International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 2, June 2014, PP 14-25
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Developing and Enhancing the Security of Digital Evidence Bag

Yatan Dahiya
M.Tech (Computer Science & Engineering)
Shri Baba MastNath Engineering College
Asthal Bohar, Rohtak, Haryana, India
Maharshi Dayanand University, Rohtak
yatan90@gmail.com

Ms. Sunita Sangwan
HOD, Department of CSE
Shri Baba MastNath Engineering College
Asthal Bohar, Rohtak, Haryana, India
Maharshi Dayanand University, Rohtak
Kashisuni5@gmail.com

Abstract: *The Internet is growing explosively, as is the number of crimes committed using computers. In a case of cyber crime the evidence is in electronic or digital form (0s & 1s; bits & bytes). 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 the art of gathering evidence during or after a crime. 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 and also discuss about cyber forensics. The main focus of this paper is providing security to digital evidence.*

Keywords: *Computer forensics, computer security, policies, Digital Evidence, Cyber forensics.*

1. INTRODUCTION

As technology has advanced, computers have become incredibly powerful. Unfortunately, as computers get more sophisticated, so do the crimes committed with them. 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. When attacks are successful, forensics techniques are needed to catch and punish the perpetrators, as well as to allow recovery of property 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. 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.

2. NETWORK SECURITY AND FORENSICS

Networks are exposed to internal and external threats. These threats can use the victim's network as a base for launching attacks on associated networks such as denial of service (DoS). Another potential threat can be an alteration of information through the victim's network. Internal trusted participants can also launch attacks on the network by abusing their level of privilege.

This requires the development and maintenance of proper situational awareness. Network forensics is defined as the monitoring, recording, and analysis of network traffic and events. It is

performed in order to discover the source of security breaches as well as providing information to assist in the response to recovery from attacks or other potential problems. One key role of the forensic expert is to differentiate repetitive problems from malicious attacks.

There are three groups of people who are interested in the network forensics area:

- Law enforcement
- Operators of critical infrastructure
- Education systems.

The two main types for network forensics are:

- General network forensics
- Strict network forensics

The purpose of general network forensics is to obtain malware attack sig-natures and utilizes them for an intrusion detection system (IDS) and as an aid to firewall configuration. This is to enhance the security posture within the network; while the strict network forensics obtains the evidence to be used in a court of law. Currently, forensic methods are known as dead forensic (after the cybercrime fact); and live forensic (during the cybercrime fact). This thesis proposes to extend current network forensic techniques by the introduction of a DEB in order to enhance analysis techniques.

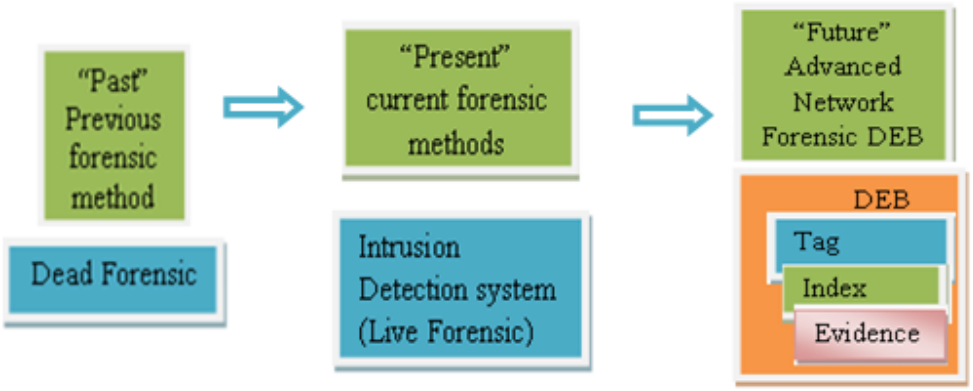

Fig1.1. *Logical Methods in the Development of Forensic Practices*

3. EVIDENCE CAPTURING TECHNIQUES

3.1. Live Incident Response Forensic

When acquiring files selectively from a live system, greater attention should be given when creating a forensic duplicate. This is because when acquiring files from a live system action taken may alter the original evidence. It is also important to gather volatile data at an early stage of a malware incident. This can pro-vide valuable leads, such as details about remote servers that the malware is communicating with. There are various tools in the operating systems themselves which can be used to obtain volatile data. For instance, Linux commands are useful for collecting volatile data from a live system. However, one can argue that if a system can be compromised by malware it cannot be trusted. Therefore, in reality it can be said no system can be trusted. This makes it necessary to use a toolkit of utilities for capturing volatile data that has minimal interaction with the subject operating system. The use of such utilities is critically important and can reveal hidden information by a root kit. In this paper, an overall methodology for preserving volatile data will be briefly demonstrated on a Linux machine in a forensically sound manner. This will be implemented by using a case example within the pro-posed testbed to demonstrate the strengths and shortcomings of useful Linux commands from a forensic perspective. These commands must be tested and assessed before trying to achieve the goal of combining them into one group.

