Computer Forensics:

The Key to Solving the Crime

Lisa Oseles

INSS 690

Term 1

7 October 2001

loseles@hotmail.com

Table of Contents

A. Abstract

The continuing technological revolution in communications and information exchange has created an entirely new form of crime, cyber crime. Cyber crime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence. This has developed into a science called computer forensics. The process of acquiring, examining, and applying digital evidence is crucial in the success of prosecuting a cyber criminal. With the continuous evolution of technology, it is difficult for law enforcement and computer professionals to stay one step ahead of the technologically savvy criminals. To effectively combat cyber crime, greater emphasis must be placed in the computer forensic field of study, including but not limited to financial support,

international guidelines and laws, and training of the professionals involved in the process.

B. Introduction

Computer technology has advanced by leaps and bounds in recent years. Businesses are increasingly utilizing these technological advancements to improve their business operations and market potential. We, as consumers, can pay our bills online; order anything from books to groceries to automobile tires online; we can even try on clothing. Internally, businesses use such technological tools as wireless LANs, WANs, and palm pilots to share data and information, netmeetings and VTCs to coordinate project efforts, and data warehouses to store their continuously growing data bank. With this vast amount of important and sensitive data flowing around in cyber space, it is readily available to fall into unintended or malicious hands. Unfortunately, it does so every day. When someone “steals” data from cyber space or uses information for unintended purposes, it is called cyber crime. With the increase usage of computer technology, cyber crime is on the rise, which makes the topic of this paper, computer forensics, even more important.

In the “old days” the key to solving crimes was obtained from fingerprints, toxicology reports, trace analysis, paper documents, and other traditional means. While these still provide very important forensic pieces of the puzzle in many crimes committed today, technology has added another dimension with digital evidence. Often more information can be gained from the analysis of a computer than that of a fingerprint. The entire story of a crime may be told with the recovery of a file thought to have been deleted. Just as with other forensic sciences, law enforcement and legal professionals are quickly recognizing that computer forensics can provide critically important evidence and may hold the key to solving the crime. As greater emphasis is placed on digital evidence, it will become increasingly critical that the evidence be handled and examined properly.

C. What is Computer Forensics?

Judd Robbins, a prominent computer forensics investigator, defines computer forensics as “the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.” Other experts have taken the definition a step further, believing computer forensics has evolved into a science. Noblett et al., as well as the FBI, define computer forensic science as “the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media.” Basically, computer forensics is digital detective work. It is searching a digital crime scene for evidence, containing and preserving the evidence, analyzing the evidence, often times in a certified lab environment, and then finally presenting the findings in legal proceedings and court. In other words, it is similar to performing an autopsy, except on a digital device versus a human body.

What is electronic data? Electronic data can include “any record, file, source code, program, computer manufacturer specifications, and other information imprinted on a computer storage device.” (The Center for Computer Forensics 2000) In today’s business world, electronic evidence can take many forms. It can be classified financial documents, sensitive personnel records, privileged medical patient data, customer lists including addresses and phone numbers, e-mail, or even the bosses itinerary for his next business trip. Any and all of this data is subject to exposure to people who could potentially use it in unintended ways.

When the electronic evidence is contained in a single location, such as a computer or floppy disk, the forensic process is simple. However, the Internet has enabled the flow of data from country to country and in essence created a cybernetic world without borders. Because of this, cyber crime has also become borderless. Often times a criminal can target a computer thousands of miles away through the use of numerous computers or other devices along the way. This greatly complicates the forensics process. This is where the real detective work begins and knowledge of the interworkings of computers and peripherals is extremely important. Tracking down clues can be a challenge, especially when, at any time, evidence, whether a time/date stamp on a file or an editable document, can be altered and no longer a valid piece of the puzzle. The real challenge is when confronted with a crime involving a global network, tracing audit logs across numerous time zones and correlating the evidence. The resulting evidence piecing the puzzle together must be able to withstand extensive cross-examination in a court of law.

