Computer Intrusion Forensics
Research Paper

Nathan Balon
Ronald Stovall
Thomas Scaria
CIS 544

Abstract

The need for computer intrusion forensics arises from the alarming increase in the number of computer crimes that are committed annually. After a computer system has been breached and an intrusion has been detected, there is a need for a computer forensics investigation to follow.

Computer forensics is used to bring to justice, those responsible for conducting attacks on computer systems throughout the world. Because of this the law must be follow precisely when conducting a forensics investigation. It is not enough to simple know an attacker is responsible for the crime, the forensics investigation must be carried out in a precise manner that will produce evidence that is amicable in a court room. For computer intrusion forensics many methodologies have been designed to be used when conducting an investigation. A computer forensics investigator also needs certain skills to conduct the investigation. Along with this, the computer forensics investigator must be equipped with an array of software tools.

With the birth of the Internet and networks, the computer intrusion has never been as significant as it is now. There are different preventive measures available, such as access control and authentication, to attempt to prevent intruders. Intrusion detection systems (IDS) are developed to detect an intrusion as it occurs, and to execute countermeasures when detected. Intrusion detection (ID) takes over where preventive security fails. In order to choose the best IDS for a given system, one should be aware of the advantages and disadvantages of the each IDS. This paper views a forensic application within the framework of Intrusion Detection and details the advantages and disadvantages of each IDS.

Introduction

In a perfect world the need for determining the activity conducted on a network or within a computer would not be necessary; however, this is not a perfect world and there are times when it is imperative that the activity of a computer be monitored. There should be a way for an individual to observe assets, such a computer or network, in times when possible intrusion or misconduct has occurred. For this reason, computer forensics, a newly developed area of computer science, becomes an increasingly more important aspect daily and will be widely used in the twenty-first century.

The widespread use of computers has caused computer crimes to increase at an alarming rate. Computers have given criminals a new approach to carrying out their misdeeds. After a crime or a questionable act is detected on a computer, a digital investigation must follow. The investigation is used to determine the scope of the problem. The computers investigated will typically be either those used to commit the crime or those which are the targets of the crime.

During the Enron incident a great deal of paper was shredded to avoid leaving evidence of a wrong-doing. However computer forensic investigators were able to recover a large

extent of the information in electronic form [Salkever 2002]. In computer forensics, a case may be as simple as to determine whether or not an employee is engaging in improper activity on the network; or it can be as severe as determining where a major attack originated from, such as the SOBIG virus. For these reasons, computer intrusion forensics is an emerging field of essential research.

Intrusion forensics is a specific area of Computer forensics, applied to computer intrusion activities. Computer forensics, which relates to the investigation of situations where there is computer-based (digital) or electronic evidence of a crime or suspicious behavior, but the crime or behavior may be of any type, quite possibly not otherwise involving computers. Where as Intrusion forensics relates to the investigation of attacks or suspicious behavior directed against computers per se [Mohay… et al. 2003]. Intrusion detection uses standard computer logs and computer audit trails, gathered by host computers, and/or information gathered at communication routers and switches, in order to detect and identify intrusions into a computer system. Successful detection of intrusion is based either upon recognition of a known exploitation of a known vulnerability or upon recognition of unusual or anomalous behavior patterns or a combination of the two.

Computer forensics on the other hand is concerned with the analysis of any information stored by, transmitted by or derived from a computer system in order to reason post hoc about the validity of hypotheses that attempt to explain the circumstances of an activity under investigation. Computer forensics therefore, covers a much broader scope of activities than does intrusion detection, the scope of the latter being limited to reasoning about activities or detecting activities relating to computer system abuse.

Literature Review and Problem Definition

Literature Review

Computer forensics is a relatively new field of study. At the current time, there are a limited number of books published on this topic. A search on Amazon.com resulted in a finding of 15 to 20 books on the subject. Computer Forensics: Incident Response Essentials by Kruse II. and Heiser is a entry level book in this new field. The book defines computer forensics and the steps used to conduct a forensics investigation. Another book, Know Your Enemy by the Honeynet Project, looks at the tools and methods of the blackhat, hacker community. The Honeynet Project used intrusion detection systems and computer forensics to analyze the attacks of hackers in an effort to learn the motivations and skills of hackers. An informative book focusing on the subject of intrusion detection is Network Intrusion Detection, by Stephen Northcutt and Judy Novak.

A great deal of the material reviewed on computer forensics came from web sites. Online magazines, such as Dr. Dobbs, securitymanagement.com, sercurityfocus.com, and scmagazine.com, these sites regularly post articles on security and computer forensics. Also, the Department of Justice publishes information on their web site for conducting a

computer forensics investigation. There also many commercial web site for companies of computer forensic services. The commercial sites give some of the techniques that these companies use to conduct investigations.

The bulk of the literature found from books and web sites dealt with the basic steps used to carry out a forensics investigation, such as the ways the logs and hard drives can be examined to turn up evidence, and the legal ramification of computer forensics. The majority of quality literature found on the topic of computer forensics came from professional and academic journals. Professional and academic journals offer the most in-depth look into computer forensics. Some of the topics found in journals were: "An Examination of Digital Forensic Models", "Research in Progress: Risks and Solution to Problems Arising from Illegal or Inappropriate On-line Behaviors", and "Forensics Readiness".

Problem Definition

The field of digital forensics is a relatively new field of study. Many of the techniques used in computer forensics have not been formally defined. Computer Forensics is looked at as part art and part science [Honeynet Project 2002]. Computer Forensics will evolve into a science as more research and standardized procedures are developed.

A survey of the field of computer intrusion forensics will be given in this paper. The goal of this paper is to explain the advantages and disadvantages of computer intrusion forensics. A formal definition of computer forensics will be given. The paper will look at how intrusion detection systems can be used as a starting point to a computer forensics investigation. Also, the ways to preserve and recover data during a computer forensics investigation will be explored. A discussion of how some of various software tools that are used in a computer forensics investigation will be included. This paper will explain the rights granted to a company who plans to implement such tool and will provide information on tools currently available for use in computer forensics. Last, the paper will explore ways that an intrusion detection system can be used in correspondence with computer forensics.

Discussion

Computer Intrusion

The need for computer intrusion forensics arises from the event that an intrusion into a computer system has occurred. According to the CERT web site a computer intrusion is, "Any intentional event where an intruder gains access that compromises the confidentiality, integrity, or the availability of computers, networks, or the data residing on them." According William Stallings book Cryptography and Network Security, intruders can be classified into three types [Stallings 2003]:

- **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user account.