3.1.1. Volatile Data Collection Techniques

Existing tools and commands can be utilized when conducting a live forensic technique to collect volatile data such as uptime, date, time, users logged into the system, open ports and listening applications, lists of currently running processes, registry information, and attached devices (this can be important when having a wireless attached device which may not be obvious at the crime scene) and command history for the security incident. The following are some of the useful Linux commands that can be used to obtain live evidence although they tend not to perform in a forensically sound manner.

- *Script:* The script catches data in memory and writes the full recorded information when a process is terminated. By default, the script commands save data to the current location.
- *Who:* Identify users logged onto the system. Use who or w to determine who is currently logged in. Verify that a legitimate user established each session.
- *Netstat:* Determine network connections and activity. Use netstat to view open connections to the computer.
- *Ps:* Use ps to view the processes running on the computer, and try to determine if any unusual processes are running.
- *Lsof:* Use lsof to determine what files and sockets are being accessed.

3.2. Typical Capturing Evidence Processes

3.2.1. Selective Capturing Process

Selective imaging is a means of acquiring the evidence on a selective basis. When acquiring evidence, a decision should not be made to acquire the whole information of a media but only the required (relevant) amount. This has not always been so, but now, according to official good practice guidelines of The Association of Chief Police Officers in the UK (ACPO) it is now recognized that \partial or selective file copying may be considered as an alternative" when it may not be practical to acquire everything. According to, there are three types of selective imaging. They are:

- Manual selective imaging: Is when the investigator manually specifies the required files in order to obtain them.
- Semi-automatic selective imaging: Is when the investigator specifies a particular type of files or few categories. This can be based on the file extension, file hash or file signature (e.g. hex signature).
- Automatic selective imaging: Is when the investigator specifies the source and destination of the evidence required and commences the automatic capturing process.

When obtaining evidence by any of the aforementioned (selective imaging processes), one of the main difficulties encountered is recording the provenance of an item of information. In order to record such information there are some metrics that can be used to locate a file. This location can be specified by one of the following modes:

- The root folder including partition reference number
- The logical cluster of the required file
- The physical sector of the required file on the disk

One of the things to bear in mind with these modes is the attributes of provenance must meet the following criteria:

- Unique
- Unambiguous
- Concise
- Repeatable

It can be argued that in its own way each method meets these criteria. It will depend upon the technical knowledge of the person trying to understand it.

For example the general public, including even a judge or legal professional is likely to be more familiar with a folder location than a more technical disk sector or cluster reference.

3.3. Intelligent Capturing process

Intelligent imaging which is the process of embedding the knowledge of experts into an intelligent system is a good option for investigators who are not technically proficient. In order to obtain the relevant evidence this technique allows the investigator to select the type of inquiry that is being conducted. However in the case of a fraud or intellectual property theft, the investigator may not be able to recognize the type or location of the required files. The question then becomes how can the expert's level of intelligence be recognized and thus be embedded in a tool. Another question is whether all the relevant data can be captured by the tool.

3.4. Digital Evidence Bags (DEBs)

The traditional forensic process is the process of capturing an image of the original material. This capture of the evidence can be either in static or real-time - `live' forensics. A new concept for a container for digital evidence has been recently introduced. This can be used as a wrapper which provides professionally obtained evidence and an audit trail of previously performed actions.

When obtaining such evidence the actual forensic task is to capture an image of the original media. There are two problems that relate to the actual containers that contain the captured information:

1. The tool has to process and analyze the captured forensic image as a single entity.
2. The forensic utility captures the information into different format containers. That is not to say a single format container should not be used to capture evidence but the wrapper (which is the DEB) used must be consistent when capturing and storing information.

