accurate and reliable.

F. THE HEARSAY RULE

The hearsay rule itself is relatively simple. Hearsay, which is a statement made out of court and offered later in court to prove the truth of a matter asserted, is generally inadmissible. One reason for this is that hearsay often removes the ability of the defendant to confront his accusers and examine those witnesses against him. Over the years, though, it has been recognized that certain exceptions exists which would allow such statements, especially when justice demands it.

Though there is not sufficient space in this book to fully discuss hearsay there are a few items worth noting before getting to an analysis of the rule as it relates to computers. One should first note that the hearsay rule is generally divided into two distinct groups of exceptions. The first group deals with statements made where the declarant (the person making the statement) is available to testify. The second set of exceptions deals with statements made by a declarant who is unavailable–for any reason–to testify.

Some of the more common exceptions under § 803 include:

1. Present sense impression: a statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.
2. Excited utterance: a statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.
3. Recorded recollection: a memorandum or record concerning a matter about which a witness once had knowledge but now has insufficient recollection.
4. Public records and reports: records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth the (A) activities of the office or agency, or (B) matters observed pursuant to duty imposed by law.
5. Statements in ancient documents: statements in a document in existence twenty years or more then authenticity of which is established.

6. Learned treatises: to the extent called to the attention of an expert witness upon cross-examination or relied upon by the expert witness in direct examination, statements contained in published treatises, periodicals, or pamphlets on a subject of history, medicine, or other science or art, established as a reliable authority.

Section 804 also establishes some exceptions dealing with former testimony, a statement made under belief of impending death, and a statement of personal or family history. Of course these are not the only exceptions in 803 or 804, but they do give some indication of the type of statements that are allowed. It should be noted that at publication date there was no clear exception for computer searches or analysis. For that reason we have to rely on the specific exceptions already established in the rules.

Under rule 803(6) of the Federal Rules of Evidence any "memorandum, report, record, or data compilation" may be admissible if it were: (1) made at or near the time of the event, or (2) by, or from information transmitted by a person with knowledge. The record must also have been kept "in the course of a regularly conducted business activity." This means that it must be the regular practice of that business to make the record in question.

A business computer's processing and re-arranging of digital information is often part of a company's overall practice of recording its regularly conducted activity. Information from telephone calls, bank transactions, and employee time sheets is regularly processed, as a fundamental part of the business, into customer phone bills, bank account statements, and payroll checks. Logic argues that if the business relies on the accuracy of the computer process, the court probably can as well.

This is different, however, from using a company's raw data (collected and stored in the course of business, perhaps) and electronically processing it in a new or unusual way to create an exhibit for trial. For example, banks regularly process data to show each account-holder's transactions for the month, and most courts would readily accept that monthly statement as a qualifying business record. But may a court presume a similar regularity when the same bank runs a special data search for all checks paid from the account-holder's account over the past year to an account in Switzerland?

In this case, even though the report was not made at or near the time of the event, the document is probably admissible as a summary under Federal Rules of Evidence 1006. That rule allows courts to admit a "chart, summary, or calculation" as a substitute for "voluminous writing, recordings, or photographs." It should be noted as well that other parties still have the right to examine and copy the unabridged original data, and to challenge the accuracy of the summary. Of course, this also opens the way to challenges of any computer process which created the summary.

In most other respects the hearsay rule operates with computer evidence exactly as it does with any other sort of evidence. For instance, statements for purposes of medical treatment, vital statistics, or statements against interest may all qualify as exceptions to the hearsay rule, whether they are oral, written, or electronic. Clearly, an electronic statement against interest must also be authenticated properly, but it does not fail as hearsay. Conversely, a correctly authenticated electronic message may contain all sorts of hearsay statements for which there are no exceptions.

The key is that computer evidence is no longer limited to business records, and the cases that carry that assumption are distinguishable when advocates work with other kinds of electronic evidence. But even with business records, a trial lawyer well versed in the technological world who knows how to ask the right questions may find that the "method or circumstances of preparation indicate lack of trustworthiness," under Federal Rules of Evidence 803(6), to such a degree that a court will sustain, or at least consider, a challenge to the admissibility of the evidence. Computers and their products are not inherently reliable, and it is always wise to ask, in any particular case, what computers do and how they do it.

ENDNOTES

1. *State v. Baker,* 249 Or. 549, 438 P.2d 978; see also, *State v. McClure,* 504 S.W.2d 664.
2. *Foster v. Union Starch & Refining Co.,* 137 N.E.2d 499; see also, *Twin City Fire Ins. Co. v. Lonas,* 75 S.W.2d 348.
3. *Federal Rules of Evidence,* Rule 1002.

Chapter 14

FOURTH AMENDMENT PRINCIPLES AND COMPUTER SEARCHES

While this book is not designed to be a treatise on Fourth Amendment principles it is important that investigators fully understand those principles before beginning any investigation. The application of the principles for search and seizure are complicated enough, but when we add a computer into the equation the questions of *when* a warrant is needed becomes a bit complicated. For that reason it is important that the computer crime investigator fully understand the underlying principles as well as their application in specific instances.

The evolution of modern search and seizure standards has taken several

hundred years, but it is within the last fifty years that we have seen the most far-reaching standards established by the courts. Today it is clear that the courts prefer a search only with a warrant, but they will allow searches to be conducted without a warrant where circumstances dictate. Understanding what circumstances will allow the search without a warrant is important and the primary focus of this section. Let us begin with a brief restatement of the development of today's search and seizure standards.

A. WHAT DOES THE FOURTH AMENDMENT PROTECT?

Most students of the legal system have heard the legal maxim: "Every man's house is his castle."[1] The English legal tradition has long held that even the poorest of our citizens is granted the greatest legal protections against the government. One of the most forceful expressions of the maxim was that of William Pitt given while addressing Parliament in 1763. Pitt, a fiery orator who was well known for his defense of personal rights, challenged even the crown when he stood before the great body. Pitt stated:

> The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail–its roof may shake–the wind may blow through it–the storm may enter, the rain may enter–but the King of England cannot enter–all his force dares not cross the threshold of the ruined tenement.

This maxim, along with the legal principles that flow from it, focus on the protection of property rights. At the heart of the theory is the protection of right of the homeowner to control access to the property. This same concept was quickly adapted to the earliest of the Fourth Amendment litigation. From the outset it was clear that police were restricted from making entry onto property, or otherwise interfering with property rights, in order to make a search or seizure unless they had met stringent legal standards.

The concept of protecting the sanctity of the home made its way to the original colonies along with many other legal theories. By the revolution it was clear that the colonist preferred the protection they were afforded by the system. While in early litigation the Supreme Court failed to establish a clear standard for requiring a warrant in all instances of search. It is clear that there was a predisposition to protect such rights. It has really only been within the last forty years that we have begun to see some clear lines being drawn in the debate over reasonable and unreasonable searches with and without warrants.

Part of the convergence came after World War II when the Supreme Court took a clear turn toward the allowance of government intrusion onto what

was otherwise considered protected ground. Early on there was consensus that police could search a person contemporaneous to a valid arrest but no such agreement existed when it came to property. This right was expanded in *Harris v. United States,*[2] when the Supreme Court approved as "reasonable" the warrantless search of a four-room apartment pursuant to the arrest of the man found inside.

In the Harris case police arrested the defendant while still inside the apartment. Concurrent with the arrest the police conducted a search of the apartment including the room the defendant was arrested in and the adjoining rooms. Though no warrant had been issued, and in fact there was no real "probable cause" to support issuance of a warrant to search the entire apartment, the Court extended the meaning of "reasonableness" under the Fourth Amendment by allowing the search of the adjoining rooms.

The Court again addressed the issues of contemporaneous search in *Trupiano v. United States,*[3] when a reconstituted majority set aside a conviction based on evidence seized by a warrantless search pursuant to an arrest. Where the Court had broadened the police power to conduct a warrantless search of the adjoining four rooms of the Harris apartment, it now narrowed the ability to search such a wide area in *Trupiano.* In doing so the Court established what some would argue was a new standard when it held the "cardinal rule that, in seizing goods and articles, law enforcement investigators must secure and use search warrants wherever reasonably practicable."[4]

This new "cardinal rule" was not long lived, though. Two years later it was set aside when a different majority adopted the premise that the test "is not whether it is reasonable to procure a search warrant, but whether the search was reasonable." In this sense the Court focused not on the requirement for a warrant but on the probable exceptions to such a requirement. The Court held that the issue of whether a search is reasonable, "must find resolution in the facts and circumstances of each case."[5]

In many respects this new statement of the law meant that the lower courts were to look at the specific facts of each case when determining whether a warrant was necessary or not. Similar cases may require very different actions. A slight shift in facts could make the difference in each case and the lower courts were to evaluate those shifts on an individual basis.

In a single three-year period we see the court extend the ability to search beyond the person of the arrestee, take back such authority, and then extend it again. This psychosis was common among search and seizure cases of the time, and it is not until the decade of the sixties that we see a significant shift in political and social thinking. Where the Court had expanded the ability of the police to search without a warrant in the post-war era we now see it begin to curtail that power in the "Decade of Peace."

An important factor to remember at this point is that the development of search and seizure law has taken place over an extended period of time. While the issues arising in the computer crime case may seem unique, especially considering the nature of the crime itself, the new technology involved, and the likelihood that specific criminal acts are being committed which may not have been committed before, the important point to remember is that the standards of the fourth amendment still apply. The question, as we will see in coming paragraphs, is almost always one of "and expectation of privacy" and the defendant's right to such privacy.

B. RELEVANT CHANGES IN THE LAST FORTY YEARS

As noted in the section above, the Court returned its emphasis to the warrant requirement with a series of cases arising in the sixties. Certainly one of the more significant statements which clarifies the Court's shift arises in the now famous case of Terry v. Ohio. The court stated:

> The [Fourth] Amendment was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence. In the scheme of the Amendment, therefore, the requirement that 'no Warrants shall issue, but upon probable cause,' plays a crucial part."[6]

The Court further stated that, "the police must, whenever practicable, obtain advance judicial approval of searches and seizures through a warrant procedure."[7] This is an important issue to remember since many of the attacks against the warrantless search of computers or related items will fall under this theory.

Further evidence of the new paradigm is evidence by other cases from the period. During this same time the Court established many "new" standards for application of the Fourth Amendment. Many commentators have argued that the Court went too far during this era to protect the "rights of the criminals" rather than strengthen the power of the police. Constitutional pundits point out that by the seventies the Court was closely divided on which standard to apply, and for a while the balance tipped in favor of the view that warrantless searches are *per se* unreasonable. There were, however, a few carefully prescribed exceptions to this perception.[8]

A major shift in standards was the movement from viewing the Fourth Amendment as protecting property rights to that of protecting privacy rights.[9] Gradually, guided by the variable expectation of privacy approach to coverage of the Fourth Amendment, the Court broadened its view of per-

missible exceptions and of the scope of those exceptions. By 1992, it was no longer the case that the Court viewed the warrant requirement as superior and the warrantless search a true exception. The standard moved from a preference for warrants with narrowly tailored exceptions to one of "reasonableness" when measuring the question of a warrantless search.[10]

While the Court appears to follow the standard that a warrant is required it is also clear that the exceptions to the warrant requirement have multiplied. Today it can be easily said that a warrant is required where practical, but that the issue of practicality will often be measured with a very narrow yardstick. To that end, one can clearly find that if circumstances justify, and if the courts have established a clear "exception," then no warrant is required. The opposite of this, however, is that unless the actions of the investigator in conducting a search without a warrant do not fall into one of these narrowly tailored exceptions the courts might take corrective action including the exclusion of evidence from the case.

Indeed, as the Supreme Court indicated in *United States v. Leon,*[11] a warrant can save a search where probable cause is doubtful or marginal. With this in mind we can now turn to the exceptions most common in search and seizure cases and the application of these exceptions to computer crime cases.

C. EXCEPTIONS TO THE WARRANT REQUIREMENT

It is important that one recognize that a warrant is the preferred way to conduct any search or seizure. It is also important to emphasize that where practical the investigator should seek a warrant or be able to show why a warrant was not obtained. One of the first efforts by any defense attorney when dealing with search or seizure is to attack the warrantless search. The investigator who haphazardly conducts such a search has only himself to blame when the defense establishes grounds for excluding crucial evidence otherwise relevant to the crime at hand.

With this warning in mind we move to the issues of warrantless searches and the many exceptions likely to apply in a computer crime case. We begin with one of the easiest to identify and apply: Plain View.

1. Plain View

One of the best known and longest-standing exceptions to the warrant requirements is known as the "Plain View Doctrine." As explained by the courts, evidence of a crime may be seized without a warrant when the item is in *plain view* and the investigator has a legal right to be in a position to see that item.[12] In its simplest form the Plain View doctrine means that anything

in plain view of an officer, who has a right to be where he is, may be seized. In practice, though, questions about trespass and pretense often arise to cloud the issues.

Like most of our exceptions, if is often helpful in understanding the application of the Plain View Doctrine to examine various cases which have helped shape the exception. One of the better known cases is *Washington v. Chrisman.*[13] In this case the Court upheld the seizure of marijuana seeds and pipe in open view by an officer lawfully in a dorm room for other purposes. The focus was not on the reason the officer was in the room but instead on the question of whether he was in the room for a lawful purpose at all. Where the officer is present through a lawful means, either invited or otherwise authorized to be there, then the first test of the Plain View Doctrine will be met.

From a practical standpoint this means that an officer may be able to seize evidence of a crime even though the crime is not related to the purpose for the officer's presence. For instance, an officer is called to a home because of a domestic disturbance. If the officer then sees evidence of a crime he may seize that evidence even though the evidence has little if anything to do with the domestic disturbance.

Some might argue that the officer was not looking for evidence related to the purpose at hand. The "accidental" discovery of evidence of another crime should therefore not be admissible since it was not the reason the officer was there to begin with. To this end the courts have limited the exception by saying that the item must be in *plain view.* If the officer has actually conducted a search in the sense that he has moved items or opened drawers then there is no legal seizure. It is the fact that the item seized is in open and obvious view that makes it a true exception.

Similarly, where an officer, during the impounding of an automobile opens a door to conduct a routine inventory but instead finds contraband or illegal substances in plain view the officer will have a right to seize the items in question.[14] The court will only concentrate on the officer's reason for being there long enough to determine if it was legal or not. Once that determination is made then the reason for being there is immaterial. It is really immaterial that the officer was impounding the car because of unpaid parking tickets. The only concern is that the officer had a right to be in the position he was in.

This doesn't mean that "plain view" seizures are always allowed or never challenged. The reality is that some of the more controversial seizures arise when the officer is exercising authority not related to the seizure itself. One such case that addressed these issues was *Ker v. California.*[15]

In *Ker,* officers entered a residence without a warrant to make an arrest. Because of "exigent circumstances" the officers were able to legally arrest

without a warrant. During arrest, though, officers spotted and then seized illegal items in plain view. The items were unrelated to the arrest itself and ultimately were used to support additional charges against the defendant.

In addressing the issue the court again looked at the reason for the officers being present. The fact that they didn't have a warrant was a secondary concern. The first concern was whether they had a right to be where they were at all. In the *Ker* case the court held that officers who have a right to make an arrest may also have a right to seize items in plain view.

This exception also extends to circumstances where the officer is conducting a legal search with a warrant. For instance, where an officer has a warrant to search for a stolen automobile he may also legally seize evidence found in plain view not related to the stolen automobile. So long as the officer had a legal right to be where he was and so long as the item was in "plain view" then a seizure may be made.

Let us now apply this to a more specific scenario involving computers. Investigators obtain a warrant to search for a specific computer system. The computer may contain a hard disk drive with data that might be evidence of wrongdoing. While serving the warrant the officers notice a pile of printouts next to the computer. The top paper contains incriminating evidence not specifically designated in the warrant. May the investigators seize these papers?

In applying the "plain view" doctrine the first question is whether the officers had a legal right to be where they were. In this case they had one. The search warrant gave them the right to search for and seize the computer. In the act of seizing the computer the officers were in a position to see the printouts.

The next question is whether the evidence itself was in "plain view." So long as the evidence was in "plain view" the investigators have a right to seize. But what about if the evidence was actually contained several pages into the pile. Could the investigators legally move the papers to identify the evidence beneath?

If we assume that the top page had nothing incriminating on it then we must ask ourselves what right the officers had to look at pages below. If none existed no seizure may be made. This standard is similar to that used in other cases. For instance, officers looking for a dead body in a home cannot reasonably expect to find the body in a matchbox. If the officer opens the matchbox and discovers cocaine is the seizure legal? Probably not because the officer had no right to be in a position that he could see in the closed matchbox.

What makes this often confusing for some investigators (and attorneys alike) is that sometimes officers have a right to move items in order to conduct their legal business. Moving back to our legal search and seizure of the

computer we might find legal grounds for moving the papers in question. For instance, if the papers are setting atop the power cord the officers might need to move or otherwise disturb them in order to free the power cord. While an officer can clearly not randomly shuffle the papers in order to look at interior pages it is reasonable that during the move some of the papers shift thus allowing the officer to reasonably see the contents of internal pages. So long as the officer can reasonably articulate his actions then he may have a right to seize.

One might argue that "plain view" is really an issue of fortuitous action and not good police work. There is some legitimacy in that argument. And the issue is often whether the discovery (and later seizure) was made incidental to a legitimate purpose or whether the officer took some additional action to increase his chances of finding evidence. If it is the latter then the officer has acted improperly. In other words, an officer cannot create a plain view seizure by disturbing or moving other items. The seizure must be unplanned.

One last issue that must be addressed when dealing with "plain view" seizures. In order to support a seizure the officer must in fact have "probable cause" to believe the item seized is contraband or evidence.[16] What this means is that the investigator must truly believe the item in question is either contraband or evidence of a crime. Simply because the item is in plain view does not remove the probable cause requirement of the Fourth Amendment.

This brings us to the related issue of "reasonable suspicion" and seizures. Simply stated, a seizure cannot be made based solely on reasonable suspicion, but may the officer make further inquiry or investigation when the suspicion is raised by something not quite in plain view? Unfortunately, this issue is not as clear-cut as many would like to see. The courts have again suggested that each case may be different and no "bright line" test can be established.

From a practical standpoint we can establish some guidelines. To help do this we can go back to our computer seizure scenario. Officers are on the premise to seize a computer with a valid search warrant. While on the scene an officer notices a pile of printouts next to the computer desk. The top page is blank but the officer can see part of a lower page sticking out from the stack. It appears that the page has incriminating evidence on it, but the officer needs to look closer. May he move the stack to take a closer look?

The general rule is that so long as the examination does not become a search then the officer may make a closer inspection. In other words, the officer may be able to retrieve the stack of printouts in order to more closely look at that page that is exposed, but he may not be able to thumb through the stack in order to expose more information.

Simply stated, if the officer has reasonable suspicion then he may make

further inquiry. If that further inquiry creates probable cause then he may seize. The courts have always held that a seizure need not be proven later. In other words, if the officer believes he has probable cause and it turns out that the item is in fact not evidence there is no harm. The issue is simply whether probable cause existed to support the seizure and not whether the evidence was in fact sufficient to support a conviction.

2. Exigent Circumstances

The term "exigent circumstances" has been tossed about in recent years to establish various grounds upon which a warrantless search may be made. For the computer crime investigator there are at least two specific instances that constitute "exigent circumstances" and would justify the warrantless search or seizure. The first of these are circumstances where "destruction of evidence is imminent."

Because of the very nature of the computer or digital evidence a great deal of proof may be lost when the computer is turned off or when data is "dumped." For that reason the courts have long held that where there is a substantial risk of loss the officer may make a warrantless search and seizure. For instance, where the perpetrator's computer screen is displaying evidence which investigators reasonably believe to be in danger, the "exigent circumstances" doctrine would justify downloading the information before obtaining a warrant.[17]

Because the data displayed on the screen may or may not be saved to a hard disk the investigator may have the right to seize the machine. That doesn't mean that the investigator has the wholesale right to search the contents of the hard or floppy disk of the machine. Likewise, an investigator who seizes a machine because of fear of losing valuable data does not have a right to search the network the machine is connected to. Only where the "exigent circumstances" are such that the investigator might lose the data may the seizure be made.

Of course, when investigators know they must search and seize data from two or more computers on a wide-area network, they should, if possible, simultaneously execute separate search warrants. But sometimes that is not possible, and investigators must then analyze the particular situation to decide whether the "exigent circumstances" exception applies to one, both, or even more of the computers in the network. In these instances the facts will dictate the actions which the officers can take to protect the evidence in question.

The courts have helped establish some guidelines for determining when "exigent circumstances" exists. They are found in *United States v. Reed,*[18] and include:

1. the degree of urgency involved,
2. the amount of time necessary to obtain a warrant,
3. whether the evidence is about to be removed or destroyed,
4. the possibility of danger at the site,
5. information indicating the possessors of the contraband know the police are on their trail, and
6. the ready destructibility of the contraband.

When measuring the "exigent circumstances" exception the courts often use the "reasonable person" standard. Would a "reasonable person" under the same circumstances believe that "exigent circumstances" exists to support the immediate search or seizure? If so, the officer may be justified in his actions.[19]

It is important to note that the officer's fears as to destruction or alteration of evidence need not be correct as long as they are reasonable.[20] The Supreme Court has held that the proper judicial inquiry is whether an objective officer could reasonably believe that the evidence was in jeopardy. This is a modified "reasonable man" test in the sense that it requires an "objective officer" in place of the "reasonable man."

Recognizing the strong preference for warrants, courts have suppressed evidence where the officers had time to get a warrant but failed to do so.[21] Some courts have even ruled that exigent circumstances did not exist if the law enforcement officers had time to obtain a warrant by telephone. The most notable case is case is *United States v. Patino,*[22] where officers made a warrantless search after waiting at least thirty minutes for back-up. The court held that where the officer had the ability to wait that long for back-up they also had the opportunity to make a reasonable inquiry into a warrant even if it meant calling the prosecutor by telephone.

It must also be pointed out that while exigencies may justify the seizure of hardware (i.e., the storage device), this does not necessarily mean that they support a warrantless search. In *United States v. David,*[23] the court held that although the agent was correct to seize the defendant's computer memo book without a warrant (because the agent saw him deleting files), the agent should have gotten a search warrant before accessing and searching the book. The court held the exigencies allowed the agent to take the computer memo book but that once taken there was time to get a warrant to look at the files contained inside. The failure to get a warrant before concluding the search meant that seized evidence must be suppressed.

This holding is, of course, analogous to cases that address other kinds of containers. In the David case, the computer book itself was not contraband, instrumentality, fruit, or evidence of crime. It was, instead, analogous to a

small file cabinet, a locked box, or a container of data. The agent was not interested in the hardware but in the information inside. As the cases make clear, authority to seize a container does not necessarily authorize a warrantless search of the container's contents.

Staying with this analogy we can see that if the agent had seen David destroying paper files inside a file cabinet he could not have opened the cabinet once shut by David. He could, to avoid destruction of the contents further, seize the cabinet and then secure a warrant to search the contents. This, the court held, is the same whether it be a physical file cabinet or a computer.

Courts have also suppressed warrantless searches when the defendant maintained a reasonable expectation of privacy in the contents of the container. In one such case, *United States v. Turk,*[24] officers seized an audiotape which they feared would be destroyed or altered. They then played the tape revealing incriminating conversations which were used against Turk later. The court held that while they may have had a right to seize the tape itself (the physical container) the defendant also had a continuing expectation of privacy; i.e., a defendant could expect that the tape would not played without a warrant having been issued.

Investigators must always remember, however, that electronic data is perishable. This is our second clear exception under exigent circumstances. Humidity, temperature, vibrations, physical mutilation, magnetic fields created by passing a strong magnet over a disk, or computer commands (such as "erase *.*" or "format") can destroy data in a matter of seconds. Thus, the exigent circumstances doctrine may justify a warrantless seizure in appropriate cases even if someone is not physically threatening the item.

The key in this sense is that the officer must be able to articulate the reasons for believing the contents were in danger. If those reasons are sufficient then the court will sustain the warrantless seizure. But that does not mean the officer has a right to view or listen to the contents merely because he has a right to seize the container. Much like our cases above the right to seize the container may not justify the intrusion into the contents. Unless the officer can show that the contents themselves are in danger then the seizure of the container may be enough. Once the container is secure the officer can obtain a warrant for the contents.

The extension of this is that as long as the officer can show grounds for believing the contents are in danger, then he may seize the contents. This means the officer, upon proper articulation, may be able to copy or view the contents of the computer. Again, the issue is reasonableness and what would a reasonable officer under similar circumstances do.

3. Border Searches

The law recognizes a limited exception to the Fourth Amendment's probable cause requirement at the nation's borders. Officials may search people and property without a warrant and without probable cause as a condition of crossing the border or its "functional equivalent."[25] Both incoming international baggage[26] and incoming international mail at the border are subject to search without a warrant to determine whether they contain items which may not lawfully be brought into the country.

Border searches or international mail searches of diskettes, tapes, computer hard drives (such as laptops carried by international travelers), or other media generally fall under the same rules which apply to incoming persons, documents, and international mail. This means that investigators or officers working these "borders" have a right to make expanded warrantless searches which do not violate the otherwise strict provisions of the Fourth Amendment.

While border searches apply easily to persons and items within the "border zones" they do not apply to items transmitted electronically (or by other non-physical methods) into the United States from other countries. For example, if an individual in the U.S. downloads child pornography from a foreign BBS, a warrantless search of his home computer could not be supported by the border search exception.

In such cases, it is difficult to find a "border" or its functional equivalent as data travels over international telephone lines or satellite links. What seems clear, however, is that once data has been received by a computer within the United States, that data resides in the country and has passed beyond the border or its functional equivalent. Because the justification for the border search exception is grounded on the sovereign's power to exclude illegal articles from the country, that exception no longer applies once such articles (in this case electronic data) have come into the country undetected.

4. Consent Searches

Investigators may search a place or object without a warrant or, for that matter, without probable cause, if a person with authority has consented.[27] There are a number of issues which arise under consent searches, though. We begin with the question of explicit or implicit consent.

In most cases the investigator seeks explicit permission to search. Specific words are needed to create an explicit consent. To support such consent investigators often use preprinted forms that set forth the person's rights pertaining to a consent search. By signing the "waiver" the person is giving explicit consent to search.

The use of specific words is all that is necessary to create an explicit consent. For instance, the words "you may search" are preferred. They have a very narrow meaning, and when taken in context it is often difficult for someone to later say they did not give consent. But the person does not have to be that specific for there to be an explicit search. In many instances a simple "yes" answer to the question of "Can I search" is enough.

Short of those specific words the investigator will have to create the consent through the language and mannerisms in which the consent is given. This means that we may gain consent through an implicit grant rather than explicit. For instance, In *United States v. Milan-Rodriguez*[28] the defendant told police where to find a key to a locked area. This action, according to the Court, constitutes implicit consent to a search of the locked area. Thus, where a party tells police where to search or even provides the means for conducting the search they may be seen as giving consent to the search itself.