- **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
- **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

The amount of damage done by an intruder to a system can vary greatly. Some intruders are malicious in nature and others are just curious and want to explore what is on a local network. Computer users must protect themselves from intrusion. While there are no 100% effective methods of eliminating intruders completely, some methods must be used to reduce intrusions. In the event that an intrusion has taken place the last line of defense is an intrusion detection system. An intrusion detection system can alert the system administrator in the event that the system has been breeched. Once the intrusion detection system has detected an event, an intrusion forensics investigation should be conducted to note the extent of the intrusion and any damages that may have occurred and to locate the source of the attack.

Computer Forensics

Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data [Kruse II and Heiser 2002]. Computer forensics is usually used when a crime has been committed or an inappropriate activity has taken place. Some common examples of when computer forensics is used are:

- Identity theft, such as stolen credit cards numbers and social security numbers.
- To reveal if trade secrets were stolen from an organization.
- Investigate a hackers attack on a computer system.
- Finding evidence of child pornography.
- For divorce proceedings, evidence of a cheating spouse.

These are just a few examples of when computer forensics may be used. There are numerous other times when computer forensics can be employed.

Computer forensics involves many common investigative techniques used by law enforcement. The only difference is they are used on digital media [Wright 2001]. The main goal of a computer forensics investigation usually involves a conviction in either criminal or civil court. During an investigation, procedures must be followed precisely so evidence is amicable in court. Great care must be taken in the preservation and recovery of data.

Computer Forensics Investigator

A computer forensics investigator is a person who conducts an investigation on the digital media. A computer forensics investigator must be a well-rounded individual. It is not enough for the investigator to have only a strong knowledge about computers. The investigator must have knowledge in many other areas. The following are some of the skills needed in computer forensics [Broucek 2002]:

- Computer Science: knowledge of operating systems, programming languages, and computer security
- Law: computer, criminal and civil
- Information System: system management, system policies, and user training
- Social Science: socio-political issues, socio-psychological impact of computers, and hacktivism

To conduct a computer forensics investigation, the individual must have a strong background in computer science. The investigator should know many different operating systems work. The two most common systems to investigate are Windows and UNIX. Knowing these two operating systems is a must. It is possible that other types of systems will also have to be investigated besides UNIX or Windows. Next, the investigators should know a wide range of programming language such as C, C++, UNIX scripts and others. Many times the source code is changed on the investigated system, so the investigator must know what the changes to code accomplish. Last, the investigator should be up to date on computer security issues. They should know what new vulnerabilities exist that hackers are using to exploit systems.

The computer forensics investigator must be familiar with the laws of state and country they are working in. The investigator needs to know the correct techniques for document evidence to be used in a legal proceeding. The forensics investigator will need to then present the evidence they found in court as an expert witness if evidence of a crime is found.

The next area that an investigator needs to be knowledgeable in is information systems. The investigator should have a deep understanding of information system management. The more he knows about the system policies of an organization, the greater likelihood the investigator will find violations of the policy. The investigator should be able to work well with people. At times the investigator will need to work with and question the end-users in an organization.

The investigator should also know about current issues in social science and the impact of computers on personnel privacy. This is an area where the investigator needs to use sensitivity when working with the members of an organization. The investigator should also be able to understand the thinking of the hacker community. These are a few of the social issues that an investigator must deal with.

The Legal Methods of Computer Forensics

The definition of Computer Forensics has already been discussed in the previous section. To recap, Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data [Kruse II and Heiser 2002]. This definition will be modified to suit the needs of this section. Lets assume that instead of attempting to preserve information on a machine, the asset may have been compromised by an unknown assailant. The method of solving the attack would be to use computer forensics, but now we are using said information for legal issues. Computer Forensics can

further be defined as the application of computer investigation and analysis techniques in the interest of determining potential evidence, which might be sought in a wide range of computer crime, or misuse, including but not limited to theft of trade secrets, theft or destruction of intellectual property, and fraud [Robbins 1999]. This section will describe the legal aspects of the new definition and explain the rights that employers and investigators have when it pertains to forensics on an asset such as the computer.

When an investigation develops to a point where information may need to be retrieved from an asset such as a computer there are a lot of issues to take into consideration. The evidence has to remain valid through the course of the investigation to be admitted into a court of law. The investigators must also make sure that search and seizure of the asset is allowed, otherwise the investigation can be corrupted.

The following case provides a sufficient example the legal rights involved in computer forensics. In the winter of 1999, during contract negotiations, a Northwest Airlines flight attendant hosted a message board on his personal website; among the messages were anonymous messages by Northwest employees urging co-workers to participate in sick-outs, which is illegal by U.S. federal labor laws. That season over 300 flights were cancelled. Northwest Airlines subsequently obtained permission from a federal judge to search union office computers and employee personal computers, in order to obtain the identities of the anonymous posters [Caloyannides 2001]. Note that the employer was granted the right to view not only the office computer, but the personal ones as well. The question on the table is how can that be possible? One may argue that the constitution prohibits such actions and that the accused should have had some form of legal protection against such an intensive search. The fact is that it is the exact opposite.

Fourth Amendment

Here is the fourth amendment to the constitution, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and **no Warrants shall be issued, but upon probable cause**, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. Draper v. US (1959) has legally defined probable cause as "where known facts and circumstances, of a reasonably trustworthy nature, are sufficient to justify a man of reasonable caution or prudence in the belief that a crime has been or is being committed" [O'Conner 2002]. Accordingly, as long as a plaintiff can convince a judge of probable cause, a warrant to search a computer can be granted. Today, more federal judges are approving searches of computers for evidence in civil and criminal cases [McCarthy 2000].

ENRON

A recent case that is under investigation is the ENRON bankruptcy incident. The company was a multi-billion dollar organization that marketed electricity and natural gas, delivered energy, and provided financial and risk management services to people around the world. In the year 2000, ENRON had revenues of over 100 billion dollars [Parker and Waichman 2002]. In December of 2001, ENRON's stock fell to fifty cents a share. Thousands of employees lost their jobs. By January of 2002, a federal investigation was

initiated on ENRON to determine whether or not fraud caused the fall of the company [Parker and Waichman 2002].

Computer Forensics would play a pivotal part in this investigation. While companies go out of business quite frequently during the current state of the economy, it is very odd for a multi-billion dollar company to loose everything in a year's timeframe. Let us assume the asset is the computers within ENRON, but more importantly any files that were deleted that would lead to evidence of fraud. Recall that information deleted on a machine is not always completely erased; it is rather inaccessible to the user. Due to the widespread panic this incident has caused among employees and stockholders, it is possible for computer forensics experts to investigate.

