International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article | **May 2014**

Computer and Network Forensics: Imaging Digital Evidence

Yatan Dahiya
M.tech (Computer Science & Engineering),
Shri Baba MastNath Engineering College
Asthal Bohar, Rohtak, Haryana, India.
Maharshi Dayanand University,
Rohtak, India

Sunita Sangwan
HOD, Department of CSE
Shri Baba MastNath Engineering College
Asthal Bohar, Rohtak, Haryana, India.
Maharshi Dayanand University,
Rohtak, India

Abstract–

As the Internet is growing, the number of crimes using internet are simultaneously increasing. The cyber crime can be done in the form of 0s & 1s (bits & bytes) or electronic or digital form. Computer and Network Forensics field has been emerging after the growth of cyber crime. To make a crime admissible in court one has to discover and retrieve all the information about it and such an art is known as Computer Forensics. It gathers all the evidences during or after a crime. Crime can easily be prevented by the preventative capability of computer forensics. In this paper, we propose the computer policies that will discourage computer crime and enhance recovery from attacks by facilitating computer and network forensics. We will here also discuss about the cyber forensics. We'll emphasize on providing security to digital evidence.

Index Terms-Computer forensics, Computer security, Computer policies, Digital evidence, and Cyber forensics.

I. INTRODUCTION

With the advancement of technology, computers have become incredibly powerful. Unfortunately, as computers get more complicated, the crimes devoted with them are being done. Documented attack types generated by computers against other computers using an electronic network websites shut down are just a few of the hundreds. The major security measures are needed to prevent malicious attacks. Forensics techniques are then needed to discover and punish the perpetrators, when attacks are booming; it also allows recovery of property or proceeds lost in the attack. Computer and Network Forensics (CNF) techniques are used to catch evidence in a variety of crimes ranging from theft of trade secrets, to protection of intellectual property, to general misuse of computers. Forensics for computer networks is extremely difficult and depends completely on the quality of information you maintain. Computer forensic is a process of applying scientific & analytical techniques to computers, networks, digital devices & files to discover or recover admissible evidence.

Computer forensics is the integration of the assessment, identification, seizure, preservation, imaging, analysis of digital evidence to find the related data and/or the root cause of the incident / crime. Evidence might be required for a wide range of computer crimes and misuses. Forensic techniques are developed by the try and fix method, and few organizations have plans for conducting forensics in response to successful 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 AND NETWORK FORENSICS

Computer Forensics is not just about Computers, it is essentially about:

- Correct processes of investigation
- Rules of evidence
- Integrity of evidence
- Clear and concise reporting of factual information
- Provision of expert testimony

Network forensics is the process of analyzing network traffic. After-the-fact analysis of transaction logs are Real-time analysis via network monitoring.

- Sniffers
- Real-time tracing

Network forensics is scrutinizing network traffic and logs to identify and locate the suspicious system, Log Analysis, Web Access Analysis and e-mail Analysis.

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. 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.

- Floppy Disk(s)
- Hard Drive(s)
- CD, DVDs
- USB Memory Devices
- Mag. Tapes
- RFID Tags
- PDAs
- Smart Cards
- Web pages
- Voice mail
- e-Diary
- Scanner, Printer
- Fax, Photocopier M/c
- Digital Phone Set
- iPods
- Cell phone
- Digital Cameras
- Configuration settings of digital devices

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.

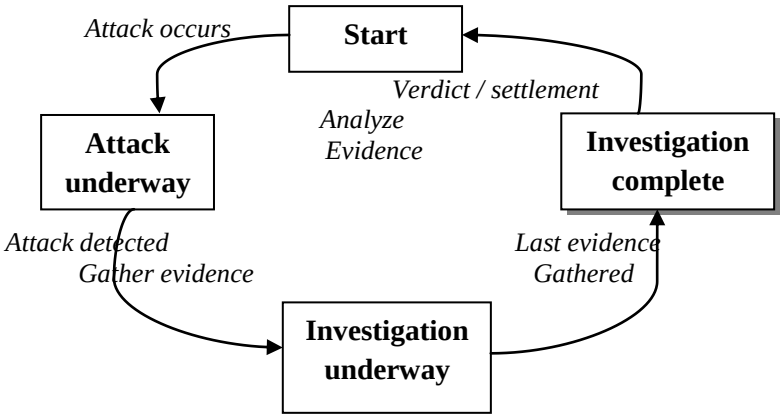

Figure 1: *Traditional forensic cycle*

III. 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.
While encrypted, deleted, and hidden files often contain valuable evidence, accessing them can cause legal problems, since it may be considered an attack of privacy. 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.

2) Copy and Retain Computer and Network Activity Log

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. 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 contains 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. 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 or 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.

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.

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.

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.

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. The chief characteristic is the rapid state of change.

D. 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 cleaver intruder, anonymity tools can be difficult for a 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.

E. 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 a strong authentication and integrity service 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.

IV. CYBER FORENSICS

Cyber forensics basically has two parts:

- Computer Forensics
- Mobile Forensics

Subcategories of Computer Forensic Analysis

❖ ***Storage Media Forensics***

Storage Media Forensics is the process of acquiring and analyzing the data stored on some form of physical storage media. It includes recovery of hidden/deleted data/files.