It is not uncommon to see a single log file from an architecture of the form being modeled in this thesis to be of 350 Gb of data over one week. This is compounded by the fact that forensic tools currently in use are being stretched beyond their capabilities. This results in the whole network forensic process becoming problematic. The situation is still difficult even when taking into account the diverse number of devices that process digital information and which are capable of having digital information extracted from them. This means that forensic practitioners have to learn, understand and use even more specialized applications in order to capture the required information.

In a networking environment, tracing attacks or analyzing system problems could lead to losing valuable information. This could occur in a case of information that had been lost or stolen. Such a problem can happen when an incident investigator misses the opportunity of recording some valuable information that was discovered. This opportunity can often not be repeated. Therefore, people in charge of the system including System Administrator (SA) are in a position of possibly neglecting to obtain important information. System Administrators have various tools to investigate a system. These tools are mostly console application and run as command line utilities. They must be highly trained so that they can cover all the processes, tasks or operations performed by the system administrator, system operator, incident investigator, security administrator, network investigator. Anyone in the role of determining the problem, the cause or effect of any abnormal or unusual system behavior problem with these tools is is that they are not able to record either the pre-formed actions or the fact that these actions were taken or even the results obtained from them. From a forensic perspective these tools do not provide information in a forensically sound manner. One can argue that the output can be logged into a log file; however, this does not insure the integrity mechanism in transit. In fact, it is not common or an easy job to record every action taken or results obtained when examining a system. Even taking notes can be extremely difficult when real live attacks are in process. The DEB forensic incident response tool permits command line applications to be executed from a special dialogue box. When the command is executed the output from each command is captured in the DEB together with an

integrity hash of the data and a time stamp of when the command commenced and completed. When all the relevant system information has been captured the DEB is closed and sealed.

3.5. Traditional Evidence Capture

In the real life of law enforcement, when a crime scene is being investigated, many elements are brought to the laboratory. It is, although not always, possible to take away a whole physical crime scene. However, it rarely happens that the investigators dismantle bricks of a building for further investigation. In contrast, within digital life, forensic investigators are able to capture potential evidence from the suspected crime scene. This is the advantage of the world of digital forensics. The data then is sealed at the scene with a seal number and, as well, a tag is attached with details such as the following:

1. Property reference number
2. Case/Suspect name
3. Brief description of the item
4. Date and time the item was seized/produced
5. Location of where the item was seized/ produced
6. Name of the person who is taking custody of the evidence
7. Incident/Crime reference

The tag may also include \continuity sections" in which the details of all the investigators involved are recorded at the time of their actual investigation of the evidence (chain of custody). This is to ensure that the data is being recorded from the time the item was seized to the time it is being shown as legal evidence. This section shows the following details of the person who takes custody of the item:

1. Name/Rank
2. Signature
3. Date and time when the custody is being taken by the person.

Bags of different size, type and shape can be sealed at a crime scene. The actual number will depend on the size of the captured data and its type. However, using a consistent wrapper allows other specialist laboratories to process the item. For instance, some items may require DNA analysis while others may require fingerprint analysis or just an interpretation of their con-tents by a particular specialist. All of these depend on using a consistent bag wrapper. The question becomes how to create a consistent bag wrapper in a radically changing digital world such a method can be applied in a radically changing digital world.

3.6. Digital Evidence Capture

At present, the processes of \dd" image or the proprietary format produced by the forensic tool vendors, are the equivalent to the physical evidence capture process. Performing the \dd" file raw capture; there is no defined technique for attaching basic forensic details such as date and time of capture, name of the person who carried on the process or even any method for integrity check [10]. It is however possible to include such details manually or perform some integrity check separately (e.g. md5 hash). However, this can be extremely difficult when dealing with a real-time evidence equation.

Some proprietary forensic tools allow users to enter details at the beginning of the capture process. They also enable users to generate a hash to maintain the integrity of evidence. These techniques tend to capture the whole evidence into a single file (one bag), which can become a problem if the size of evidence is too large. This problem requires a fragmentation of chunks from which the file is later backed up. Another problem could occur when the capacity of a single storage device is insufficient and will thus require using a number of devices for storage proposes. In order to be able to process the content of either of these types of data capture output, the fragmented files must be combined back together so that the application can process the evidence from the whole file [10]. The idea of dividing a file into chunks could be extremely challenging as

one could argue that separating a content of a file into chunks and combining them again could violate the integrity of the original file (the evidence). The above scenario becomes more complicated if data is being captured in real-time, for example as a network packet capture. This type of application is similar in principle of the `dd' capture process but the difference is that the amount of data to be captured is unknown when the process is commenced.