D. Background

Computer forensics has been around in one form or another since the invention of the computer. Evidence from computers has been used in courts for almost 30 years. Initially, judges accepted the evidence just as any other evidence. However, as technology advanced, traditional rules and reasoning became more difficult to apply to digital evidence. The law enforcement community realized that some changes needed to be made. The US Federal Rules of Evidence of 1976 addressed some of the “technological” differences. Many other laws have since been implemented to better handle this “unconventional” evidence, to include the Electronic Communications Privacy Act of 1986, the Computer Security Act of 1987, and the Economic Espionage Act of 1996.

As early as 1984, the FBI, as well as other law enforcement agencies began developing programs to assist in the examination and analysis of computer evidence. Many federal and state agencies, as well as agencies in other countries, now have specialized departments whose primary function is to develop methods of gathering and analyzing evidence from a “digital crime scene.” This is an ever-changing field since the digital crime scene is constantly changing with new developments in technology. One such agency within the U.S. is the National Infrastructure Protection Center (NIPC). The mission of the NIPC encompasses such responsibilities as detecting, assessing, responding, and investigating illegal acts involving computer or information technologies. This is typical of such agencies and the impact on citizen’s lives goes unnoticed to most.

The use of computer forensic evidence is widespread. Judd Robbins presents a handful of such uses:

- **Criminal prosecutors** make use of computer evidence where incriminating documents are found. Such crimes may include homicides, financial fraud, drug dealing, embezzlement, tax evasion, or distribution of child pornography.
- **Civil litigations** can make use of pertinent personal and business records found on the home or office computer to support cases of fraud, divorce, discrimination, and harassment cases.

- **Insurance companies** may be able to mitigate claims due to files or other evidence found on computers in connection to arson, accident fraud, or fraudulent workman's compensation claims.
- **Corporations** hire computer forensic experts to review such items as system logs, file access records, or even email traffic within the corporation to determine whether there has been a theft or misappropriation of trade secrets or corporate confidential information, embezzlement, possible sexual harassment issues within the workplace, and even personal misuse of company or government systems.
- **Law enforcement officials** often require assistance to properly conduct the search and seizure of computer equipment. If the evidence is mishandled, it is not permissible in a court of law; therefore it is important to seek the assistance of qualified professionals.
- **Citizens** may need the services of a computer forensic specialist if they find themselves wrongfully terminated from employment, sexually harassed, or discriminated against in their job.

E. Trends and Types of Cyber Crime

According to Computer Economics, there are currently 213 million people online worldwide. That figure is expected to rise to 350 million by the year 2005. This is a lot of data interchange; unfortunately many small businesses, and even large organizations, do not know how to properly protect their sensitive data thus leaving the door open to criminals.

Computers can be involved in a wide variety of crimes to include white-collar crimes, violent crimes such as murder and terrorism, counterintelligence, economic espionage, counterfeiting, and drug dealing. A 1999 Computer Security Institute (CSI)/FBI survey reported that the average bank robbery netted $2,500 where the average computer crime netted $500,000. (Armstrong 2001) The Internet has made targets much more accessible and the risks involved for the criminal are much lower than with traditional crimes. A person can sit in the comfort of their home or a remote site and hack into the Chase Manhattan Bank, transfer millions of dollars to a fictitious account, in essence robbing the bank, without the threat of being gunned down while escaping. We hear of such technological crimes almost daily, thus creating a perception of lawlessness in the cyber world. The same CSI/FBI survey revealed that both public and private agencies face serious threats from external, as well as, internal sources. Out of the 405 organizations that responded to the survey, 26% claimed theft of proprietary information, 19% reported sabotage of data or their networks, 31% experienced system penetration from an outside source, and 14% claimed financial fraud. More alarming is the ease of access to sensitive data employees have within the organization. Fifty-five percent of the organizations involved in the survey reported employees having unauthorized access to corporate information. (Computer Forensics 2001)