Another issue that commonly arises is whether consent was voluntarily given. Much like the question of explicit/implicit consent the issues of voluntariness often depend on the specific facts of the case. In other words, the courts will look to the actions of the parties to determine whether the consent was given voluntarily or not.[29]

The burden is on the government to prove that the consent was voluntary.[30] In weighing this question the court will consider all the facts surrounding the consent. While no single aspect controls the result, the Supreme Court has identified the following factors for determining voluntariness:

1. the age of the person giving consent;
2. the person's education, intelligence, and mental condition;
3. the person's physical condition;
4. whether the person was under arrest; and
5. whether he had been advised of his right to refuse consent.[31]

In computer crime cases there are several issues which make consent even more difficult to determine. One of these has to do with the scope of the search. Did the search exceed the consent given?

One example where such an issue might arise is where the search involves a machine with encrypted data. While the defendant may have given permission to search the hard drive did that consent also include the ability to "open" the encrypted files? Are these files like a locked box?

In answering this type of questions the reviewing courts must determine, on the basis of the totality of the circumstances, whether the consent given was in fact sufficient to conduct the search in question. This "totality of the circumstances" test looks at the words, mannerisms, and all other factors

present to measure the intent of the grantor.

Similarly, the courts will use "totality of the circumstances" when measuring other factors in voluntariness. For instance, has the consent been freely given or has it been coerced. The court knows that investigators and police can exert influential power over a person, but is the mere presence of a police officer enough to coerce a person into giving consent where he/she otherwise would not? Generally speaking it is not. So long as the action of the police does not become coercive then the consent is generally seen as voluntary.

Another issue closely related is the ability to refuse the consent request. Is there an obligation on the police to tell someone they have a right to refuse the search? No. The courts have not established such a standard and it is unlikely, given the current composition of the court, that one will be created. Actual knowledge of the right to refuse consent is not essential to the issue of voluntariness, and therefore police are not required to acquaint a person with his rights, as through a Fourth Amendment version of Miranda warnings.[32]

Another issue arising with computers has to do with the proper party for consent. This arises when dealing with networks. Does a system administrator have the authority to consent to a search of a file server containing the files of all the system users? While the courts have been slow to address this issue it appears some guidelines can be applied.

In early cases such consent was considered sufficient if that party "possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected."[33] This meant that the officer must make sure that the person giving consent had actual authority to give such consent.

That requirement has changed, however, when the Court ruled that an officer need only have a good faith belief that the person giving consent has authority to act. In this sense, a third party who portrays themselves as having authority over the items to be searched may give consent to search even when they don't have actual authority in a legal sense. Even if the officer is mistaken in such belief, so long as the belief is held in good faith, the consent may be valid.[34] Thus, an officer may be deemed to have made a lawful search when a third party gives permission to search, even though it is revealed later than the party did not have the right to give such consent.

a. Scope of the Consent

A person who consents to a search may explicitly limit this consent to a certain area.[35] When the limits of the consent are clearly given, either at the time of the search or even afterwards, investigators must respect the boundaries. In *Vaughn v. Baldwin,*[36] the IRS was conducting an audit of a dentist.

The dentist voluntarily turned over records to the IRS investigators. The IRS kept the records for months and refused several informal requests for their return. Plaintiff then formally, in writing, revoked his consent to the IRS and requested immediate return of the records. The IRS failed to return the records in a timely fashion.

The plaintiff sued and the IRS returned the originals but kept the copies. The court found that the IRS had violated the Fourth Amendment by keeping the records beyond the time formally granted by the taxpayer. Although the IRS was entitled to copy the records while they lawfully had them, they could not keep the records once the dentist revoked his consent. The court also considered the length of time the IRS held the records both before and after the formal revocation of consent. The court acknowledged that the IRS originally had consent to keep the records, and thereby consent to copy or otherwise evaluate the records, but that upon revocation of the consent they could not keep the records even it were "for a reasonable time" to make copies.

Consent may also be limited implicitly. In *United States v. David,*[37] the court held that while the defendant had consented, pursuant to a cooperation agreement, to share some of the information contained in his hand-held computer his attempt to prevent investigators from seeing the file password constituted a limit on his consent. Although the agent did nothing wrong by leaning over defendant's shoulder to watch him enter the password, the government clearly exceeded the implicit limits of David's consent when investigators used the password to read the whole contents of the computer without David's permission.

b. Third-Party Consent

We have already seen that investigators may use consent to search computers as well as other containers. We have also seen that investigators may rely on that consent to conduct their search even if the consent later proves to be worthless. The good faith action of the investigator is the issue to be weighed and not the actual ability to give consent. Does this same concept hold true when the consent is given by a third party?

It is not uncommon for several people to use or own the same computer equipment. If any one of those people gives permission to search for data may investigators search all files or only those "owned" by the person giving consent?

These are two questions which can arise in a computer crime investigation. As a general rule an investigator may rely on the consent of a third party so long as that person has authority over the computer. What this means is that if the person giving consent has authority over the computer,

even if it only temporary authority, then the investigator may rely on that consent in order to conduct the search.

This is somewhat like the standards applied in automobile cases. The law has long presumed that the driver of the automobile has "custody and control" of the vehicle. It is presumed that the person having such control has the authority to consent to a search of the vehicle. Since the driver is ultimately responsible for operation of the vehicle, and thereby responsible for the contents of the vehicle, then they have the authority to consent. A computer is not much different.

Where the possessor or user has custody and control of the computer it may be presumed that they have authority to give consent. In these examples, all users have assumed the risk that a co-user might discover everything in the computer. Likewise, there is the assumed risk that the co-user might also loan the computer to another or even consent to a search by a law enforcement officer.

c. General Rules of Consent

The ability of a third party to give consent is often called the "common authority" rule. In *United States v. Matlock,*[38] the Supreme Court stated that one who has *common authority* over the premises or effects of another may consent to a search even if the absent co-user objects. In an important footnote, the Court said that "common authority" is not a property law concept but "rests rather on mutual use of the property by persons generally having joint access or control for most purposes." The Court further stated that "it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched."[39]

Extending this analysis, a third party with common authority may consent even if he is antagonistic toward the defendant. One could even argue that sharing access to a common premises with an unsympathetic person would objectively increase the risk of disclosure, and thus reasonable expectations of privacy actually diminish. This is especially true where the consenting individual agrees to a search of common premises to exculpate himself from the defendant's criminal activity.[40]

One case where such actually happened was *United States v. Long.*[41] In this case the wife was in fear of her husband and had moved out of the home. Even though she no longer lived in the home she had completely surrendered her rights of control over the family home. The court held that the wife had authority to grant consent to the police to search even though the husband was not present and the husband had changed the locks.

There are some exceptions to this otherwise broad rule. Where two or

more people enjoy equal property rights over a place, and by reasonable extension to items of property such as computers, they may still have exclusive and private zones within the shared premises when such have been reasonably set aside. For instance, housemates with separate bedrooms, spouses with private areas or containers, and housemates with separate directories on a shared computer may reasonably expect to own that space alone.

The larger question in such shared arrangements is when do these individual expectations overcome another's common authority over premises or property? Although there is no bright line test, courts have generally regarded such areas where exclusive control is maintained as being protected.[42]

Courts may also honor claims to privacy where the defendant has taken some special steps to protect his personal effects from the scrutiny of others. For instance, the placement of an item in a special place (such as a closet in a bedroom) or other place not normally considered "common area" may be enough to grant a higher expectation of privacy. Likewise, where another lacks ready access to the item in question there may be a higher expectation of privacy.[43]

In one such case the Fourth Circuit held that a mother's authority to permit police officers to inspect her 23-year-old son's room did not include his locked footlocker in the room. The court stated that the authority to consent to search "cannot be thought automatically to extend to the interiors of every discrete enclosed space capable of search within the area." The Court further stated that enclosed spaces such as "valises, suitcases, footlockers, strong boxes, etc.–are frequently the objects of [man's] highest privacy expectations, and that the expectations may well be at their most intense when such effects are deposited temporarily or kept semi-permanently in public places or in places under the general control of another."[44]

In a footnote, the Court also noted that not every "enclosed space" within a room is exempt from the reach of the authorized search area. A rule of reason applies, one that considers the circumstances "indicating the presence or absence of a discrete expectation of privacy with respect to a particular object."

One way this relates to the computer crime case is the expectation of privacy one might have on a shared computer. For instance, does the creation of a separate directory–one set off from other shared directories–create a higher level of privacy than found for shared directories? The courts have looked at this issue in a limited context.

Simply setting of a separate directory may not be enough to warrant the higher level of privacy needed to overcome a third party consent search. On the other hand, the more effort that is taken to set that directory and its contents aside the more reasonable the expectation of privacy becomes. Thus, creating a separate personal directory on a computer may not sufficiently

mark it as exclusive, but protecting that separate directory with a secret password may "lock the container" so that none may enter with express consent or a warrant.

The courts have also placed a bit of a burden on investigators to go beyond merely asking for permission. The investigator must actually have grounds for believing the person granting permission has the authority to do so. Where other factors indicate otherwise the consent itself may not be enough. For instance, in *Illinois v. Rodriguez,*[45] the Supreme Court held that a consent search is valid when police are reasonable in thinking they have been given authorized consent. The Court cautioned that police cannot simply rely upon someone at the scene who claims to have authority if the surrounding circumstances indicate otherwise. If such authority is unclear, the police are obligated to ask more questions. Determining who has power to consent is an objective exercise, the Court stated, and the test is whether the facts available to the police officer at the moment would warrant a person of reasonable caution to believe that the consenting party had authority over the premises.

d. Spousal Consent

Under the *Matlock* "common authority" approach, most spousal consent searches are valid. Although spouses who create exclusive areas may preclude their partners from consenting to a search, that circumstance will be unusual. Indeed, spouses do not establish "exclusive use" just by being the only one who uses the area; there must be a showing that the consenting spouse was denied access.

One example of this can be found in *United States v. Duran,*[46] where the defendant and his wife lived on a farm with several outbuildings. The wife consented to the search of a building that she believed defendant used as a private gym. Upon entering the police found marijuana plants inside the gym area. In addressing the issue of consent the court emphasized the presumption that the entire marital premises are jointly held and controlled by the partners, and said this presumption can be overcome only by showing that the consenting spouse was actually denied access to the area in question.

With spouses, as with roommates, the creation of a "reasonable belief" rule allows investigating officers to draw reasonable conclusions based upon the situation they encounter, about who has authority to consent. In the absence of objective evidence to the contrary, investigators will be reasonable in presuming that spouses have authority to consent to a search of anything on the marital property. Based on the *Duran* holding it would appear that the proof of exclusivity is foist upon the defendant.

e. Parental Consent

In discussing the ability of a parent to consent to the search of a child's room we must first distinguish between adult children living at home and minor children. One of the side notes to many of the more recent computer cases is that the defendants were often adults living at home with parents. This creates a situation somewhat like that of a housemate, and to some extent this has been covered in our earlier section.

Under the *Matlock*[47] rationale a parent may have the ability to consent to the search of all common areas in a family home. The ability to consent may be limited, though, when the area is no longer a common use area. For instance, where an adult child living at home with a parent has a separate entrance there may be a higher expectation of privacy. Similarly, where the adult child has placed locks or other devices on doors to restrict entry to a room there may be a higher expectation of privacy. For all practical purposes the issue is decided by looking at the not only the question of commonality in area use but also in the relationship between adult child and parent.

With regard to minor children, the courts have found parents to hold superior rights in the home and "even rather extraordinary efforts by the child to establish exclusive use may not be effective to undermine the parents' authority over their home, including rooms occupied by the child."[48] Therefore, if parents consent to a search and seizure of floppy disks or passwords locked in the minor child's room, that consent should be upheld.

f. Employer Consent

The first issue that arises when dealing with consent by an employer is the question of employer type. As a general rule, an employer falls into one of two categories: public (government) or private. Public employers are often restricted by the contents of the Fourth Amendment while private employers have much more latitude.

In construing the reach of the Fourth Amendment into the workplace, the Supreme Court has held that government employers may search employee offices, without either a warrant or the consent of the employee, when the search is administrative in nature. Anything else may fall under the protections of the Fourth Amendment.[49]

The Court found that government employees can have a reasonable expectation of privacy even though the physical area is owned by the government. The realities of the workplace, however, suggest that an employee's expectation of privacy must be reduced to the degree that fellow employees, supervisors, subordinates, guests, and even the general public may have access to that individual's work space.

Recognizing that government agencies could not function properly if supervisors had to establish probable cause and obtain a warrant whenever they needed to look for a file in an employee's office, the Supreme Court held that two kinds of searches are exempt. The first are commonly identified as "non-investigatory, work-related intrusions" which are necessary for the conduct of business. Such intrusions include the ability of an employer to go into an office to search for a file, record, or other work-related item.

The second is "investigatory search for evidence of suspected work-related employee misfeasance." These intrusions are permissible without a warrant so long as the search is not intended to produce evidence used at a criminal trial. The search should also be "reasonable" to the extent that only the areas most appropriate for the evidence sought have been searched and should be judged by the standard of reasonableness.[50]

When judging reasonableness the courts have given us some guidance. For instance, the Supreme Court has stated that "[n]ot everything that passes through the confines of the business address can be considered part of the workplace context. . . ."[51] For example, the contents of an employee's purse, briefcase, or closed luggage do not lose their private character just because the employee has brought them to work.

While the circumstances may permit a supervisor to search in an employee's desk for a work-related file, the supervisor usually will have to stop at the employee's gym bag or briefcase. This analysis may have interesting implications for "containers" like floppy disks, which certainly may be either work-related or private, depending on the circumstances. It will probably be reasonable for employers to assume that floppy disks found at an office are part of the workplace, but there may be cases where a court will treat a floppy disk as if it were a personal container of private items.

This brings us to an interesting area, and one not fully examined by the courts yet. As a hypothetical let us presume that the employee maintains a floppy system (or CD-RW drive) which is used to archive files. In this case, though, the employee uses the device to store child pornography accessed through the Internet. An employer enters the officer with the intent of looking for archived files but instead finds the pornographic material. Is this "search" valid?

Applying the standards available to us at this point the short answer would be yes. Since the employer provided the computer, along with floppy drive, for the purpose of creating backups of work-related material it would be reasonable for the supervisor to look in the disk in the drive. The fact the employee left such disk in the drive lessens the expectation of privacy. Contrast this, though, with a similar situation but the employee now places the offending disk in a closed box inside the desk drawer. Is there a difference?

This is why the "reasonableness" standard will be so hard to measure. The fact is that the actions of the employee may very well have been reasonably designed to raise the level of privacy. Of course, some might argue that simply keeping such offensive material at work might lower the expectation of privacy since the employee knows work-related material is also kept in the office. Thus, an employer who reasonably believes he is looking for work related material may be protected when he discovers something much different.

Of course, there may be some government agencies where employees do consent (either expressly or tacitly) to searches of even private parcels because of the nature of the job. For example, employees with security clearances who work with classified material may expect that their purses, briefcases, and other bags may be inspected under certain circumstances. The factual variations on this "reasonable expectation" theme are endless, and–as the courts have recognized–are tied absolutely to the details of each case.

To this point the courts have not fully addressed the appropriate standard to be applied when a government employee is being investigated for criminal misconduct or breaches of other non-work-related statutory or regulatory standards. In a case involving employee drug testing, at least one court has noted, in dicta, that "[t]he government may not take advantage of any arguably relaxed 'employer' standard for warrantless searches . . . when its true purpose is to obtain evidence of criminal activity without complying with the more stringent standards that normally protect citizens against unreasonably intrusive evidence-gathering."[52]

It would appear that whenever law enforcement is conducting an evidence-gathering search, even if the search is to take place at a government office, investigators must either obtain a warrant or fall within some generally recognized exception to the warrant requirement. Appropriate consent from a third party is, of course, one of those exceptions.

Generally speaking, an employer (government or private) may consent to a search of an employee's computer and peripherals if the employer has common authority over them. Investigators and prosecutors must consider whether, under the facts, the employee would expect privacy in those items and whether that expectation would be objectively reasonable. Relevant factors worth considering include whether:[53]

1. the area/item to be searched has been set aside for the employee's exclusive or personal use (e.g., does the employee have the only key to the computer or do others have access to the data);
2. the employee has been given permission to store personal information on the system or in the area to be searched;
3. the employee has been advised that the system may be accessed or

looked at by others;
4. there have been past inspections of the area/item and this fact is known to the employee; and
5. there is an employment policy that searches of the work area may be conducted at any time for any reason. And when the employer is the federal government, another factor is
6. whether the purpose of the search was work-related, rather than primarily for law enforcement objectives.

There are currently no cases specifically addressing an employer's consent to search and seize an employee's computer (and related items). But there are cases that discuss searches of an employee's designated work area or desk. For example, the Seventh Circuit has upheld the search of a hotel room that served as a welfare hotel's business office after the hotel owner consented.[54]

The room searched was used by the defendant/manager of the hotel for hotel business, the hotel's books were stored there, and the room was also used by doctors and welfare officials when they visited residents. The manager kept the key to the room. In affirming the manager's theft and forgery convictions (based in large part on documents seized from the business office/hotel room), the Seventh Circuit found that the hotel owner had the requisite control over and relationship to the business office to consent to its search.

The court rejected the manager's argument that she had sole control over the business office because she generally had the key. The court found that the owner could request access to the room at any time, that the room was shared with others (visiting physicians and welfare officials), and that the items sought were business records (e.g., welfare checks that the manager had forged). Thus, the manager did not have exclusive control over the area nor was it for her personal use. In addition, the purpose of the search was "employment related," since the manager was defrauding the employer and the customers.

Another case worth looking at is *United States v. Gargiso*.[55] In this case the Second Circuit upheld the search of a locked and wired-off area in the basement of a book company. The company's vice-president consented to the search. The defendant, an employee of the book company, objected to the search. Both the defendant and the vice president had supervisory authority over the area searched, and both also had keys to the area, as did other company personnel. The court found that the vice president's control over the area was equal to that of the employee's, making the consent effective. The vice president had sufficient control over the area to permit inspection in his own right and the employee had assumed the risk that the vice president would do so.

In both cases we see the employer, or the employers designate by way of supervisors, consenting to a search. In both cases the court looked to the authority of the supervisor to consent as well as the reasonable expectation of privacy. It is likely that this type of analysis will be applied in computer cases as well. Thus, when an employer controls a network it might be said that he has authority to authorize a search. Of course, one must also remember the statements earlier concerning expectations of privacy and the lengths to which one might go to protect that privacy. With that in mind let us turn to a more detailed analysis of the computer network and rights of privacy.

g. Networks: System Administrators

As we have seen to this point the courts will often examine the "totality of the circumstances" when deciding these questions. The pivotal question is when does an employee create a true expectation of privacy while at work? For stand-alone computers there may be a bit easier task at hand. After all, the use of passwords and other privacy devices will help us establish such expectations. But what about networks such as the LAN or WAN?

The difficulty is a practical one. In the physical world, individuals often intuitively understand their rights to control physical space and to restrict access by others because they can observe how everyone uses the space. For example, with filing cabinets, employees can see whether they are located in private areas, whether others have access, whether the cabinets are locked, and who has the keys. While explicit company policies certainly help to clarify the situation, employees can physically observe company practices and will probably conclude from their observations that certain property is or is not private.

When we move to the electronic environment the boundaries become much more fuzzy. Because we can't see the electronic barrier set up by a directory, password, or closed file it is harder to imagine them as being "private." Employees cannot see when a network administrator, supervisor, or anyone else accesses their data. They cannot watch the way people behave with data, as they can with a file cabinet, and deduce from their observations the measure of privacy they ought to expect.

As a practical matter, system administrators can, and sometimes do, look at data. But when they do, they leave no physical clues that would tell a user they have opened one of his files. Lacking these physical clues, some users who are unfamiliar with computer technology may falsely but honestly believe that their data is completely private. Will the courts hold this false belief to be one that society is prepared to recognize as reasonable? Will the courts still find it reasonable, even when a user knows that there are such people as system administrators who are responsible in some fashion for

operating and securing the entire network?

Prosecutors who face these issues should be ready to argue that reasonable network users already understand the role and power of system administrators. In fact, the shared network is much more akin to a public library than to a private filing cabinet. No library patron would expect privacy when they place a document inside a book in the library. Too many other people have access; not to mention the librarians and other library staff charged with keeping the books in order and well preserved. Likewise, network administrators have certain "librarian-like" duties necessary to maintain an efficient network.

Absent some guarantees to the contrary, reasonable users will also expect system administrators to be able to access all data on the system. As a general rule many network administrators now publish "rules" setting out their right to access data as a "housekeeping" part of their job. Unless these policies specifically state that certain areas are private, the user generally assumes they will be accessible by network workers.

From a practical standpoint investigators should not assume that network administrators have full access (and right to give consent) to everything on the network. The effective investigator will presume some expectation of privacy is in place by users and work from the presumption that a warrant may be needed. This way, when the investigator encounters such roadblocks as passwords or encrypted files, he will already be prepared to take appropriate legal action.

One area where an investigator might also be careful is in the access of information that might be destroyed or altered before a warrant is issued. As we have discussed in earlier sections this creates a true exception to the warrant requirement. An investigator may then request a network administrator give consent to allow a copy of the files to be made. True access is not yet made (and will come when the warrant is obtained) but by securing the files beforehand the investigator has prevented potential disaster.

As with most of the consent issues we have examined, the circumstances of each case will dictate the wisest approach. For the most part, though, investigators and prosecutors should explore all these questions before they just ask a system administrator to produce a user's files. One should remember that warrants are preferred and that exceptions are just that.

h. Informants and Undercover Operatives

As in other types of investigations, it is often helpful to use informants or undercover investigators to develop evidence. In some cases, such as the lone hacker, they may be of limited value. In other cases, such as WAREZ sites or pornographic distribution points, the informant may be able to access

information not readily available to law enforcement.

One question that has arisen in earlier BBS cases is whether the access granted to an informant is enough to also allow investigators to enter. In other words, as an investigator can you use an informer to gain access to areas that you would not otherwise be admitted to.

In addressing this issue it is important to consider the way many BBS and other limited systems are set up. These highly controlled environments may have various levels of access granted to different users. For our purposes let us use some of the common pornographic sites found on the Internet today. Most commercial sites require the user to have an access code before they are permitted to see material on the site. Most of the time this limited access is a moneymaking method, but in others it is a way to limit potential criminal liability for illegally distributed materials.

These systems often have multiple levels of access. Once a user is admitted to the "public areas" he may be later "invited" to enter more secure areas of the site. As a general rule the System Operator (sysop) may even require an "introduction" from another member before allowing the new user the highest level of access. This method gives some control to the sysop and establishes a clear expectation of privacy as to certain materials.

Both the Ninth and Tenth Circuits have addressed cases where informants were used to access higher levels of closed systems. Each of these federal appeals courts have written, in dicta, that an undercover participant must adhere scrupulously to the scope of a defendant's invitation to join the organization.[56] In other words, if I am invited to join, but told that I cannot allow others to use my privilege, then I must adhere to such proscriptions.

What this means is that in a closed system, such as a BBS or other system with limited access, the informant or undercover agent must not exceed his authorized access. The simple fact is that granted access to the individual informant is not in and of itself a grant of access to anyone else. Thus, the law enforcement officer using the informant may not have access to the same areas.

One can see the justification for this by analogy to other cases. For instance, in a drug case it is clear that permission to enter a crack house given to an informant is not the same as permission given to the uniformed police officer. The informant may certainly enter but the police cannot even though he may claim to be using the informant's rights of entry.

Does this mean that what the informant sees inside is useless? No. In fact, everything the informant sees can be used to obtain a warrant later. The warrant is then used to gain access to the system not otherwise granted by the owner. Just like the information gained by an informant in a drug house, the informant may observe and report as much as they are allowed to see.

i. Public Schools

The issues arising from warrantless searches in public schools are a relatively recent phenomena. Many have argued that since the public schools are supported by tax dollars there is little or no expectation of privacy, and as such school authorities–including school police–should have a right to search anywhere on school grounds.

Opponents have strongly argued that the expectation of privacy does not stop merely because one chooses to use a public facility. It is also argued that if searches are allowed at public schools then they will next be allowed in public restrooms, public recreation areas, and other public places where one might expect even a modicum of privacy.

In *New Jersey v. T.L.O.,*[57] the Court set forth the principles governing searches by public school authorities. The Court held that the Fourth Amendment does apply to searches conducted by public school officials because "school officials act as representatives of the State, not merely as surrogates for the parents." However, "the school setting requires some easing of the restrictions to which searches by public authorities are ordinarily subject."

The Court explained that neither the warrant requirement nor the probable cause standard is appropriate when dealing with the public school setting. Instead, a simple reasonableness standard governs all searches of students' persons and effects by school authorities. The Court explained that this single rule will permit school authorities "to regulate their conduct according to the dictates of reason and common sense."[58]

This case does not give school authorities unlimited power to search. From the outset it is clear that a search must be reasonable before it will be allowed. The Court had held that there must be "reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school."[59]

School searches must also be reasonably related in scope to the circumstances justifying the interference, and "not excessively intrusive in light of the age and sex of the student and the nature of the infraction." In applying these rules, the Court upheld as reasonable the search of a student's purse to determine whether the student, accused of violating a school rule by smoking in the lavatory, possessed cigarettes. The search for cigarettes uncovered evidence of drug activity which was later held admissible in a prosecution under the juvenile laws.[60]

ENDNOTES

1. 5 Coke's Rep. 91a, 77 Eng. Rep. 194 (K.B. 1604).

2. 331 U.S. 145 (1947).
3. 334 U.S. 699(1948).
4. Id. at 705.
5. *United States v. Rabinowitz,* 339 U.S. 56, 66 (1950).
6. *Chimel v. California,* 395 U.S. 752, 761 (1969).
7. *Terry v. Ohio,* 392 U.S. 1, 20 (1968).
8. See, *G.M. Leasing Corp. v. United States,* 429 U.S. 338, 352-53 (1977) (unanimous); *Marshall v. Barlow's, Inc.,* 436 U.S. 307, 312 (1978); *Michigan v. Tyler,* 436 U.S. 499, 506 (1978); *Mincey v. Arizona,* 437 U.S. 385, 390 (1978) (unanimous); *Arkansas v. Sanders,* 442 U.S. 743, 758 (1979); *United States v. Ross,* 456 U.S. 798, 824-25 (1982).
9. One of the pivotal cases leading to this change was *Katz v. United States,* 389 U.S. 347, 353 (1967).
10. See, *Illinois v. Rodriguez,* 497 U.S. 177, 189 (Justice Stevens joining Justice Marshall's dissent); *New Jersey v. T.L.O.,* 469 U.S. 325, 370 (1985) (Justice Stevens dissenting); *California v. Acevedo,* 500 U.S. 565, 585 (1991) (Justice Stevens dissenting).
11. 468 U.S. 897, 914 (1984).
12. See, *Horton v. California,* 496 U.S. 128 (1990).
13. 455 U.S. 1 (1982).
14. *Harris v. United States,* 390 U.S. 234 (1968).
15. 374 U.S. 23 (1963).
16. *Arizona v. Hicks,* 480 U.S. 321 (1987).
17. *United States v. David,* 756 F. Supp. 1385, 1392 (D. Nev. 1991).
18. 935 F.2d 641, 642 (4th Cir.), cert. denied, 112 S. Ct. 423 (1991).
19. See, *United States v. Arias,* 923 F.2d 1387 (9th Cir.), cert. denied, 112 S. Ct. 130 (1991); see also, *Mincey v. Arizona,* 437 U.S. 385, 392-93 (1978).
20. *United States v. Reed,* 935 F.2d 641 (4th Cir.), cert. denied, 112 S. Ct. 423 (1991).
21. *United States v. Houle,* 603 F.2d 1297 (8th Cir. 1979).
22. *United States v. Patino,* 830 F.2d 1413, 1416 (7th Cir. 1987); cert. denied, 490 U.S. 1069 (1989).
23. 756 F. Supp. 1385 (D. Nev. 1991).
24. 526 F.2d 654 (5th Cir.); cert. denied, 429 U.S. 823 (1976).
25. *United States v. Ramsey,* 431 U.S. 606 (1977); cert. denied, 434 U.S. 1062 (1978).
26. *United States v. Scheer,* 600 F.2d 5 (3d Cir. 1979).
27. *Schneckloth v. Bustamonte,* 412 U.S. 218, 219 (1973).
28. *United States v. Milan-Rodriguez,* 759 F.2d 1558 (11th Cir.); cert. denied, 474 U.S. 845 (1985), and cert. denied, 486 U.S. 1054 (1988).
29. *United States v. Scott,* 578 F.2d 1186, 1189 (6th Cir.), cert. denied, 439 U.S. 870 (1978).
30. *United States v. Price,* 599 F.2d 494, 503 (2nd Cir. 1979).
31. See, *United States v. Mendenhall,* 446 U.S. 544, 557-8 (1980); see also, *United States v. Caballos,* 812 F.2d 42 (2d Cir. 1987).
32. *Schneckloth v. Bustamonte,* 412 U.S. 218, 231-33 (1973).
33. *United States v. Matlock,* 415 U.S. 164, 171 (1974) (valid consent by woman with

whom defendant was living and sharing the bedroom searched). See also *Chapman v. United States,* 365 U.S. 610 (1961) (landlord's consent insufficient); *Stoner v. California,* 376 U.S. 483 (1964) (hotel desk clerk lacked authority to consent to search of guest's room); *Frazier v. Culp,* 394 U.S. 731 (1969) (joint user of duffel bag had authority to consent to search).