SOBIG Virus

The case of the SOBIG blaster worm virus that clogged the networks of systems across America in an attempt launch a full-scale assault on the Microsoft Corporation is another instance where computer forensics was employed. During the reign of this virus, it was estimated that the number of infected machines were in the hundreds of thousands. The solution was not as simple as downloading a patch because there was not enough bandwidth available to do so [Fisher 2003]. On Friday, August 29th, 2003, federal agents arrested 18-year-old Jeffrey Lee Parson for intentionally damaging a computer, a violation of U.S. criminal code [Hachman 2003].

This investigation also warrants the use of computer forensics. The probable cause for this case would be the millions of dollars lost due to network shutdowns and lost work. The same would be the case for the majority of the exploitation viruses that are out there. Many of these hackers feel a sense of security in that they assume their actions cannot be tracked and believe that their personal computer cannot be searched. This is not the case in this scenario. This particular virus was broadcasting out on the Internet instead of the traditional method, via email. Under this circumstance, it is imperative that computer forensics be used in this matter. The assets in this scenario would the number of computers affected by this virus, the vulnerability is the Microsoft Vulnerability that was discovered by the attacker, and the threat is the virus clogging the bandwidth of the networks, producing a denial of service attack, which results in a lack of productivity to millions of computer users.

Legal Rights

These two cases are brought up to provide examples of where Computer Forensics is necessary. The probable cause has already been identified, and it is now time to define the legal procedures necessary to maintain the evidence for a court of law. This procedure will work for government investigations as well as employer searches. The one thing to remember is that as long as there is probable cause a search warrant can be issued and computer forensics can take place. Employers must be careful when searching through an employees work area. While government employees are bound to the fourth amendment, employers need to identify the reason the search is work-related. Therefore, items such as briefcases, purses, and gym bags are still off limits to employer searches [Cybercrime 2001].

Seizing Computers

Investigators must be specific when seizing hardware for investigation. Under normal circumstances the employee's/attacker's computer (desktop, monitor, keyboard, and mouse) would be collected; however, in the networking age the computer in question may be just a dummy terminal and all the potentially hazardous information hidden on the server or dispersed throughout the network [Cybercrime 2001]. It is imperative that the first step is specific in what should be gathered and only hardware that will not cripple the network of the company is taken.

Once the appropriate hardware has been marked for seizure, it is important to transport it in the proper fashion. For most computer forensics investigations, the personal computer is a standard desktop with a monitor, keyboard, and mouse; however, more complex systems must be handled in a special way. Here is that list of transport guidelines:

- Agents are to protect the hardware from damage
- Disassembly of hardware must be done in such a way so that reassembly can occur without damaging the hardware.
- Photograph the area where the hardware is before disassembly and prepare a wiring diagram. Any inconsistencies could result in tainted evidence.
- All floppy, magnetic, and removable disk drives must be protected according to manufacturer standards
- All hardware must be kept in a dust and smoke free environment with the temperature set between 40 – 90 degrees Fahrenheit [Cybercrime 1999].

The proper procedures must be followed with the forensics team in possession of the confiscated computer equipment. The computer seized must be stored properly at all times. A chain evidence of custody must be in place. The chain of custody documents who has custody of the evidence at all times [Crayton 2003]. It is important that the forensics team documents not only who has the equipment, but also for what length of time and when it was returned to storage. Also, the investigator should document anything done with the evidence. For example, if the investigator runs a program to search for key words on a hard drive it should be added to a log. The log should contain the name of the command that was run, the time it was run, and the results.

Once the hardware has been retrieved properly, it can be searched using the forensics tools that are available. The Recycling bin, hidden folders, and log files would be the first spots to search for information on the computer. If data is suspected to have been deleted, then the solution would be to use a data retrieval tool to find the data in one of the hidden sectors of the storage medium. It is important that the machine under investigation be copied using a GHOST utility so if a mistake should occur, it is always possible to return the original configuration. While this is a big aspect of Computer Forensics, it is not the only one. There are other uses for this science and it will be discussed in the other sections of this paper.

Computer Forensics Methodologies

During a computer forensics investigation there are a variety of steps that must be taken. The following steps, defined in the book Computer Forensics: Incidence Response, form the basis for conducting a forensics investigation. Each of these steps can be further refined.

1. Acquire the Evidence
2. Authenticate the Evidence
3. Analysis the Evidence
4. Present the Evidence

Along with this methodology developed by Kruse II and Heiser, other more formal methodologies have been developed. These methodologies have been established to aid in the proper sequence of actions taken in an investigation. Some of the methodologies are abstract and can be used in any situation which concerns digital evidence and others are aimed at a certain implementation.

The paper "An Examination of Digital Forensics Models" gives five methodologies that can be used for digital forensics. The first methodology was established by Farmer and Venema and is targeted towards the UNIX operating system. Second, Mandia and Prosise established an incidence response methodology. Third, the US Department of Justice created a digital forensics mythology which is more abstract then the first two methodologies and hence could be applied to a wider range of platforms. The DOJ Methodology has four phases "collection, examination, analysis and reporting". Fourth, The Digital Forensics Research Workshop developed a framework based on academic work. It consists of the stages "identification, preservation, collection, examination, analysis, presentation and decision". Last, the authors of the paper created an abstract model for digital forensics. The abstract model consists of nine phases "identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence".

Each of the methodologies described above has its benefits and drawbacks. For example, the benefit of the abstract model is that it can be used in any situation where digital evidence is involved, not just for examining computers. The disadvantage of using an abstract model is the processes may not be defined as precisely. In some cases when a problem is well defined it may be beneficial to use a non-abstract model. So when investigating a UNIX system, the Farmer and Venema model may suffice compared to an abstract methodology.

Computer Forensics and Security Policies

An organization should build their security policy around the event that it is inevitable that computer forensics will be needed in the future. If an enterprise has a plan in place for when an intrusion takes places, it will greatly aid the organization into the forensics process. All employees of an organization should be trained on what to do in the event of

an intrusion. Failing to provide employees with training and written procedures can jeopardize a computer forensics investigation. For instance, an employee may think he is aiding in helping to contain an incident and in actuality may be damaging evidence. Along with the typical computer user of the organization, system administrator should also be train. While the system administrator knows a great deal about their system, they may not have the proper training of what to do in the event the computer forensics is needed. For these reason the security policy of an organization should contain what to do in the event that computer forensics is needed.

Intrusion Detection Systems

Computer crime arising from computer misuse often manifests itself as anomalous behavior, both of individual systems users and of the system as whole. Although improvements to operating system security continue, the available computer security features are still not good enough to detect many anomalous behavior patterns by system users. Intrusion detection uses standard logs and computer audit trails, gathered routinely by host computers, and /or information gathered at communication routers and switches, in order to detect and identify intrusions into a computer system. There are many forms of intrusions, they can be divided into two main classes or models that are often employed in IDSs [Mohay…et al. 2003].