Recently a survey was conducted to determine where the FBI was focusing their computer forensic efforts. An alarming 70% of their workload is centered on white-collar crime. This type of crime includes health care fraud, government fraud to include erroneous IRS and Social Security benefit payments, and financial institution fraud. These are high dollar crimes made easy by technology. The other 30% of the workload is split equally among violent crime (child pornography, interstate theft), organized crime (drug dealing, criminal enterprise) and counterterrorism and national security. (Information Assurance Technology

Analysis Center 2000) As shown by this survey, computer crime is widespread and has infiltrated areas unimaginable just a few short years ago. The FBI caseload has gone from near zero in 1985 to nearly 3000 cases in 1997. It is no doubt considerably higher today. They have gone from 2 part-time scientists to 120 personnel in regional field offices throughout the country. Technology has brought this field of study to the forefront.

F. <u>Roles of a Computer in a Crime</u>

A computer can play one of three roles in a computer crime. A computer can be the target of the crime, it can be the instrument of the crime, or it can serve as an evidence repository storing valuable information about the crime. In some cases the computer can have multiple roles. It can be the "smoking gun" serving as the instrument of the crime; it can also serve as a "file cabinet" storing critical evidence. For example, a hacker may use the computer as the tool to break into another computer and "steal" files, then store them on the computer. It is important to know when investigating a case what roles the computer played in the crime and then tailor the investigative process to that particular role.

Applying information about how the computer was used in the crime also helps when searching the system for evidence. If the computer was used to hack into a network password file, the investigator will know to look for password cracking software and also password files. If the computer was the target of the crime, such as an intrusion, audit logs and unfamiliar programs should be checked. Knowing how the computer was used will help narrow down the evidence collection process. With the size of hard drives these days, it can take a very long time to check and analyze every piece of data it contains. Often law enforcement officials need the information quickly and having a general idea of what to look for will speed the evidence collection process.

G. Acquisition of Evidence

Legal Issues

There are many rules and regulations investigators must abide by if the evidence is to be permissible in court. One of the most important items in the acquisition of evidence is the search warrant. The warrant should include wording that will allow investigators to seize a computer and any related computer evidence thought to be involved in the crime. The role of the computer will determine whether all or only part of the computer system should be seized. For example, a counterfeiter may have used his computer, scanner, and printer to scan and produce counterfeit currency. In this case all three items should be confiscated to provide hard evidence for the prosecution of the case.

There are many aspects of computer evidence that the courts treat carefully. Email, for example, is sensitive and often times considered personal. Strong justification must be provided before email is allowed to be reviewed. If evidence is believed to be contained in emails, the search warrant should specify this. The warrant must also include details such as whether network and file servers can be searched, if backup media can be confiscated, and if the search should be conducted on site or after the removal of the hardware, software, and peripherals to another location, such as a certified laboratory.

Often computers are used for multiple purposes, especially home computers. Data unrelated to the crime should be left untouched. Also, doctors, lawyers, and clergy use computers to process and store documents related to their profession. Much of this information is confidential and privileged. A doctor, for example, may be part of a HMO scam, falsifying documents. These documents are critical to the case but may also contain privileged information about patients. While critical evidence must be obtained, care must be exercised to protect innocent third parties and their personal information.

Practical Issues

How much personal property are authorities authorized to seize? Authorities must only take items related to the case. The type of crime and knowing the role of the computer will provide insight as to what should be taken. If the computer was used to store evidence, all storage media should be seized for review as possible evidence. If the computer was used to run programs to collect and analyze data, books located in the area may help the experts understand how the programs work and what actually happens within the computer.