34. *Illinois v. Rodriguez,* 497 U.S. 177 (1990). See also *Florida v. Jimeno,* 500 U.S. 248, 251 (1991) (it was "objectively reasonable" for officer to believe that suspect's consent to search his car for narcotics included consent to search containers found within the car).
35. *United States v. Griffin,* 530 F.2d 739, 744 (7th Cir. 1976).
36. 950 F.2d 331 (6th Cir. 1991)
37. 756 F. Supp. 1385 (D. Nev. 1991).
38. 415 U.S. 164 (1974).
39. Id. at 171 n.7.
40. For an excellent discussion of this area see, W. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 8.3(b) at 244-45 (2d ed. 1987).
41. 524 F.2d 660 (9th Cir. 1975).
42. *Frazier v. Cupp,* 394 U.S. 731, 740 (1969).
43. *United States v. Block,* 590 F.2d 535 (4th Cir. 1978).
44. Id. at 541.
45. 497 U.S. 177 (1990).
46. 957 F.2d 499, 504-5 (7th Cir. 1992).
47. 415 U.S. 164 (1974).
48. See, LaFave § 8.4(b), at 283.
49. *O'Connor v. Ortega,* 480 U.S. 709 (1987).
50. Id. at 725-6.
51. Id. at 717.
52. *National Federation of Federal Employees v. Weinberger,* 818 F.2d 935, 943 n.12 (D.C. Cir. 1987).
53. See generally *O'Connor,* 480 U.S. at 717 (employee's expectation of privacy must be assessed in the context of the employment relationship).
54. *United States v. Bilanzich,* 771 F.2d 292 (7th Cir. 1985).
55. 456 F.2d 584, 587 (2d Cir. 1972).
56. *United States v. Aguilar,* 883 F.2d 662, 705 (9th Cir. 1989), cert. denied, 498 U.S. 1046 (1991); also see, *Pleasant v. Lovell,* 876 F.2d 787, 803 (10th Cir. 1989).
57. 469 U.S. 325 (1985).
58. 469 U.S. at 343.
59. Id. at 342.
60. Id.

APPENDICES

Appendix A

IDENTIFYING THE COMPUTER COMPONENTS

---

1. A Brief History of the Modern Computer
2. Advances in Computer Design
3. Desktop IBM Compatible Computer System
   a. System Components
   b. System Components
      i. The Case and CPU
      ii. The Motherboard
      iii. Bus Slots and I/O Cards
      iv. Peripherals
      v. Data Storage
      vi. Powe Supply and Connectors

---

1. A BRIEF HISTORY OF THE MODERN COMPUTER

A modern computer is largely a collection of electronic switches used to represent as well as to control the routing of data elements. As we discussed in an earlier chapter the computer is an electron manipulator. It uses electrons to represent data in a very simple way. We can think of it much like a light switch with an on and off position.

By the use of *binary digit representation* the computer sets up a series of "on" and "off" statements to represent information. In essence, the presence of an electron in a given spot of the processor represents an "on" state while the absence of an electron equals "off." By manipulating and analyzing these on and off states the computer performs its assigned tasks.

In a binary digit system the representing electron is either present or not. To borrow an analogy by way of a common communication system used by many roommates over the years we can say that a binary digit representation system is much like the "tie on the doorknob." In this example, one roommate wishes to entertain a

guest in the apartment and does not want the other to interrupt. A signal is devised where the presence of a tie on the exterior doorknob tells the second roommate not to enter. The tie is either on the doorknob or it is not. Such a signal is a true binary system.

The computer uses this simple system in the same way. The electron is either present or it is not. When the processor looks for the electron it will either find it or it will not. If the electron is missing then the processor does one thing but if it is present then the processor does another.

Typically these single states of presence or absence are known as *bits*. The term bit is short for *Binary Digit,* and for our purpose is the presence or absence of the electron. An "on" bit means the electron is present and an "off" bit means it is absent.

By stringing the *bits* together we create *bytes*. The traditional *byte* is eight *bits*. In other words, a *byte* is a series of eight "on" or "off" states. By placing these bits in specific orders we create the equivalent of computer words.

A common method for explaining this system to students is to construct a platform with a light on it. The light represents the "bit." When the light is off then there is no electron in place. (See Figure A-1). When the light is off then we can say that the light is in the *zero* (0) or *off* state.

Figure A-1. Light bulb diagram.

To represent the *on* state, also known as the one (1) state, we would simply turn the light on. Figure Appendix A-2 illustrates this concept with the illuminated light bulb. This simple *on* or *off* system allows us to create simple messages. A light in the on position would tell our roommate to stay out while a light in the *off* position would signal the coast is clear.

Figure A-2. Light bulb (lit) diagram.

We can create more complicated messages by combining groups of lights. Computers use this system when they combine the single bit (the on or off light) with seven other bits to create a byte. In doing this we have in fact created multiple combinations which can then be used to represent a single message. Figure A-3 is an example of an eight light bulb (8 bit) system with none of the lights lit.

Figure A-3. Series of light bulbs.

In the above example all the light bulbs are in the *off* or *zero* state. This in itself may have a meaning, depending on our program, or it may be simply a *null* state meaning that there is nothing there. To create our code we simply assign a word, letter, number, or phrase to each combination of lights. For instance, if the first light is *on* and all the others are *off* then we can say that this state represents the letter "A" in our alphabet (see Figure A-4).

Figure A-4. Series of light bulbs (lit).

Turning on the number two light, while leaving all the others off, can then represent the letter "B." We can then move through the combination of lights, with one on and the others off, until we arrive at the letter "H." In this example, if we can only have one light on at a time then we are restricted to no more than 8 combinations (not counting all off). We can expand our abilities, though, by simply allowing multiple lights to be on in combination with each other.

For instance, we turn the first two lights on to represent the letter "I," and then work our way through the sequence until we cover all the letters in our alphabet. In this sense, to represent "I" we might illuminate the first two lights and leave the next six in the off position. The letter "J" would therefore have the combination of light 1 and 3 on with the others off. By using this combination each letter in the alphabet is eventually assigned a light combination.

With this system there are sixty-four different combinations of lights, and each combination represents a different character, word, or message. We cannot only cover the twenty-six letters of the western alphabet (A through Z) but also the ten base numbers (0 through 9). That leaves us plenty of room for basic punctuation as well. The point, as you have probably gotten by now, is that with such a system we are limited only by our own imagination on what combinations we can use to create entire sentences, paragraphs, and complicated equations.

2. ADVANCES IN COMPUTER DESIGN

All computers, from the earliest to today's extremely fast and complicated models, use this same basic system for instruction and communication. The earliest computers used vacuum tubes as switches to signify the on or off state. The tubes worked but made the processing slow since it took longer for the mechanical tubes to respond to the on or off signal.

The speed of these new computing machines was greatly increased when engineers working at Bell Laboratories invented the *transistor* in 1948. The invention of the *transistor,* also known as the *semiconductor,* was one of the most important developments leading to the expansion of computers. The transistor is essentially a solid-state electronic switch which speeds up the on and off states. Now, instead of waiting for a mechanical switch in a vacuum tube to open or close the modern computer waits microseconds for an electronic switch to flip.

A positive side effect of the transistor is lower power consumption. Vacuum tubes tended to get very hot. As such, the machines had to be kept cool and the tubes had to be spaced carefully inside the computer case. This meant that computers in the early years were large machines with special cooling systems. Today's transistor runs at much lower temperatures and allows engineers to shrink the overall package to a surprisingly small size. Heat is still an issue inside every computer, but the problems of the earlier years have been greatly reduced by transistor design.

Early transistors contained single relay switches, but in 1959 engineers at Texas Instruments invented a new circuit that contained multiple relays. The new chip, known as the *integrated circuit* (IC), was a new semiconductor design that contained more than one transistor on the same material. This meant that engineers could connect the transistors without wires. In other words, instead of having a transistor on one side of the device connected to a transistor on the other side with wires the *IC* allowed the two transistors to be built virtually side by side. An interesting note is that the first ICs had only six transistors built onto them. Today, the Pentium IV class chip has over six million built onto a silicon wafer not much bigger than a deck of cards.

The next step in computer evolution came in 1969 when Intel introduced a memory chip capable of storing just over 1,024 bits. This was commonly known as a *kilobit* or *1k bit.* One must remember that a bit is a single unit. Grouping eight bits together creates the byte. Thus, the new Intel chip held 1,024 bits or roughly 128 bytes.

This was a phenomenal accomplishment at the time and helped launch Intel on the path to a future as a leading manufacturer in computer chip technology. To put this in perspective, though we must first point out that today memory chips are measured in millions of bytes rather than thousands of bits. Where the 1969 Intel chip held 1,024 bits (or 128 bytes) the computers sold for home use today contain 32 megabytes of memory or more. In fact, the newest computers now boast 256 megabytes of memory on a single chip.

While Intel's contributions to memory were impressive their most significant work came in the form of the microprocessor. The microprocessor in a computer is the equivalent of the engine in an automobile. The engine is the main component that makes a car run. The same can be said about the microprocessor when it comes to computers.

The first microprocessor, the Intel 4004, was introduced in 1971, and operated on 4 bits of data at a time. Originally the 4004 was supposed to be the brains for a new calculator, but it was soon adapted as a general purpose microprocessor. The chip handled 4 bits or four "on" or "off" units at one time.

This greatly limited the speed of the earliest computers, but that would soon change as advances quickly came about. The chip's successor, introduced in 1972, was dubbed the 8008. This chip is commonly referred to as an 8-bit processor because it worked on 8 bits at a time.

While Intel was working on developments in processor technology other manufacturers such as IBM were working on larger computer systems. Initially IBM focused on the business market and other, sometimes much smaller, manufacturers focused on the home and hobbyist market. Intel was certainly a prime choice for the new computers, but they were not the only manufacturers. Other manufacturers such as Motorola introduced their own microprocessors as well, and by the early eighties hobbyist had several choices in chips on the open market.

Early "microcomputer" kits based on the 8008 chip were developed by 1973. Though not very powerful by today's standards, these early kits allowed hobbyist to control small electronic components such as lights and switches. Most of the work in this area was done by students or others interested in electronics. These earliest of the personal computer systems were really nothing more than toys to most, but they did help signal the strong interest for computers that was already being felt throughout the industry.

The introduction of the Intel 8080 processor signaled an emphasis on more powerful micro-processors in the market. The 8080 was ten times faster than the earlier 8008. The processor was also capable of accessing the now much larger memory chips such as the new 64k chips.

In the January 1975 issue of *Popular Electronics,* a magazine targeted at hobbyist, the world was introduced to the *Altair* computer kit. This is considered by most to be the first personal computer. The kit included an Intel 8080 processor, a power supply, a front panel with a large number of lights and 256 bytes (not kilobytes) of memory.

The kit sold for $395, but what was important about this kit is that it laid the firm foundation for later personal computer design and use. The kit included an "open

architecture bus" (slots) that prompted various add-ons and peripherals from aftermarket companies. Many of today's PCs still use this open architecture which allows users to expand the computers to use special add-on devices. The kit also inspired other companies to write programs in the *CP/M* (Control Program for Microprocessors) operating system.

Another interesting tidbit is that a then small company serving a relatively tiny niche of the computer market introduced their own version of a programming language for the Altair. The company was *Microsoft* and the language they developed for the Altair was *Microsoft Basic.* Microsoft used this stepping stone to gain access to other manufacturers as the computer market began to grow.

Also in 1975 IBM entered the microcomputer market with the introduction of its Model 5100. This was the first computer designated commercially as the "Personal Computer." The machine had 16k of memory, a built-in 16-line display capable of displaying 64 characters across, and a built-in *Basic* language interpreter. Data storage came through a DC-300 cartridge tape drive, which came with the machine for a price of nine thousand dollars ($9,000.00).

Obviously IBM was not interested in the true hobbyist market. At that time users, who often called themselves *hackers,* spent no more than $500 on components used to build a low-budget kit. IBM did not realistically enter the *Personal Computer* market until 1980. In the seventies the company continued to produce high-end machines targeted at larger companies. By late in the decade, though, IBM had begun its move to dominate the growing market. Their new machines targeted the small and medium size businesses for sales.

While Microsoft was still focusing on the large business market there were other, much smaller, companies that focused on the hobbyist and personal user. In 1976 another new company which would make a large impact on the PC market emerged. The company's name was *Apple,* and their first product was the Apple I Computer.

Like many of the early computer companies during this time, Apple was literally started by two friends in their garage. The new Apple, which sold for $695, consisted of a main circuit board screwed to a piece of plywood. A case and power supply were not included at that price. Typically the system was sold to an electronic hobbyist who could build his or her own power supply.

The Apple I was Steven Wozniak's first contribution to the personal computer field. It was designed over a period of years, and was only built in printed circuit-board form when Steve Jobs insisted it could be sold. It debuted in April 1976 at the Homebrew Computer Club in Palo Alto, but few took it seriously. The Apple I was based on the *MOStek 6502* chip, whereas most other "kit" computers were built from the Intel 8080. The Apple I was sold through several small retailers, and included only the circuit board. A tape-interface was sold separately, but you had to build the case.

Just over a year later Apple introduced the Apple II computer. The system soon caught on as a favorite among hobbyist. The Apple II was also based on the 6502 processor. Soon thousands of Apple fans began buying add-ons for their new computers, and the personal computer market began to flourish.

Within two years the Apple II computer became the most popular computer in the relatively narrow field. Soon it was clear that there were only two types of personal computer systems on the market. On one side was the Apple with its throngs of supporters and massive software offerings. On the other were the die-hard users who had worked on the original Altair system using primarily CP/M as the operating system.

This all changed in 1980 when IBM decided to enter the personal computer market seriously. The company established the Entry System Division, located in Boca Raton, Florida, to develop its new line of Personal Computers. Soon twelve IBM engineers and designers produced what would be known as the *IBM PC*.

One of the significant moves by the design team was the choice of the 8088 processor. The 8088 offered a much larger memory address limit and an internal 16-bit data bus. The system allowed only an 8-bit external data bus, and later this would hamper development of peripherals for the system, but in the early stages this combination allowed for the development of an entry level computer. Likewise, the limitation on memory address limit (1 megabyte initially) built into the 8088 limited some programs. That was all eventually overcome with new chips, but in time it set up a tremendous controversy for users.

The IBM machines quickly replaced the machines running CP/M in the market. Apple and IBM competed during the early part of the decade, but IBM was quickly taking the lead. A significant help in this movement came from Microsoft. Once again in the right place at the right time, Microsoft developed the operating system for the IBM machines. This was not the only interesting move that Microsoft made in the still young personal computer industry.

Some say that it was a brilliant move by Bill Gates (co-founder of Microsoft) to basically give the operating system away initially. The system, dubbed *DOS* for Disc Operating System, was the heart of the computer. All application programs had to be written to run under the operating system, and of course Microsoft was now one of the leading sources for the new application programs. In essence, by giving away the operating system Bill Gates guaranteed that it would be on almost every computer sold during the time. This meant that there was a built-in market for Microsoft's other products such as their spreadsheet, word processor, and other programs.

Another contributing factor is the availability of the IBM components through other sources. Smaller manufacturers could "clone" the IBM system by buying the parts directly. Soon, IBM's worst competition was based on its own designs. For Bill Gates, though, the market was like a candy store. As "clones" quickly hit the market, including from manufacturers whom Gates had made deals with for the distribution of low-cost DOS operating systems, the Microsoft Empire began to grow.

Apple was not completely out, and new innovations brought Apple back to the forefront of personal computing. Apple's big push came with the introduction of the *Graphical User Interface* or *GUI* (pronounced Gooey) which they acquired from Xerox. The *GUI* had its roots in the fifties but was not developed until the seventies when a group at the Xerox Palo Alto Research Center (PARC) developed the *Alto,* a GUI-based computer. The Alto was the size of a large desk, and Xerox believed it

unmarketable. Jobs took a tour of PARC in 1979, and saw the future of personal computing in the Alto. Although much of the interface of both the Lisa and the Mac was based (at least intellectually) heavily on the work done at PARC, and many of the engineers there later left to join Apple, much of the Mac OS was written before Job's visit to PARC.

The machine Apple chose to introduce its GUI based OS was *Lisa*. Named for one of its designer's daughters, the Lisa was supposed to be the next big thing in computing. Aimed mainly at large businesses, Apple said the Lisa would increase productivity by making computers easier to work with.

The Lisa had a Motorola 68000 Processor running at 5 Mhz, 1 MB of RAM, two 5.25" 871k floppy drives, and a built in 12" 720 x 360 monochrome monitor. The Original Lisa had two floppy disc drives, but by 1984 Apple moved to a single 400k disc drive with an external five (5MB) megabyte hard drive. The original Lisa's price came in at a whopping $9,995 which made it prohibitively priced for most medium to small business.

Apple soon set about upgrading the machine, lowering the price, and by 1984–when Apple introduced the Macintosh–the Lisa sold for less than $5000. The price decrease did not substantially raise sales, but there was enough there for Apple to be convinced the GUI-based OS would be a viable alternative to the "command prompt" oriented IBM systems.

Work continued to develop the GUI systems, and by 1984 Apple was poised to make a dramatic shift in computer focus. A new line of computers known as the Macintosh was introduced. The machine originally sold for $2,495, and included a keyboard, mouse, built-in monochrome monitor, and a 3.5" floppy drive that held 400k discs.

The Mac was built around the new Motorola 68000 chip running at 8 MHz, which was significantly faster than previous processors. Users found the Apple system easier to learn and employ. One of the major advantages was the use of graphics to symbolize commands that had once been typed on the keyboard. For instance, instead of typing in the name of the program one wished to run, the user of the Mac simply used the new *mouse* to "point and click" on an icon. The clicking of the mouse button acted as the command to launch the program.

Other common tasks, such as highlighting text in a document for formatting, became "point and click" tasks instead of lengthy typed commands. The mouse also allowed users greater control over many items not easily manipulated before. For instance, the Mac came with a "drawing" program that used the mouse, somewhat like an electronic pencil, to actually draw very advanced graphical works.

Not to be outdone, the folks at Microsoft soon developed a GUI based operating system of their own. Not really a stand-alone system initially, the *Windows* operating system worked with the already present DOS. Users could "shell" in or out of Windows as needed. Over time users began to rely on the GUI-based systems and more programs moved away from keyboard commands to the now popular "point and click" method for computer operation.

Today Apple enjoys a moderate portion of the market, but not near what it once had in the home or hobbyist markets. Many Apple users are "die hard" fans of the

company and its flamboyant CEO, Steve Jobs. The majority of the computing market today, though, is based on the Microsoft Windows environment using the Intel 808x class processors. This combination has undergone significant changes in the past two decades and we see today computers that are capable of doing multiple tasks simultaneously. The computer world has also undergone significant changes and in the next section we will see what those changes have brought.

3. THE DESKTOP IBM COMPATIBLE COMPUTER SYSTEM

We have intentionally stayed away from an in-depth discussion of the mini and mainframe class of computers. We have also stayed away from a discussion of the blazingly fast "supercomputers" as well. The reason for this is simply money. Most consumers, and most criminals, cannot afford the larger computer systems that are available. There is more crime being committed using the average "home" or "desktop" computer than any other machine. For that reason we will concentrate on computer components that are found in the desktop class of computers.

While Apple continues to hold a small share of the overall computer market Microsoft Windows and Intel based machines (commonly called *WinTel*) dominate the market. As we discussed in the earlier section these computers are based on the original 8086 class machine introduced by IBM in the early eighties. For a time there was competition for the operating system between IBM's *OS/2* and Microsoft's *Windows 3.x* series, but within three years *OS/2* had fallen in user base to less than ten percent.

Today the standard Personal Computer (PC) sits on the desktop and is based on the Intel processor running the Microsoft Windows operating system. From a practical standpoint all WinTel systems still fall under the IBM compatible label and fit neatly into three categories:

- PC/XT Class Systems running 8-bit architecture
- AT Class Systems running 16, 32, and some limited 64 bit architecture
- Pentium Class Systems running 32 and 64 bit architecture

Avid computer users might find it hard to believe anyone is still using technology from the eighties but surprisingly there is still an estimated twelve percent of the computer market using the PC/XT class computers. Most of these systems are found in small businesses where the operator's lowest priority is keeping up with the latest technology craze. The machines still operate well and do the jobs they were originally purchased to do. Not surprisingly, though, criminals using the PC/XT class computer today commit few computer crimes. These machines are typically used for word processing, spreadsheet or financial programs, and database.

The AT Class computer is another that has fallen by the wayside among those seeking cutting-edge technology. One reason these computers are still around, though, is that the demand for "backward compatibility," the ability of a new software package to work with older machines, by consumers is very high. Systems

based on the Intel 80386 and 80486 processor are capable of running *Windows 3.0* through *Windows 95* without much modification. A few 80486 class computers can even run *Windows 98* and *2000* programs, but these machines have been highly modified in terms of memory management and hard disc storage capability. These systems are not so much distant cousins of the newer *Pentium*-based machines as they are simply older siblings.

Statistically we see more computer-related crimes being committed by perpetrators using relatively new technology. This means that the majority of crimes today are being committed on the Pentium class computer running Windows 95, 98, 2000, ME (Millennium), and even the XP version of the operating system. Of course, the generation of computers and programs will likely bring with it other unique problems. For now, though, to be an effective investigator it is important that one understand the current technology as well as the basics of system architecture and software design. Even though computer systems will change, the one constant which remains is the need to comply with certain physical and electronic certainties. With that in mind let us now move to the examination of the interior workings of the modern computer system.

a. System Architecture

The PC/XT class system (circa. 1984) focused on the expansion capabilities of the computer. The term XT stood for "eXTended" class computer, and this meant that the computer could be expanded by adding new "daughterboards" to the basic system. These systems had an 8-bit 8088 processor and an 8-bit *Industry Standard Architecture (ISA) Bus* for system expansion. The processor was capable of handling 8-bits at a time while the exchange between processor and system components also occurred at 8-bit intervals.

An easy way to think of such architecture is to compare an 8-bit system to an 8-lane highway. A single lane road can convey traffic, but only one automobile may travel the roadway at a time. With an 8-lane highway we would see 8 automobiles traveling the same direction at the same time. Conceivably the 8-lane highway would be eight times faster than the single lane roadway. This increased traffic pattern meant that computers worked faster. It also meant that instructions to the computer could be more complicated.

The *bus* is the name given to expansion slots in which additional plug-in circuit boards can be installed. The 8-bit designation comes from the fact that the ISA Bus systems can send or receive 8-bits of data in a single cycle. The data in an 8-bit bus is sent along 8 pathways simultaneously.

The next generation expanded the PC even more. The *AT* class system bumped pathways to a 16-bit architecture. The AT system, which stood for *Advanced Technology,* had a 16-bit version of the ISA Bus. Later AT class machines included a 32-bit *Enhanced Industry Standard Architecture* or *EISA.*

IBM soon offered a 16 and 32-bit *Micro Channel Architecture Bus* (MCA) which they linked to the Personal System 2 (PS/2). Other advances included a move to a 32 and 64-bit *Peripheral Component Interconnect Bus* (PCI) which is now common in many of

today's Pentium class machines. Most systems using the Pentium class processor (or the AMD processor with similar computer power) have at least three expansion slots using the PCI architecture. More powerful machines may even include five or six expansion PCI slots.

Figure A-5 depicts a motherboard which contains the expansion slots. In this photo the slots are marked to show both the PCI and ISA type slots. Original motherboards used the ISA standard, and as designs improved boards began using combinations of bus architecture.

These enhancements to the computer architecture meant that computers would perform faster. It also meant that computers could perform more complicated tasks in the same time it took to do simpler tasks. Soon the operating systems began to take advantage of hardware innovations.

In the early days of personal computer use the machine could run the operating system and only one application program at a time. The application program was the workhorse of the computer world. Applications included word processors, spreadsheets, database, and educational programs. As the hardware capability increased users found that new operating system changes allowed them to run more than one application at a time. The term *multitasking* was adopted to refer to a computer that was capable of performing several functions at a time. For instance, a user could download a file over a modem while the computer printed a document and the user himself typed on the word processor.

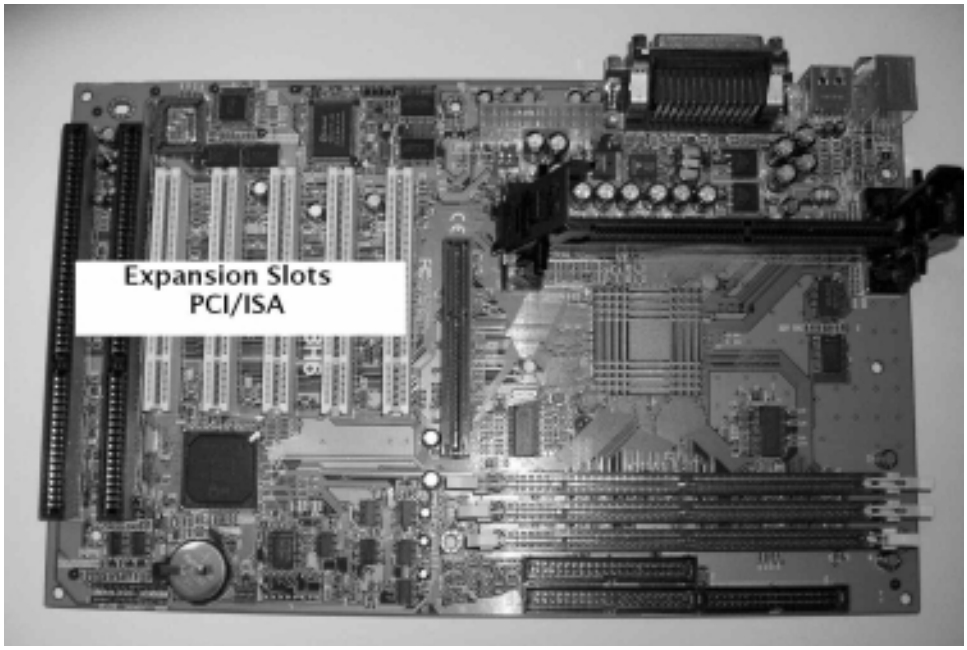


Figure A-5. Unpopulated ATX motherboard.