4. REQUIREMENTS OF FORENSIC EVIDENCE

This provides guidance on the management of electronic records that may be used as evidence in judicial or administrative proceedings. Such management applies whether the evidence is to be used by a plaintiff, defendant or for referral to appropriate authorities for investigation.

While this provides guidance to the management of electronic records relating to litigation in New Zealand and Australia, the processes and procedures of that management of electronic records are consistent with global industry best-practice and will increase the value of digital evidence in many other jurisdictions.

It also discusses the main forensic structure that is required in the de-signing of the DEB architecture. The idea behind this chapter is to have a universal DEB structure that can be used by any digital investigator around the globe. A Proof of Concept (PoC) of a novel approach to a DEB design is further discussed and demonstrated in the tests and results chapter.

4.1. Overview

IT evidence is a broad term used to describe any records generated by, or stored on a computer system that may be used as evidence in court proceedings. IT evidence also encompasses computer-generated or stored records that detail management decisions which may be subjected to regulatory or judicial scrutiny. IT Evidence can be divided into three categories:

- records that are generated by computers;
- records that are merely computer-stored; and
- Both generated records and stored records. The distinction hinges upon whether a human or a computer created the records' actual contents.

Records that are generated by computers refer to documents which contain the writings of users and which happen to be in electronic form. E-mail messages, word processing files and internet chat room messages are good examples. The main evidentiary issue is demonstrating that it is a reliable and trustworthy record of what was stated. In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Common examples are log files, telephone records, ATM transaction receipts. The key evidentiary issue here is demonstrating that the computer program generating the record is functioning properly. A third category of IT evidence is a combination of the previous two records that are both computer-stored and computer-generated.

4.2. Principles for the Management of IT Evidence

The principles for the management of IT evidence only give assistance, not authority. Although individual jurisdictions will have specific evidentiary requirements, practitioners must ensure that the electronic records produced, collected, analyzed are presented in accordance with these principles in order for them to be admitted and therefore accepted by courts. The following defines guiding principles for the management of IT evidence. These relate to:

4.2.1. The obligation to provide Evidence

Investigators have to keep updated with regulatory, administrative and best-practice in order to provide forensically sound evidence. It is also important to understand the steps by which the actual weight of the evidence can be maximized.

4.2.2. Design for Evidence

The following must be considered when using any tool to create the evidence necessary for legal case of evidence:

- The capability of altering electronic evidence;

- The capability of authenticating electronic evidence;
- The reliability of tools generating such evidence;
- The time stamps and the date of creating, accessing and altering evidence;
- The chain of custody of who is taking care of the evidence; what do you mean by this and;
- The safe custody and handling of the evidence

This also applies to the design or acquisition of new ICT systems or the upgrade of existing systems.

4.2.3. Evidence Collection

Collecting evidence must be stored in a forensically sound manner. Two elements must be considered when collecting evidence:

- The evidence must be technologically robust
- The evidence must be legally robust

4.2.4. Chain of custody

There must be a method of recording all access to and handling of evidence.

4.2.5. The original, copy and original copy

It is always crucial to have another copy of the original one in case any the computer and/or the information and evidence contained therein is damaged. It is also important to make sure that any performed actions on the original or a copy are appropriate and are appropriately recorded and documented.

4.2.6. Personnel

From a management perspective it is essential to ensure that personnel who carry the design, production, collection, analysis and presentation of evidence have appropriate training, experience and qualifications to confidently perform their roles.

