

Policies to Enhance Computer and Network Forensics

Alec Yasinsac, *Member, IEEE*, and Yanet Manzano

Abstract— The Internet is growing explosively, as is the number of crimes committed against or using computers. As a response to the growth of computer crime, the field of Computer and Network Forensics emerged. Computer forensics is the art of discovering and retrieving information about a crime in such a way to make it admissible in court. It is after-the-fact in that the only preventative capability of computer forensics is as a crime deterrent. In this paper, we propose enterprise network and computer related policies that will deter computer crime and enhance recovery from attacks by facilitating computer and network forensics.

Index Terms—computer forensics, computer security, policies.

I. INTRODUCTION

As technology has advanced, computers have become incredibly powerful. Unfortunately, as computers get more sophisticated, so do the crimes committed with them. Distributed Denial of Service Attacks, ILOVEYOU and other viruses, Domain Name Hijacking, Trojan Horses, and Websites shut down are just a few of the hundreds of documented attack types generated by computers against other computers usually using an electronic network.

The need for security measures to prevent malicious attacks is well recognized and is a fertile research area as well as a promising practitioner's marketplace. Though there is an immense effort ongoing to secure computer systems and prevent attacks, it is clear that computer and network attacks will continue to be successful. When attacks are successful, forensics techniques are needed to catch and punish the perpetrators, as well as to allow recovery of property and/or revenue lost in the attack.

Computer and Network Forensics (CNF) techniques are used to discover evidence in a variety of crimes ranging from theft of trade secrets, to protection of intellectual property, to general misuse of computers. The ultimate goal of computer and network forensics is to provide sufficient evidence to allow the criminal perpetrator to be successfully prosecuted. As such, CNF efforts are mainly centered in law enforcement agencies.

Any enterprise that depends on, or utilizes, computers and networks should have a balanced concern for security and forensic capabilities. Unfortunately, there is little academic or industrial research literature available on CNF. Forensic techniques are developed by the try and fix method, and few organizations have plans for conducting forensics in response

to successful attacks. We propose several categories of policies that will help enterprises deter computer crime and

will position them to respond effectively to successful attacks by improving their ability to conduct computer and network forensics. These policies correlate to a taxonomy of approaches common to computer attacks. We present policies in the following categories: Retaining Information, Planning the Response, Training, Accelerating the Investigation, Preventing Anonymous Activities and Protecting the Evidence.

II. COMPUTER ATTACK TAXONOMY

Hacking attacks come from many different sources, spanning skill levels from novice to true computer expert. Interestingly, regardless of the skill level, McClure et. al documented a pattern of activity that hackers generally follow, consisting of the stages of probing, invading, mischief, and covering their tracks [9].

Probing is the attacker's reconnaissance. In this step, attackers create a profile of an organization's structure, network capabilities and content, and security posture. It is during this phase that the attacker will find their desired targets and devise a plan to circumvent the security mechanisms that are in place.

Penetration is the next step in the attack. Probing provided enough data to make an informed attempt to access the target enter the target system. For example, if the system has configuration errors, such as access via FTP or trivial file transfer protocols (TFTP) to the full file system, then access is gained quickly through those vulnerabilities.

After gaining initial access, the attacker will use their newly gained status to expand their capabilities within the target system. The objective of this step is to exploit system configuration errors and vulnerabilities to gain additional privileges, such as breaking into root accounts.

Once access is gained and a sufficient level of capability is established, the attacker will progress to the mischief stage. Here they exploit their dubiously gained access level to install trojanized utilities, record passwords, delete files, or whatever malicious behavior that they had in mind.

Before they retreat, the attacker attempts to cover their tracks. If the attacker was able to disable event logging, they reset the configuration to its previous setting. They attempt to clear event logs and hide files that they have left behind.

Examination of these activity patterns provides valuable information in finding ways to stop attacks. They also provide valuable insight into things that can be done to enhance the ability to catch and prosecute attackers that are able to penetrate security mechanisms.

III. COMPUTER AND NETWORK FORENSICS

The evidence found during a forensic investigation may depend on the type of crime committed. For example, in a criminal case, incriminating evidence may be found such as documents related to homicides, financial fraud, drug or embezzlement record keeping, or child pornography. In a civil case, evidence of personal and business records related to fraud, divorce, discrimination, or harassment could be found.