Other enhancements to system components meant even bigger changes. A computer processes data with the Central Processing Unit (CPU or Processor) but it needs an area to store data as well. This area is commonly called *memory* and initially it was very expensive. As we noted in the earlier section, Intel was a leading developer of memory for the first PCs, and as advances were made in memory technology the prices began to drop. This meant that users at all levels benefited from industry advances.

Advances in processor architecture doubled every eighteen to twenty-four months on an average. Likewise, memory capability doubled at the same rate. A by-product of this rapid advancement meant that prices had to fall. As manufacturers announced newer, faster, and better chips they had to sell the old line as well. The new chips, both processor and memory, tended to be high priced, but prices for the last generation typically dropped dramatically. Today, a hobbyist or other computer builder can find several generations of any given chip still available. For instance, at the time this book was produced the 2.2 Ghz Intel Pentium IV class microprocessor was just being released. At the same time consumers had the choice of all the slower Pentium IV class processor plus the Pentium III, and Celeron processors. The fastest Pentium IV costs over $500 while the entry level Celeron cost less than $100.

Soon computers went from processing 8-bit packets of data to 32 and 64-bit packets. The 8, 16, and even 32-bit machines dropped in price. Memory went from a few kilobytes to megabytes in just a few years. Machines with lower memory capacity soon dropped in price. This meant that a consumer at all levels could buy "entry level" computers for pennies on the dollar compared to years past. The IBM 5100 series once sold for over $9,000, but as computers moved forward we were soon able to buy a faster machine for under $2,000. Today, an entry-level computer with 32-bit EISA and PCI bus sells for under $500. This machine has 32-bit architecture, 20 gigabyte hard disc drive for storage, and at least 128 megabyte of Random Access Memory (RAM).

b. System Components

To this point we have concentrated on the architecture of the system processor and bus. We also hinted at enhancements to memory and storage capacity. It is now time to examine what is actually in a computer and how all this fancy talk of architecture fits together. We begin with an overview of the computer system itself and then move to the individual components within that system.

i. The Case and CPU

Since many of the electronic components of a computer system are fragile they are often enclosed in a case or box. Most cases are made of lightweight aluminum, steel, or plastic. On occasion this case, with its contents, is referred to in a generic sense as the CPU or simply as the computer. It is important to note that this case is not the entire computer system, but merely one of the many components to the system. As we proceed in this section one will quickly learn the difference between the

various components and their proper names.

Most investigators use a computer every day to write reports or perform other job tasks. The typical computer is comprised of the main computer (the case which contains the processor, drives, memory, and expansion cards), monitor, keyboard, mouse, and printer.

While many users refer to their computer itself as the CPU the reality is that it is not. The case and its individual components make up a part of the computer system. The CPU is also part of the overall computer system, and is probably the most important part. The CPU is the computer's microprocessor chip. It is the brains of the outfit.

The CPU is an Integrated Chip (IC) using *VLSI* (very-large-scale integration) technology to pack several different functions into a tiny area. The most common electronic device in the CPU is the transistor. As discussed in the earlier section, today's CPUs may contain 6 million or more transistors in a single chip.

Many confusing specifications are often quoted in discussions of processors. The reason for this is that the microprocessor may include specifications for data bus, address bus, and speed. This means that the speed of the processor is measured by what it does and how it does it. We can think of it much like an automobile where we measure the overall engine by displacement, horsepower, and fuel economy. Each measurement is important, but they also each tell us something different about the particular engine inside the car.

The best place to start when discussing the processor is the *Data Bus.* As one may recall from earlier sections, a bus is simply a series of connections that carry common signals. The data bus is the connection that carries the data between the processor and the rest of the motherboard. The larger the bus (wider) the faster data will be moved.

We can see the importance of the Data Bus more clearly when we think of the earlier discussion of bits and bytes. Computers generate signals that are represented by these off and on data bits. This means that data in a computer is sent as digital information consisting of a time interval in which a single wire carries 5 volts to signal a 1 data bit. The presence of the 5 volts, for the assigned time, gives us an "on" state.

When signaling a 0 data bit the wire carries 0 volts. In other words, no voltage on the line means no signal or a *zero* state. Again, one must remember that this is during a measured period of communication between the processor and the peripheral sending data. As you will recall from our earlier discussion on the binary system this allows us to have an "on" or "off" setting. This means that the more connections we have the more of these voltage signals that can be sent. As you will also recall, a 1-bit bus sends 1-bit of data at a time while an 8-bit bus will send 8-bits at a time.

By measuring the data bus we are merely measuring the ability of the computer to communicate between the processor and the other components of the motherboard. Thus, a computer with a 1-bit data bus can send only 1 bit down a particular roadway at a time. An 8-bit data bus allows eight bits at a time. The more bits the faster the speed of data exchange.

Another way to measure computer power is the *address bus.* The address bus is the set of pathways that carry the addressing information used to describe the memory

location to which the data is being sent or from which the data is being retrieved. As with the data bus, each connection in the architecture carries a single bit of information. The single bit is a single digit in the address. The more connections (digits) used in calculating the addresses the greater the total number of address locations. The size (width) of the address bus indicates the maximum amount of RAM that a chip can address.

In further understanding this we will stay with the highway analogy. If the data bus is the highway, and if the size of the data bus is equivalent to the number of lanes, the address bus relates to the house number or street address. The size of the address bus is equivalent to the number of digits in the house address number. For example, if the house we are looking for is on a street in which the address is limited to two-digit (base 10) number, no more than 100 distinct addresses (00 to 99) can exist for that street (10 to the power of 2).

Add another digit and the number of addresses available increase accordingly. For instance, a three-digit (3-bit) numbering system allows us to have up to 1000 distinct addresses (000 to 999). This system is equal to 10 to the 3rd power. Each added digit increases the addressing capability accordingly.

As one can quickly see, the need to advance the ability of the computer to address the data being manipulated is directly proportional to the speed by which the computer completes a task. Over time the advances in processor capability focused on an increase in this address system capability. This is illustrated by the information in Table A-1, which describes the memory-addressing capabilities of the more popular Intel family of processors.

It is important to note that the data bus and address buses are independent. Chip designers can use whatever size they want for each. This means that the designer may include a relatively broad data bus but limited address bus. Such a scheme would surely affect the overall speed of the computer, and as a general rule chips with larger data buses have larger address buses.

The size of the bus provides important information about a chip's relative power, measured in two ways. The size of the data bus is an indication of the information-moving capability of the chip while the size of the address bus tells us how much memory the chip can handle. There is yet another way to measure chip power and that is chip speed.

Table A-1. Memory-addressing Capabilities.

Processor	Bus Width	Bytes	Kilobytes bytes	Mega bytes	Giga
8088/8086	20-bit	1,048,576	1,024	1	–
286/386SX	24-bit	16,777,216	16,384	16	–
386DX/486/Pentium	32-bit	4,294,967,296	4,194,304	4,096	4
Pentium II/III (P6)	36-bit	68,719,476,736	67,108,864	65,536	64

Unfortunately, chip speed is often confused with overall chip capacity. In reality, a slower speed chip with sufficient bus capability can actually outperform one with a higher speed rating but smaller bus capacity. That is why it is important that one understand not only the chip speed but also bus size when evaluating a chip's power.

When engineers talk about chip speed they usually are referring to the frequency of the crystal oscillator. The crystal oscillator controls clock speeds using a sliver of quartz in a small container (usually made of tin). As voltage is applied to the quartz it begins to vibrate (oscillate) at a harmonic rate dictated by the shape and size of the crystal. The oscillations emanate from the crystal in the form of a current that alternates at the harmonic rate of the crystal. This alternating current is the clock signal. A typical computer system runs millions of these cycles per second and for that reason the speed is usually measured in megahertz (one hertz is equal to one cycle per second).

The smallest element of time for a processor is a single cycle. Every action requires at least one cycle and usually multiple cycles. For example, to transfer data to and from memory the 8086 class chip needs four cycles. To accommodate the system the engineers build-in *wait states* which are single cycles where nothing happens. These wait states insure that the processor is not getting ahead of the rest of the system. So in our example the 8086 with dual wait states will require four cycles plus two wait states to transfer data from memory.

Obviously, the faster computers require fewer cycles to perform a single task. The 80286-class processor requires only two cycles, plus any wait states designed into the processor, to transfer the same data. Today's Pentium processors have improved so that they require only a single wait state, and the more advanced line of Pentium chips (PIII and PIV) have twin instruction pipelines allowing them to perform two functions in a single cycle.

If we combine the three criteria we have just examined together we can see that the overall speed of the computer will vary greatly depending on the various components. An 8-bit data bus connected to a processor requiring 4 cycles for each instruction will be much slower than an 8-bit bus and a processor requiring only 1 cycle per instruction. In other words, just because a computer has a higher "megahertz" rating (the speed of the clock) does not mean it is faster than other machines with lower clock ratings. Data bus, address bus, and clock speed all combine to tell the whole story of computing power. Unless one understands all three it is difficult to fully understand the power of the computer.

With that in mind let us now turn to another area where speed can be very important. This is in the area of *motherboards* and *Add-on Cards,* which are also referred to as *daughtercards*. Both of these components contain electronic parts that affect the speed of the computer. We begin with a brief look at the motherboard.

ii. The Motherboard

The term *motherboard* comes from traditional electronics vernacular and refers to the main circuit board in an electronic system. The term is not unique to computers but is used in virtually all levels of electronics using the printed circuit board. The

main board in any system is commonly called the *motherboard* with *add-on boards* dubbed as *daughterboards*. For our purposes the motherboard is merely the main system board in the computer system while the daughter board is added on to the motherboard.

There is no true standard as to what must be placed on the motherboard as far as components are concerned. Today you will find some motherboards with only the processor, those chips necessary to serve the processor, a few expansion slots (also known as bus), and memory. Other motherboards will include video monitor controllers, disc drive controllers, and even a hard-wired speaker.

We have already seen a typical motherboard found in a Pentium class machine depicted in Figure A-5. In understanding the motherboard it is first important that one recognize that these main boards are made in a variety of sizes. The size of the board is determined in part by the case that will house it. The arrangement of the components on the board is also affected by the size of the board, the motherboard now shown in Figure A-5a is a common in size and general shape to those in today's PC.

Larger cases of course have more room, and so some boards are specifically designed for these cases. The board designed to fit in the *ATX* class case, which is usually a mid-tower design, is similar to that in Figure A-5a. Other common motherboard sizes are the *WTX, Micro-ATX,* and *AT form factor,* and each has its own unique size and shape needs.

Another important consideration when evaluating the motherboard is the type of processor it will accommodate. There are several designations with the most common today being the *Slot A, Socket 7, Socket A,* and the new *478* line. Figure A-5a shows an unpopulated board which means one without memory, CPU, or other components. These components will be added by the user and allow for greater versatility by both manufacturer and builder.

The newest level of Intel processor uses the *Socket 423* and *478*. These main boards often have some of the additional features such as video and audio devices built onboard. This is sometimes referred to as being *hardwired,* which is a holdover term from the earlier days of computer designed. This means that the components are actually built onto the board instead of being added as a daughtercard later.

The advantage to having some of the components onboard is increased speed.

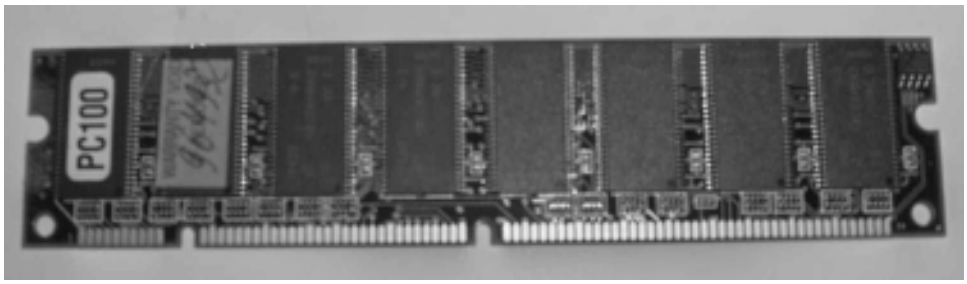


Figure A-5a. PC100 speed RAM Memory Module.

The connections between processor and component are faster when the items are built into the design of the board. A common problem, though, is that building such components directly on the motherboard limits later expansion or alternatives. That is one reason that daughtercards remain popular and why many boards are unpopulated.

The motherboard also contains many other electronic components that help the system run. These include the chipsets which is used in support of the main processor. The board also contains various electronic components such a diodes, crystals, and various items for control of the electronic information. As a rule the investigator need not be familiar with all of the individual electronic components, but it is a good idea to be familiar with the expansion slots of the motherboard as well and slots for memory and CPU.

Memory contained on the motherboard falls into two categories: *RAM* and *ROM*. *Random Access Memory* (RAM) is that memory used by the computer and accessible by the consumer through the operating system or application programs. This memory stores the data needed by the processor or to be displayed through one of the peripherals. A Pentium class machine typically uses at least 32 megabyte of RAM and some machines allow as much as 4 gigabyte of RAM onboard. Currently 128 Megabyte (Meg) of RAM is considered to be the minimal amount needed to effectively run the computer, and in recent months many consumers have begun adding 1 gigabyte or more of RAM to their new systems.

Random Access Memory, like many of the components in the computer, has undergone some significant changes in the past few years. At one point the memory chip was actually a part of the motherboard. As memory demands grew and need to upgrade memory increased, there was a need to mount memory chips into removal slots. Eventually memory was mounted on individual boards which were then plugged into slots on the motherboard. The typical memory in today's Pentium class computer is based on the Single Inline Memory Module (SIMM) or Dual Inline Memory Module (DIMM). These allow the user to quickly swap memory configurations without the need for major renovation to the motherboard. Figure Appendix A-6 depicts a SIMM, and one can easily see the metal connectors at the bottom of the picture where the memory module is plugged into the memory slot on the motherboard.

Memory comes in a variety of packages, pin configurations, types, and formats. There are two basic types of RAM available today: *SDRAM* (synchronous dynamic RAM) and *RDRAM* (Rambus dynamic RAM). The type of memory chosen for a given computer system depends on the RAM sockets (area where the SIMM is "plugged-in") installed on your motherboard. Most systems available on the market today take SDRAM in 168-pin DIMMs (dual in-line memory modules). Older Pentiums and later 486 PCs use FPM and EDO RAM which come in a 72-pin SIMMs (single in-line memory modules) configuration.

RAM modules are usually a little more than an inch high and four to six inches wide. As one will note, the SIMM has an area for contact which is usually gold or tin. This is called the "edge connector," and refers to the ability of the SIMM to connect to the RAM slot. The number of pins refers to how many gold (or tin) contact

strips are on the edge connector side of the SIMM or DIMM.

You can buy DIMMs that hold up to 256MB or more, but it should be noted that not all motherboards support all module sizes. To determine the limitations of a system the investigator should check the motherboard or PC manual to determine the connector slots in place. Older systems may have 30-pin SIMM slots, which are rarely produced anymore, while the newer systems have 168 pin slots.

Depending on the type of motherboard you have, memory modules can also be of a certain type, speed, or, in some cases, a metal type. The types of RAM used in PCs over the past few years include (from fastest to slowest): SDRAM (used in DIMMs only), EDO (extended data-out), old-fashioned FPM (fast-page mode), DRAM (found in SIMMs only), and DRAM (used in both DIMMs and SIMMs).

Most motherboards will accept a specific type of memory, and it is virtually impossible to mix the four types. While a few motherboards can use more than one type of memory module most will not allow the user to mix types. For instance, you might find a motherboard that allows both FPM and DRAM, but they cannot be mixed. Today most manufacturers do not allow such choices and simply limit the motherboard to a single memory type.

SDRAM speed is measured in megahertz (MHz), and it is important that the SDRAM match the speed of the system bus. If the two are not exact then the system will not perform properly. Most new computers use PC100 or PC133 SDRAM. This means that the RAM communicates with the CPU via a 100MHz or 133MHz bus.

Older DRAM (EDO and FPM) speeds are measured in nanoseconds (ns). Instead of carrying the PC100 or PC133 designation the chips often were labeled something similar to 100ns. The lower the "ns" designation the fewer nanoseconds the RAM used to work. The smaller the number, the faster the RAM, and of course this was all relative to bus speed and connection.

An interesting point to consider when addressing the issue of memory is that most of today's systems use the SIMM socket. The contacts, also known as leads, are usually plated with tin or gold. As a general rule users should not mix the two contacts; i.e., use gold with gold and tin with tin. If gold and tin are mixed then the user runs the risk of oxidation, and this greatly affects machine performance. Manufacturers of DIMMs addressed this issue by making all contacts out of gold.

Until a few years ago, virtually all PCs depended on *parity* RAM, a primitive form of error checking. In practice parity meant that for every eight bits of data stored, an extra parity bit was added and used in special calculations to ensure that the data was good. In the early days of the Pentium era, when memory was hard to come by and prices were high, many PC manufacturers switched to non-parity RAM. Most systems encountered today do not support parity at all, but some have an option which can be engaged at time of setup.

Error Correction Code (ECC) RAM is another method for checking memory errors. This RAM not only checks for errors but can even correct some of them along the way. ECC RAM is more expensive than other types of RAM. For this reason ECC RAM is often found in higher end machines such as network or file servers. Machines that demand higher levels of accuracy or extreme use, especially

those containing "mission-critical applications," often use ECC RAM.

Today's computers have such fast processors that new types of memory are being developed just to keep up with them. One of the more popular of the new memory modules is RDRAM (also known as *Rambus*). This is a much faster memory originally designed for graphics applications, and it has now found its way into some cutting-edge systems.

A drawback to this new memory is that one may not simply swap out SDRAM DIMMs and plug Rambus memory in their place. To take advantage of the RDRAM, the computer's motherboard must have a chipset with the proper Rambus circuitry. RDRAM is packaged in *RIMMs* (Rambus in-line memory modules), which are roughly the same size and shape as DIMMs.

A number of manufacturers, including Hitachi, IBM, Kingston, Micron, NEC, Samsung, Toshiba, and Viking, are already in the RIMM business. One feature that's particular to RIMMs is a heat sink which helps keep the memory cooler. Because individual chips are mounted more closely together on RIMMs than on DIMMs or SIMMs, manufacturers had to come up with a way to direct heat away from them. The heat sink provides cooling capability but gives the RIMM a very different look from it's DIMM and SIMM cousins.

Another newcomer to the RAM game is *DDR SDRAM* (double-data-rate SDRAM). DDR SDRAM is roughly twice as fast as standard SDRAM, and like RDRAM, it is not compatible with older systems. DDR SDRAM looks very similar to other SIMMs or DIMMs, but one can easily tell the difference by looking at the connector edge.

Only the fastest machines today can use the DDR SDRAM. This 184-pin DIMM requires a processor that is fast enough to handle the extra bandwidth. The Intel and AMD processors running at 1Ghz or faster clock speed are generally recommended. *PC1600* DDR SDRAM is made for motherboards and processors with a 200MHz (100MHz doubled) bus, and *PC2100* DDR SDRAM is designed for motherboards and processors with a 266MHz (133MHz doubled) bus. PC2100 RAM will work on motherboards with a 100MHz bus, but you won't see any dramatic boost in performance. There is now also PC3200 and in by the time this book is published the next generation of RAM will be available.

The second type of memory found on the motherboard is the Read Only Memory (ROM). This memory typically holds system information. The algorithms for system startup and operation are commonly stored in ROM. The information is permanently "burned into" the memory chip and instantly accessible to the processor at startup. In comparison, the RAM memory is virtually wiped clean when the power is shut off. Thus, the startup routines–those instructions necessary to make the computer run in the first place–would be lost if they were stored in ROM. As a general rule ROM memory is only as large as is necessary for these startup and operation routines.

iii. Bus Slots and I/O Cards

If the motherboard and processor are the brains of the computer then the *Bus Slots*

and *I/O Cards* (Input/Output cards) are the arms and legs. We use *I/O Cards,* also known as expansion cards or *input/output* cards, to expand the tasks our computer can perform. For instance, if we wish to print out the data we have manipulated with our computer we will need a printer. The printer is connected to the computer through a print card and this print card (I/O Card) is connected to the processor through the bus slot. Likewise, the scanner, modem, audio speakers, and many other items are added to our system through the expansion slots (bus slots) on the motherboard. The I/O Cards are also commonly called daughtercards since they are additions to the motherboard.

Once again we find ourselves dealing with a system of buses. As you will recall from the earlier section the bus is nothing more than the pathway (the connection) between one component and another. When we deal with add-on cards we are dealing with the I/O (Input/Output) bus. As a general rule when a novice refers to the computer bus they are generally referring to the I/O bus which is also known as the expansion bus. Before getting too far into the I/O bus architecture, though, it is worth first discussing two related buses.

The *Processor Bus* is the communication pathway between the CPU and the immediate support chips. Each component communicates with other components through a bus or system of buses. The sole purpose of the processor bus is to communicate with the main system bus, and typically this is the fastest (widest) bus in the whole computer system.

The *Memory Bus* is used to transfer information between the processor and the main memory (RAM). In some systems this bus (pathway) is part of the processor bus itself, but in other machines the pathway is a separate system. As a general rule the memory bus includes a dedicated chipset that is responsible for transferring information between the processor and memory. In most of today's Pentium class computers there is a special memory controller chipset that controls the interface between the faster processor bus and the slower memory.

One reason to focus on these is to show how complicated the computer system really is and how each part of the system can affect another part. Processor and Memory Bus are usually very fast (wide) while other bus connections might be slower. This is especially true when we move to the expansion bus used to connect to other devices within the system.

This is one of the reasons a computer seems to slow down so much when a new component is added to the system. For instance, when one adds a new hard disc drive with a narrow bus (8-bit) it will ultimately slow the whole computer system. The 32-bit pathways between processor and RAM allow rapid exchange of data, but when data has to go through the hard disc, either for storage or retrieval, then the exchange slows down. We can think of this using our highway analogy from earlier bus discussions to better understand this process.

As we have already established, a 1-bit connection was equal to a one-lane highway. An 8-bit system was similar to an 8-lane highway. In this analogy, though, we see that information routed between memory and processor might run along the super fast 8-lane highway bus, but then be detoured on the slower single lane bus of the memory. When that information has to route through the disc drive it moves

from the freeway to the county road. Think of it this way, if we have 8 trucks traveling an 8-lane highway they can travel side by side. They arrive at the destination (the processor) at the same time. But when we route those same 8 trucks through the hard disc, and thereby onto a narrower roadway, we must now put the trucks one after the other. They no longer arrive at the processor as a single 8-truck unit but as 8 individual trucks in single file.

Because there can sometimes be a stack up of data between these devices today's high end computer systems include a *cache* system. The cache allows the computer to store information being sent through a slower bus in a holding zone (somewhat like a warehouse) until it is needed. This frees up other components so that the processor may work closer to full speed. With this in mind we now turn to the other devices that are connected through the various expansion slots and their respective bus.

Anything that goes to or from any device–including the processor, video monitor, disc drives, and printer–travels over the I/O bus. When this connection is slowed then it ultimately slows the entire system, and for that reason engineers have worked for years to improve the performance and design of the I/O bus. That means that we now have several "standards" in the industry for bus architecture.

Two of the earliest bus designs were the ISA and MCA as discussed in the earlier section. Later improvements brought us the EISA, VESA Local Bus (VL-Bus), and the PCI bus. Those who use laptop computers are also familiar with the PC-Card Bus (formerly known as PCMCIA). Each bus was developed to address a specific need. Each is still used on many of today's computers, and that is why the investigator must be familiar with the architecture schemes as well.

The differences among the various buses consist primarily in the amount of data that they can transfer at one time. The ISA 8-bit architecture is used in the original IBM PC and clones. A 16-bit version of the bus emerged a few years later as did a 32-bit version. These increases in bus architecture came about at the same time processors moved from 8-bit to 16 and then 32-bit architecture.

As the PC developed many of the improvements available meant the addition of the new architecture to the newest computer. But that did not always mean the old architecture was left out. In many instances the computer contained a combination of new and old technology.

With the introduction of the 32-bit chips the ISA (Industry Standard Architecture) quickly became less dominant in the market. The bus system could not handle the power of the faster chips, and this lead to the introduction of the MCA (Micro Channel Architecture) bus. The MCA is technically superior to the ISA but did not catch on as a system standard; due in part because of licensing standards established by IBM.

IBM not only wanted to replace the old ISA standard but also to receive royalties on the new standard. The company required vendors that licensed the new proprietary MCA bus to pay royalties on the new bus and also pay royalties on past use of the earlier ISA bus. Many of the manufacturers did not like this system of licensing the new MCA bus so they sought an alternative. The immediate response was the development of the EISA bus.

The EISA bus (Extended Industry Standard Architecture) was announced in 1988 as an alternative to IBM's MCA bus. The developer, Compaq Computers, sought to establish an immediate niche in the market by simply giving the new technology away. Where IBM intended to sell their new MCA architecture, along with collecting for past use of ISA, Compaq chose to distribute the EISA bus to major manufacturers who agreed to use their system instead of IBM. Compaq even formed the EISA Committee, a non-profit organization designed specifically to control development of the EISA bus, as a way of insuring future development and support.

The stratagem backfired. In fact, the release and subsequent distribution of the new bus never really got off the ground. IBM had a significant head start with their new MCA bus and the Compaq bus didn't start appearing on machines until 1989. Adding to the problem was the fact that the powerful computer industry media never really jumped on the bandwagon. Without support from this important part of the industry most consumers really never knew that EISA could rival MCA in speed and power.

Some machines do use the EISA bus, but these are generally centered on disc array controllers and server-type network cards. While EISA provides markedly faster hard-drive throughput when used with devices such as SCSI (Small Computer System Interface) bus-mastering hard drive controllers it simply never got far enough to be considered a true success. What saved EISA was the simple fact that it was really an extension of ISA. Both bus systems use the same slot design for connection. For that reason many new machines have a slot that handles both the ISA and EISA bus cards.

By the early eighties the need to increase bus speed and capability was once again at the forefront of technology news. The Video Electronics Standards Association (VESA) developed a standardized local-bus specification known as VESA Local Bus or simply VL-Bus. Beginning in August 1992, and continuing through 1994, the VESA Local Bus was the most popular local bus design. The VL-Bus offers direct access to system memory at the speed of the processor itself. The system also moves data 32 bits at a time, enabling data to flow between the CPU and a compatible video subsystem or hard drive at the full 32-bit data width.

The VESA also helped to clear up another traditional bottleneck for data transfer. The exchange of data between the hard disc and the processor was often slowed by the bus connection or the drive speed. Even when manufacturers addressed the drive's speed, the swiftness of the drive to write or read from the platters, there remained the problem of speed in the bus. In other words, even when drives became capable of recording or accessing data faster there was still a bottleneck at the bus. VESA systems opened this bottleneck and increased data transfer at the hard drive from a relatively slow 5-megabyte per second to a more respectable 8-megabyte per second.