❖ ***Source Code Forensics***

It is to analyze Software Source Code for malicious signatures and determine software ownership or software liability issues.

– Review of actual source code.

–Examination of the entire development process, e.g., development procedures, documentation review, and review of source code revisions.

Cyber Forensic Process for Analysis of Digital Evidence

- Identification
- Acquisition / Seizure
  - Integrity (Hashing) checksum
  - Imaging
- Analysis
- Documentation
  - Report preparation for Judiciary

V. DIGITAL EVIDENCE

It is Latent, like fingerprints or DNA and extremely fragile & resilient; it can be altered easily and damaged or destroyed. It can transcend borders with ease & speed (networked systems). Evidence basically is in digital form or we can say that Data recovered from digital devices **or** Data relating to digital devices are also digital evidence.

Some of the common practices – curiosity may destroy digital evidence. Direct analysis will make it unacceptable in a court of law.

Digital Evidence should be –

1. Admissible, conform to legal requirements
2. Authentic, relevant to the case
3. Complete, & not just extracts
4. Reliable - collected & handled appropriately
5. Believable & understandable

Types of Digital Evidence

❖ *Volatile (Non-persistent)*

Memory that loses its contents, if power is turned off; e.g. Data stored in RAM (semiconductor storage). System BIOS on CMOS RAM - battery powered.

Volatile Data Collection Process

- Collect uptime, date, time, and command history for the security incident.
- As you execute each forensic tool or command, generate the date and time to establish an audit trail.
- Begin a command history that will document all forensic collection activities.
- Collect all types of volatile system and network information.
- End the forensic collection with date, time, and command history.

❖ *Non-volatile (Persistent)*

No change in contents, even if power is turned off; e.g. Data stored in a tape / floppy disk / hard disk (magnetic storage), CD / DVD (optical storage), ROM (semiconductor storage; USB Thumb Drives -EEPROM).

VI. IMAGING OF DIGITAL EVIDENCE

Direct Analysis of Org. Digital Evidence (Strictly Forbidden)

We will make change in MAC (Modified, Accessed, and Created) details – Date & Time of a file. Analyzing a live file system / original evidence also changes the state of the evidence (MAC details). Any analysis on the original digital evidence makes it tampered digital evidence. Digital evidence will not be accepted by court and render it useless

• ***Solution*** – analyze a clone or image of the original digital evidence.

Logical Vs Physical Backup

• What is logical back up?

A logical backup copies the active directories and file of a logical volume. It does not capture other data that may be present on the media such as deleted files or residual data stored in the slack space.

•What is forensic imaging (physical backup) or imaging?

Generating a bit for bit copy of the original media including free space and loose space, also called physical back up.

Advantage of the imaged Digital Evidence

- Analyzing a imaged digital evidence
- Preserves the original evidence
- Prevents inadvertent alteration of original evidence during examination
- Cloned image may be created again if required

Imaging

- Always ensure that the integrity & security of the org. evidence is maintained.
- Suspected org. evidence (hard disk) must be connected through a write blocker.
- The destination disk should be a freshly wiped (Sterilized) disk, even if it is new.
- Entire disk imaging is better than partition (Volume) wise imaging.
- Every action should be documented.
- Document the Make, Model, Serial No and Size of the hard
- disk in to multiple forms like Chain of Custody, Seizure Note, etc as required
- Note down the SIZE (or Capacity) of the Suspected (Source) hard disk and always connect it through Hardware
- Write blockers.
- Be cautious when you choose the SOURCE & DESTINATION hard disks in the Forensic Imaging software.
- Always select the Forensic Image as RAW Image Type which could be acceptable by all the Open / Commercial Forensic software applications
- Get appropriate (Same or larger) size of the new sterilized hard disk for storing the forensic image of the suspected hard disk & document the details such as Make, Model, Serial No and Size.
- Once imaging (Acquisition) is over, document summary report of the acquisition process. (Acquisition hash value of the disk)
- On completion of the process, disconnect the destination hard disk, label it carefully and preserve separately.
- Once imaging is over then preserve it in a safe location. (Best option is to make multiple copies of the image).
- Keep your suspected (Source) hard disk and imaged (Destination) hard disk separately into Anti -static covers and label accordingly. Send these to Cyber Forensic Lab preferably by a person and not by Post / Courier.

VII. 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.

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.

REFERENCES

[1] AOL COMPUTING'S WEBOPEDIA, AOL 1996. http://AOL.PCWEBOPEDIA.COM/
[2] "COMPUTER EVIDENCE PROCESSING," NEW TECHNOLOGIES INC., APRIL 2000. http://WWW.FORENSICS_INTL.COM/ART5.HTML
[3] "COMPUTER FORENSICS," SC MAGAZINE, OCTOBER 1998, http//WWW.INFOSECNEWS.COM
[4] "ELECTRONIC FINGERPRINTS," NEW TECHNOLOGIES INC., APRIL 2000. 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
[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] "COMPUTER FORENSICS – AN OVERVIEW" BY DOROTHY A. LUNN, SANS INSTITUTE; http://WWW.GIAC.ORG/PRACTICAL/GSEC/DOROTHY_LUNN_GSEC.PDF
[12] "FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT" BY NATIONAL INSTITUTE OF JUSTICE, USA; (http://WWW.OJP.USDOJ.GOV/NIJ)