CNF experts are not only hired by lawyers. CNF techniques are sometimes needed by insurance companies to discover evidence to decrease the amount paid in an insurance claim. Individuals may also hire CNF experts to support a claim of wrongful termination, sexual harassment, or discrimination.

Gathering evidence is at the heart of CNF. In computer-related crimes, evidence is accumulated from information collected by different components of the system. The information does not become evidence until a crime is committed and this data is used to find clues. For this reason, we call the data collected by the system potential evidence. There are many sources of potential evidence in computers and network components.

Files are an obvious source of potential evidence. Application output word processors, spread sheets, etc. are almost always valuable potential evidence, as are hidden application files that may contain history information, caches, backups, or activity logs. Occasionally, sophisticated criminals may encrypt incriminating files or attempt to hide them with system-oriented or otherwise unlikely looking names. There are numerous sources of potential evidence, which we discuss more exhaustively in the section dedicated to establishing recommended policies.

Because gathering potential evidence may not be as easy as finding application files on a computer, it requires someone with special skills. CNF experts are specially trained with the skills necessary to successfully carry out a forensic investigation. A forensics expert must have the investigative skills of a detective, the legal skills of a lawyer, and the computing skills of the criminal. Even with these skills, CNF is not an exact science, so there is no guarantee that an expert will find sufficient evidence. However, experienced forensics specialists can find more potential evidence than even the best hackers will expect.

In Figure 1, we present a state transition model of the traditional forensic cycle. In this traditional model, forensic

activity begins after the crime is committed, or later, after the crime is detected. In Figure 2, the cycle begins with forensic activity that allows evidence gathering to begin before crimes occur. The bulk of the after-the-fact activity consists of analysis of evidence already gathered.

IV. POLICIES TO ENHANCE COMPUTER AND NETWORK FORENSICS

A. Retaining Information

1) Copy and Retain Application and Local User Files

The first step that an enterprise interested in being able to catch and prosecute cyber criminals on their networks should take is to institute a policy that systematically stores and retains the contents of application and user files as potential evidence. The value of retaining central backups of local files is well known as a reliability protection technique, and the costs and complexity of storing such backups are declining.

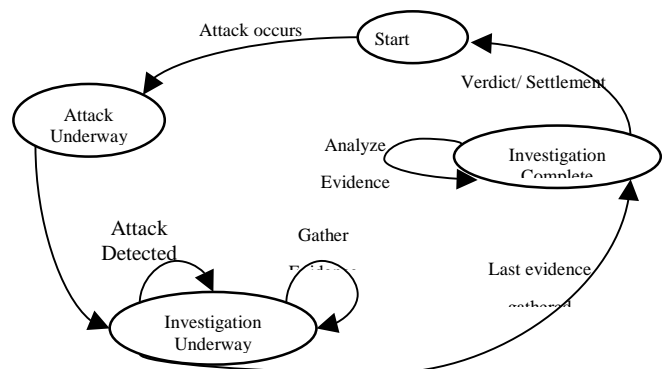


Figure 1

This policy is a must, since application files often contain the best potential evidence of any data on the system.

What may not be as obvious is the necessity to have a corresponding policy that protects the ability to use the backups as evidence in court. While encrypted, deleted, and hidden files often contain valuable evidence, accessing them can cause legal problems, since it may be considered an invasion of privacy.

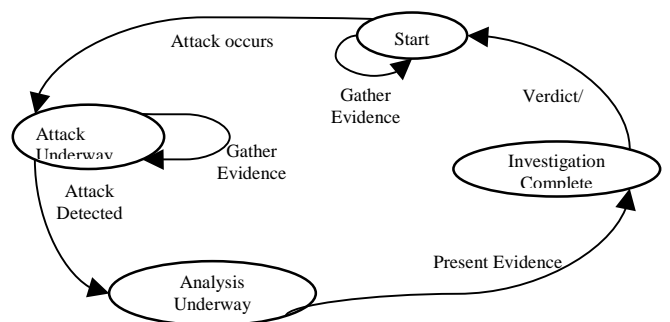


Figure 2

It is necessary for a company to establish a policy that explains that employees have no expectation of privacy, and that the company has the right to access any file in its system without permission, no matter who created the file. Otherwise, the employee may be able to claim to have had a "reasonable expectation of privacy" regarding the files. If it is shown in court that the employee did not know the company could access his files without asking, the court may decide that the evidence was gathered illegally because it violated the employee's privacy and the evidence may not be admissible. Worse yet the employee may turn the situation around and sue the company for invasion of privacy.