If the computer and its peripherals are taken from the crime scene, care must be exercised in disassembling the equipment. If the computer is on at the time of seizure, rather than shut it down normally, the power plug should be pulled from the back of the computer. This will prevent any malicious programs from being activated if the computer power system was “booby trapped”. Pictures or a videotape of the computer set up should be taken before it is disassembled. Notes should be taken and every cord labeled as to where it was attached. There are many ways to set up a computer and its peripherals but it will need to be set up in the lab exactly as it was at the crime scene. This will affect the analysis of the evidence.

If the suspect is present, authorities must not let the individual touch the computer. If the person insists on powering down the computer, ask the person to write down the steps or draw a diagram. However, do not follow the instructions; just pull the plug. During analysis the instructions can be tested and if they activate any destructive programs, additional charges can be brought against the suspect for attempted evidence tampering.

Computer forensic experts must only collect evidence relevant to the case at hand. Their job is to collect the evidence, analyze it, and present the facts. Investigators must remember that technical ability does not mean legal authority. Just because it is technically possible to access email on a confiscated system doesn’t mean they have the authority to do so.

H. Examination of Evidence

Once the computer system has been seized, it is time to examine the evidence. This requires experts in the computer forensic field. When searching a computer for evidence of a crime the investigator must examine it as a detective, not as computer user. There may be many elements of the computer structure that will give clues of a crime, however, if the detective searches for only one item, it will be like looking for a needle in a haystack. It is important not to target one piece of information but rather let the digital data, as a whole, tell the story.

Examination and Analysis

There are several guidelines to adhere to when examining computer evidence. First, computers should not be simply turned on. This will change some of the data on the machine. Every time a computer is powered on the access times of certain files is altered; this may be crucial information to the investigation. So, one of the first things that must be done is to lock the original media. There are several methods that can be used to do this. One is to write-protect it, similar to write-protecting a videotape. Another method is to disconnect the hard drive and boot from a floppy disk, then reconnect the hard drive to perform the investigation. A third method is to put the hard drive into a trusted machine and set it as a slave drive. The preferred practice will depend on experience, available tools, and company policy.

The next step is to make an exact copy of the disk. There is software available that will make a mirror image of a hard drive, bit-by-bit. It is very important that it is an identical copy. The method used must be recorded in detail to later prove the original image was not altered and the copies are true copies. Methods that use the cyclical redundancy check (CRC) method are the best, verifying the integrity of a block of data as it copies it by producing a unique mathematical representation of the data. All analysis must be done on the copy rather than the original data. Also the defense and prosecution teams should be supplied with a copy of the data to allow their own experts to perform an analysis.

The actual examination of the disk is next. Using a copy of the disk, free space is examined as well as file slack. Free space is the available storage space on the disk. This includes space where files may have resided at one time but have since been deleted. These areas can provide key evidence to the case at hand. File slack is the space available from the end of the file to the end of the cluster. For example, if a cluster is 512 bytes and a file only uses 312 bytes, the free or unallocated space is 200 bytes. Valuable evidence may also be concealed here as well. Swap files must also be examined. Swap files are files used to cache information between memory and the hard drive. These files may contain valuable information.

A key word list must also be developed to search media for data pertaining to the case. Using background information about the case, deductive reasoning and common sense, a thorough list of key words can be developed. This word list can then be fed into an automated forensics text search tool to more efficiently locate relevant evidence. The data produced is analyzed and documented; documentation is very important and will be addressed in more detail later.

There are a variety of approaches to the actual examination of the evidence. The methods employed will depend on the type of allegations under investigation and the type of operating system on the computer. With the size of hard drives approaching 30Gb, it would be impossible for a human to examine all the data that may be stored on a computer system. Special software has been developed to assist in the examination of evidence. There are many small computer forensic consulting firms around today and many have developed their own software. This independent development of software is largely due to restrictions on major evidence gathering programs by government agencies and the law enforcement community.