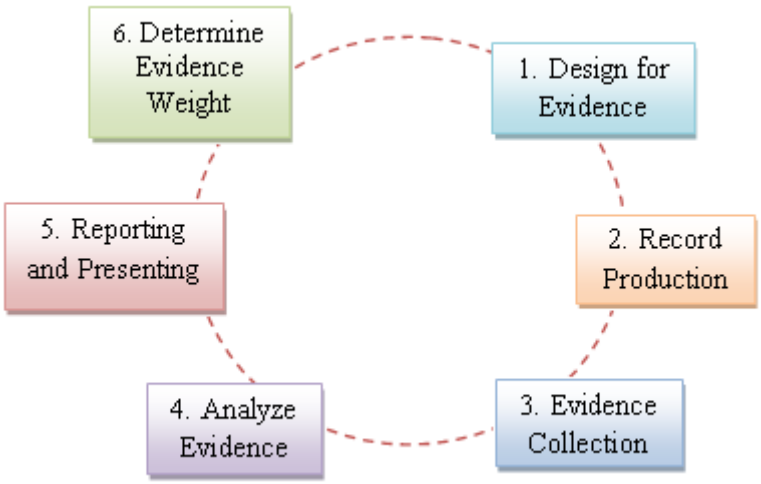

Fig2. *IT Evidence Management Lifecycle*

4.3. IT Evidence Management Lifecycle

This section introduces the IT evidence management lifecycle and explains how the principles can be applied to each of the six lifecycle stages. While actual evidence is unknowingly generated when a criminal leaves his/her DNA or fingerprints, digital evidence is generated by computer systems which have the capability of increasing their evidential value. In addition, the computer generated digital evidence has to be carefully processed and handled in order to increase its evidentiary weight. The IT evidence management life cycle is illustrated in Figure 2

Stage1. *Design for Evidence*

There are four objectives when designing a computer system to increase the evidentiary weight of electronic evidence

1. Electronic records must be able to be identified, available and usable;
2. The author of electronic records must be able to be identified;
3. The authenticity of the electronic records; and
4. The time stamps and the dates of creating, accessing and altering electronic records;
5. The reliability of computer programs must be able to be established.

Another important objective is the design of the procedures that are to be conducted by personnel for collecting, analyzing and reporting digital evidence. Such procedures are discussed in the relevant stage of the lifecycle and should be;

1. Designed prior to them being necessary; tested to ensure that personnel are able to carry them out; and
2. The design of each procedure must be clear (unambiguous) and decrease the amount of decision-making.

The author of electronic records is identified

Identifying human author: the author of a computer-stored record should be able to be identified electronically. Prior to recording the author's electronic identity, a user authentication system should be used. Authentication is any process by which users verify that someone is who they claim they are. This usually involves a user name and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition or fingerprints.

The evidential weight of the recording of the author's identity will depend on the strength of the user authentication system. ISO 9798:1977| Entity Authentication, for example, specifies techniques used by authentication systems for corroborating user or computer identification.

Identifying the computer author: Each computer program generating elements of the electronic record must be clearly identified in the record. This may be achieved by, for example:

- Clearly identified, unique and consistent labeling of file names; or
- Clearly identified, unique and consistent labeling within the record.

Human and computer authors because electronic records may consist of both computer-stored and computer generated elements, both must be identifiable. For instance, a financial spreadsheet includes typical human numerical entries and the calculation formula. It also includes computer-created records derived by the spreadsheet program from the computer-stored records. Therefore, both the human author and the system author must be able to be identified.

Establishing the authenticity of electronic records

Two elements must be achieved in order to establish the authenticity of electronic records

1. The original electronic record must be able to be identified; and
2. Each alteration must be identified as to whether it was a human or computer author and recorded.

The time stamps of electronic records

As electronic records are being generated or altered it is important that management ensures that time and date stamps exist in their computer system and are maintained by the organization. In order to achieve this, a timestamp must be activated at the time of creation of each record. As the electronic record is being altered the timestamp must be updated. RFC 3339|Date And Time on the Internet: this provides the timestamps which specifies a format for timestamps that may be used. Also see for example ISO/IEC 18014 - Time-stamping Services. All computer system clocks must be synchronized to a central reference to ensure the right time is being conducted.

Amongst others the Universal Time Coordinated (UTC16) provides a central reference for computer sys-tem clocks.

Establishing the reliability of computer systems

In order to ensure a precise recording of the author's statement it is important to establish the reliability of the computer systems that generate the electronic records and that those systems operate correctly and precisely. Their reliability must be demonstrated by the following:

1. the computer program was built correctly i.e. the output is: i) consistent with its design; ii) predictable; and iii) repeatable.
2. There was no fault or errors in the program when the electronic record was created, copied or altered. In other words the program was operating correctly during the capturing process.

Formal design criteria: When designing the formal criteria for a soft-ware program the methodologies of, for example, ISO 15504-Software Process Assessment or by accreditation to the appropriate level of the Capability Maturity Model17 (CMM) should be adhered to. When buying a software program the formal assessment criteria of the manufacture can be used to clarify the reliability the new software.