In early 1992, Intel spearheaded the creation of another industry group formed to increase throughput speeds. The group worked to overcome the weaknesses of the ISA, MCA, EISA and now VL-Bus systems. The group was called the PCI (Peripheral Component Interconnect) Interest Group. Rather than tap directly into the processor bus the PCI standards called for a new set of controller chips to extend

the bus' capabilities.

From an engineering standpoint the PCI bus adds another layer to the traditional bus configuration, and the immediate concern would be decreased speed due to the additional layer. To alleviate that potential problem the PCI bus bypasses the standard I/O bus and instead uses the system bus to increase the overall clock speed and take full advantage of the CPU's data path. The PCI bus is especially aggressive in Pentium-based machines, and since 1993 has become the industry standard for the PII through PIV class machines.

Today, a typical Pentium class desktop computer will have at least three PCI slots with an additional one to three ISA or EISA slots. The ISA/EISA slots are maintained for use with 8 and 16 bit cards that still find their way onto the market. This is known as backward compatibility, and users demand such functions as the computing market makes significantly fast advances.

By the mid-nineties computer use had firmly entrenched itself in the office and home. It now moved to the mobile world as laptop and notebook computers improved. By the very nature of the laptop or notebook there is an immediate problem with expansion. The cramped space inside today's laptop means that traditional ISA/EISA or PCI cards will not fit. To address this issue the industry saw the development of a new group along with new standards. These focused on the expandability of the notebook and laptop computer.

To offer the laptop user more expandability the Personal Computer Memory Card International Association (PCMCIA) established several standards for new credit-card-sized expansion boards. The expansion boards were originally known as PCMCIA cards. Most were the size of a credit card (2.1 by 3.4 inches). These new expansion cards were the development of a consortium of more than 300 manufacturers including IBM, Toshiba, and Apple. The cards are known today as *PC-Cards,* and they offer expansion capabilities including more memory, fax/modems, SCSI adapters, local-area-network (LAN), and other devices. The cards are divided into four categories designated PCMCIA Type I, II, III, or IV, with each addressing the specific need in one of the above categories.

iv. Peripherals

Computers must have data. This means they must have input. Input is the process of entering data into the computer. Without input the computer has nothing to compute. Computers may also give data once it is computed. This is normally called output. A significant portion of the computer is devoted to the process of receiving input and giving output. This is typically done through components called *peripherals.*

An interesting tidbit that many computer users do not realize is that the earliest computers did not have monitors, as we know them today. In fact, many computers did not have a monitor of any kind. Instead, they had a system of lights that told the user the computer was working. Output was not viewed on a monitor but typically read from a printout (produced by a printer). It soon became clear that not all output needed to be printed. If the user could view the output in a human-readable fashion without printing then many computer task could be simplified. This meant that

engineers needed to find a way to display computer output through a means other than a row of lights or words on a printed page.

In the fifties electrical engineers made tremendous advances in television and the computer industry was soon a beneficiary of these advances. As computers continued to evolve engineers chose to use the television's cathode-ray-tube as a means of displaying output. Soon the display terminal was born, and the cathode-ray-tube (CRT) became a common part of all computer systems. The CRT screen, that area the user viewed, was typically small, averaging no more than five inches across.

Over time the demand for higher quality displays increased. The first CRTs displayed nothing but a series of dots arranged to form letters. These dots, known as pixels, were initially widely spaced (a few hundredths of an inch apart), but engineers worked to decrease the pixel distance. Pixels grew smaller and the distance between pixels also diminished. At the same time methods for displaying the output through computer code advanced. By the early eighties CRTs were capable of displaying graphical output along with the alphabetic. The size of the display area grew to over nine inches.

Early CRTs were monochromatic; that is, they could only display one color. Green and amber were the two preferred colors. Consumers began displaying information in more ways than before. Spreadsheets now sported pie charts to help explain the numbers and early graphical computerized games began to hit the market. The demand for graphics meant a higher demand for better CRTs with color. The first successful color monitors used the primary colors of red, green, and blue to create colored patterns. The monitors, commonly called RGB monitors, were primitive compared to today's standards. They marked a significant change in consumer technology, though.

Eventually, computer monitors began to mimic television monitors and the industry moved toward full color, graphical ready systems. Computer color monitors were now up to thirteen inches across and looked similar to small televisions. In fact, some early "entry level" consumer computers such as the Commodore®, Atari®, and others actually used small color television sets as their principal monitors.

Monochromatic CRTs are almost non-existent for the PC today. As we enter the twenty-first century we use monitors capable of displaying millions of colors and rivaling the best television picture. Fifteen inch monitors are considered "entry level" and many systems sport seventeen, nineteen, and even twenty-one inch monitors. All of this is of course possible by the tremendous increases seen in interface technology. Processors, buses, and every other part of the computer system has increased together.

The massive changes in monitors had a side effect. Graphics became more important. After all, psychologists have long known that man is a visually oriented species. We often prefer a picture to the printed word, and in computers this meant that the Graphical User Interface (GUI)-based system would become more popular than the text based DOS systems of years past. This also meant that we would change the way we input data into the computer.

Just as monitors helped change the way we received output there would be changes in the keyboard to reflect our need for better input. The keyboard has long

been the traditional method for inputting data into the computer. The keyboard reflects the setup of the traditional typewriter. Letters of the alphabet are displayed using the "QWERTY" model most of us learned in junior high or earlier. In fact, as I sit in my office writing this tome I use a modified keyboard that places my hands at an angle more conducive to good typing posture and longer periods of comfort. The arrangement on the keys is virtually the same: QWERTY. The difference is that there have been additional keys added to the original keyboard to more efficiently use the power of my computer.

The first major change to the keyboard was the addition of a 10-key pad to the right of the typing keys. The keyboard now combined the traditional typewriter style key layout with the arrangement of the 10-key calculator. This change allowed users who worked with numbers, such as those doing accounting or balancing a checkbook, to enter numeric values faster than with the number keys of a traditional typewriter keyboard.

Soon other changes appeared on the computer keyboard. One of the more significant changes was the addition of the *function keys*. Since the keyboard is used primarily to give commands to the computer there was an immediate need to shorten the keystrokes needed for those commands used most often. For instance, in early word processors the user had to strike an awkward combination of keys, sometimes two or more together at the same time, to save their work. Today, users merely touch the "f12" key and the computer immediately displays a menu allowing the work to be saved. This function key also allows users to do in one keystroke what normally took five.

Other peripherals have made similar advances. Printers, once clunky machines which used mechanical imprint heads much like a manual typewriter, now produce ink sprayed printouts in a fraction of the time it once took. Laser technology is also used to create high definition printouts in both monochromatic and color copies. In fact, today's computer printers rival last century's high-end printing presses in both quality and output capability. Some relatively inexpensive printers also print "photo quality" graphics on high quality photo paper that look almost as good as real photographs.

Peripherals have also become very sophisticated allowing users to capture text or graphical material from outside sources. For well under one hundred dollars, a user can buy a scanner capable of capturing a high quality copy of an original document, photograph, or chart. Link this scanning capability with the newest printer technology and one can imagine how easy it would be to mass-produce reasonably good copies of paper money. That is one of the reasons the Treasury Department now prints their paper money with inserted metallic strips and other tricks designed to spoil the would-be counterfeiter.

While the U.S. government seems to be ahead of the game in spoiling such operations there are other equally valuable documents that are quickly being targeted by cyber-criminals armed with cheap scanners and decent quality printers. With the increased capability of printers we have also seen an increased capability in software. For instance, advances in drawing and design software now put the highest level of drafting technology within easy reach of even the teen-age consumer. This means

that not only can the would-be counterfeiter scan the document into the computer in almost perfect condition but they can now use high-end software to correct any mistakes that occur.

One of the most dangerous peripherals on the market today is the high-speed modem. The modem, which stands for *mod*ulate and *dem*odulate, allows the user to communicate over the telephone line with any other computer similarly equipped. Initially modems were used to send textual information between computers. Technology soon advanced so that graphics and pictures could be transmitted as well. As modem speeds increased it took less time to transmit large amounts of data over ordinary phone lines. Today, anyone with a modem can transmit the contents of an entire book in less than three minutes. Graphical representations of almost anything can be scanned and then transmitted in the time it normally takes to photocopy a document.

v. Data Storage

The ability to store data has grown more and more important for computer users. At one time the computer was a calculating device and not focused on long-term storage of data. In fact, in the earliest days of computers much of the information input was stored on printed cards or external media such as tapes. The user loaded the material by running the punched cards through a card reader, which then input the data into the RAM.

Today we use data storage much more efficiently and rely on it much more than in the past. One reason is that data storage capability, like so many other components of the computer, has advanced rapidly in the last part of the twentieth century.

Some of the most effective means for data storage have been the use of magnetic media. In the early eighties most PC class computers used an audiocassette or a floppy disc drive for storage. The audiocassette used traditional audiotape to store data just like it recorded music or voice. The "write" head of the cassette deck encoded the magnetic particles on the tape so that when the lower powered "read" head scanned the tape later it would "read" the contents.

The same principle was used in floppy disc drives. A magnetic coating was placed on a plastic, vinyl, or celluloid diskette. Early diskettes were housed in a slightly thicker housing. The housing was about as thick as thin cardboard. The diskette inside was supple and the housing was not much better. When held at the edge the disc literally flopped; thus the name floppy disc.

Early floppy discs held relatively small amounts of data. For instance, the Apple II disc held roughly 143k (kilobyte) of data while the later IBM version of the floppy used a similar size disc but technology allowed manufacturers to cram a whopping 360k of data onto the same disc space. Quickly storage capacity increased. Soon engineers were able to store more data in a smaller space. As storage capability began to increase the size of the diskette itself grew less important, and engineers came up with a smaller (3.5 inch) diskette which they encased in a hard plastic shell.

The 3.5 inch floppy disc held more data than its 5.25 inch cousin. At the same

time the disc kept the data safer and allowed users to carry it around easier. In fact, the new disc actually fit into the shoot pocket (breast pocket) of an average adult male. The disc held 720k of data, and later disc storage was increased to 1.44 megabyte.

Interestingly, the new "floppy" really was not floppy any more because the storage media was held inside a hard plastic case.

Storage also moved from being a temporary, transportable peripheral to an integral part of the system itself. The *hard disc* was created to serve as a fixed point of storage; in fact, the first hard disc were actually called *fixed disc*. The hard disc worked on a similar magnetic system to the floppy disc. In the floppy the magnetic coating was placed on a flaccid plastic surface. The hard disc used magnetic coating as well, but the coating was placed on a hard surface such as aluminum or glass. These discs, often called platters, made the storage device much more effective and long lasting. The typical life of a floppy disc was usually a few months. Long-term storage was never recommended for the floppy, but with the new hard disc it was possible to safely protect data for an extended period.

Both floppy and hard disc technologies rely on the principle of a magnetic coating on the surface, which is read or written to by a "head" suspended above the platter. A "write" head in the drive arranges the magnetic particles on the surface and the "read" head is able to decipher the arrangement. The read and write heads travel across the platter surface at only a few microns distance. For that reason it is not a good idea to bump or jostle the computer while the disc drive is running. Data may be lost and in worst case scenarios the disc may be damaged.

In many of today's machines, including the entry-level computers, the disc storage capacity of a hard disc drive is measured in gigabytes. A gigabyte is roughly equal to 1,073,741,824 bytes of data. As an historical note the original hard disc used by Apple and IBM cost as much as $2000 and held no more than five megabyte. Today, a 60-gigabyte hard disc drive costs less than $200 and fits in less than 1/3 of the space.

Storage on the computer comes from other sources as well. Tape based storage systems continue to be popular especially for archival purposes. Tape tends to last longer and is more stable than the magnetic disc type storage media. For that reason large capacity tape systems are now used to store data for periods longer than a few weeks. Similar to these tape systems are the new "Zip Drive" systems. High capacity storage, generally for archival purposes, is the best selling point.

The popularity of the Compact Disc (CD) for audio has found its way into computers as well. Today a CD-based system is used in most consumer line computers. Entry level machines include a CD drive which allows the machine to read the CD. Most programs now come on Read Only CDs (CD-R) and not on floppy discs. As a storage media the CD is also very popular. Drives which allow users to both read and write to a CD are now very popular. These drives, commonly called CD-RW (CD-ReadWrite), allow users to store up to 650 megabyte of data on a single CD.

The massive storage capacity of the CD makes it a very popular item for sharing information. Entire libraries, including encyclopedias, can be stored on CD. And the CD is very stable. The data is stored on the CD by burning a pit into the substrate

of the CD surface. The CD-R disc has the data burned in permanently. The CD-RW disc allows the user to burn in the data with an initial laser and then change the data with a stronger laser as needed.

The newest generation laser-based storage systems are the DVD discs. The Digital Versatile Disc (DVD) is very popular for movies and is growing in popularity among computer users. One drawing point is the massive storage capable with the DVD. The CD stores 650 megabyte but the DVD, which is roughly the same size, stored up to 4 gigabyte of data. This is a significant increase.

At the time of the writing of this chapter the only hold back to DVDs becoming the standard for data storage was the price. A DVD-RAM drive was over $500, but prices were expected to drop dramatically in coming months.

vii. Power Supply and Connectors

Also inside the case is the power supply for the computer system. The power supply is rarely a concern to investigators, but it must be identified so that the investigator securing a computer will know what he is inspecting. The power supply can also be a very dangerous part of the computer system since it is capable of producing deadly shocks.

The power supply of a desktop system can be easily identified since it is often enclosed in a steel case and has a fan. The power supply is located at the top-left corner of the case. Multicolored wires hang from the back of the supply, and this is used to power the individual components of the computer. The upper right corner of the case is where drives are stored. The motherboard typically rests along the back wall of the case. Room for the expansion slots is allowed in the center, and one can see the back of the case where the cards are accessible to the user.

Additional fans are often added to fast systems, but almost all systems have at least one fan connected directly to the power supply. The fan is to help cool the power supply as well as the interior of the case. Heat is the enemy of everything electric so it is important to keep the system cool. Some users add additional fans to their system when they have loaded the motherboard with expansion cards or added other heat-producing peripherals/components. A typical machine might include a floppy disc drive, hard disc drive, CD and CD-RW drives, modem, audio card, and video card.

Running from the power supply are various power connectors. These are used to power the different components of the system. The most common devices which require this power are the storage drives such as the floppy and hard disc, CD, CD-RW, and DVD drives. Special power connectors are included and identified by their unique shape.

Appendix B

UNDERSTANDING THE SOFTWARE

A. Introduction to Software
B. Operating Systems
   1. UNIX
   2. Linux
   3. Mac OX
   4. Windows
C. Application Programs
   1. Business Software
      a. Word Processors
      b. Spreadsheets
      c. Database
      d. Graphics
      e. Presentation
      f. Communication
      g. Other
   2. Entertainment Software
      a. Games
      b. Graphics
      c. Educational
      d. Other
   3. Utility Software
      a. System Maintenance
      b. Software support
      c. Other

---

1. INTRODUCTION TO SOFTWARE

The term software is often used in the generic sense to refer to any program or code running on the computer hardware. It is important the investigators understand there are different types of software. From a practical standpoint software is divided into two very broad categories with the first known as the Operating System (OS). The Operating System, as we will see in coming paragraphs, runs the computer and allows the second type of software to perform. The second category of software is commonly called Application Software. In the last section of this chapter we will examine the various types of application software available today.

B. OPERATING SYSTEMS

The *Operating System,* also known as the *OS,* is the software that actually runs the computer system. It is the software that carries instructions to the CPU telling it how to handle the data being manipulated by the user. Today's operating system combines command structures for each part of the computer system; including, CPU, memory, I/O cards (sound, video, printer, etc.), and even parts of the application software. The OS makes the computer system operate.

A PC system has a distinct hierarchy of software that controls the system at all times. Each layer of the system is controlled ultimately by the operating system. As an example, as this chapter was being typed the computer was busy downloading the latest *Visual Basic*[1] updates from Microsoft's website. The OS allowed the system to perform multiple functions with a seamless interface to the user. The OS juggled the work being done by two application programs (the word processor and FTP program) while at the same time handling requests from the RAM, hard disk, and modem.

The most popular OS on the market today, at least for the personal computer, is Microsoft *Windows.*[2] While this software is a very powerful OS it is not the most powerful in use today. In fact, the Windows platform is actually a distant second when compared with the power of *UNIX.*[3] Where Windows limits itself to the PC genre of computers the UNIX OS runs on a wide variety of machines, from micros to supercomputers, and is considered to be highly portable. In fact, UNIX is still the preferred OS for major computing tasks and is often credited as "running the Internet."

1. UNIX

Prior to UNIX most software was created for a specific purpose. The computer manufacturer was also the software manufacturer in the earliest days of computing. Software was designed to run on a specific machine, often restricted to just that machine as well, and the application was custom built for the customer. Customers in the earliest days of the computer industry were typically large corporations, universities, and government agencies. The entities had the budgets necessary to buy custom developed software, and in many instances the software was unlike anything

else being used by other entities.

By the sixties there began to be significant changes in the computer industry. Software moved away from being simply a component of the computer system and was soon a stand-alone industry of its own. Hardware and software were now distinct from each other, and a new level of the computer industry emerged. Early programmers were often electrical engineers who programmed the machines out of need rather than choice. In this stage, though, programmers emerged as dedicated professionals quite separate from their engineering counterparts.

One of the most important changes in software development came with the outgrowth of UNIX. The UNIX system fostered a distinctive approach to software design by interconnecting simpler tools rather than creating large monolithic application programs.

The UNIX operating system was designed so that several programmers could access the computer at the same time and share its resources. Prior to this it was not uncommon for single users, or small dedicated groups of users, to access the computer system. In many instances, the job of "data input specialist" or "data entry" person was given to one of two people in each office. Only these people worked with the computer system, and requests for data input or computing jobs were made through these individuals.

There were also instances when only one job at a time could run on a computer system. There was no such operation as "multitasking" when it came to computers. The data entry clerk used punch cards[4] to enter the information and the computer was left to work the job. Output was to a limited terminal, printout, or other method.

As the power of the computer increased users were able to access or enter information in a more efficient manner. Computers were also able to perform multiple functions simultaneously. The UNIX operating system was one of the first to coordinate the use of the computer's resources while also coordinating the use of each user. This meant that one person could run a spell-check program while another created a document at a different terminal. This was an important step in the development of computing power since it allowed multiple users to perform different tasks without concern for the others on the system.

This type of operating system also controls all of the commands from all of the keyboards and all of the data being generated regardless of which station is being used. What this means is that each individual user is tied to the computer but is allowed to work separately from all the others. This was known as "real-time sharing" of resources and was vastly different from other computers which allowed only one user at a time to operate the system. This alone made UNIX one of the most powerful operating systems developed to that point.

UNIX continues to be used even in today's personal computer dominated market. As stated earlier, it is UNIX that actually runs the main computers that are the backbone of the Internet. Of course, one must recognize that the OS has undergone some significant changes and upgrades since the original release. Because of this UNIX is routinely used to run background applications for network and Internet systems. Many telecommunications switches and transmission systems are ultimately controlled by a UNIX-based system for administration and maintenance.

It is clear that most casual users will never use UNIX, and most would not know the OS even if they saw it operating. To the casual or uneducated observer, the UNIX system looks somewhat like the old MS-DOS system of just ten years ago. It is important to understand that the majority of today's computer users have never used a "command line" OS (one that requires the user to type in commands at a prompt rather than click on an icon) because they have only used the Windows or similar OS.

For the criminal investigator the need to understand UNIX is important for two reasons. First, the savvy investigator should be able to identify the most common OS that he is likely to encounter. This includes UNIX as well as a few of the UNIX-like OS currently on the market. It is also important that the investigator have a working knowledge of UNIX so that he may be able to properly address issues that arise under a UNIX system. For instance, computer intrusions made via the Internet may involve the use of UNIX to access routers and other background systems.

With that in mind let us now turn to a basic description of UNIX. In understanding UNIX it is important to remember that is was written by programmers for programmers. This means simply that the OS follows certain principles and practices common to programming. The major difference from other OS, such as Windows, is that UNIX is not designed to meet the needs of a broad audience. It is instead designed to meet the needs of a narrow market of specifically educated individuals.

The UNIX system is effectively organized into three levels.[5] These are:

- The kernel, which schedules tasks and manages storage;
- The shell, which connects and interprets users' commands, calls programs from memory, and executes them; and
- The tools and applications that offer additional functionality to the operating system.

The kernel is the heart of the operating system. The kernel controls the hardware and turns part of the system on or off at the programmer's command. If you ask the computer to list all the files in a directory (UNIX command, *ls*), the kernel tells the computer to read all the files in that directory from the disk and display them on your screen. From the kernel the programmer, or other user, can control the basic functions of the computer and its peripherals.

The shell has a single function which is to serve as the interpreter between the user and the computer. There are several types of shells on the market, but the most notable are the *Bourne Shell* and the *C Shell* (no pun intended). These are commonly called "command driven" or "menu-driven" shells, and they make it easier for users to access the power of UNIX.

The shell also provides the functionality of "pipes." A pipe allows a user to link a number of commands together to perform a given task. For instance, a user may form a pipe, which calls information from a file on a disk drive, manipulates the data in some way, and then displays the data via the printer. These are in fact three different commands, but by using the pipe the user creates a single efficient command.

What this means is that the output of one command effectively becomes the input to another command.

There are hundreds of tools available to UNIX users. UNIX is supplied with its own traditional tools, and there are many other tools written by third party vendors for specific applications. Typically, tools are grouped into categories for certain functions, such as word processing, business applications, programming, or utilities.

As an operating system the UNIX OS is certainly powerful, but it is not the only operating system one might encounter in a computer crime case. In recent years a UNIX-like OS has emerged and has rapidly become a very popular alternative to both UNIX and Windows-based systems. This new OS is commonly referred to as Linux or sometimes called GNU/Linux.

2. Linux

Linux is the newest of the OS to make a splash on the computer scene. Originally written by a twenty-one year-old student at the University of Helsinki (Finland), the program was an offshoot of the *Minix* OS. Minix operated on the Intel 80x86 (mostly 386 and 486) system and was a direct descendent of UNIX.

The developer, Linus Torvalds, had written the basic code for the new OS and was looking for help in the development. In reality Torvalds was looking for a low-cost alternative to some of the high-priced operating systems already on the market. He posted a message on a popular electronic bulletin board seeking developers who would be willing to work on the project. He obviously found plenty of help, and today there are an estimated ten million users worldwide.

What makes this OS so unique is the way in which it has developed. Dedicated teams of programmers working for a specific company develop most operating systems, but Linux never started that way. Instead, Torvalds wrote the basic code on his own then "open sourced" it to those who were willing to work on the project with him. In other words, instead of keeping the inner workings a secret, something that most major software manufacturers do regularly, Torvalds gave away his best code so that others might improve on it. Over time the product Torvalds created evolved into what we now know as Linux.

Like UNIX, the central nervous system of Linux is the kernel. This is the part of the operating system that runs the whole computer. The kernel is also the part of Linux that has changed the most over time. It is the part that Torvalds originally distributed and which is constantly being upgraded by all those other Linux programmers in the world. Fortunately, the system has developed along relatively stable lines, and thanks to a concerted effort by the countless developers the code remains "open source" even today.

Any user interested in experimenting with Linux can quickly find a copy of the kernel on the World Wide Web. The kernel is under constant development and is always available in both the latest stable release and various degrees of experimental releases. This way, users who need the more stable code can obtain it without the need of paying high prices (something still important to users like Torvalds) while those who wish to explore the boundaries of the OS may download the latest exper-

imental releases.

Progress on development is very fast, and the most recent kernels give us an OS that rivals even some of the best commercially available software. The kernel design is modular which allows the OS to load whatever functionality it needs when it needs it, and then free the memory afterwards. Because of this, the kernel remains small and fast yet highly extensible. This is a major advantage to some and one of the reasons for the exploding popularity of the OS. Other OS often load huge chunks of code, even though not needed, and this slows down even the fastest of today's computers.

Another advantage to Linux is the stability it presents. Computers running Linux have been known to run constantly for up to five months without a single crash. Compare this to the most popular line of OS (Windows) and one recognizes immediately the difference. Because the Linux OS compartmentalizes so much of the code there is little overlap, so even when one section does cause a general fault there is little likelihood that the entire OS will crash.

Speed is a third major advantage that Linux has over other OS on the market. A Linux equipped 80386 computer will actually compute data faster than a *Windows '98*[6] equipped *Pentium II*[7] class computer. The Linux OS is so much faster that power users such as NASA, *Sandia National Labs,* and Fermilabs have built very potent yet inexpensive supercomputers by creating clusters of Linux boxes running in parallel chains.

Another surprising fact is that many ISPs (Internet Service Providers) operate their service using Linux on the slower (and much less expensive) 386, 486, and early Pentium class computers. What this means is that the average home user connects using the fastest Pentium IV or AMD processor but is being serviced by a slower–and some might say archaic–Linux based 80386. Of course the real speed comes by way of the connection between computers, but even those few microseconds of processing power seem to add up when it comes to efficient electronic communication.

The reason so many ISP's use Linux is simple, cost. An ISP can use the older machines, which are already available or can be purchased rather inexpensively, with a very inexpensive OS to provide the same–or sometimes superior–service to other systems. This means a higher profit margin and less down time for the ISP owner.

One should not assume that because Linux is low-cost (or nearly no cost) that it is not powerful or easy to use. Those who have become accustomed to the GUI interface can rest easy since there are many versions of Linux equipped with an intuitive graphical interface. There are more than a dozen different, highly configurable graphical interfaces that serve as a shell for the system. Commonly called "Window Managers" these shells run on top of *XFree86,* a free implementation of the X Window System.

Two of the more popular add-ons are *KDE* (the K Desktop Environment) and *GNOME* (the GNU Network Object Model Environment). These offer the point-and-click, drag-and-drop functionality associated with other user-friendly environments (for example, Macintosh), but are extremely flexible and can take on a num-

ber of different looks and feels. There are even methods for setting up the KDE system so that it looks much like the more popular Apple Mac OS and the Microsoft Windows environment.

A distinct advantage to Linux is the networking capability that is inherent in the OS. After all, Linux is a descendent of UNIX, which is where the idea of networking really originated. What is important to remember is that most of the protocols common on the Internet were developed for the UNIX environment, and Linux is a direct beneficiary of that development.

The final point to be made for Linux is the usability side of the equation. Linux is a relatively simple OS and can be easily understood by most users. More importantly, though, the OS has seen tremendous third-party development of application software to run on the OS. What this means is that the common user will find virtually every program type imaginable for Linux that would be found on any other OS. This makes Linux a viable, if not always popular, alternative to the more expensive operating systems.

3. Apple Mac OS

In earlier sections we briefly discussed the development of the Apple computer and the later Mac line. Today the Mac is more popular than ever, even though it controls a relatively small portion of the overall market. The majority of Mac users are found in education, entertainment, and the graphics industry. The Mac is very popular not only because it is easy to use but it also a very powerful computing system.

At the heart of the Mac computing system is the Mac OS. An offshoot of the original Lisa OS, the Mac OS relies heavily on a graphical user interface (GUI). User input is traditionally given through the keyboard or mouse. The user merely moves the mouse on the desk, which in turn makes a pointer on the monitor screen point to a graphical representation.