2) Copy and Retain Computer and Network Activity Logs

While application files have a clear connection to computer users, system and network information may be equally as telling of user activities. Logged network activity can reveal the actions of a criminal in the clearest detail of any source. Thus, system logs are a vital source of potential evidence.

An enterprise should keep records of network events such as logging in or out of a computer and accessing network services such as remote Telnet, or FTP sessions. These records are very useful during an investigation because they contain information about the activities of a specific user, as well as dates, and times of those activities. This information correlated with internal events such as email or web access, and external events such as phone records, witness testimony, and physical evidence, can provide a Timeline [7]. The Timeline serves as a guide to place the different events in the system, and correlate them to the whereabouts of a suspect, helping either to establish an alibi or to discover incriminating evidence.

The type of information kept in logs depends on the applications available to the user and on the system configuration. Web browsing generates Hypertext Transfer Protocol (HTTP) traffic, while the foundation of electronic mail is the Simple Mail Transfer Protocol (SMTP). HTTP and SMTP traffic contain valuable information to anyone investigating suspect network activity. These protocols can be tracked in network devices.

Email and Web access information should be logged and retained. If an attack occurs and an inside attack is suspected, it may be necessary for the forensic expert to check the employee's email and web access information for traces of incriminating evidence. It may also be necessary to monitor employee's activities for a period of time to gather evidence.

If activity is monitored, the enterprise must address the problem of invasion of privacy. If an employee does not know that the company can monitor his activities, the court may find that the employee had a reasonable expectation of privacy and the evidence gathered may not be admissible. As with divulged files, the employee may sue the company for invasion of privacy. The solution consists of establishing a

policy that says what is and what is not acceptable use of company equipment and that an employee has no expectation of privacy when using company equipment [3].

Network devices, such as routers and servers, are good sources for collecting Internet related evidence. A router is a computer that directs data, in the form of packets, through the network. Servers are computers that answer requests for services, such as list servers, mail servers, and news servers. It is necessary for companies that use these network devices to keep logs of the data packets that flow through them. Keeping records of these data packets allows static monitoring and reproduction of activity across the network.

Telecommunication Control Protocol/Internet Protocol (TCP/IP) packets are of particular interest during a forensic investigation and are a good example of why enterprises should retain network traffic logs. When a message is sent through the Internet, it is formed and transmitted in TCP/IP packets, then reassembled on the other end. Each TCP/IP packet contains a header which includes information about the source and target computer. The addresses are of particular interest during a forensic investigation. The origin address may provide us with information about the attacker's identity, the destination address may provide information about a specific target within a system, and the data may identify the attack itself.

Each TCP/IP packet contains several additional fields that can be useful during an investigation. For example, error checking information can be used to verify that data goes with addresses. Additionally, the header contains six extra bits that are left empty when the packet is sent. Most firewalls are configured to check these six bits and throw away packets that have information in this six bits. However, the information in these bits may be relevant if an attack occurs. So, if a system finds one of these packets, it should redirect it to a safe place and keep a record of it.

An often overlooked source of vital information is system documentation. No matter how experienced the investigators are, they cannot know all the nuances of all makes and models of computer and network hardware and software. Technology advances very fast. Both hardware and software are replaced very quickly, sometimes by entirely new programs, and sometimes by newer versions. Because of this constant change, it is difficult to keep up with the documentation of all the software and hardware in use. It is easy to throw out or lose outdated material, especially when a lot of new material is coming in to replace it. However, the ability to process and examine the potential evidence may be directly tied to special hardware, software, and/or written instructions contained in manuals. These manuals must be retained and accessible to the investigation team.

B. Planning the Response

Even if all the potential evidence policies recommended above are enacted, failure or hesitation to go into action when

an attack occurs may result in greater damage occurring from the attack. Additionally, the opportunity may be lost to catch the perpetrator and quickly restore the loss. Effective CNF requires an effective Attack Response Plan to formally answer the who, what, when, and where questions of CNF.