Source code: In order to ensure the reliability of a software program, its source code has to be analyzed by experts. When acquiring an open source software program or producing it, the source code should be retained. In order to enable a software demonstration from its source code. However, when buying a software program the buyer must ensure that a guarantee of its source code (same version) is available at any time.

Stage2. *Production of Records*

At this stage of the life cycle critical operations are performed. The main objective of this stage is to be able to initiate the following:

- a particular software generated an electronic record ;
- for computer-stored records, the human author ;
- the timestamps of creation; and
- Being able to make sure that the software is operating correctly when the electronic records are being created or altered.

When maintaining electronic records of evidential significance best-practice controls should be applied to all computer system operations. For instance, those indicated in ISO 17799 - Code of Practice for Information Security Management part 8 -Communications and Operations Management

In order to show that a particular software program was performing correctly when the electronic records were being captured, the following requirements have to be met:

- That the computer program was operating; and
- That the computer program is valid as to its reliability.

Circumstantial evidence may also be used to demonstrate that a computer program is operating correctly. For example, a statement by a person asserting that he/she was using a particular computer program at a particular time and that he/she observed certain things, could be strong evidence of the operation of a computer program that produces computer-stored records. In addition when designing or using a computer software program which generates electronic records, a record of operational faults must be maintained. For further details on this matter see ISO 17799-Code of Practice for Information Security Management part 8.4 Housekeeping.

Stage3. *Evidence Collection*

Relevant information (evidence) has to be obtained when securing the original copies of those obtained of this information. As stated above under the section Principles for the Management of IT Evidence the process of acquiring evidence must not be performed on the original.

Standards for evidence collection: The standard of the evidence collected are one factor determining the evidential weight of electronic records. Forensically Sound In order to ensure that the evidence presented is admissible, forensically sound procedures must be followed. These procedures must show the original and every action, whether human or computer generated, thereafter in order to be admitted as evidence.

Best Evidence: The judiciary will decide whether the evidence is admissible. For example, in Australia the judiciary has significant discretion to recognize records as evidence even when the forensic specialists themselves have not collected the electronic records admitted as evidence. When forensic specialists get involved, the value of evidence does increase however, it is not wise to rely on this judicial discretion. By following the correct procedures at each and every stage the weight of the evidence will increase and speak for itself.

Contemporary notes: Contemporary notes written at the time the evidence was obtained can be relevant even some years later when the investigators or personnel who made those notes are called to appear before the Court to give evidence. This may happen years after the evidence collection process was performed. For this reason contemporaneous notes are very important and must record any actions that were performed whether on the original or other copies. These contemporaneous notes may include the process of decision-making such as why those decisions were taken, persons consulted and authorities sought. It is necessary that contemporaneous notes include facts such as actions performed and observations made. These observations must not be opinions. It is also far more important to ensure that those notes do not interfere with the evidence presented.

Chain of custody: Any personnel who have gained access to a particular electronic record at any given time must be identified. This is from the creation of the electronic records, to the presentation of the evidence. The electronic records evidential weight will be substantially reduced if the chain of custody cannot be adequately proved or is discredited. This is to avoid any potential allegations of data tampering or misconduct which can com-promise the Court case.

Evidence copy: When relevant information is produced as evidence, a copy of the evidence will be provided to the Court and the other party so the chain of custody can be demonstrated. An individual can be responsible for the chain of custody and so monitor all access to it. The copy of evidence may be created by:

1. Regenerating the electronic record of evidence as a hard copy (a printed document)
2. Copying the evidence to another “offline” media (e.g. floppy disk, CD-rom, backup tape, external hard drive); or
3. Utilizing system access privileges to control access. When an electronic record of c) evidence is copied, it is a must provide proof that the copy has not been tampered. It is recommended that a number of evidence-copies should be created and a chain of custody be established for each copy.

Custody log: The individual in charge of the evidence copy must maintain a log recording of:

1. Users who access the evidence;
2. The time stamps, date and purpose for each user's access; and
3. When any copy of the evidence is removed, the time and date of removal and return must be logged.
4. All activity related to the digital evidence should be documented ac-cording to the planned procedures for the custody of evidence.