- Misuse intrusions, where well-defined attacks are aimed at known weak points of a system. Due to the fact that these attacks have been experienced before and are therefore well defined/documented, very often a purely rule based detection system encapsulating the known information about the attack is applied.
- Anomaly intrusion. These are harder to quantify and are based on observations of normal system usage patterns, and detecting deviation from this norm. There are no fixed patterns that can be monitored and as a result a more "fuzzy approach is often required.

Anomaly-based IDS's uses a typically statistical profile of activity to decide whether the occurrence of a particular component event or event pattern is normal or anomalous. If normal, then the activity is considered to be harmless and thus legitimate. On the other hand, if it is anomalous then it is potentially unauthorized and harmful.

Signature-based IDS's attempts to match a sequence of observed events with a known pattern of events which is characteristic of an attack of some sort, such as a buffer overflow attack and password guessing. If no match is found with any of the known attack event patterns (signatures), then the activity under scrutiny is considered to be harmless and thus legitimate. Solely signature-based IDS cannot recognize a new or previously unknown type of attack; anomaly-based IDS on the other hand cannot categorically identify a sequence of events as an attack.

In both cases, the IDS reaches a conclusion based upon computed data that is more informative than what is allowed by the legal definition of what constitutes computer evidence. This is because the latter is constrained by formal rules of law that might require the exclusion of information that might nonetheless be relevant and informative. By contrast, an IDS can exploit any and all such information including knowledge of the

target operating system and architecture. That is, any relevant computer system information is grist for the IDS mill, and is used by the IDS as a basis for its decision-making. As a result, whether signature-based or anomaly-based, they are typically technically sound, but do not necessarily stand up in court.

Intrusion Detection Systems and a View to Its Forensic Applications

The ultimate goal of Intrusion Detection is to identify, preferably in real-time, unauthorized use, misuse, and abuse of computer systems by both systems insiders and external penetrators. In the case of anomaly intrusions, intrusion detection is based on the idea that the anomalies that may surface in a system are symptoms indicating illegal, intrusive or criminal activity.

The ultimate goal, with a view to a forensic application however, would be to obtain sufficient evidence to in order to trace the crime back to the criminal. Within a computer system the natural blanket of anonymity afforded the criminal encourages destructive behavior while making it extremely difficult for law enforces to prove the identity of the criminal. Therefore, the ability to obtain a fingerprint of system users and their typical behavior is imperative in order to acquire some hold on identifying the perpetrator.

The study of available log files would always be uses as fundamental in evidence collection. However, many times at a higher level it is necessary to posses a more in-depth ability to narrow the field or even establish a list of possible suspects. As we all know, the compute crime is always the result of human activity on a system, be it system users or intruders. So at this level, it is not only desirable to have some logging activity to provide evidential information, but also some artificially intelligent mechanism to collate and collect profile of system users. For example, it is useless to know that User John Doe has logged in at 8pm by viewing the logs without knowing that User John Doe never logs in at 8pm. The knowledge that User John Doe never logs in at 8pm can only be obtained by knowing the typical behavior of User John Doe, or the behavioral profile of Use John Doe.

The basics of intrusion detection have been discussed. Intrusion detection systems can form a starting point that can be used by a computer forensics investigator. Next, we will look at how computer forensics can be used to provide further analysis into an investigation.

Data Preservation, Recovery and Examination

The analysis of data in a computer forensics investigation involves three main steps: preserving, recovering and examining data. Recovering data in a computer forensics investigation is a major dilemma. The data that an investigator is looking for can be almost anywhere. It could be on the suspect's computer or in a remote location. A major problem is locating the computer on which the sought-after evidence is located. In a network environment it can be very difficult. Network analysis tools may be needed to help track down the location. Once the computer is located, the hard drive is where the

majority of evidence can be found, but it is not the only place. Some of the places to look for evidence in an investigation are:

- Hard drives
- Memory
- System logs
- Email servers
- Network traffic
- Intrusion detection systems

These are just a few places where evidence can be discovered. If possible the computer system that holds the evidence should be seized. The investigator may not always be able to confiscate the computer, for instance it may be hard to justify taking a live server down for analysis. When possible, the best solution is to power the computer down and preserve the data on it. One drawback of powering down a computer is that evidence which may reside in memory will be lost when the system is shut down.

Preserving Data

The next step that should be taken in an investigation, after the evidence has been seized, is data preservation. The data should be put on a write protected medium. Hash functions should be used to authenticate the integrity of the data. There are programs available that can be used to take a hash value of the entire drive. If the data is not properly preserved and the case makes it to court, a conviction will be unlikely if the data is contaminated, even if there is substantial evidence. It is common to copy data to a read-only medium such as a CD-Rom to prevent the data from being altered. Another solution is to make a copy of a hard drive to another hard drive. For further examination, drive should then be mounted read only to prevent contamination of the data on that drive. An investigator should never use the original storage medium when investigating. These are the main steps that should be taken when preserving data in an investigation.

Recovering Data

After the data has been preserved, the next step is recovering and examining the data. There are many techniques that a suspect can use to hide information, depending on the level of skill of those in question.

Data can be located in odd places or have misnamed files. For example, it is common to give files names that look like they would be used by common programs or the operating system. Most people would not question such files. It is also possible to put files in place where few people would look. A common techniques is to put files in folders used by the operating system and give them names that a close to those used by the OS. One technique to find these files is to search for key words that these files are likely to contain.

Files may be protected by passwords. While passwords may deter many users, the investigator should be able to recover these files. Password cracking programs can be used to gain access to password protected files. There are few passwords that cannot be cracked. Most people use weak passwords which makes recovering these files fairly easy with the right software.

The evidence sought after may be encrypted. It is usually infeasible to try to crack encryption unless weak encryption is used. It is highly unlikely that strong encryption can be broken but it may be possible to find the encrypted files on other parts of the drive [Wolfe 2001]. An investigator is probably better off leaving these files alone or else convincing the suspect to decrypt them. If the private keys can not be obtained, there may be a trace of the encrypted file residing on the drive from before it was encrypted.

The evidence sought after may have been deleted from the hard drive. It is usually possible to retrieve deleted files. When a file is deleted, a pointer to the file is removed from the file system table and it is then inaccessible to the operating system. If a file is deleted, it will still reside on the hard drive unless it is over-written with a new file. So it is possible to recover this data by reading the individual sectors of a drive. In addition, slack space is another area on a drive where information can be retrieved. The slack space is the extra space that is left over at the end of sector [Wolfe 2001]. It is possible to examine the slack space and recover parts of files that have also previously been deleted. The one drawback to examining the slack space is it will not turn up the complete file sought after, since part of the sector has been overwritten with a new file. Figure 1, shown below, shows the clusters on a disk and the slack space. These are a few of the techniques commonly used to recover data on a hard drive.