1) *Establish a Forensics Team.*

Dealing with CNF requires the commitment of a forensic team [5]. According to Robert Graham, a response team should include members from upper management, Human Resources, the technical staff, and outside members. The upper management member can ensure that the decisions made by the forensic team are balanced with the overall goals and best interests of the enterprise and that the decisions of the team have appropriate weight. Because of the personnel issues involved, there should be a member from human resources department. There should also be a member of the Information Technology (IT) staff on the forensics team. Security issues are often handled separately from normal IT activity. In such a case, the forensics team should work hand in hand with the IT department.

2) *Establish an Intrusion Response Procedure*

The enterprise should establish a step-by-step guide that employees can follow if an attack is suspected. A mistaken response by an employee that detects an attack can damage any subsequent CNF effort. For example, many attacks contain "track covering" routines [2] that are triggered by as simple an action as a key stroke. These routines may destroy hard disk drives or delete system logs.

Additionally, well-meaning users are likely to compromise potential evidence by accidentally violating some chain of custody or other legally inappropriate action. The guided response of any employee to a suspected attack should be clearly spelled out in the enterprise intrusion response procedure and should begin by requiring users to simply notify the CNF investigative team. The procedure should include who to contact, how to contact them, and what information to report.

3) *Formalize the Investigative Procedure*

The procedure to follow during a preliminary investigation is similar to that followed by a computer forensics expert during a forensic investigation. However, since the preliminary investigation is not as rigorous as the investigation carried out by a computer forensics expert, the procedure for it is also less rigorous. The goal here is not to restrict the investigators from freely utilizing their forensics skills. Rather, it is to provide a baseline of activity that must be accomplished when intrusions are detected.

A potential preliminary investigation procedure for a suspected crime involving an enterprise owned computer may contain the following actions:

1. Determine the exact nature of the computer crime or

abuse and whether it is ongoing or complete.

2. Make two exact copies of affected disk drives using a disk imaging tool. Conduct CNF analysis on one copy and retain the other so that the evidence remains intact, while allowing the employee to return to work on the production system(s).
3. Copy computer and network logs
4. Limit access to affected systems

C. *Training*

Any computer crime-aware enterprise must train its personnel to be able to carry out the CNF response plan. There should be training for all computer users to make sure they know the CNF procedures that are to follow and how to use them. There should also be special training for the response team.

1) *Training the Response Team.*

Once a response team is assembled, the members of the team need to be prepared for the kinds of decisions they will have to make. For example, one of the more difficult questions to deal with during an attack, says Michael Anderson, a former IRS high-tech investigator who founded New Technologies Inc. in 1997, is "To pull the plug or not? Is it nobler to lose all temporary files by cutting off power without a proper shutdown? This is a problem if criminals use an uninterruptible power supply and do all their work in memory. Or is it nobler to shutdown properly and risk a booby trap that wipes out data at the touch of a key? [11]"

Most of the time, this is a no win situation. The best we can do is calculate which will cause the minimum losses. For example, if the company under attack is an online trading service, pulling the plug might be the best answer. Going off-line on such a service will certainly disrupt business, but may be better than having hackers trading away the stock of valued clients.

2) *Training The Investigative Team.*

The investigative procedure that follows an attack needs to be carried out with precaution and the investigative team must have computer forensics skills. We have to make sure the investigative team members have the abilities necessary to follow the investigative procedure.

During a preliminary investigation, the investigative team will use these skills to determine whether an attack actually occurred, and if possible to identify the crime by determining how it was committed and who did it, and find the evidence left behind. In order to do this, the investigative team needs to understand the steps followed by the attacker so that they can be retraced.

The team must also know where to find possible evidence. It is essential that forensics investigators be expert in computer and network administration so that they know the technical in's and out's of the target systems. They should also

receive training in hacking techniques and be familiar with known and generic vulnerabilities in systems.

Finally, forensic investigators must be well-versed in the legalities of evidence gathering. Many classic evidence gathering techniques are not usable to a computer investigator because of the nature of computer and information systems. The chief characteristic is the rapid state of change. For example, log files may be changed or updated hundreds of times per day. To be usable in court, the investigator must undeniably show that, through all the updates, the log file that is presented:

1. Contains information that relates to the alleged crime
2. Has not been tampered with
- 3) *Training for All Personnel That Use Computers*

It is necessary to train all personnel in company security policies. The general personnel should be familiarized with the response procedure. The last step of the response procedure is to alert the response team, so it is necessary for employees to also be familiar with the structure of the response team. No matter how much planning we do, we cannot ensure the success of the response unless we test the procedure under real circumstances. It is not advisable to wait until an attack occurs to try the response procedure. It is instead advisable to simulate an attack, and put the response to the test. This way the employees, as well as the response team, will have some experience when a real attack occurs.