Tools of the Trade

As in any criminal case, all evidence is subject to scrutiny in the courtroom. It is imperative that digital evidence withstands such scrutiny. To ensure the evidence produced is legitimate, many software tools have been developed to assist the computer forensic examiner. Below are just a few of the tools on the market today and their main function:

- AcoDisk – a CD recovery tool
- Coroners Tool Kit – a kit of UNIX and LINUX data collection and analysis tools
- CRCCMD5 – software used to compare copies of files to ensure they are identical; it compares the contents of the files and produces a hash. If the hash is the same, the copies are identical.
- DtSearch – a keyword indexer and search tool
- Encase – forensic software application that manages and enables viewing of all evidence
- GetFree – a tool that collects all available disk space, saves it to a separate location, and then analyzes the space with another tool
- GetSlack – similar to GetFree, except it collects all the file slack on a particular drive, saves it to a location and makes it available for analysis with another tool
- IMAGE MASTER – produces an image of a disk
- Net Threat Analyzer – a tool that identifies past Internet activity; examines Windows swap files and reveals evidence of browsing activity.

Even though there are many tools available to gather and analyze computer forensic evidence, it still requires an expert. There are many things that can go wrong along the way that can destroy the evidence as well as the case. An experienced professional will avoid mishaps and produce evidence creditable in court. Once the evidence has been examined and analyzed it must be determined whether or not the results answer the investigative questions. The computer forensic expert is only the examiner, not the investigator. He should present the facts, not make any conclusions.

I. <u>Utilization of Evidence</u>

Documentation

Not altering the evidence is the most important element in the computer forensic process; documentation is the second most. The who, what, where, when, and how of the computer forensic process must be documented during every step of the investigation. The more detailed the process and it's accompanying documentation, the better. Often times, computer related crime cases will not go to court for 3-5 years and memories are likely to fade during this time. Professionals recommend using an evidence collection notebook, ideally a non-spiral notebook, so if a page is removed it will be noticed. The responsibility for recording in and maintaining the evidence collection book, to include control and accountability, should be the sole responsibility of one individual.

Witter (2001) recommends recording the following minimum administrative items in the evidence collection notebook:

- Who initially reported the suspected incident along with time, date and circumstances surrounding the suspected incident.
- Details of the initial assessment leading to the formal investigation.
- Names of all persons conducting the investigation.
- The case number of the incident.
- Reasons for the investigation.

The following computer forensic details must be annotated as well (Witter 2001):

- A list of all computer systems included in the investigation as well as their system specifications. Each item's identification tag should also be noted.
- Network diagrams, either hand-drawn or obtained from the organization housing the network.
- A list of all applications running on the systems under investigation.
- A copy of the organizations standard policy concerning who is allowed access and use of the system.
- Name(s) of system administrator(s) responsible for maintenance of the system.
- A detailed list of steps used in collecting and analyzing the evidence. Specifically the list needs to identify the date and time of each task performed on the evidence, who performed it, exactly what was done, where the task was performed, either in the lab or at the crime scene, and the results of the analysis.
- An access control list containing dates and times of whom had access to the collected evidence.

The last item is very important. It tracks, for example, the evidence from its original source, the home or office, to the courtroom. This tracking, or chain of custody, is critical when dealing with electronic evidence because the evidence can very easily be altered or even destroyed. Proving the chain of custody was never broken authenticates the electronic evidence.