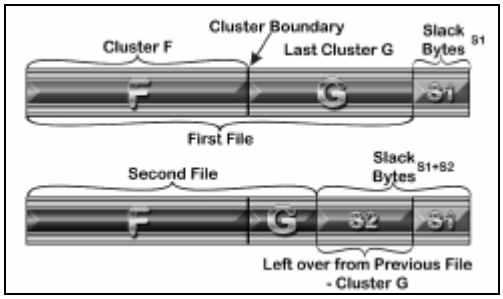

Fig. 1 Hard Drive Space [Wolfe 2002]

All of these cases require special techniques for the data to be retrieved and reconstructed. Various software tools and techniques can be used in the recovery, which will be discussed later in the paper.

System Logs

While a great deal of information can be gained from the host computer, information also can be obtained from a server. The majority of events that take place in a computer system are recorded in log files on servers. By failing to collect the system logs, valuable information can be overlooked. Logs can contain information such as user name, password, access time, device used, functions performed, and other information depending on the type of log [Kruse II and Heiser 2002]. By examining the logs, it can be proved which user account actually performed the questionable act. Also, Firewalls and Intrusion Detection Systems have logs that can be evaluated for suspicious activities. Many network routers also have logs that the investigator can examine to reconstruct evidence. By examining the logs in an information system it may be possible to piece together a crime that occurred [Melia 2002].

The first step that should be taken when examining a UNIX system is look at /etc/syslog.config [Kruse II and Heiser 2002]. From this file it can be determine what events are logged and where the logs are stored. There is a much better chance that the logs will be valid if they are stored on another machine. It is relatively easy for an attacker to modify the logs on a system to cover there tracks. For this reason the logs should be stored on another host when possible. In the book Computer Forensics: Incident Response Essentials the authors give a few things to look for that should raise questions about the log entries.

- Missing logs
- Time periods without log entries
- Unusual activity at odd hours
- Fail logons
- Oversized records (possible buffer overflow attack)
- Failed use of su
- Logons from unusual sources
- Attempts to access password configuration files

The amount of information that can be gathered from logs is highly influenced by the services that are logged by the system. If a computer is not set up to log many activities the amount of evidence found in the system logs will probably be minimal. Also, the more activities logged, the harder it will be for someone to cover their tracks. A multi-tiered logging strategy should be used to provide the highest assurance of the quality of the log files [Tan 2001].

These are the basic steps that should be taken when conducting an investigation. Two of the most valuable places to look for evidence in an investigation are on hard drives and system logs.

Software Tools

Preserving and recovering data in an investigation is done with a large assortment of software tool. A computer forensics investigator is severely limited in their capabilities without the proper tools. There are many different categories of software tools available for use in a computer forensics investigation. For instance there are tools to analyze a drive, and tools to analyze a network. There are also three main variations of software that is generally used: commercial, open source, and operating system utilities. No single tool can be used in all situations, so a computer forensics investigator will use many different software programs. The investigator must select the correct tool depending on the objective to be accomplished.

Hard Drive Tools

One of the first things done in an investigation is to determine information about the hard drive on the suspect system. The investigator should have software tools to find general information about a hard drive. The tools should give information about the number of partitions and file systems used on the drive. Partition Magic is a good commercial program that can be used. One nice feature of Partition Magic is that a drive can be examined in read-only mode [Kruse II and Heiser 2002]. Operating system programs such as fdisk for Windows or fsck for UNIX can also be used for this purpose. A tool

such as Partition Magic is usually able to determine a greater number of different types of file systems than the tools provided by the operating system.

An image of a hard drive should be taken before the examination of data takes place. The hard drive in question should never be analyzed in an examination; instead an exact copy should be examined. For this reason, a good drive imaging program is needed. Many backup programs only backup files and don't copy slack space, unallocated areas, and swap files [Wolfe 2001]. A drive imaging program should be used that will create a bit copy of an entire drive. The dd command with the UNIX operating system is the most popular choice to create a copy of a hard drive, since it is widely available and does a good job. Furthermore, Symantec makes the product Norton Ghost that also can be used to image a hard drive.

A program that takes hash values of the individual files and the hard drive as whole should be used. A hash function accepts a variable size message *M* as input and produces a fixed-size message digest H(*M*) as output [Stallings 2004]. It is common to use the MD5 hash algorithm to take the message digest of files to be compared. The message digests are then used to validate the integrity of files. The values are also used in court to prove that the files were not modified during the investigation. A frequent use of message digest values can be taken of all the library files of the operating system when it is installed. At a later time, the current hash values can be compared with the previous values to see if any changes occurred. If there are discrepancies between the values, the system files have been changed. This method is used to help locate malicious code. The one problem with using message digests is they can't validate the integrity of files that are changed frequently such as logs. Hash values are best suited for files that stay static such as system library function. Tripwire is a popular commercial program that takes the hash values. The program then automates the process of comparing the message digests of files.

Hex Editors can be used to examine clusters on the hard drive. A hex editor can look at individual sectors of a hard drive and/or examine individual files as a whole. Files that are deleted can be recovered by a hex editor. A hex editor will give the hex values that are contained on a hard drive. As explained before it is possible to examine the swap, slack and deleted space on a drive and reconstruct the files. It is also possible to view the ASCII text converted form hex directly in many hex editors. Figure 2 in the appendix shows a sample output of a Hex Workshop, a hex editing program.

Network Tools

Packet sniffers are used to analysis network traffic. Sniffers can be used when analyzing a live attack on a computer system. A sniffer captures the packet on a network and can subsequently be used to analyze a live attack. By analyzing the individual packets, it may be possible to locate the address where an attack is coming from. One problem with this approach is it is possible to spoof an IP address. Some popular packet sniffers are tcpdump, dsniff, and ethereal. A sample output from the program ethereal is shown in appendix Figure 3.

Intrusion Detection Systems are used to monitor a system for attacks. By using an IDS, an attack on a system can be reconstructed and examined. Earlier in the paper a formal overview of the techniques of intrusion detection system was given. An intrusion detection system is one of the first places that should be examined when starting an investigation. By using an IDS it may be able to determine how an attacker gain access to the system. A popular open source IDS is snort.

Tools to Search and Recover Files

Various types of file viewers come in handy for viewing unknown file types. A file view will give a preview of the file without actually opening the file. Quick View Plus is a program that supports over 225 file types that can be used. One nice feature of Quick View Plus is that it can be used to identify files on windows with incorrect file extensions. The previews of the files are then shown in the correct format even with the incorrect file extension. Also, the program can be used to convert formats such as text or hexadecimal. Quick View Plus is shown in the appendix in Figure 4.