D. Accelerating the Investigation

Once an investigation is launched, it must be a goal to conclude as quickly as possible. An investigation interferes with company activities, especially since the equipment in question may not be available for use. Additionally, the longer the investigation takes, the greater the chance that potential evidence will be destroyed or compromised. Finally, the problem needs to be corrected as soon as possible to allow recovery of whatever was lost and to prevent connected and future attacks.

The following policies facilitate forensic investigations, allowing potential evidence to be gathered with the least possible resistance.

1) Prohibit Personal File Encryption

Encrypted files should be prohibited in a company system unless specifically authorized. When a forensic investigation is in progress, one of the first steps is to recover application files. Personal encryption technology may be used when an attacker does not want anyone to have access to the content of a file. Cryptanalysis of encrypted files is a very difficult and time consuming process. If the encryption system was sufficiently strong, it may not be possible to ever recover the original contents. During an investigation, we cannot count on the owner to give us the key to decrypt the file, so it is wise to avoid this situation.

2) Prohibit Disk Scrubbing Tools and File Shredding Software

Deleted files are also a source of potential evidence. The process of recovering deleted files is usually not difficult or time consuming. However, it can be made very difficult and time consuming by using scrubbing tools and shredding software, which are programs designed to destroy information. They wipe clean the targeted space by writing over clusters several times. In some cases, even after the clusters are overwritten several times, the data or at least part of it can be recovered; however, the time spent in data recovery increases greatly. So, in order to avoid unnecessary delays and costs for the recovery of deleted files, it is advisable for the company to prohibit the use of this kind of software.

3) Utilize Data Indexes

The first step of an investigation is to check all the potential evidence collected. This is easier said than done, especially since extensive logging produces a great volume of data. The amount of time to search through each entry in a log file is analogous to the amount of time necessary to go through all the books on a shelf one by one. When we are in a library we don't conduct an exhaustive search for a desired book; rather, we use catalogs. We search by indexes and once we find the book we want, we lookup it up in the shelves.

A similar concept can be used to cut down the time necessary to inspect all the potential evidence. The idea is to create an index of the data kept in logs for investigative purposes only, and refer to the original information only when necessary. One way to build this kind of index is by keeping summaries of the log data collected.

The Internet gets faster every day, and millions of packets flow across the network. As a result, the log files contain massive amounts of information about packet flow. In order to search through these logs faster during an investigation, we create summaries that include the most relevant information from each packet and use these summaries as indexes. Examples of the type of information we may want to include in the summaries are the date, source/origin, destination, service port, and duration of TCP connection occurring on the network, the URL from every web request, the origin and destination of SMTP sessions, and the user identification from all Telnet, FTP, and rlogin sessions [12].

4) Utilize Information Fusion

An invaluable source of potential evidence is the output of Intrusion Detection Systems (IDS). IDSs monitor the activities in an environment and then determine if the activities represent an attack, or are a legitimate use of the environment. An IDS produces Indications and Warnings (IW) values that are analyzed to determine if an attack has occurred. The output from the IDS is also a large volume of data.

One way to speed up the inspection of this output is to use information fusion techniques to correlate all the values of warning and indication [13]. This allows the investigation to go much faster since the investigative team can look at the entire representation of the events that occurred instead of trying to synthesize bits and pieces.

Two techniques used to fuse information are single-object and multiple-object information fusion. Given IW values for a component from different intrusion detection techniques, single object fusion determines a composite IW value for the component. Multiple-object information fusion uses composite IW values from multiple components to determine a system level IW value [13]. The best technique depends on the output from the intrusion detection system.

E. Preventing Anonymous Activities

One negative result of the Internet explosion is the threat that it creates to personal privacy. This threat is being countered with a myriad of tools to allow users some level of anonymity on electronic networks.

Anonymity is a valuable and necessary concept to protect personal privacy on the Internet. It can help systems to resist traffic analysis, eavesdropping, and other attacks by preventing the transport medium from knowing who is communicating with whom. A network intruder can find out that communication is taking place, but not the source or destination parties.