One of the more notable points to the Mac OS is its relative immunity to the more common computer viruses seen today. One reason for this is simply that the Mac is not a favorite target. In other words, the person producing the virus is often schooled in the languages used on the PC (Microsoft Windows based systems, especially) and focuses his efforts on that platform. This does not mean that the Mac is completely immune from computer viruses. Indeed, if a virus designer were intent on creating such a bug then the Mac would be just as vulnerable as the average PC. The simple fact remains, though, that the Mac, while a great OS, does not demand the attention that the more popular Windows-based systems receives.

For investigators it is important to recognize that the Mac is probably the second most likely computer to be encountered in an investigation. The reason is not superiority of the Mac OS to Linux, Unix, or any of the other OS, but merely that the Mac is so easy to use that it is very popular with all types of users.

An interesting note to this phenomenon is that the majority of crimes involving the Mac tend to focus on crimes needing high levels of graphical work; i.e., forgery, counterfeit, and similar crimes. This does not mean that all Mac users are graphics experts, it is just that the Mac seems to be especially suited to such work and is there-

fore the most likely choice.

4. Windows

Windows is clearly the most popular of the OS we will examine. Today's Windows OS is a grandchild of the original Microsoft Disk Operating System (MS-DOS) developed by Bill Gates and company more than twenty years ago. The original Windows OS acted much like a UNIX shell in the sense that it worked on top of the DOS OS subsystem. The original OS was the direct progeny of the DOS OS, but it was not always as powerful or stable as it should have been.

The original Windows OS went through at least five revisions before it was ready to dump the ties to DOS.[8] With the release of Windows '98 the OS moved to a fully functional and stand alone version of itself. The later versions of the '95 edition brought the OS into the 32-bit environment, and the Windows '98 version provided fully integrated 32-bit, protected-mode OS with the ability to perform preemptive multitasking. What this means is that Windows '98 (and later versions) is a very complex and powerful OS.

Windows, like Mac and the Linux Shells, relies on a graphical user interface for communication between the user and the computer system. Under that fancy graphic interface, though, is the true power of this OS. The Windows environment brings together more than six hundred previously unrelated tasks and management items. Where the original operating systems primarily managed the disk, memory, and I/O tasks, today's Windows 2000 OS manages everything from the printer font size to the constantly expanding array of applications from third party vendors.

In the next few years we will see the Microsoft Windows environment take on even more radical changes as we move into what Microsoft calls "Distributed Computing." Instead of working with an OS on one desktop (or laptop) computer, tomorrow's user may well link to a series of OS routines running on the Internet or other network connection. One example of this principle is seen in the use of *Web Robots* (bots) and similar tools. Other tools, commonly called "Applets," have extended our power as computer users, and it is likely that this power will be extended further when the computer of tomorrow relies on a system of distributed protocol.

In understanding the complexity of today's Windows OS, and the potential for an even more complex OS tomorrow, one need only understand the changes that have occurred in the last few years. An easy way to get a feel for the depth of those changes is to look at the size of the OS itself. The earliest versions of MS-DOS could be stored on a single floppy disk. As the OS began to grow, evolve, and change it became larger. Today, a user who purchases Windows 2000, XP, or NT, will find their new OS housed on multiple CDs rather than a single disk. Windows 2000, the full version, now takes up at least twelve CDs (which hold up to 650 megabytes each). What once fit into a few thousand kilobytes of space now takes up several gigabytes.

Another major change can be observed in the way programs are stored and accessed by the computer. The earliest OS was a single file or collection of just a few files. The application software that ran under the OS was often a single file as well.

Today, the integrated nature of the Windows OS, especially with its shared *DLL* and *SYS* files, means that hundreds, if not thousands, of individual files will reside on the computer's hard disk drive. The OS is no longer a stand-alone entity but is instead a collection of hundreds of interactive routines or data.

To get a good idea of how crowded the average hard disk on a powerful desktop computer can become we need to look at the files as listed in Windows Explorer. Another way, and one that is very impressive by its sheer volume, is to monitor the computer maintenance tasks, such as routine virus scanning, to see how many files are checked. On the computer where this book was written the average virus scan examined more than thirty thousand different files including more than two thousand for Windows alone. Many of these were only a few kilobytes in size while others were a megabyte or more.

For now, it is important that the investigator understand that the OS is the part of the computer software that makes the computer itself operate. There are many other types of OS out there, and we have only covered the most popular or powerful available. The investigator must understand that there are both unique and chilling uses for the OS, and by understanding the place the OS plays in the overall picture the investigator can be better prepared to handle those issues that might later arise.

C. APPLICATION PROGRAMS

The term "Application Software" is a broad term used to describe all those programs that actually do our work for us. The OS allows the computer to work, but it is the application software that allows the user to work. More specifically, when a user wishes to perform tasks using a computer system it is normally a piece of application software that they will use. The application software runs in harmony with the OS, but it is the application software that performs the tasks assigned.

Application software falls into three very broad categories. The first we will call "Business Software," and this includes programs such as Word Processors, Spreadsheets, Database, and many others. The second category we call "Entertainment Software." The most common program in this category is the PC game, which has become very popular in the last two decades, but there are also many other programs that fit into this category. The last category of software is known as "Utilities." Utility software is broadly classified as a product that services another software package or the computer system itself.

1. Business Software

Those who keep up with computers know that business software is a constantly changing and evolving industry. It seems that just when one gets really good at the current version of a particular program the manufacturer comes out with a new version that promises even more power and convenience. Fortunately, for most of us the software we use today will still be an effective tool for many years to come. The need to buy the latest software each time a new version is released is based more on

perceived rather than actual need. With that in mind we will examine business applications from a generic perspective rather than focusing on each individual name-brand program.

At the outset it is important to remember that the three categories of software we set out above may have many packages that cross over from one category to the next. For instance, many of today's top graphics programs fit into both the business and entertainment category. Software such as Macromedia's *Flash 5.0* are inexpensive enough for the average home user to purchase but powerful enough for corporate users to depend on. Another example can be seen in the selection of word processing programs on the market. Microsoft's *Word 2000* is a very powerful program found on a majority of business computers today, but it is also common on most home computers.

a. Word Processors

The most popular, and most widely used business software in use today is the word processor. This software has replaced the common typewriter of just a few years ago. Today most offices use computers to create documents rather than type letters, and the typewriter is often relegated to a corner or back room.

Word processors come in all shapes and sizes. They range in power from the most robust to the very simple. They allow users to create complicated documents with multiple sections, complex tables, and multiple selections of fonts, symbols, and pictures. Today's word processor has more power than the most complicated publishing software of just a few years ago. Even with all that complexity and power they still do just one thing, but do it very well. Word processors allow us to communicate in writing.

Word processors are so necessary to the modern computer user that many OS now include a simple program as part of the OS. These programs are often called "text editors" and were first introduced with the earliest commercial OS for the PC. They were not only used to create documents for distribution but also assist users with entering strings of commands to the computer. Over time these text editors began to add features that allowed users to create documents with underlined characters, super and subscript, bold, and even colored text.

The more powerful word processors allow the user to format the document in dozens of different ways. They allow users to create complicated tables, perform routine functions such as sort and calculate, and even write highly specialized documents such as screenplays with ease and flare. Today's word processor even allows the user to insert text side-by-side with graphics, photographs, and symbols. In essence, the word processor of today is so powerful that it allows even the home user to "publish" documents that are equal in quality to those produced by the best commercial publishers. Of course, the user will often need other programs and hardware to accomplish this task, but for now it is important simply to recognize the power of the modern word processor.

For the investigator the word processor is both a blessing and a burden. The word processor makes it easy for anyone with a computer to manipulate text in hundreds

of different ways. In fact, a dedicated perpetrator armed with a powerful word processor can easily create, alter, and manipulate any document at will. Add a good quality printer and the offender can now publish a document that is as good, if not better, than the original.

b. Spreadsheets

Unless you are an accountant or otherwise keep track of lots of numbers there is little need for the average user to even own a spreadsheet. The Electronic Spreadsheet, like the word processor, is a modernization of an old work tool. In decades of the past the accountant, bookkeeper, and even homeowner tracked expenses and transactions using a series of journals and record books. The spreadsheet takes all those pages from the journals and puts them in a single electronic storage container.

The worth of a spreadsheet is measured by its ability to manipulate numbers. Each spreadsheet uses a grid system of "cells" to store numbers. The cells are then linked or combined through "formulas" to allow the user to calculate and manipulate the numbers. When the number in a given cell is changed it is then used to recalculate the new totals, which are often displayed in a cell of their own, or to alter still other cells.

c. Database

The database is nothing more than an electronic filing cabinet. In fact, that description is so valid that many database designers often use the analogy of a filing cabinet when constructing the user interface. They may even go so far as to include a graphical interface that looks much like a file cabinet or manila file folder.

Like the spreadsheet, the database is measured by its ability to manipulate data. The most powerful database in use today commonly uses the Structured Query Language (SQL) or similar paradigm. These often use the Relational Database design, which means that the data of information stored in the database has a relation to other data in storage.

Dr. E.F. Codd first proposed relational database theory in 1970. At the heart of the theory is the concept that data elements can be linked by their relationship to other items. For instance, in our chapter on Information Theft we discuss the historical peculiarities of an early era baseball player by the name of "Babe" Ruth. Baseball fans will immediately recognize the "Sultan of Swat" as one of the best hitters of all time.

In designing a relational database on baseball statistics we link the data for statistics on number of times at bat, number of hits, walks, strikeouts, and ultimately home runs. Each player who is entered creates a new set of entries. As the database grows we can manipulate the data to compare the best and worst hitters, those who have the most or least strikeouts, and those who have the highest or lowest number of home runs. The Relational Database allows us to form those relationships between the data. There are other types of database as well, but the Relational Database is

certainly the most common in use today.

d. Graphics

There are hundreds of programs that fall under this relatively broad category of business software. We can first begin by dividing the category into those programs that create original pieces and those that manage acquired material. One must recognize that a number of programs are capable of doing both, but most generally does one much better than they do the other.

Programs that create original material frequently offer users a wide selection of tools. One might think of these programs as creating an electronic canvas for the computer artist. Just as a painter might use different brush sizes, shapes, and textures to create a new painting, so too, does the computer artist. The software provides tools that mimic the painter's brush, the sculptor's knives, and the printer's type selection.

There are two groups under the category of those that use existing creations. The first of these are those that work with photographs. These programs are now common for users of the scanner and digital camera. The user acquires the original photograph in an electronic form, usually by scanning it with the scanner or digitizing the photo, and then manipulates the photo to create a new work. These programs often include a standard array of tools not unlike those found in the programs that create original works. Electronic brushes, knives, fonts, and other tools can be used to alter or touchup the photo. These programs also use other tools to add, erase, or simply alter the photograph's contents.

One should also remember that the industry itself has changed in a way that makes it much easier for a would-be criminal to effectively use the computer. Originally many of the graphics programs used proprietary routines and methods for performing their specific tasks. They often saved the product in a specialized file that could be accessed only by a product of that same company or by a product that was licensed to another company. What this meant is that many items produced on a given piece of software could not be altered by a competing brand. It may be viewed, but not changed.

The downside of this practice was that users could not easily share their own work with others. A graphics artist using one software package could not send his work to other artists unless that person also had the same software. Again, they might be able to view the original work, but if modification or change was needed then they could not do so without the proper software.

Over time this began to change. First, there were software packages produced, often by underground programmers, which would allow a user to open, manipulate, or even change the file settings of a given file. One could easily convert a proprietary file from one type to another with such programs. These programs may have been a violation of licensing or copyright protection, but the industry demanded them so the infringement was often ignored.

Eventually, standards for the creation, storage, and exchange of graphics began to emerge. Today many of the better applications now include conversion routines or

the ability to open and save files to a variety of file types. This means that users can more readily exchange files without the need to buy or maintain multiple platforms or software packages.

e. Presentation

There have been very few crimes that have used presentation software to conduct the crime. The reason for including this topic is to educate the reader of the various software packages available. Presentation software, as the name implies, allows the user to present material to an audience or individual. This software includes packages such as Microsoft *PowerPoint*® and the newest versions of multimedia packages.

In recent years we have seen a dramatic increase in the number of presentation programs that use the multimedia concept. These include software from companies like Real Media, Macromedia, and many others. These programs allow the user to create either dedicated or stand-alone presentations that can be easily viewed on the computer or other device.

Many of these programs allow the user to add video, audio, and still photographs all in one package. The Real Media company produces a line-up that includes Real Slideshow, Real Presenter, and Real Audio. These packages allow the user to "stream" the presentation over the Internet or other network connection, and can be set up so that the presentation resides on the users own computer.

Macromedia has moved to the front of animated presentations with their lineup which includes the powerful Flash program. Flash, now in its fifth version, incorporates many of the best principles from other presentation packages while allowing the user the ability to create new material as well. Many Internet sites are now using Flash creations to showcase products or services that otherwise were left for simple text and still picture shows.

f. Communication

Communication software has made dramatic changes in the last decade. The ability to send large amounts of data across phone lines, cable, or a satellite connection now allows many users opportunities only dreamed of before. For instance, a user today, connected through a cable or DSL system, can easily exchange a ten-megabyte file in less than two minutes.

One of the most dramatic changes to come from communications software is the ability to send "real time" video and audio over the Internet. Inexpensive digital cameras are used in many homes, offices, and business to send low-resolution video to sites around the world. Of course, at the same time the criminal user has found a way to transmit copyright or other protected material as well. This is where the computer crime investigator is likely to encounter communication software.

g. Other

There are hundreds of other programs that fall into this category. Some are sim-

ply an extension or variation of the five categories mentioned above. For instance, there are dozens of dedicated packages based on the word processor model. Each of these programs uses a basic text editor to manage words, but they do so in a very specific fashion. One example is the dedicated screenplay software that is now used by many writers. This software is dedicated to the production of a screenplay in a format accepted by the television and film industry. Though it is a word processor at the core the simple fact remains that such programs can be considered as stand-alone products.

For the investigator the ability to recognize and identify every business, entertainment, or other program that is on the market is impossible. One must be familiar, though, with the most common programs that are out there, and with those that have the highest potential for being used in a criminal enterprise. As one proceeds through the rest of the text it is important to consider the type of hardware and software that might be used in each crime example. Where appropriate we will certainly discuss the specifics of both as we discuss the individual crimes associated with computers.

2. Entertainment Software

From a practical standpoint there are often only two distinct areas where an investigator is likely to see entertainment software. These include the illegal copying or distribution of the software and the involvement of software for pornographic or other restricted use. This does not mean that an investigator can simply ignore the entertainment area. The simple fact is that entertainment software can be used for many other purposes than just crime, and even these can be of interest to law enforcement.

a. Games

One example of non-criminal use of software that may be of interest to the law enforcement officer is the "reality" based games now on store shelves. One such "game" is titled "Beat Down" and it depicts the various life choices faced by a would-be criminal gang member. One of those choices includes the need to kill a cop as a method of proving one's loyalty to the gang. While this type of violent portrayal is not illegal it is of interest to one educated in the theories of criminology. Certainly one could argue that such displays meet the definitions found in certain theories, and may help explain some of the recent violent acts against police.

b. Graphics

Games are not the only form of entertainment software available to users. Graphics programs that allow users to create or alter graphics using their computer are almost as popular. These programs include photograph manipulation, artistic, and presentation lines. Each is designed to give the user unique tools or abilities to work with just about anything that can be graphically represented.

Our best example is found in the earlier section of this chapter. With a simple graphic program we could easily transform an otherwise routine senior photo into an exotic masterpiece. Well, maybe not a masterpiece, but a relatively good piece of work considering it took less than thirty seconds to cut and paste the image into place. This is why graphics programs are so important to the investigation. If a no-talent artist can transform a senior photo into something unique imagine what a talented crook could do.

c. Educational

Other types of entertainment software that investigators may encounter include educational titles. Most are harmless, but from time to time the investigator encounters one software that is somehow involved in a crime. Again, the point of this chapter is not to fully explore every form of software available but to have investigators become knowledgeable in what they are likely to encounter.

3. Utility Software

The final genre of application software that we will discuss is commonly referred to as utility software or simply utilities. These packages fall into three distinct categories.

a. System Maintenance

The first of these categories are known as "system maintenance" packages, which are used to maintain the user's system at peak performance levels. These programs include the popular offerings from McAfee, Microsoft, and many others.

In recent years utility manufacturers have begun bundling their best programs into "System Suites." These packages include five or more of the best system utilities manufactured by the particular company. Some of the more popular packages include Norton SystemWorks, Ontrack System Suite, and Gizmos '98. Each package typically includes software that monitors your PC's health, fixes errors, protects against viruses, and purges unwanted applications. Prices range from just around $30 to over $90 per package.

b. Software Support

The second category of software is the "support" group, which includes print spoolers, RAM managers, and a wide range of programs designed for specific purposes. This group also includes the now mandatory "virus" detection software that is necessary for any computer connected to the Internet or other external source. Also included are compression routines, crash prevention, disk management, file conversion, and performance enhancement packages.

c. Other

The last group of utility software worth mentioning are those that fall in the category of security and encryption. Most packages concentrate on security issues for networked computers, especially those connected to the Internet. These products include software designed for almost all OS and computer makes. They also include specialty software that works on mail, data transfer, and outside access.

ENDNOTES

1. Visual Basic is a trademark and wholly owned by the Microsoft Corporation, http://www.microsoft.com.
2. Windows is a trademark and wholly owned by the Microsoft Corporation, http://www.microsoft.com.
3. UNIX is a trademark and wholly owned by The Open Group, http://www.opengroup.org/.
4. Punch cards were just larger than the average personal check in use today, but were often made from a much heavier stock of paper. The paper, which was almost as thick as a thin sheet of cardboard, was blank in most instances. Information was placed on the card when the data entry personnel literally punched holes in the card, usually through a special terminal, which was then fed into the punch card reader. The reader identified the contents of the card by the placement and number of holes in the card. A typical computation might need several hundred cards, and in complicated matters there may even be thousands of cards used to feed information into the computer. An alternative to the punch card system was the punch tape. This tape, which is commonly associated with stock market "tickers" from the early part of the twentieth century, used the same principles. Information was punched on the tape and the computer "read" the information when it was fed through the tape reader.
5. "Computing Science and Systems: The UNIX System." *AT&T Bell Laboratories Technical Journal,* 63 No. 6 Part 2, October 1984, pp. 1577–93. (Not available on the Web)
6. Windows '98 is a trademark and wholly owned by the Microsoft Corporation, http://www.microsoft.com.
7. Pentium, Pentium II, Pentium III, and Pentium IV are all trademark and wholly owned by the Intel Corporation, http://www.intel.com.
8. Windows was sold in the original version, 2.0, 3.0, 3.1, 3.11, and later the Windows '95 version. There were small upgrades and changes along the way as well leading some versions to carry an additional designator such as 3.11.1 or Windows '95 SR1 (Service Release 1).
9. PowerPoint is a trademark and wholly owned by the Microsoft Corporation, http://www.microsoft.com.

Appendix C

NETWORKS AND COMMUNICATION SYSTEMS

A. Network Basics
   1. Clients and Servers
   2. Wiring and Cable
   3. Network Interface Cards
   4. Switches
   5. Bridges
   6. Routers
   7. Modems
   8. Network Management
B. Local-Area Networks: Ethernet, Fast Ethernet, and Gigabit Ethernet
   1. Ethernet Basics
   2. The 5-4-3 Rule
   3. 10Base2
   4. 10BaseT
   5. 10BaseF
   6. 100BaseT
   7. 100BaseT4
   8. 100BaseFx
   9. 1000BaseX
   10. CSMA/CD
   11. I/G and U/L
   12. Subnetwork Access Protocol (SNAP)
   13. Cisco's Inter-Switch Link (ISL)
   14. Propagation Delay
   15. Error Conditions
C. Token Ring
D. High-Speed Lan Technologies
E. Wireless Connections
F. Remote Access and Wide-Area Networks

The term network has grown to mean many different things when talking about computer systems. It may refer to the Internet, which is the largest network currently operating, or it may refer to a single connection between two computers in one room. In the first case there are literally thousands of computers united through a maze of electronic connections that stretch around the world. The latter is as simple as running a single cable between two computer ports and "booting up" the appropriate software.

For the criminal investigator the term network means simply the connection of two or more computers. The means of such connection can often be very complicated, and it is not necessary for the investigator to be a network expert. It is necessary, though, that the investigator at least understands the basic theories and practices of modern network computing. To that end, it is important that one recognize that by connecting two or more computers you create a network. It is also vital that one understand that a network is useless if the computers cannot communicate with each other. It is this ability to communicate, to pass data back and forth, which makes the computer network so useful, and so vulnerable.

As with many investigations, it is imperative that the investigator understand the topic thoroughly, and this is especially important when dealing with computer crimes. Networks can be very complicated or they may be relatively simple. The key to both understanding networks and investigating crimes involving networks is to first understand how networks work, and that is where we will start in this chapter.

A. NETWORK BASICS

Every network includes at least two computers, but may include dozens or even thousands. The methods used to connect the computers and to operate the network itself is commonly called the "topology." The term "topology" means simply the layout of the network. There are several topologies available for today's computer network.

One of the more common methods is to connect computers using a specialized device known as the *network interface card* (NIC). The NIC allows the computers to send data over a specifically prepared wire or cable. The NIC also allows the com-

puters to connect to the hub, router, switch, or other devices equipped with similar connections.

At the heart of the network system is the *Network Operating System* (NOS) which is in fact a specialized form of operating software. There are several NOS available with Microsoft Windows NT, Novell NetWare, AppleShare, or Artisoft LANtastic being the more popular. Each use proprietary processes for communication, but they also each share a great deal of standardized schemes that allow them to communicate with each other. Thus, a user on a Novell system can, with the proper NOS setup and connections, communicate easily with users on other NOS systems.

The primary purpose of the computer network is to enhance communication and cooperation between users. For instance, in an office where several people must share a printer a small network can ease some of the burden, not to mention the costs of multiple printers. Networks also allow users to communicate together via electronic mail (e-mail) or other schemes. Of course, the size of the network will determine the complexity as well as the potential topology choices available.

One of the more common network topologies is called a *Local Area Network* (LAN). The focus in this setup is on the sharing of resources among known users within a confined area. Figure C-1 depicts a simple Local Area Network in a small office setting using the basic components. In this example two computers are connected using standard cable and a common NOS such as Microsoft Windows NT.

By definition the LAN is determined not by the number of computers but by the proximity of those computers and their connection. In the above example the LAN has two computers connected directly to each other. This is commonly known as a "peer to peer" connection since each computer has the same relative rank in the network system. Other LAN systems may use computers which have unequal rank within the network. In these systems a single computer, commonly called a *server,* is used to store most of the data as well as application software. Individual computers known as "work stations" are connected to this system but often have less power or authority within the system.

A network can be expanded to include computers outside the immediate area and even other networks as well. By combining networks together, users can send e-mail, share links to the global Internet, or conduct videoconferences in real time with other remote users. These networks are called Wide Area Networks (WAN).

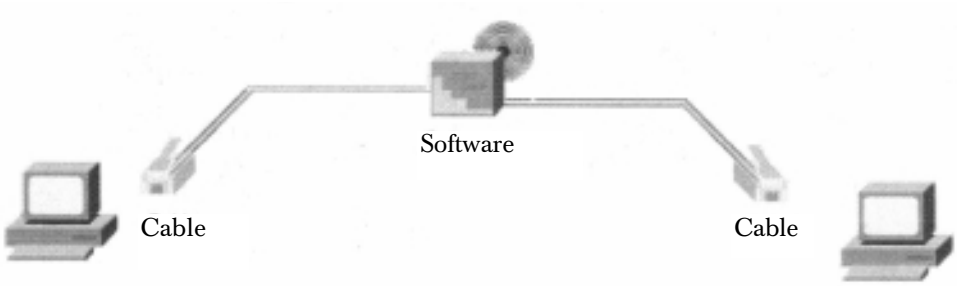


Figure C-1. Simple network.

Many of today's corporate networks use PCs as servers and are often linked together to form the backbone of the network system. Figure C-2 shows a typical server desk system with multiple PCs connected together to form a chain of servers. Systems of this magnitude will also typically use other devices to help communicate between computers on the network.

Most networks–even those with just two computers–also contain a hub or switch to act as a connection point between the computers. Hubs, which are also called repeaters, are simple devices that interconnect groups of users. Hubs forward any data packets, including e-mail, word-processing documents, spreadsheets, graphics, print requests, etc., they receive over one port from one workstation to the remaining ports. Figure C-2 shows a simple network using a Hub.

By connecting computers through the hub the network effectively shares the bandwidth between the users. The speed at which data is transferred from one computer to the other will depend on the rate of the connecting devices (NIC, hub, etc.). As a general rule, the overall speed of a network is often rated in "megabytes per second" of data transfer. Faster networks are being developed, but for now most network connections still run in megabyte increments.

1. Clients and Servers

As the network grows it becomes more complicated, and there is a need for a central unit to work as the server. In network terminology, the server is a central computer that acts as a principal storage point for files or application programs shared on the network. In this sense the term "central" is not being used simply to refer to the physical location of the server, but instead to the role the computer plays among all those on the network. In many instances the server may be the more powerful of the various computers on the network, but it need not be. In fact, some of the more

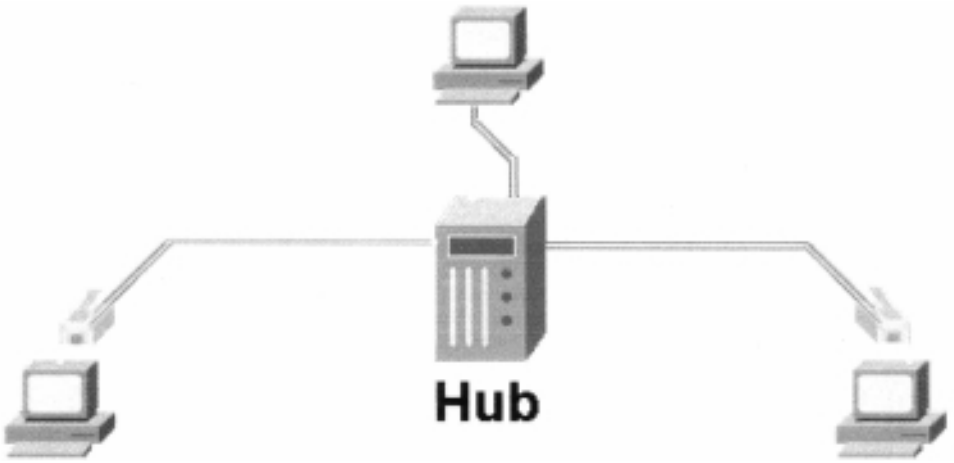


Figure C-2. Network with hub.

familiar LAN setups today use a moderate server with the more powerful computers on the peripheral serving "client side" applications.

Servers also provide connections to shared peripherals such as printers, plotters, or other devices. In the simplest networks this is the most common role a server plays. It is the main storage for shared files and access to shared devices. As mentioned in the previous paragraph, some LANs allow "client side" applications to run on individual computers which are then connected to a server for access to shared resources.