Searching through text files is crucial in an investigation. There is a wide-range of text searching programs that are used to find files containing certain key words. UNIX commands such as grep can be used to search text files by using regular expressions. There are numerous other programs on UNIX that can be used to search text such as sed and awk. Using the windows operating system, one can use the built in search function of the operating system. If a more powerful program is required, there are many commercial products. One of the leaders in this category is dtSearch (Appendix Fig. 5).

Recovering files may also involve the need for cracking passwords. Many password cracking programs can be used, depending on the application that must be cracked. There is a password cracking programs for virtually any program that uses a password. These programs can crack operating system password, instant message passwords, and Microsoft Office passwords, to name a few. One example is L0phtCrack, which is used to crack Windows NT passwords.

All Purpose Tools

Programs made specifically for forensics investigations are available, such as EnCase and ForensiX. EnCase is the industry standard software used by law enforcement. EnCase combines many of forensics tools described above into an integrated package that can help simplify an investigation. The one drawback to EnCase is the price tag attached to it. The corporate forensics edition of EnCase costs $2,495.00. Encase is probably the most powerful forensic tool available on the market. Encase provides the majority of the tools discussed above. EnCase also add tools that are specific to forensics such as creating a log of forensics activity. ForensiX is a similar program to EnCase, except that it is designed for the lunix platform. The Coroner's Toolkit is another popular all purpose tool that is designed to conduct an investigation in the UNIX environment.

A forensics investigator should be familiar with all available programs to aid in an investigation. Each program serves it own purpose. In the future, more programs will be developed to ease the computer forensics process. However, no single tool will be able

to do everything in every situation. The more software tools that an investigator is familiar with, the greater the rate of success will be.

Evaluation and Results

There are several difficulties in addressing Intrusion Detection Systems with Computer Forensics. First, the theoretical requirements of an IDS in terms of performing its primary mission may be at odds with the requirements of collecting an preserving forensic evidence. The primary mission of an IDS is to detect and respond to security incidents. The definition of a security incident should be, at least in part, determined by the organization's security policy. Therefore, the detailed definition of the IDS' primary mission is partially determined by the security policy, not by some overarching standard or generic procedure. The result is that there can be a wide disparity among requirements for an IDS from organization to organization. That contrasts significantly with the relative static set of requirements for developing and managing evidence for use in a legal proceeding.

A second difficulty is that an IDS, by design, does not manage its information in the sense that a forensics systems does. There is a requirement within a forensic system for, among other things, the maintenance of a chain of custody whereby all evidence can be accounted for and its integrity attested to from the time of its collection to the time of its use in a legal proceeding.

The third difficulty deals with the architecture of the IDS. The ability of a program to perform widely disparate tasks implies an architecture that may or may not be present currently in an IDS. Thus, there develops the need for a standard architecture for intrusion detection systems that also are capable of forensic data management.

A major problem with the current approaches to anomaly detection is that it is difficult to define normal user behavior. Misuse detection approaches (Rule-Based), on the other hand, detect only known attack patterns with high accuracy. In a dynamic environment it will be almost impossible to created user profiles that determine the normal behavior. Therefore, it would be better to look at intrusion detection systems that observe the behavior of process rather than users. Intrusion detection tools of the future must be able to more effectively deal with detection evasion techniques and encrypted network traffic. An automated Intrusion Detection System for detecting anomalous behavior will help tremendously to alleviate some of the burdens that are placed on Security Administrators.

Summary

A survey of the field of computer intrusion forensics is given in this paper. To reiterate computer forensics deals with the preservation, identification, extraction, documentation and interpretation of computer data [Kruse II and Heiser 2002]. The paper explored a wide-range of areas dealing with computer forensics. The legal issues surrounding an investigation were discussed. Next, the skills need to be possessed by the investigator were examined. After that, the computer forensics methodologies were discussed along with incorporating forensics into an organization security policy. Subsequently, a basic

overview of intrusion detection systems and how they relate and aid in computer forensics was discussed. Furthermore, some basic steps need to preserve, recover and examine data were discussed. Last, a wide-range of software tools were examined that can aid in the investigation process.

One of the most important parts of computer security is being prepared. While it important for an organization to take the normal security precautions such as having a firewall, anti-virus software and patching the operating system regularly for known vulnerabilities, it is also important that an organization is prepared for the inevitable event of an intrusion. An organization should include in their security policy what to do in the event of an intrusion and methods to be used in a computer forensics investigation. There are many things that an organization can do that will aid in the forensics process after an intrusion. First, an enterprise should use an Intrusions detection system, so the intrusion can be noticed and contained as quickly as possible limiting the damage caused. Next, an organization could also use a program such as tripwire to compare the hash values on a system to detect if any files have been changed. Also, the organization should store the log file of a computer in a remote location. Last, the most important thing is to educate the user of what to do in the event of an intrusion.

The birth of the Computer has brought about, what is known as the "Information Revolution". Never before has such a wealth of data, both public and private, been so accessible and obtainable. With this revolution have come certain undesirable elements, being the underworld of computer fraud and crackers, who quite often achieve their aims by breaking into compute systems and impersonating legitimate system users. Many methods preventing intrusions into computer systems have been implemented, but these will always be imperfect.

Current intrusion detection systems operate at high level of data manipulation and are ineffective for detecting intrusions that can occur at a low network level. All the intrusion detection approaches use input in the form of audit data created by the operating system. The audit data provided in most cases tends to be problematic; special programs such as data mining are needed to subtract meaningful data from the records. [2]

Today's intrusion detection systems are not yet intelligent enough - a human still needs to interact too much in setting up and maintaining intrusion detection systems. Also, it might be possible in the near future to combine firewalls, computer intrusion forensics and anti-virus scanner technologies to form a robust Intrusion Detection Systems (IDS) that can detect all types of intrusions in real time. An automated system for detecting anomalous user behavior will help alleviate a, sometimes unrealistic, burden on systems administrators. However, these automated systems are not only useful during a violation but can be an invaluable forensic tool after the fact.

Computer intrusion forensics will be an emerging field of study in the twenty-first century. The need for computer forensics will continue to increase as computers become even more prevalent in society. As further research takes place in this field, computer forensics will continue to move from being an art, towards a scientific field. Evidence of

the increased popularity of computer forensics is a small number of colleges have begun to offer programs in computer forensics, such as University of Central Florida and University of Texas at Dallas. Computer forensics investigators will become an integral part of an organizations security department.