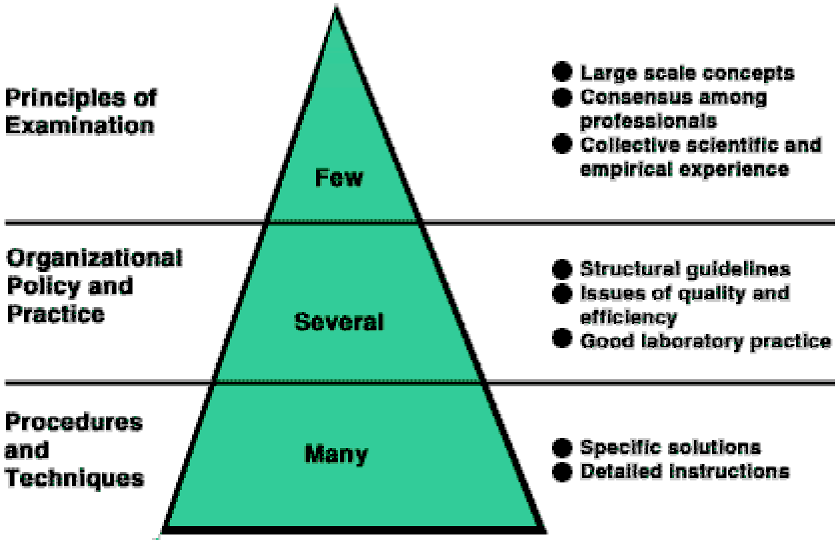
Testimony

Once all the evidence has been gathered and analyzed it needs to be presented to those deciding the case. Lawyers often defer to the experts to help build their case and to educate those involved. Many private companies offer litigation services. It is important that experts be able to explain the electronic evidence in terms easily understood by everyone from the jury, to the lawyers, and even to the judge. An experienced computer forensic expert can seal the case.

J. Weaknesses in the Process

In the course of my research, I have identified three main weaknesses within the computer forensic process. I will address training first. Computer evidence must be handled very carefully because it is extremely volatile. Personnel first on the crime scene must be trained on how to protect such unstable evidence. Because computers are everywhere, law enforcement officials from big cities on down to the smallest of towns should receive basic computer evidence protection training. Network operators should be trained on how to detect an intrusion and analyze their network logs. Lawyers should receive training on the basics of computer operation. This will provide a general understanding of the generation of computer evidence and better enable them to prosecute or defend the case. Many private organizations offer computer forensic seminars and classes. With the rise in computer crime, it is undoubtedly a worthwhile investment for any organization.

The next weakness I will discuss is the lack of systematic technical procedures and standards. No two computer crimes are the same because computer systems and devices differ so much. Since computer crime can easily be an international crime, basic guidelines must be established worldwide to help ensure the evidence collection process starts off on the right foot. Noblett, et al recommends a three-level hierarchical model as shown below:



Principles of Examination
Few
● Large scale concepts
● Consensus among professionals
● Collective scientific and empirical experience
Organizational Policy and Practice
Several
● Structural guidelines
● Issues of quality and efficiency
● Good laboratory practice
Procedures and Techniques
Many
● Specific solutions
● Detailed instructions

This model implies that there are few basic principles of examination. They include large-scale concepts that apply to nearly every examination. There is also a need for several organizational policies and practices that provide structural guidance. Such guidance ensures forensic examinations are planned, performed, monitored, recorded, and reported in orderly fashion guaranteeing the quality and thoroughness of the examination. Lastly Noblett, et al recommends numerous procedures and techniques specific to the situation. This includes software and hardware solutions most appropriate to the forensic problem, whether it is a UNIX system, a network intrusion problem, or simply a stand-alone home computer.

The third weakness that I identified in my research is differences among countries in their computer forensic methods and laws. Each country has it’s own policies and methods. However, what is accepted in one country is not always accepted in another. This presents a problem when confronted with international crimes, which have become more frequent as a result of the World Wide Web. Even though the World Wide Web has no boundaries, law enforcement does. When crossing international boundaries, investigators are confronted with cultural and political differences, as well as evidence handling differences. This complicates investigations that leap from server-to-server and country-to-country. In some countries the networks are owned and governed by government agencies. There may be little, if no cooperation between governments to investigate a crime; for example what we consider hacking in the US is not even considered a crime in some countries. Hackers realize this and continue to hack because they are protected by their legal system.