In a simple network the software running the network is loaded onto every computer. In a system using a server, the software is loaded onto the server with only "client side" software loaded on the work stations connected to the server. This means that valuable disk space is saved on the hard drives of the individual units connected to the server, and speed is gained by dedicating one machine to the task of server.

Not all networks have a server, and in many instances those networks that are set up without a server use the "peer to peer" topology. This means that each computer on the network is equal to every other computer. Where a server is used then it is the server that decides which computer gets what information and when they are served. In the "peer to peer" system users can exchange files and e-mail, copy files onto each other's hard drives, and even use printers or modems connected to just one computer. But as more users are added to the network, a dedicated server can provide a central point for management duties such as file backup and program upgrades.

2. Wiring and Cable

The methods for connecting computers together have expanded in recent years. Today there are three distinctive methods for connecting a computer network. The first of these relies on a wiring system not unlike that used for telephone service. In fact, the most common wire used in small networks is known as *twisted pair,* and it uses a wire system that is not too far removed from that seen in most telephone systems.

Twisted pair wiring comes in several standards with the *unshielded twisted-pair* (UTP) *Category 3* wire as the most popular. The *UTP Category 3* wire is also used for phone lines and is a good choice for entry level users or those who do not demand the highest speeds. The wire looks very much like the extension used to extend a telephone's reach within a physical location. A small LAN, with no more than ten or so computers, is perfect for this category of wire and connectors.

For users who are connecting more than a dozen computers the heftier *UTP Category 5* wire is preferred. Though similar in overall appearance the wire is thicker and capable of carrying the loads demanded by larger local area networks.

One of the drawbacks to twisted pair wiring is the limited bandwidth that can be attained. Bandwidth refers to the amount of data that can be transferred along a single connection. The broader the bandwidth the more data that can be transferred over the network connections; i.e., the more computers you have connected the

broader you want your bandwidth to be. For most LANs the connection using standard NICs and twisted pair wire is sufficient. For larger networks, such as those with several hundred connections, the bandwidth becomes a concern since slower speeds means potential productivity loss.

It is also a concern when dealing with massive amounts of information or data. For instance, even a small LAN can be overwhelmed when the users take advantage of the latest multimedia products on the market. Streaming media is one product that needs higher bandwidth to be most effective. Imagine connecting ten computers to a single server then demanding that all ten users be able to watch the same training video online. The bandwidth required to stream this type of presentation might require much more than the speed available with a low-cost NIC and twisted pair wiring.

When twisted pair is not a choice, many network engineers choose one of the many types of coaxial cable available today. This cable resembles the round cable used in most cable television connections, but is often of a higher quality to allow for broader bandwidth.

Like twisted pair, coaxial cable also has its limitations. When speed or bandwidth are at a premium many engineers opt for *fiber optic*. Fiber optic cable is usually reserved for connections between "backbone" devices in larger networks. As one might imagine, as speed increases, so too, does price of the connection. Fiber optic connections are more expensive than either coaxial or twisted pair type wiring. We will see more about wiring in coming sections, but for now it is important to understand the relationship between the various components in a network system.

3. Network Interface Cards

Network interface cards, also called network adapters, are usually installed inside a computer case. Most of today's PCs use a NIC that connects through an open *PCI* slot. There are also *ISA* and *USB* (Universal Serial Bus) cards on the market. For the portable or notebook computers the standard *PCMIA* type card is also available as a NIC. This credit card-sized PC Card format, which is installed in a slot usually accessed through the side of the laptop, can also be used to plug in a modem or other peripheral.

There are several NICs available on today's market. The most common standard is the *Ethernet,* which allows users a great deal of options for speed and price. One must remember that each card generally communicates only with other cards of that same category. For instance, Ethernet NICs support only Ethernet connections while other cards support their own topology.

Much like other computer components, speed is used to rate NICs. The more common ratings are for 10, 100, and 1000 megabyte per second cards. This refers to the amount of data that can be sent through the card. As a general rule the higher the rating of the card the more likely it will be "backward compliant" with slower cards. In other words, a card rated at 10-mbps will only communicate with other cards at the same rating. A card with a rating of 10/100/1000 speeds may cost more than the 10 speed card, but the added speed capability means that it will communi-

cate with any of the computers equipped with 10, 100, or 1000 speed cards.

The NIC is also dependent on the cable that is used. Twisted-pair (also called 10BASE-T) is usually found with cards with a rating of 10 while coaxial (also called 10BASE2) works with the 10/100 cards. Again, one can mix the cards and cabling in a network, but special attention must be given to which computers are equipped with which cards. Servers are typically equipped with the fastest cards and cable while work stations (also known as clients) are equipped with slower cards.

Some NICs will also support wireless networking, which uses radio technology to transmit a signal through the air instead of over a wire. These NICs handle most of the same functions as a NIC in a wired network. The big advantage is that a wireless NIC can transmit data faster than any cable system. The downside is that a wireless NIC costs almost three times that of a standard cable-ready NIC, and there are some drawbacks because of the physical requirements of the transmission. If speed is the highest level of importance then wireless may be the way to go, but not all users have an unlimited budget for their network design.

4. Switches

In the earlier section we spoke of Hubs, which are often seen as a first line for connecting multiple computers through a network. As the network becomes more complicated there arises the need for smarter and faster connections. The next level of connecting device is the *switch*.

The big difference between a switch and a hub is the technology used to relay packets of material. A hub simply sends the packet on to all other computers on the system while the switch forwards the data packet only to the appropriate port for the intended recipient. To insulate the transmission from the other ports, the switch establishes a temporary connection between the source and destination, and then terminates the connection when the conversation is done.

5. Bridges

A level up from the switch is the bridge. As the network becomes crowded with users or traffic, bridges can be used to break them into multiple segments. Switches are basically multiple bridges in a single device. Bridges help reduce congestion by keeping traffic from traveling onto the network "backbone" (the spine that connects various segments or *subnetworks*).

If a user sends a message to someone in his own segment, it stays within the local segment. Only those packets intended for users on other segments are passed onto the backbone. In today's networks, switches are used where the simplicity and relative low cost of bridges are desired.

6. Routers

If we rate hubs and switches based on relative capability to direct traffic then we might say the router is the highest level of traffic cop in the network. The hub pret-

ty much ignores the packet address as material comes through as it blindly sends the data to all computers along its connection. The switch, on the other hand, uses part of that address to direct the data packet along the line. The bridge is even better still since it uses more of the packet address to direct the data to not only the proper connection but even the proper computer on that connection. The router is the smartest of this group and allows network engineers to connect multiple computers or even individual networks to each other.

When connecting to a network of this type the network architect has established a network road map called a "routing table." The router is central to this scheme, and can help ensure that packets are traveling the most efficient paths to their destinations by using the routing table and the packet address. If a link between two routers fails, the sending router can determine an alternate route to keep traffic moving.

Routers also provide links between networks that speak different languages. The language of the computer network, as we will see in coming sections, is known as a *protocol.* One network may speak one protocol while another uses a different protocol. The router speaks both languages and can help speed data along the appropriate path regardless of which protocol is used.

Examples of protocols include Internet Protocol (IP), Internet Packet Exchange (IPX), and AppleTalk. Routers not only connect networks in a single location or set of buildings, they also provide interfaces (known as "sockets") for connecting to wide-area network (WAN) services. These WAN services are offered by telecommunications companies to connect geographically dispersed networks.

7. Modems

To this point we have concentrated on continuous connections between networked computers. Not all connections are kept on, though. The most common method for most people to connect to the Internet (and other networks) is still with a *Modem.* These are also known as "dial-up" connections because the user must dial-up the telephone to connect to the Internet Service Provider or other connection.

When sending data across telephone lines the modem converts or modulates the information from digital format into an analog signal. When the information reaches the next connection it is then reconverted back into digital form through a process called demodulation. The word Modem is actually a combination of the words *Mo*dulate and *Dem*odulate.

8. Network Management

Of course all of this connection is meaningless unless the computer knows how to send the information or data. That is where Network Management Software comes into play. This software allows the network administrator to monitor traffic flow, new equipment, and troubleshoot network problems. Most management software allows the manager to monitor the various connections including the hubs, switches, routers, and bridges in the system. The software also monitors traffic volume, poten-

tial route problems, and network topology. Most management software runs in the background, but proprietary systems–such as those used by Novell–often have an up front appearance.

B. LOCAL-AREA NETWORKS: ETHERNET, FAST ETHERNET AND GIGABIT ETHERNET

Ethernet networks have been around since the late seventies and remain the leading network technology for many networks. The Ethernet is built upon a system for packet management that is commonly referred to as *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD). Simply put, an Ethernet workstation sends data packets through the NIC, and the Ethernet topology is used to monitor those messages. When a computer user gives a command to send data, the Ethernet card "listens" for a "quiet" network. The Ethernet system will only send the packet when no other packets are traveling on the network. If the card detects another packet then the card holds the data until a clear connection can be made.

One can easily think of this system as a very polite group of friends having lunch together. When one friend talks the others remain quiet and listen. When that speaker is done then another begins only when there is absolute quiet. Unfortunately, in most conversations, just as in most network travel, there are times when two speakers will try to talk at the same time. The protocol will dictate which should be quiet and which will continue, but the simple fact is that a collision of conversation has already occurred.

On the Ethernet system, if multiple stations sense an opening and start sending at the same time, a "collision" also occurs. Each then stops transmitting, waits for a randomly selected amount of time, and then listens for traffic again. In theory, because the computer selects a random length of time, a time which will vary with each new event, there is little likelihood that both computers will select the same period of time to wait before checking for a clear network. In this sense, one will choose a time period shorter than the other; thus, the shorter time period allows that system to send, which means a similar collision is avoided.

Simply stated, the first one to finish the wait will begin transmitting and the second will then hear a busy network. The delayed station waits again. This wait stage lasts only milliseconds, in most instances, but it certainly increases the possibility the station will not find an open network. Thus, the collision detection portion of the protocol allows the system to solve collisions with a minimal disruption to the user. The user generally will not notice such delays since they occur in very short periods of time, and thus the whole system appears to work effortlessly.

Because there is always the potential for continued disruption the system has a built-in failsafe that works relatively well on most systems. If the network is so congested that the station fails to send data after sixteen (16) consecutive attempts then the Ethernet card instructs the original application to start over again. As one can quickly see, this protocol works quite well as long as the network is not overly congested. Of course, the more users on a network the more likely it is that there will be a busy network when one's card attempts to send data. This means that the num-

ber of collisions increase as does the amount of time spent waiting.

Collisions are normal occurrences, but too many can slow the network. Collision rates begin to cause congestion when more than 50 percent of the total network bandwidth is used. Files take longer to print, applications take longer to open, and users are forced to wait. At 60 percent or higher, the network can slow dramatically or even shut down.

As noted in the previous section, Ethernet bandwidth or data-carrying capacity (also called *throughput*) is commonly rated at 10 Mbps. *Fast Ethernet* and *Gigabit Ethernet* also use similar paradigms for collision detection, but they do so at a much greater speed. Fast Ethernet is commonly rated at 100 Mbps while Gigabit Ethernet is rated 1000 Mbps. What this means is that the data being transmitted is carried along the route much faster which in effect means less traffic on the network. In other words, a file transmitted along an Ethernet connection might take as much as thirty seconds to clear the network. This means that other NICs are waiting before they can transmit. With the Fast Ethernet connection this time is cut significantly. This means that a data packet taking 30 seconds on a standard Ethernet connection will travel at roughly 1/10th that time on a Fast Ethernet connection, and almost 1/100th of that time on a Gigabit Ethernet connection.

1. Ethernet Basics

Ethernet was originally developed by Digital, Intel and Xerox (DIX) in the early seventies and was designed as a "broadcast" system. What this meant is that a station on the network can send messages whenever and wherever it wants. All stations may receive the message, however only the specific station to which the message is directed will respond.

The original format for Ethernet was developed in Xerox' Palo Alto Research Center (PARC) in 1972. Using *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD) it had a transmission rate of 2.94Mbps and could support 256 devices over cable stretching for 1 kilometer. The two inventors were Robert Metcalf and David Boggs.

The "Ether" part of Ethernet denotes that the system is not meant to be restricted for use on only one medium type, i.e., copper cables, but can also run on fiber cables or even radio waves. Traditionally, Ethernet was used over coaxial cable which is commonly called 10Base5. The term has specific meaning with the "10" denoting that the cable can carry data at up to 10Mbps. The term "base" means that the signal is *baseband,* which in turn means that the cable is used for the whole bandwidth. This connotes that only one device can transmit at one time on the same cable. It is much like a one-way street.

The "5" denotes 500 meter, which means that the cable cannot be extended more than that length and still carry a quality signal. This is an important consideration in designing larger networks since the 500 meter limit can be quickly reached when routing cable behind walls and through a busy office. As a general rule, the cable is run in one long length forming what is often referred to as a *Bus Topology.* Stations attach to it by way of inline *N-type* connections or a transceiver which is literally

screwed into the cable using what is lovingly known as a "Vampire Tap."

This system also uses a 15-pin *Attachment Unit Interface* (AUI) connection (also known as a DIX connector or a DB-15 connector), and is often used for a drop lead connection (maximum of 50m length) to the station. Designers also note that segments are terminated with 50-ohm resistors, and the shield should be grounded at one end only.

2. The 5-4-3 Rule

An Ethernet system can be very large. Up to 300 devices can be set up on one network, but there is a fundamental limit. This limit, known as the *5-4-3 rule,* means that no more than four (4) repeaters (hubs, switches, etc.) can be used on one system. This in turn means that only five segments (for a total length of 2,460 m) can be connected together. Also, of the five segments only three can have devices attached, but each segment may have as many as 100 devices per segment. This gives us the total of 300 devices which can be attached. Systems that use this topology are often called a *Thicknet broadcast domain.*

3. 10Base2

Because of some of the limitations in the 10Base5 system it is common to see thick coax used in *Risers* to connect *Repeaters.* The repeaters provide *Thin Ethernet* coaxial connections for runs up to 30 workstations. Thin Ethernet, also known as *Thinnet,* uses RG-58 cable which is commonly called 10Base2.

As with 10Base5, the name carries certain descriptions of the cable itself. The "10" and "Base" designations remain the same as with 10Base5, but the "2" now denotes a 200 meter maximum length rather than the 500 seen above. From a practical standpoint this most designers rarely run the system more than 185 meter while the minimum length between stations is 0.5 meter.

Each user connects to the *Thinnet* by way of the Network Interface Card (NIC) equipped with a *British Naval Connector* (BNC). At each station the Thinnet terminates at a T-piece, and at each end of the *Thinnet* run (or 'Segment') a 50-ohm terminator is required to absorb stray signals. This allows designers to avoid what is commonly called "signal bounce" and provide a "cleaner" connection.

A segment can be appended with other segments using up to four repeaters, i.e., five segments in total. Two of these segments however, cannot be tapped and can only be used for extending the length of the broadcast domain (to 925m). What this means is that 3 segments with a maximum of 30 stations on each can provide up to 90 devices on a Thinnet broadast domain.

4. 10BaseT

It is becoming increasingly important to use Ethernet across Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP) wiring. This setup is commonly called 10BaseT (the 'T' denoting twisted pair). Of course, the "10" and "Base" still mean the

same as with 10Base5 and 10Base2.

One of the more popular topologies is called the Star. In this system each station has a NIC that contains an *RJ45* socket. The socket is then used by a 4-pair RJ45 plug-ended drop lead to connect to a nearby RJ45 floor or wall socket. For those not familiar with these specific connectors it can be easily described as looking much like a telephone wall outlet and connector.

Each port on the hub sends a *Link Beat Signal* which checks the integrity of the cable and devices attached. A flickering LED on the front of the port of the hub tells you that the link is running as defined. The maximum number of hubs (or, more strictly speaking, repeater counts) that you can have in one segment is four, and the maximum number of stations on one broadcast domain is 1024.

5. 10BaseF

The 10BaseF standard developed by the IEEE 802.3 committee defines the use of fiber for Ethernet. The 10BaseFB allows up to 2km per segment (on multimode fiber) and is designed for backbone applications such as cascading repeaters. The 10BaseFL describes the standards for the fiber optic links between stations and repeaters, again allowing up to 2km per segment on multimode fiber. In addition, there is the 10BaseFP (*Passive components*) standard and the Fiber Optic Inter-Repeater Link (FOIRL) which provides the specification for a fiber optic MAU (Media Attachment Unit) and other interconnecting components. The 10BaseF standard allows for 1024 devices per network.

6. 100BaseT

Fast Ethernet is the most popular of the newer standards and is an extension to 10BaseT. The 100 denotes 100 mbps data speed and it uses the same two pairs as 10BaseT (1 and 2 for transmit, 3 and 6 for receive). The actual data throughput increases by between 3 to 4 times that of 10BaseT.

Where 10BaseT uses *Normal Link Pulses* (NLP) for testing the integrity of the connection, 100BaseT uses *Fast Link Pulses* (FLP) which are backwardly compatible with NLPs but contain more information. Fast Link Pulses are used to detect the speed of the network (e.g., in 10/100 switchable cards and ports), and this allows the NIC to switch as necessary. The tenfold increase in speed is achieved by reducing the time it takes to transmit a bit to a tenth that of 10BaseT. The slot-time is the time it takes to transmit 512 bits on 10Mbps Ethernet (i.e., 5.12 microseconds) and listen for a collision (see earlier). This remains the same for 100BaseT, but the network distance between nodes, or span, is reduced. Many network engineers use the term 100BaseX to refer to both 100BaseT and 100BaseFx.

There are two classes of repeater, Class I and Class II. A Class I repeater has a repeater propagation delay value of 140 bit times, whilst a Class II repeater is 92 bit times. The Class I repeater (or Translational Repeater) can support different signalling such as 100BaseTx and 100BaseT4. The Class II repeater (or Transparent Repeater) can only support one type of physical signalling.

7. 100BaseT4

Increased speed and data handling move rapidly up as we progress through the remaining cables. For instance, 100BaseT4 uses all four pairs of wires and is designed to be used on Category 3 cable installations. Transmit is on pairs 1 and 2, receive is on pairs 3 and 6, while data is bidirectional on both pairs 4 and 5 and on 7 and 8. The signaling is on three pairs at 25MHz each using 8B/6T encoding. The fourth pair is used for collision detection. Half-Duplex is supported on 100BaseT4.

8. 100BaseFx

100BaseFx uses two cores of fiber (multimode 50/125um, 60/125um or single-mode) and 1300nm wavelength optics. The connectors are SC, Straight Tip (ST) or Media Independent Connector (MIC). The 100BaseT MAC mates with the ANSI X3T9.5 FDDI Physical Medium Dependent (PMD) specification. At half-duplex you can have distances up to 412m, whereas Full-duplex will give 2km. There is also a proposed 100BaseSx which uses 850nm wavelength optics giving 300m on multi-mode fiber.

9. 1000BaseX

This cable is commonly used for Gigabit Ethernet. The 1000 refers to 1Gb/s data speed, and is a further extension of 10/100BaseT using CSMA/CD. The cable can be run up to 500m on multimode fiber (1000BaseSX, 'S' for Short Haul using short-wavelength laser over multimode fiber) and at least 25m on Category 5 cable (1000BaseT). Many cable manufacturers are enhancing their cable systems to 'enhanced Category 5' standards in order to allow Gigabit Ethernet to run at up to 100m on copper.

The Category 6 standard has yet to be ratified, and is not likely to be due until the end of 2000. Currently, on normal 62.5/125um multimode fiber, Gigabit Ethernet (1000BaseSX), using 850nm wavelength, can run up to 220m. Using 1300nm wavelength, Gigabit Ethernet (1000BaseLX where the 'L' is for Long wavelength laser, or Long Haul) can run up to 550m on 62.5/125um multimode fiber. Using 50/125um multimode fiber Gigabit Ethernet can run up to 500m using 850nm wavelength and 550m using 1300nm wavelength. Electronics for 1300nm is more expensive and so this is currently an issue as many multimode fiber installations using 62.5/125um fiber and so 220m is often the limit for the backbone when it should be 500m to satisfy ISO 11801 and EIA/TIA 568A. 1000BaseLX ('L' for Long Haul) runs on Single-mode fiber up to 5km using 1310nm wavelength.

10. CSMA/CD

As mentioned earlier, Ethernet uses Collision Sense Multiple Access with Collision Detection (CSMA/CD). When an Ethernet station is ready to transmit, it checks for the presence of a signal on the cable. If no signal is present then the sta-

tion begins transmission, however if a signal is already present then the station delays transmission until the cable is not in use. If two stations detect an idle cable and at the same time transmit data, then a collision occurs. On a star-wired UTP network, if the transceiver of the sending station detects activity on both its receive and transmit pairs before it has completed transmitting, then it decides that a collision has occurred.

On a coaxial system, a collision is detected when the DC signal level on the cable is the same or greater than the combined signal level of the two transmitters, i.e., significantly greater than +/- 0.85v. Line voltage drops dramatically if two stations transmit at the same and the first station to notice this sends a high voltage-jamming signal around the network as a signal. The two stations involved with the collision lay off transmitting again for a time interval that is randomly selected. If the collision occurs again then the time interval is doubled, if it happens more than 16 times then an error is reported.

A Collision Domain is that part of the network where each station can 'see' other stations' traffic both unicast and broadcasts. The Collision Domain is made up of one segment of Ethernet coax (with or without repeaters) or a number of UTP shared hubs. A network is segmented with bridges (or microsegmented when using switches) that create two segments, or two Collision Domains where a station on one segment cannot see traffic between stations on the other segment unless the packets are destined for itself. It can, however, still see all broadcasts as a segmented network no matter the number of segments and is still one Broadcast Domain.

Special network adaptors used in devices such as network analysers and transparent bridges use promiscuous mode. What happens is that the network controller passes ALL frames up to the upper layers regardless of destination address. Normally the frames are only passed up if they have that particular device's address.

Full-Duplex Ethernet can exist between switch ports only and uses one pair of wires for transmit and one pair for receive. NICs for 10BaseT, 10BaseFL, 100BaseFX and 100BaseT have circuitry within them that allows full-duplex operation and bypasses the normal loopback and CSMA/CD circuitry. Collision detection is not required as the signals are only going one way on a pair of wires. In addition, Congestion Control is turned on which 'jams' further data frames on the receive buffer filling up.

Half-Duplex allows data to travel in only one direction at a time. Both stations use CSMA/CD to contend the right to send data. In a Twisted Pair environment when a station is transmitting, its transmit pair is active and when the station is not transmitting it's receive pair is active listening for collisions.

11. I/G and U/L within the MAC address

With an Ethernet MAC address, the first octet uses the lowest significant bit as the Individual/Group address (I/G bit). For the investigator this is important since it also means that the address does not have such a thing as the Universally/Locally (U/L bit) administered. Instead, the U/L bit is used in Token Ring A destinations starting with the octet 05. It is also important to note that is is a group or multicast address

since the first bit to be transmitted is on the right-hand side of the octet and is a binary '1.' Conversely, '04' as the first octet indicates that the destination address is an individual address. Of course, in Ethernet, all source addresses will have a binary '0' since they are always individual.

The first 3 octets of the MAC address form the Organizational Unique Identifier (OUI) assigned to organizations that requires their own group of MAC addresses. The investigator can find the OUI by logging onto the *standards* page of the Institute of Electrical and Electronics Engineers (IEEE). The page can be found on the World Wide Web at: http://www.ieee.org.

12. Cisco's Inter-Switch Link (ISL)

A major supplier of switches, hubs, and other network hardware is the Cisco Corporation. Cisco uses a proprietary tagging method called Inter-Switch Link (ISL) which takes a different approach to tagging the Ethernet frame. Instead of increasing the frame size by inserting fields, ISL encapsulates the Ethernet frame.

Cisco's Inter-Switch Link (ISL) allows what they call Per VLAN Spanning Tree (PVST) which in turn means that Virtual Local Area Networks (VLAN) multiples can exist across a trunk link. Multiple Spanning Trees allow load sharing to occur at layer 2 by assigning different port priorities per VLAN. The link 802.1q only allows Mono Spanning Tree (MST), i.e., one instance of Spanning Tree trunk.

ISL only runs on point-to-point links on Fast Ethernet (copper or fiber) and Token Ring (ISL+). Although ISL will operate over 10Mbps links it is not recommended! ISL runs between switches, from switches to routers and from switches to Intel and Xpoint Technologies NICs which understand ISL, thereby allowing servers to distinguish between VLANs.

13. Error Conditions

In assessing network topology, and especially when detecting the difference between an attack and a faulty system, it is important that the investigator understand the typical errors that might occur on a network. There are several, and rather than giving each one its own coverage we will simply address them together in this one section.

The first error worth mentioning is commonly known as a runt. A runt is a complete frame that is shorter than 64 bytes (512 bits). This is smaller than the normal frame allowed along a network, and may indicate some problem along the line. For instance, a runt can be caused by a collision, corrupted software, or a faulty port. A runt may also be caused by an unauthorized interruption in signal, which can come from several sources including intentional disruption.

The opposite of a runt is a long. This is a frame that is between 1518 and 6000 bytes long. The long is normally due to faulty hardware or software on the sending station, but may also be caused by other factors. Both the runt and long are often caught by the NOS.

From time to time a frame that is is greater than 1518 bytes can still be processed.

This is defined as a dribble. In many instances a dribble is the result of two frames joined together.

Software problems are not the only things that cause errors over a network. When a device on the network has electrical problems network administrators call this a Jabber. Ethernet relies on electrical signaling to determine whether or not to send data, so a faulty card could stop all traffic on a network as it sends false signals causing other devices to think that the network is busy. This shows itself as a long frame with an incorrect separator, FCS, or an alignment error.

The Frame Check Sequence (FCS) Error defines a frame which may or may not have the right number of bits but still may have been corrupted between the sender and receiver. In many instances the corruption occurred because of a Jabber or from other interference on the cable.

Frames are made up of a whole number of octets. If a frame arrives with part of an octet missing, and it has a Frame Check Sequence (FCS) error, then it is deemed to be an Alignment Error. This points to a hardware problem or possibly an Electro-Magnetic interference on the cable run between sender and receiver.

An incorrect packet broadcast onto a network that causes multiple stations to respond all at once is often called a Broadcast Storm. When such an event occurs the incorrect packet broadcast may even cause other incorrect packets to be sent which in turn causes the storm to grow exponentially in severity. When this happens there are too many broadcast frames for any data to be able to be processed. Broadcast frames have to be processed first by a NIC above any other frames. The NIC filters out unicast packets not destined for the host but multicasts and broadcasts are sent to the processor. If the broadcasts number 126 per second or above then this is deemed to be a broadcast storm.

An acceptable level of broadcasts is often deemed to be less than 20 percent of received packets although many networks survive at levels higher than this. Some broadcast/multicast applications such as video conferencing and stock market data feeds can issue more than 1000 broadcasts each second.

We have already discussed collisions in our earlier sections. Collisions are a normal occurrence on an Ethernet network. The more devices there are within a segment (Collision Domain) the more collisions are likely. One of the more common causes are badly cabled infrastructure (poor wiring or connection) which causes unnecessary collisions simply because a device is unable to hear other devices transmitting.

If a collision rate is greater than 50 percent of total broadcast then it is considered a problem. If the cause of the collisions is simply congestion, or too many devices on the network, the network administrator may choose to install more hubs, switches, or routers. This reduces the chance of a collision occurring on each of the segments thereby releasing more bandwidth for real traffic.