Non-readable electronic records: There is data which may be stored within non-readable files (or even readable) that is evidentially useful but which can be easily altered or deleted by certain computer software. For ex-ample, the slack space of a disk drive may include deleted files or encrypted files that may contain key electronic records. This can be an issue when reaching the lifecycle stage of analyzing electronic records. Since non-readable files can be easily altered or deleted by computer soft-ware, investigators need to pay more attention when locating those non-readable files so as not to tamper with their contents when collecting evidence.

*Limitations***:** When collecting evidence, investigators must follow rules that control the access of or declaration of particular information. If any of these rules are violated, the credibility of evidence will be comprised. This could decrease the weight of the evidence and in the worst case scenario even prevent the evidence from being admitted in Court. Personnel who do not follow the rules may expose themselves to penalties. For example: The Telecommunications (Interception) Act (1979) provides for criminal penalties for the unauthorized interception of a "communication". Evidence collectors must be able to determine if an electronic message (e.g. e-mail or IRC19) constitutes a communication or if it is merely data.

Stage4. *Analyze evidence*

The objectives of this stage of the lifecycle are to:

1. Assemble from IT evidentiary records material facts;
2. deduce from IT evidentiary records opinions relating to those facts; and
3. Determine what other IT evidence is lacking that will assist the enquiry.

Use evidence copy In order to analyze an electronic record, an evidence copy of the original must be used while the original remain in a safe condition (untouched). Only original electronic record is used to certify

- If copies are duplicates of the original; or
- If the original has been altered.

Personnel qualifications: The analysis process of the IT evidence should be conducted by professional people who are appropriately qualified for the function they are performing. It is important to decide whether an ordinary or expert witness is required. While ordinary witnesses' analysis is on matters of fact only, expert witnesses may provide matters of opinion from the IT evidence.

Completeness of evidence: IT evidence is circumstantial. Specialists conducting analysis of IT evidence must be provided with details of:

- Why the evidence is required?
- the circumstances in which the electronic records were created?; and
- The computer systems creating the electronic records.
- Material electronic records may be neglected or their significance diminished without a thorough understanding of the background.

Stage5. *Reporting and presentation*

In this stage of the life cycle, the aim is for investigators to convince decision-makers (management, lawyer, Judge, standards for evidence collection forensic...etc) of the validity of the facts and opinions retrieved from the evidence.

For most IT evidence, the original electronic record consists of electronic impulses stored on media. It must be converted into human readable format prior to presentation, either by computer print out or by using a computer program.

If IT evidence is to be used in legal proceedings, the investigator will be advised of the suitable manner and form in which the evidence should be reported and presented.

Stage6. *Determine evidentiary weight*

The objective of this stage is to assess the evidentiary weighting of the electronic records and the reports. Assessment of the evidentiary weighting of electronic records occurs during all stages of the lifecycle. In earlier stages of the lifecycle (i.e. one through five) assessment is performed by the participants or stakeholders such as lawyers. A final assessment is performed by an independent arbitrator who may be a Magistrate or Judge; a member of a tribunal or an arbitrator; or senior organizational management.

Two criteria are used to measure the evidential weight of electronic records

1. Probative value: Has the electronic record relevancy, authorship, authenticity, correct operation and reliability been established? ; and
2. Rules of evidence: Has the electronic record been collected and handled correctly in accordance with the rules?

Each of these criteria encompasses many factors.

Probative value: Records must relevant and all relevant electronic records must be presented and more importantly, records must be relevant to the matter at hand. Organizations must demonstrate that the procedures used to collect electronic records were reasonable and robust enough to discover obvious, lost or hidden material. The following must be satisfactorily established

1. Authorship;
2. Authenticity; and
3. Correct operation and reliability of the computer program.

Rules of evidence: With some exceptions, the aim of the rules of evidence is to exclude evidence that is either irrelevant or unreliable. If organizations collect and handle IT evidence in accordance with this handbook, they will minimize the risk of having such evidence excluded by operation of any applicable rules of evidence.

5. CONCLUSION

This paper has described the situation of multiple threats and vulnerabilities on multiple servers. It has also discussed the need to have multiple intrusion detection systems based on different networks. The foundation of this dissertation was the importance of multiple entities. These entities included attacks, vulnerabilities, and servers: firewalls, IDSs, databases and web server. All these entities will combine in a novel testbed based on an active network which enabled us to join individual strengths together and to overcome their specific weaknesses. Another significant factor of this research will be the creation of a unique DEB along with IDSs output and open-source networking tools. We also will provide the security to DEB.

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)