Efforts are being made to standardize procedures relating to digital evidence. The G8 group, consisting of Canada, France, Germany, Great Britain, Italy, Japan, Russia, and United States, has proposed six principles for procedures relating to digital evidence. These six principles are (Gottfried 2001):

- All standard forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not alter the evidence.
- People accessing the original digital evidence should be trained to do so.
- All activities relating to the seizure, access, storage, or transfer of digital evidence must be completely documented.
- Individuals are responsible for all actions taken while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for complying with these principles.

While this is a start in standardizing digital evidence procedures, there is still a long ways to go. There are many countries yet to adopt any such procedures, and many that probably will not. To do so would be an economic strain and many countries simply do not have the resources to train people in computer forensics. Yet these are likely the countries that pose the greatest criminal threat.

K. Conclusion

With the ongoing advancements in communications networking and information exchange, computer-related crimes have risen. Hi-tech offenses such as computer hacking, spreading of viruses, Internet fraud, and e-mail abuse will continue to rise over the next several years. For most organizations it is not a question of “will we become a victim” but rather “when will we become a victim” of a computer crime. Due to this trend, it has become crucial in the prosecution process that law enforcement officials and computer forensic specialist handle the evidence properly and present it thoroughly. Many agencies offer training in the proper acquisition, examination, and utilization of electronic evidence. If the evidence is to withstand the scrutiny of the courts, the evidence must be handled according to the letter of the law. Not being able to use the information collected in court is worse than not having it at all.

The field of computer forensics will continue to grow and we will begin to see agencies with trained digital detectives on staff, not only to combat external and internal threats but also to analyze and prepare protective procedures and applications for the agency. Until the security of our systems gets better, there will be a continuing need for computer forensic experts.

L. References

Armstrong, I. (2001 April). Security Magazine. “Computer Forensics: Tracking Down the Clues.” [online]. Available: www.scmagazine.com

_____. (2001, July 20). Attorney General Remarks Cybercrime Announcement [online]. Available: www.usdoj.gov

Bates, J. (1997, February). “Fundamentals of Computer Forensics.” *International Journal of Forensic Computing* [online]. Available: www.forensic-computing.com

Betts, B. (2000 March). “Crime Seen.” [online]. Available: www.nlectc.org

_____. (2000 July 27). CERT Coordination Center. “How the FBI Investigates Computer Crime.” [online]. Available: www.cert.org

_____. (2001). Computer Forensics. “The Last Step in Defending Your Computer System.” [online]. Available: www.softmart.com

_____. (2000 September). *Dr. Dobb’s Journal*. “Forensic Computer Analysis: An Introduction.” [online]. Available: www.ddj.com

_____. (1994 July). Federal Guidelines for Searching and Seizing Computers. [online]. Available: www.

Information Assurance Technology Analysis Center (2000). “Introduction to Computer Forensics”.

Gottfried, G. (2001 February 5). “Emerging Technology: Taking a Byte Out of Crime.” [online]. Available: www.networkmagazine.com

_____. (2001). Knowledge – Internet Statistics. “Worldwide Internet Population.” [online]. Available: www.commerce.net

Mares, D. (2001). “Forensic Software Sources.” [online]. Available: www.dmares.com

_____. (2001). National Infrastructure Protection Center [online]. Available: www.nipc.gov

Noblett, et al. (2000 October). "Recovering and Examining Computer Forensic Evidence." *Forensic Science Communications* [online]. Available: www.fbi.gov

_____. (1997 September). Police and Security News. "Computer Forensics Article" [online]. Available: www.computerforensics.com

Robbins, Judd. "An Explanation of Computer Forensics" [online]. Available: www.computerforensics.net

_____. (2000). The Center for Computer Forensics [online]. Available: www.computer-forensics.net

Villano, M. (2001, March 1). CIO Magazine. "I.T. Autopsy." [online]. Available: www.cio.com

Witter, F. (2001, April 20) "Legal Aspects of Collecting and Preserving Computer Forensic Evidence." Information Security Reading Room [online]. Available: www.sans.org