Unfortunately, when used by a clever intruder, anonymity tools can be difficult for an CNF investigative team to overcome. For an investigation, we need to know when, how, and who was in the system, which is very difficult to do if anonymity is allowed. We need to find a balance between privacy and forensic capabilities.

1) Onion Routing

"The Onion Routing research project is building an Internet based system that strongly resists traffic analysis, eavesdropping, and other attacks both by outsiders (e.g. Internet routers) and insiders (Onion Routers themselves). It prevents the transport medium from knowing who is communicating with whom; the network knows only that communication is taking place [10]." A positive aspect of onion routing is that it can be installed at different points in the network. It can be installed in each of the user machines, in the router, in the firewall or at some point in the Internet. If it is installed at the firewall, it would allow the enterprise owner to see everything that goes on behind the firewall, but it will still provide anonymity for the company outside the firewall.

2) Require Date, Time, User Stamps in File

During an investigation, time, date, and suspect are three key elements. When an investigation is in progress, the investigator needs to know what date a file was created, or

modified, or deleted, and who did it. This is a key point to be able to determine what happened exactly. Establishing and enforcing a policy of enabling this automatic administration capability of most application packages can prove invaluable to the investigative team.

3) Use Strong User Authentication

No unauthorized access to the system should be allowed. Whenever a user tries to connect to the system, the enterprise must make sure that it is a valid user. Passwords are the most widely used method of authentication today. However, passwords are vulnerable to attack. Strong authentication based on encryption is key to enabling effective CNF.

4) Use Strong Access Control Mechanisms.

Authorization identifies entities, but does not control who sees or does what on the system. Access control is a mechanism for limiting use of resources to authorized users [8]. This process establishes a relationship between users and files or other resources. We can establish the permissions on each resource, specifying which users have access to the resource, or we can establish the permissions on the users, specifying which resources each user can access. This policy provides a start point for the investigation, since we know that if an attacker modified a file, it had to do it through one of the people that had permission to access that file. Instead of checking every employee to find a start point, we search the employees that have access to the particular file.

F. Protect the Evidence

Protecting the evidence is a key step in computer forensics. In order for evidence to be useful, we must be able to prove its authenticity and integrity. We mentioned earlier that potential evidence could be compromised by being handled improperly, but we must also consider the damage the data might suffer maliciously after it is gathered, e.g. by an attacker trying to destroy evidence of a crime or an employee trying to erase incriminating data from log files.

1) Exercise Rigid Control Over Administrative Access for Systems Housing Potential Evidence

A cornerstone of effective CNF is to have strong authentication and integrity services that controls administrative access to network devices. While all computer criminals are not sophisticated, many will be, and weak control of administrative access is a blueprint for disaster in protecting potential evidence.

2) Encrypt Evidence Files and Connections

The evidence gathered should be protected at least with a password. However, password protection alone may not be enough to guarantee the security and integrity of the data. Passwords can be broken using password cracker software, so they are not very reliable. It is preferable that we use encryption. "Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access

to a secret key or password that enables you to decrypt it [1]." Potential evidence such as log files, IDS output, and the data indexes should be encrypted and protected with strong authentication.

3) Apply Strong Integrity Checking Technology.

Just protecting the data is not enough. To use the potential evidence in court, we must be able to show that the evidence has not been corrupted. To accomplish this, periodic integrity checks should be conducted on the data collected.

V. CONCLUSION

Computer related crime is growing as fast as the Internet itself. Today, enterprises focus on implementing preventative security solutions that reduce vulnerabilities, with little concern for systematic recovery or investigation. We propose six categories of policies that will enable or facilitate after-the-fact action that can reduce the impact of computer crime and can deter computer crime from occurring.

Some of the policies that we propose are simple actions that responsible network managers already engage as a matter of system reliability or as part of a disaster recovery procedures. The focus on computer and network forensics distinguishes these policies from backup and recovery needs. The procedures for CNF require systematic application and detailed documentation, else the information may not be admissible in court. Further, backup and recovery procedures

routinely ignore temporary information and other important sources of potential evidence.

Moreover, CNF is much broader than just providing ready sources of potential evidence. An enterprise that is serious about CNF will establish a CNF organization and a training plan, complete with CNF policies and procedures.