A Late Collision occurs when two devices transmit at the same time without detecting a collision. This could be because the cabling is badly installed (e.g., too long) or there are too many repeaters. If the time to send the signal from one end of the network to the other is longer than it takes to put the whole frame on to the network then neither device will see that the other device is transmitting until it is too late.

The transmitting station distinguishes between a normal and a late collision by virtue that a late collision is detected after the time it takes to transmit 64 bytes. This means that a late collision can only be detected with frames of greater size than 64 bytes, they still occur for smaller frames but remain undetected and still take up bandwidth. Frames lost through late collisions are not retransmitted.

Excessive Collisions describe the situation where a station has tried 16 times to transmit without success and discards the frame. This means that there is excessive traffic on the network and this must be reduced. For normal Ethernet traffic levels, a good guideline is if the number of deferred transmissions and retransmissions together make up for less than 5 percent of network traffic, then that is considered healthy. A transmitting station should see no more than two collisions before transmitting a frame.

On detection of a collision, the NIC sends out a Jam signal to let the other stations know that a collision has occurred. A repeater, on seeing a collision on a particular port, will send a jam on all other ports causing collisions and making all the stations wait before transmitting. A station must see the jam signal before it finishes transmitting the frame otherwise it will assume that another station is the cause of the collision.

C. TOKEN RING

An alternative to the Ethernet network system is one known as Token Ring. In this system a token travels through the network, which must be set up in a closed ring, and stops at each workstation to ask whether it has anything to send, and if the workstation has nothing to send then the token moves to the next station. If there is data to send, the sending station converts the *token frame* into a *data frame* and places it into the ring. The frame continues around the ring moving from one station to the next. At each station the data set is repeated until it reaches the destination station which then copies the frame into memory.

The data then continues further around the ring until it arrives once again at the sending station. The sending station then strips the data frame from the ring and releases a new token to start the process all over again. As a general rule a Token Ring network operates at either 4 or 16 Mbps. Even the fastest token ring is not much faster than the slowest Ethernet, but it is often much cheaper to build and operate. Token Ring networks are often the first network to be built by a user since they can be easily migrated to a faster Ethernet system.

D. HIGH-SPEED LAN TECHNOLOGIES

One can quickly see that the Token Ring and Ethernet technologies are very limited. Small networks, or those connected to larger networks, might work fine on a Ethernet system, but for super networks there is a need for something much faster. One of the top choices for many network designers is the Fiber Distributed Data

Interface (FDDI). The FDDI is another token-passing technology, but it operates at speeds up to 100 Mbps.

The FDDI network system requires a different wiring (fiber) and different hubs/switches than those used in the Ethernet systems. Speed was the main reason many network designers installed a FDDI system, but the system is rapidly losing ground to the equally speedy Fast Ethernet standard. Another technology has also emerged to challenge FDDI systems. It is known as Asynchronous Transfer Mode (ATM) and it operates at a range of speeds up to 622 Mbps.

The ATM system is a popular choice for large companies and those who serve as the backbone of extremely demanding networks. One of the special features that ATM allows is the use of real time voice and video traffic over network lines. This is a perfect setup for large companies who need to send video mail or video training material over their intranet. ATM can also be used for wide-area networks connecting geographically separated sites.

If ATM is not fast enough then one can go with the super speed of a Gigabit Ethernet. These systems operate at speeds up to 1000 Mbps. Of course, the real disadvantage for the average user is simply price. A well-designed and installed Gigabit Ethernet system serving forty or so users can cost over one million dollars ($1,000,000.00).

E. WIRELESS CONNECTIONS

Earlier we discussed the idea of running a wireless network. In recent years the Institute of Electrical and Electronics Engineers (IEEE), an international group that creates standards for electrical goods, has ratified standards for both Ethernet and Fast Ethernet systems. The IEEE has also created a set of new standards for high-speed wireless networking.[1]

The new standards specify the use of Direct Sequence Spread Spectrum (DSSS) technology. What this does for the industry is give a clear vision of what will be allowed and what is expected. At the heart of this standard is the requirement that the DSSS system offer throughput of up to 11 Mbps. Of course, compared to the Gigabit Ethernet system this may not sound very fast. The thing to keep in mind is that while the Gigabit system runs considerably faster it is also much more expensive than other systems.

A relatively simple LAN using the new IEEE standard, and running wireless, means a cut in cost at several steps. First, there is no wire to run, which means that there is no expense for wire or for the installation. Second, the technology for building the wireless network cards already exists so there is little cost for initial research or development. Third, and probably most important, the use of wireless network means that smaller network groups can be created freeing bandwidth for only those requests that need to go outside the group. This is a good solution for the LAN manager, and in some instances may even be a step up for managers of larger WANs.

F. REMOTE ACCESS AND WIDE-AREA NETWORKS

When evaluating a network system and its topology the investigator must remember that a LAN serves a smaller group of usually local users. These are networks generally set up for users in the same building or within the same general geographic region. A LAN is a good choice for a small campus-type environment, but does not work as well for users spread across a large area. The Wide Area Network (WAN) connects users spread between various sites. A WAN may be a single entity or a grouping of smaller LANs. The users do not even have to be in the same city, same state, or even same country. Many WANS also include dial-up connections.

In general, LAN speeds are much greater than WAN. For example, a single shared Ethernet connection runs at 10 Mbps, but even the fastest of today's analog modems runs at only 56 kbps. That is less than one percent (1%) of the speed of an Ethernet link. Even the more expensive, dedicated WAN services such as T1 lines don't compare (with bandwidth of 1.5 Mbps, a T1 has only 15% of the capacity of a single Ethernet link). For this reason, proper network design aims to keep most traffic local, contained within one site, rather than allowing that traffic to move across the WAN.

G. ANALOG VS. DIGITAL

The difference between analog and digital signals is very important for data communications. The most familiar analog communication is a phone call. Varying electrical voltage reflects the variations in the volume and tone of the human voice. By contrast, digital communications uses a series of 1s and 0s to carry information from point to point. Modems actually convert the digital data of one computer into an analog signal for transmission over the phone lines. On the receiving end, another modem converts the analog signal back into a series of 1s and 0s, so that the receiving computer can interpret the transmission.

Today, phone companies can offer fully digital service between LANs (leased lines such as 56K, 384K, and T1s are digital services), or ISDN (which allows dial-up connections on an as-needed basis). When it comes to moving data, digital communications are less susceptible to errors and faster than analog signals because they are not vulnerable to problems such as electrical noise on transmission lines.

H. ISDN

ISDN operates at 128 kbps and is available from your phone company. Charges for ISDN connections usually resemble those for analog lines–you pay per call or per minute, usually depending on distance. ISDN charges also can be a flat rate, if they are linked to a local Centrex system.

Technically, ISDN comprises two 64 kbps channels that work separately. Load balancing or "bonding" of the two channels into a 128 kbps single channel is possi-

ble when you have compatible hardware on each end of a connection (for example, between two of your sites). What's more, as a digital service, ISDN is not subject to the "line noise" that slows most analog connections, and thus it offers actual throughput much closer to its promised maximum rate.

You can make ISDN connections with either an ISDN-ready router or an ISDN terminal adapter (also called an ISDN modem) connected to the serial port of your router. Again, modems are best for single users, because each device needs its own modem, and only one "conversation" with the outside world can happen at any one time. Your ISDN router, modem, or terminal adapter may come with analog ports, allowing you to connect a regular telephone, fax, modem, or other analog phone device. For example, an ISDN router with an analog phone jack would allow you to make phone calls and send faxes while staying connected via the other ISDN digital channel.

I. LEASED LINES

Phone companies offer a variety of leased-line services, which are digital, permanent, point-to-point communication paths that are "open" 24 hours a day, seven days a week. Rather than paying a fee for each connection, you pay a set amount per month for unlimited use. Most appropriate leased lines for small- and medium-sized businesses range in speed from 56 kbps to 45 Mbps (a T3 service). Because they all work the same way, choosing the right line for you depends on the number of users and the amount of remote traffic the network will carry (and how much bandwidth you can afford). A common service for businesses with substantial WAN usage is a T1 line with 1.5 Mbps of bandwidth.

By "point-to-point," we mean that leased lines use a direct, physical connection from your business or branch office to the phone company's switch, and then to your other offices. Often, the phone or data services company may need to install new cabling.

J. CABLE MODEM/ROUTER

Cable modems offer extremely fast and relatively inexpensive access to the Internet. A cable modem connects directly to the same line that provides cable TV service to a home or business, and then to an Ethernet NIC in a PC.

Whereas a traditional dialup modem provides access at speeds up to 56 kilobits per second (kbps), a cable modem can deliver transmission rates of up to 10 megabits per second (Mbps)–nearly 200 times as fast. And unlike dialup modems, cable modems have a connection to the Internet that is "always on." In other words, you won't face busy signals or delays while your computer connects to the Internet.

Likewise, because you are sharing the connection with multiple users on your cable system, your performance will depend on how many users are on line at once. Another caution: in today's cable modem systems, users on a single segment of cable

are essentially connected to a single local-area network (LAN). To prevent neighbors from accessing files on a computer, the file sharing options of that computer should be turned off.

K. REMOTE ACCESS SERVERS

Remote access servers are like funnels for incoming calls from remote users. A remote access server allows multiple people to immediately connect to the network from homes, remote work sites, or anywhere they can find an analog or a digital phone line. They make good sense when you want to provide many individuals or small sites temporary access to your central network via modems, rather than the permanent link of a leased line.

They also prevent the busy signals that remote users might encounter if they were all dialing up a single modem. A remote access server can have multiple phone lines "pooled" to a single listed phone number, allowing a user to rotate through the phone lines transparently until finding an open line. As usage increases or decreases, support staff can order more lines to match the demand without affecting the phone number that users are familiar with calling.

L. DIGITAL SUBSCRIBER LINE SERVICE

Digital subscriber line (DSL) technology is a high-speed service that operates over ordinary twisted-pair copper wires supplying phone service to businesses and homes in most areas. DSL is often less expensive than ISDN in markets where it is offered today.

Using dedicated equipment in the phone company's switching office, DSL offers faster data transmission than either analog modems or ISDN service, plus–in most cases–simultaneous voice communications over the same lines. This means you don't need to add lines to supercharge your data access speeds. And because DSL devotes a separate channel to voice service, phone calls are unaffected by data transmissions.

There are several types of DSL including asynchronous DSL (ADSL), synchronous DSL (SDSL), high-bit-rate DSL (HDSL), ISDN DSL (IDSL), and very-high-bit-rate DSL (VDSL). ADSL delivers asymmetrical data rates (for example, data moves faster on the way to your network than it does on the way out to the Internet). Other DSL technologies deliver symmetrical data (same speeds going in and out of your network). The different types are dependent on "upstream" and "downstream" speeds. With ADSL, the most common DSL today, traffic moves upstream at 1 Mbps and downstream at 8 Mbps. SDSL is the next most popular DSL technology. With SDSL, traffic moves at the same speed in both directions. Speeds reach up to 1.54 Mbps.

Additionally, DSL comes in residential and business services. Residential DSL services include high-speed and affordable Internet access. Business DSL offers the

same high-speed, affordable access with enhanced business functionality which can include differentiated classes of service (CoSs) offered by service providers for guaranteed service levels, integrated toll-quality voice service, and business-class security. The type of service (ToS) available to you will depend on the carriers operating in your area. Because DSL works over the existing telephone infrastructure, it should be easy to deploy over a wide area in relatively little time. As a result, the pursuit of market share and new customers is spawning competition between traditional phone companies and a new breed of firms called competitive local exchange carriers (CLECs). If you choose DSL service for connecting your business to the Internet or for giving remote sites and users high-speed access to your central network, your carrier will help you install the appropriate hardware and software.

M. VIRTUAL PRIVATE NETWORKS

As businesses grow, they need to connect a rising number of remote offices and individuals to their central network to share information and resources electronically. Traditionally, this has been accomplished by building a private WAN, using leased lines to connect offices, and dial-access servers to support mobile users and telecommuters.

For a small or medium-sized business, a traditional private WAN can be costly to build and manage. The leased lines, telecommunications services, and equipment needed to interconnect offices can be expensive, and each added location requires a new leased line. Individuals or small branches dialing into a central site via the public telephone network incur long-distance charges, and managing dial-access servers at the central site can be resource intensive and complex.

Now, businesses have an alternative for connecting remote sites and users to the main company network–virtual private networks (VPNs). A VPN offers the security and full data access of a private WAN, but because it runs over the Internet, it is more affordable and flexible.

- More affordable–Remote users can connect with central network resources through a local link to an ISP at the price of a local call. This is a much more cost-effective method than making a long-distance call to the central site.
- More flexible–New sites can be added easily without need for extensive new equipment or an additional, dedicated private line. VPNs also simplify the task of creating an extranet, giving customers or suppliers password-protected access to a portion of a private network–for example, to order products, check status of shipments, or submit invoices.
- More reliable–VPNs take advantage of the equipment and full-time expertise of the vast public network infrastructure and the companies that oversee it.

Offering access to your internal network through the Internet might seem like a recipe for data disaster, but VPNs use tunneling and encryption to protect your private traffic. Tunneling creates a temporary, point-to-point connection between the

remote and central sites, blocking access to anyone outside. Encryption scrambles the data on the sending end and reassembles it on the receiving end so it cannot be read or changed while in transit.

N. GOOD NETWORK DESIGN: THE 80/20 RULE

The key to good network design is how you place clients in relation to servers. Ideally, client computers should be placed on the same "logical" network as the servers they access most often. (By contrast, a "physical" network connection would mean that a client and server were attached to the same hub. A logical connection can be defined in your network software so that users in one area of a building can be in the same logical network segment as a server located at the opposite end of that building.) This simple task minimizes the load on the network backbone, which carries traffic between segments.

A good general rule: In a properly designed small to medium-sized network environment, 80 percent of the traffic on a given network segment should be local (destined for a target in the same workgroup), and not more than 20 percent of the network traffic should need to move across a backbone (the spine that connects various segments or "subnetworks"). Backbone congestion can indicate that traffic patterns are not meeting the 80/20 rule. In this case, rather than adding switches or upgrading hubs, it may be easier to improve network performance by doing one of the following:

- Move resources (applications, software programs, and files from one server to another, for example) to contain traffic locally within a workgroup.
- Move users (logically, if not physically) so that the workgroups more closely reflect the actual traffic patterns.
- Add servers so that users can access them locally without having to cross the backbone.

After you have ensured proper network design and resource location, the next step is to determine the optimal technology to meet your growing needs.

O. UNDERSTANDING NETWORK PROTOCOLS

For our purposes we can limit networks to three major categories. The first is also the largest in the sense that there are more computers connected. It is the Internet. The Internet is a loose collection of large and small networks brought together for the purpose of data exchange. The magic of the Internet is that there is no "home office," it is not controlled by any one company or government agency, and it is virtually free to anyone who has the equipment needed to access it. The Internet exists simply because the users allow it. It is the most complicated of the networks we will work with, and is rapidly becoming the choice venue for most computer criminals.

The second category of networks is those that we dub "public networks." What makes this form of network "public" is the fact that almost anyone can gain admission to it by simply connecting through the right device. A perfect example of a public network would be the system used by many of today's corporate giants. These companies have moved their presence to the World Wide Web (a part of the Internet) and have allowed almost any user the ability to access the network by entering through the Internet. Other forms of public networks include "dial-up" connections and those that are accessed through private connections.

The third category of network is the "private network." This type of network is relatively well protected and closed to all but those authorized to be on it. Private networks include the Local Area Network and the Intranet. The private network allows users within the system to access resources on the network freely. For instance, a small law office establishes a Local Area Network where all of the attorneys, secretaries, and paralegals are connected through a central hub, by connecting in this way the users can share printers, send private e-mail between each other, and share other computing resources such as hard drives.

In all of these instances we will deal with several different computers which will serve different purposes. For instance, in our law office a single, powerful computer may serve as the "host" by storing the network software, main hard disk, and central mail service. This machine is often called a "network server" since its job is to serve the other computers connected to it. Depending on the network topography and the manner in which the computers are connected to each other, the server may house all of the data accessed by the users or merely serve as a central point to which all messages must pass.

Computers that are being served by the network server are called "nodes." These computers may be powerful enough to work as stand-alone systems or they may be "dumb terminals" with only enough power to connect to the server. In either case, the node generally connects to the server using a predefined set of rules called a protocol.

Network protocols define services that may or may not be available from one computer to another. For instance, the network server may house confidential information on the hard disk drive. Only those computers with the right password, as defined by the protocol, may access that information. Without knowing the protocol, or the rules of the system, the connecting computer simply will not be allowed to access the data in question.

One might also think of the network protocol as a common language spoken by computers. This allows computers from different manufacturers to communicate. They may even be computers using different operating systems such as the Windows and Mac OS. Normally, without some agreement on the language to be used, these two computers will not communicate with each other. It would be like a native of China and Brazil meeting together in France for the first time. Without a common language the two would not be able to communicate even though they are at the same spot. With a common language, though, they can not only communicate when right beside each other but also from around the world.

There are a number of different network protocols, and each will vary according

to the manufacturer of the network technology. For instance, the makers of Novel Netware use one set of protocols for communication between all computers using the Netware system. Users of the Microsoft Windows NT system communicate with a very different set of protocols. In this sense, each user of the Novel protocols may be able to communicate with other Novel users, but not necessarily with Microsoft users. Fortunately, there are a few protocols that perform across almost any platform, and many of the major network technology manufacturers include these protocols with their proprietary systems as well.

The most common protocols in use today are those found on the Internet. They are commonly called the TCP/IP pair. TCP stands for Transmission Control Protocol, and IP stands for Internet Protocol. These two work together to allow uncommon computers from around the world communicate through a common language. For the investigator it is imperative that he understand the basics of TCP/IP in order to investigate any crime involving a network. We begin by first examining the use of encapsulation to create multiple layers of software for use in the communication process. The idea of encapsulation is based on a need to protect the overall system from potential failure.

ENDNOTE

1. IEEE 802.11b.

Appendix D

COMPUTER SEIZURE CHECKLIST

In the criminal investigation of computer-related crime one of the first tasks is to properly secure the computer system in question. Whether the computer is a target of the criminal activity, an instrumentality of the crime, or merely contraband the investigator must insure that the computer is safely protected from external tampering or contamination. The checklist in this appendix will help investigators to make the right decisions about the seizure and securing of a computer system.

1. **Secure the area immediately around the computer**–This step includes the identification of potential hazards in and around the computer and the work area. In some instances criminal computer users will lay traps in the area or on the computer itself to try to injure the investigator or in the alternative destroy potential evidence. Before taking action to secure the computer or to recover evidence the investigator should make sure the area is clear of potential hazards to himself and the system.
2. **Identify all components and peripherals connected to or with the computer**–Computer systems are the true sum of the individual parts. A computer system may include the monitor or display device, keyboard, case (with internal components), printer, scanner, and other devices hooked to the computer.
3. **Photograph the computer and peripherals in question**–Before taking any steps to secure data the investigator should have the computer photographed just as it appeared at the time of the initial contact. Photographs should also be taken when the computer is being seized and removed. The photographs should depict the layout of the computer system (where the peripherals and other items were in relation to the computer case, monitor, etc.) and the steps taken in dismantling the system.
4. **Photograph the monitor screen to capture any display**–This may need to be completed in two steps. If the monitor is on and displaying potential incriminating evidence, or if it is simply on so that one can see any display–then an initial photograph will document the condition at the time of the initial seizure. If the monitor is on but a screen saver is being used then the first

photographs should show the condition of the monitor and system prior to the forensic efforts.

5. **Preserve volatile data**–See the material in the text pertaining to the seizure of computer and electronic data. At minimum, steps should be taken to secure any data which may be lost when the computer is turned off or in some way manipulated.
6. **Check the integrity of system**–This simply means that the investigator should insure that the computer is hooked into a proper outlet, has adequate grounding or electronic protection, and that it can be examined without loss of data or injury to persons involved.
7. **Make a forensic copy of the hard drive or disks**–A forensic (duplicate) copy of the disk or hard drive will help protect potential data or evidence. Even if the computer is not to be turned off or seized the copy will help investigators to control the data itself.
8. **Complete onsite forensic tasks before shutting the computer down**–The computer may not always be seized as part of the investigation, so investigators must make sure that they have completed all necessary forensic tasks while they have control of the system. Once they release the system then the investigation or later forensic work will be tainted by the loss of control.
9. **Check and Double-check the integrity of anything seized at the scene**–If the computer is to be shut down at the time of a seizure then it is likely most evidentiary data will be lost almost immediately. Even if the computer is not to be seized, the surrender of control over the computer will likely end with the loss of potential evidence. For that reason investigators must be absolutely sure that they have completed all tasks necessary to identify, protect, and ultimately seize evidence necessary to the case.
10. **Turn off the system and unplug it before disassembly**–This is very important even if the investigator is an experienced computer technician. Movement of the computer case and other components raises the risk of both static electricity and accidental electrical discharge from several of the computer components. The power supply in the typical PC case has enough stored electricity to cause severe damage to the computer and the investigator. By turning off the computer and then unplugging it from the power source the risks of unexpected damage is reduced tremendously.
11. **Use grounding and anti-static devices when opening, working on, or moving the computer**–Friction, low humidity, and many other factors can add up to costly damage to the computer system even from the slightest movement. Investigators should use proper clothing, bags, and other containers when working on or with the computer system. This is especially important when taking the computer system apart and when moving it. Anti-static bags or similar containers should be used to store important components such as disks, drives, motherboards, circuit boards, and other items which can be damaged by electrical current.
12. **Maintain a strong chain of evidence**–Computers are now so much a part of our daily lives that many investigators, police officers, and criminalists

often take them for granted. The computer seized in an investigation should be treated just as if it were a gun from a homicide scene. Protect the evidence and system by maintaining a strong chain of custody from the moment of seizure all the way up to the moment the evidence is turned over to the courts.

GLOSSARY

Address Resolution Protocol (ARP): A method for finding a host's Ethernet address from its Internet address. An ARP request is sent to the network, naming the IP address; then the machine with that IP address returns its physical address so it can receive the transmission.

Anonymous remailing: A private, usually commercial, internet based business which allows users to login anonymously and mail or resend (remail) electronic mail messages without disclosing their true identity.

Anti-static bracelet: Used to ground the computer investigator or other user so as to avoid transfer of static electricity to the computer chassis or components.

Backbone Network: In a hierarchical network, the backbone is the top level, employing high-speed data transmission and serving as a major access point; smaller networks connect to the backbone. See discussion under *Internet.*

Central Processing Unit (CPU): Sometimes referred to simply as the *processor* or *central processor,* the CPU is where most calculations take place. In terms of computing power, the CPU is the most important element of a computer system.

daughterboards: A secondary electronic board which plugs into a main or motherboard. Personal computers use a motherboard and then add peripheral control as well as additional components by adding a daughterboard.

Distance factor: The physical distance between the computer perpetrator and the victim as an integral part of the overall investigation.

Domain Name Service (DNS): A database system that translates an IP address into a domain name. For example, a numeric address like 232.452.120.54 can become something like xyz.com.

Dynamic Host Configuration Protocol (DHCP): Dynamic Host Configuration Protocol. Windows NT Server software that assigns an IP address to each node in a network.

Dynamic IP Address: An address assigned to the user each time the computer logs onto the network. Dynamic IP addresses change and are useful for those who move their computer or change locations of their connection.

Email clients: The application software used by the individual computer user to access email accounts for sending and receiving email.

Ethernet: The most popular type of local area network, which sends its communications through radio frequency signals carried by a coaxial cable. Each computer

checks to see if another computer is transmitting and waits its turn to transmit. If two computers accidentally transmit at the same time and their messages collide, they wait and send again in turn. Software protocols used by Ethernet systems vary, but include Novell Netware and TCP/IP.

Forensic: That which belongs to, is used in, or is suitable to the courts or to public discussion and debate.

Forensic Science: Relating to or dealing with the application of scientific knowledge (as of medicine, chemistry, biology, etc.) to legal problems.

Grounding strap: See antistatic bracelet.

Hypertext Transport Protocol (HTTP): The protocol most often used to transfer information from World Wide Web servers to browsers, which is why Web addresses begin with http://. Also called Hypertext Transport Protocol.

Incident response: A focused sub-genre of computer service and management which identifies and responds to potential hazards or incidents where the computer is an intended target.

Internet: The global network of computers linked through a backbone system which allows users to connect smaller networks or individual computers together. The major portions of the Internet include electronic mail (email) and the World Wide Web (WWW). The Internet was originally developed for the United States military, and then became used for government, academic and commercial research and communications. The Internet is made up of large backbone networks (such as MILNET, NSFNET, and CREN), and smaller networks that link to them. There are over six million hosts on the Internet: mainframes, minicomputers or workstations that support the Internet Protocol. The Internet is connected to computer networks worldwide that use various message formats and protocols; gateways convert these formats between networks so that the Internet functions as one big network. UNIX utilities such as FTP, Archie, Telnet, Gopher and Veronica have been widely used to access the Internet.

Internet Service Provider (ISP): A company that provides Internet access through a local network system. Individual users "logon" to the ISP network, which then allows them to connect to the Internet and other outside networks.

Intranet: A closed or limited system of networked computers usually found within a business or similar environment. An Intranet can be connected to the Internet; however, the distinguishing characteristic is the ability to close the network connections to only a limited number of computers within the system itself.

Local Area Network (LAN): A network that connects computers that are close to each other, usually in the same building, linked by a cable or wireless (radio frequency) connections. See also Wide Area Network.

MAC: See Media Access Control.

Media Access Control (MAC): The unique network interface identifier burned into each piece of hardware at the factory. Used by the network to locate a piece of hardware in the loop or system.

Microprocessor: A silicon chip that contains a CPU. In the world of personal computers, the terms *microprocessor, processor,* and *CPU* are used interchangeably. At the heart of all personal computers and most workstations sits a microprocessor.

Microprocessors also control the logic of almost all digital devices, from clock radios to fuel-injection systems for automobiles.

Network interface: Also known as the Network Interface Card (NIC) this piece of hardware allows the individual computer to connect to the network. Today network interface cards come in three varieties: Modem connector, Ethernet connector, and Wireless connector.

Open Systems Interconnection (OSI): A model developed by ISO (International Organization for Standardization) to allow computer systems made by different vendors to communicate with each other. The goal of OSI is to create a worldwide open systems networking environment where all systems can interconnect. Most communications protocols today are based on the OSI model.

Processor: *See Microprocessor.*

Recursive Searching: In mathematics and computer science, recursion is a particular way of specifying (or constructing) a class of objects (or an object from a certain class) with the help of a reference to other objects of the class: a recursive definition defines objects in terms of the already defined objects of the class.

Static IP Address: A static or dedicated IP Address is a type of account from an ISP where your computer(s) are assigned the same IP Address at all times. While this used to be a requirement for web-site serving, it is usually used today for security purposes.

Subdomain: In the DNS hierarchy, a subdomain is a domain that is part of a larger domain name. A DNS hierarchy consists of the root-level domain at the top, underneath which are the top-level domains, followed by second-level domains and finally subdomains.

Top-level-domain: The part of a web address that identifies the domain within which the address fits.

Web Browser: A program such as Mosaic, Netscape, Internet Explorer, and others that are used to view pages on the World Wide Web.

Wide Area Network (WAN): A network that connects computers that are widely divided or spread across a wide area such as on a campus or large corporate park.

INDEX