Appendix

Sample Program Output

Hex Workshop, hex editor output:

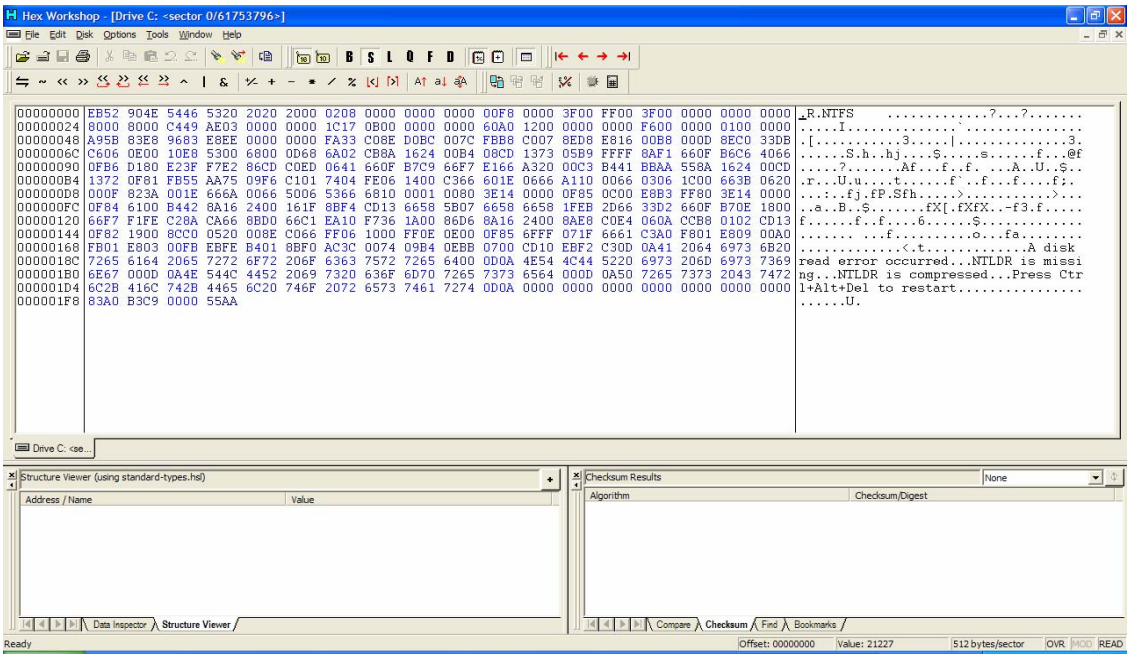

Fig. 2 Hex Workshop Hex Editor

Ethereal, packet sniffer output:

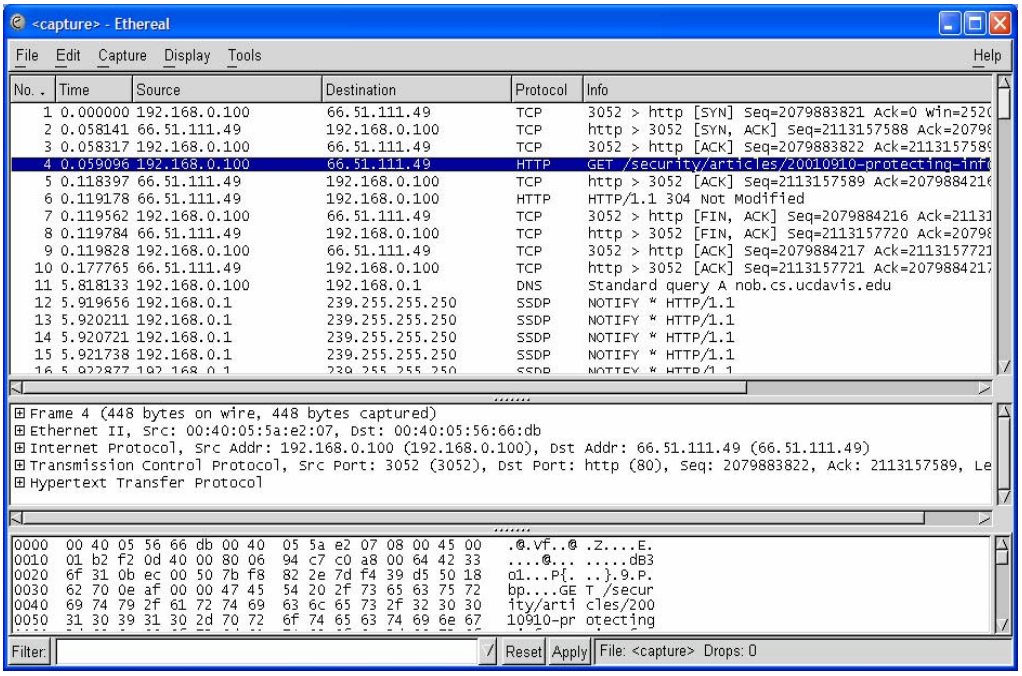

Fig. 3 Ethereal packet sniffer

Quick View Plus output:

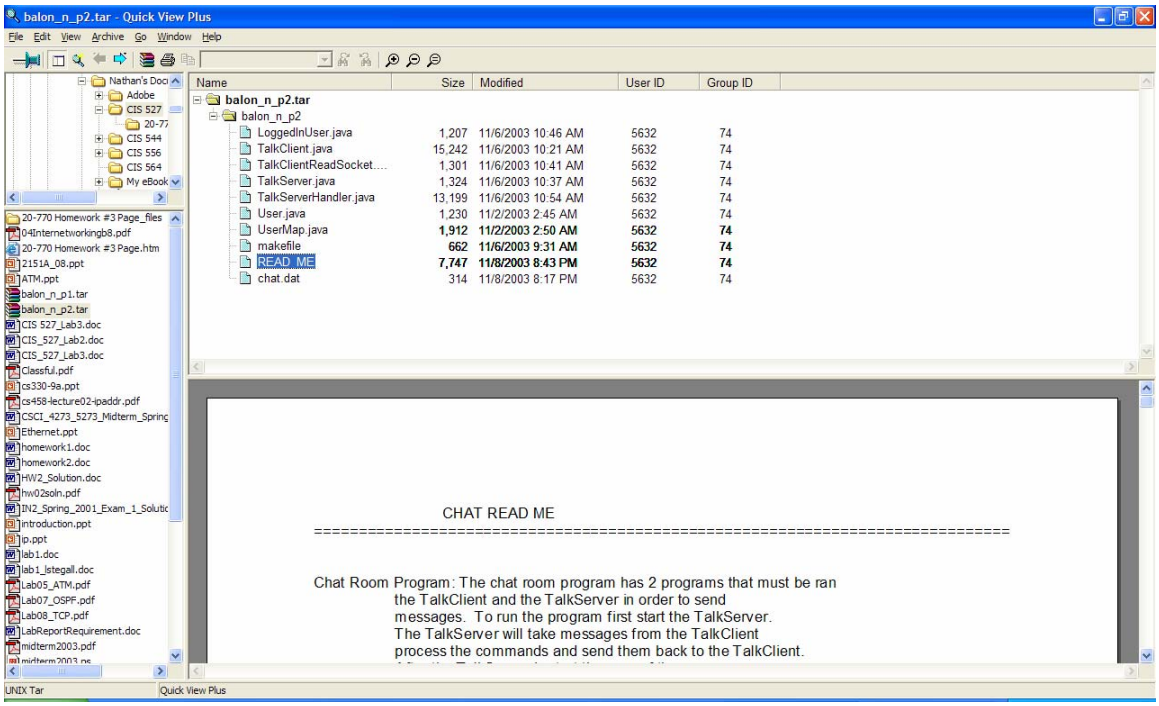

Fig. 5 Quick View Plus

dtSearch, text searching program:

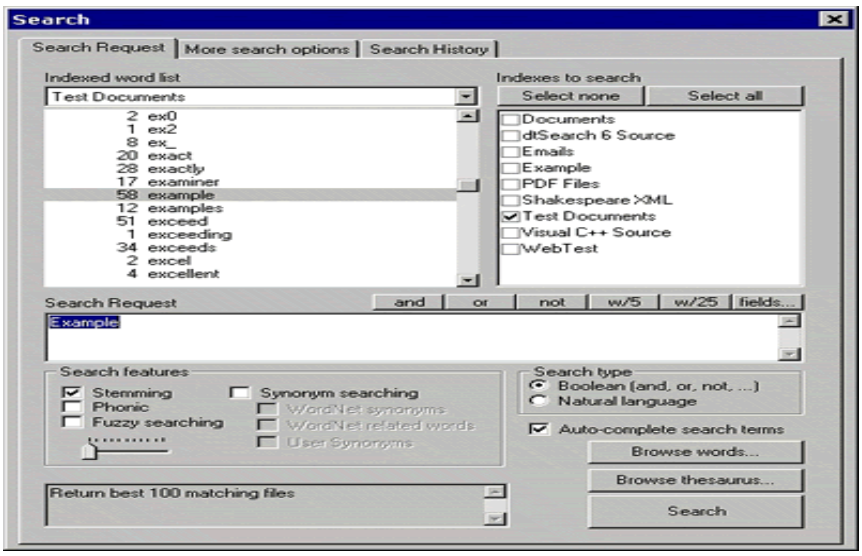

Fig. 4 dtSearch

References

Barber, Richard. "The Evolution of Intrusion Detection Systems-The Next Step" Computer & Security, Vol. 20, Issue 2, 1 April 2001, pages 132-145

Biermann, E., Cloete, E., and Venter L.M. "A comparison of Intrusion Detection systems". Computer & Security, Vol. 20, Issue 8, 1 December 2001, Pages 676-683

Broucek, V. & Turner, P. "Research in Progress: Risks and Solution to Problems Arising from Illegal or Inappropriate On-line Behaviors: Two Core Debates within Forensics Computing" EICAR Conference Best Paper Proceedings. 2002. pp. 206-219. Copenhagen: EICAR.

Caloyannides, Michael. Computer Forensics and Privacy. Boston, MA: Artech House, 2001.

Crayton, Christopher The Security+ Exam Guide: TestTalker's Guide Series. Hingham, MA: Charles River Media, Inc., 2003.

Department of Justice. "Searching and Seizing Computers and Related Electronic Evidence Issues." *Computer Crime and Intellectual Property Section. 17 Dec 2001 http://www.usdoj.gov/criminal/cybercrime/searching.html (23 Non 2003)*

Fisher, Dennis. "Blaster Worm on the Move" *eWEEK Enterprise News and Reviews Online. 12 Aug. 2003http://www.eweek.com/print_article/0, 3048, a=46260, 00.asp* (8 Sep 2003)

Hachman, Mark. "Feds Send Message With Blaster Arrest" *eWEEK Enterprise News and Reviews Online. 29 Aug. 2003 http://www.eweek.com/print_article/0,3048, a=58615, 00.asp* (8 Sep 2003)

Honeynet Project. Know Your Enemy: Revealing the Security Tools, Tatics, and Motives of the Blackhat Community. Reading, MA.: Addision-Wesley, 2002.

Kruse II. Warren G. and Heiser. Jay G. Computer Forensics Incident Response Essentials. Reading, MA.: Addison-Wesley, 2002.

McCarthy, Michael. "Privacy: Can your PC be Subpoened?" *The Wall Street Journal Online. 23 May 2000. http://zdnet.com.com/2100-11-502433.html?legacy=zdnn(23 Nov 2003).*

Melia. John. "Linkin' Logs to Fraud". Security Management. Arlington: Nov. 2002 Vol 46. Issue 11; pg. 46, 6 pgs

Northcutt, S. and Novak, J. Network Intrusion Detection 3rd Edition. Indianapolis, Indiana: New Riders, 2003.

O'Connor, Thomas R. "Criminal Justice Megalinks." 2001. http://faculty.ncwc.edu/toconnor/315/315lect06.htm (22 Nov 2003).

Parker and Waichman, Attorneys and Counselors at Law. "ENRON Stock Fraud" 2002. http://www.enronstockfraud.com (23 Nov 2003).

Salkever. Alex. "Hot on the E-trail of Evidence at Enron" Business Week Online. Jan. 29, 2002. http://www.businessweek.com/bwdaily/dnflash/jan2002/nf20020129_3701.htm

Stallings, William. Cryptography and Network Security: Principles and Practice 3rd Edition. Upper Saddle River, NJ: Prentice Hall, 2003.

Stallings, William. Data and Computer Communications 7th Edition Upper Saddle River, NJ: Prentice Hall, 2004.

Tan, John. "Forensics Readines" @stake, Inc. Cambirdge: MA. 2001.

Reith. Mark., Carr. Clint., and Gunsch. Gregg. "An Examination of Digital Forensic Models". International Journal of Digital Evidence(IJDE) 2002, 1:3. htttp://citeseer.nj.nec.com/577105.html

Robbins, Judd. The Computer Forensics Expert Witness Network. 1999. http://www.computerforensics.net

Wolfe Henry. B. "An Introduction to Computer Forensics: Gathering Evidence in a Computing Environment". Informing Science. June 2001. pg. 569, 7 pgs.

Wright. Jon. "High-tech Holmes". Security Management. Arlington: July 2001. Vol. 45, Issue 7; pg. 44, 6 pgs