As people get more and more comfortable with computers, and technology advances, society becomes more computer dependent. In an era where everything from the stock market to air traffic control is managed by computers, security becomes a survival issue. In today's society, computer crime is a serious problem. Preventive measures are not enough anymore, we must find a way to catch and prosecute computer criminals, and computer and network forensics is the gateway to archive it.

We should not leave everything to computer forensics experts. If we are going to find a solution to the computer crime problem, it will be through a collaborative effort. Everyone from individual users, to company owners have to get involved. This paper proposes policies to enhance the forensics of computer security by helping experts in the field do their job faster and more efficiently. It is up to the companies and users to adopt these policies according to their needs.

REFERENCES

- [1] AOL COMPUTING'S WEBOPEDIA, AOL 1996. [HTTP://AOL.PCWEBOPEDIA.COM/](http://AOL.PCWEBOPEDIA.COM/)
- [2] "COMPUTER EVIDENCE PROCESSING," NEW TECHNOLOGIES INC., APRIL 2000. [HTTP://WWW.FORENSICS_INTL.COM/ART5.HTML](http://WWW.FORENSICS_INTL.COM/ART5.HTML)
- [3] "COMPUTER FORENSICS," SC MAGAZINE, OCTOBER 1998, [HTTP://WWW.INFOSECNEWS.COM](http://WWW.INFOSECNEWS.COM)
- [4] "ELECTRONIC FINGERPRINTS," NEW TECHNOLOGIES INC., APRIL 2000. [HTTP://WWW.FORENSICS_INTL.COM/ART2.HTML](http://WWW.FORENSICS_INTL.COM/ART2.HTML)
- [5] "FAQ: NETWORK INTRUSION DETECTION SYSTEMS," VERSION 0.8.3, MARCH 21, 2000. [HTTP://WWW.ROBERTGRAHAM.COM/PUBS/NETWORK_INTRUSION_DETECTION.HTML](http://WWW.ROBERTGRAHAM.COM/PUBS/NETWORK_INTRUSION_DETECTION.HTML)
- [6] FERBRACHE, DAVID AND STURT MORT, MALICIOUS SOFTWARE AND HACKING, INFORMATION SYSTEMS SECURITY, VOL.6, NO.3, P. 35_54, 1997.
- [7] CHET HOSMER, "TIME LINING COMPUTER EVIDENCE," 1998 IEEE INFORMATION TECHNOLOGY CONFERENCE, INFORMATION ENVIRONMENT FOR THE FUTURE, 1998.
- [8] KAUFMAN, CHARLIE, RADIA PERLMAN, AND MIKE SPECINER, NETWORK SECURITY, PTR PRENTICE HALL, NEW JERSEY, 1995.
- [9] MCCLURE, STUART, JOEL SCAMBRAY AND GEORGE KURTZ, HACKING EXPOSED, MCGRAW_HILL, CALIFORNIA, 1999.
- [10] P. SYVERSON, M. REED, AND D. GOLDSHLAG, "ONION ROUTING AND ACCESS CONFIGURATIONS," DARPA INFORMATION SURVIVABILITY CONFERENCE AND EXPOSITION 2000, VOL.1, PP 34_40, IEEE COMPUTER SOCIETY PRESS
- [11] RADCLIFFE, DEBORAH, "HANDLING CRIME IN THE 21ST CENTURY", CNN.COM, DECEMBER 15, 1998. [HTTP://WWW.CNN.COM/TECH/COMPUTING/9812/15/CYBERSLEUTH.IDG/](http://WWW.CNN.COM/TECH/COMPUTING/9812/15/CYBERSLEUTH.IDG/)
- [12] RANUM, MARCUS J., NETWORK FORENSICS AND TRAFFIC MONITORING, COMPUTER SECURITY JOURNAL, COMPUTER SECURITY JOURNAL, VOLUME XII, NOVEMBER 2, 1997.
- [13] YE, NONG, JOSEPH GIORDANO, JOHN FELDMAN, AND QIU ZHONG, "INFORMATION FUSION TECHNIQUES FOR NETWORK INTRUSION DETECTION," 1998 IEEE INFORMATION TECHNOLOGY CONFERENCE, INFORMATION ENVIRONMENT FOR THE FUTURE, 1998