ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Digital Forensics

Vaishnavi Ganesh
Asstt.Professor Computer science and Engineering Department Priyadarshini Indira Gandhi College of Engineering, Nagpur,India

Manuscript Info

Manuscript History:

Received: 15 September 2015
Final Accepted: 22 October 2015
Published Online: November 2015

Key words:

Digital forensics, Investigation model, forensics process, digital crime, digital devices.

Corresponding Author

Vaishnavi Ganesh

Abstract

Digital forensics is a branch of forensic science concerned with the use of digital information produced, stored and transmitted by computers as source of evidence in investigations and legal proceedings. Digital forensics has existed for as long as computers have stored data that could be used as evidence. For many years, digital forensics was performed primarily by government agencies, but has become common in the commercial sector over the past several years. Originally, much of the analysis software was custom and proprietary and eventually specialized analysis software was made available for both the private and public sectors. The first part of this paper provides a brief overview of digital forensics Process, followed by the models of digital forensics. In the further part of the paper, we consider the need of the "Digital Forensic Investigation Model" which is currently an active area of research in the academic world, which aims to ameliorate procedures followed in this field. At last, we discuss challenges and future scope of digital forensics.

INTRODUCTION

Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Digital Forensic can be defined as "The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." [4] Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), Laboratory Accreditation Board (ASCLD-LAB), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations [2]. International Data Corporation (IDC) reported that the market for intrusion-detection and vulnerabilityassessment software will reach 1.45 billion dollars in 2006.

Major initiatives

- National White Collar Crime Center (NW3C)
- National Center for Forensic Sciences (NCFS)
- Digital Forensics Research Workshop (DFRW)
- Computer Forensic Educator's Working Group

(CFEWG)

- Cyber Tools Online Search for Evidence (CTOSE) – European

One important element of digital forensics is the credibility of the digital evidence. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc. The legal settings desire evidence to have integrity, authenticity, reproductivity, non-interference and minimization.

2. THE NEED FOR DIGITAL FORENSIC INVESTIGATION MODELS

It is important to understand the need of the "Digital Forensic Investigation Model" which is currently an active area of research in the academic world, which aims to ameliorate procedures followed in this field. The way Digital Forensic Science is implemented has a direct impact on

- The prevention of further malicious events occurring against the intended "target".
- The successful tracing back of the events that• occurred which led to the crime, and determining the guilty parties involved.
- Bringing the perpetrators of the crime to justice.
- The improvement of current prevention mechanisms in place to prevent such an event from occurring again.

Improving standards used by corporate security• professionals to secure their respective corporate networks. How everyone "plugged" into this digital• environment can increase their awareness about current vulnerabilities and prevention measures. There has been a need for a standard methodology used for all Digital Forensics investigations. There have been many initiatives made to have models that have a general process to be followed for such investigations [5]. Research done by the scientific community has been fairly recent, and has concentrated mostly upon coming up with good models that can be practiced [7]. Yet, it can be safely said that these models are mainly ad-hoc and much needs to be accomplished in this particular domain.

3. INVESTIGATION PROCESS OF DIGITAL FORENSICS

Investigative process of digital forensics can be divided into several stages. There are four major stages: preservation, collection, examination, and analysis .

- Preservation: Preservation stage corresponds to• \freezing the crime scene". It consists in stopping or preventing any activities that can damage digital information being collected. Preservation involves operations such as preventing people from using computers during collection, stopping ongoing deletion processes, and choosing the safest way to collect information.
- Collection: Collection stage consists in finding• and collecting digital information that may be relevant to the investigation. Since digital information is stored in computers, collection of digital information means either collection of the equipment containing the information, or recording the information on some medium. Collection may involve removal of personal computers from the crime scene, copying or printing out contents of files from a server, recording of network traffic, and so on.
- Examination: Examination stage consists in a• \in-depth systematic search of evidence" relating to the incident being investigated. The outputs of examination are data objects found in the collected information. They may include log files, data files containing specific phrases, timesstamps, and so on.
- Analysis: The aim of analysis is to "draw conclusions based on evidence found".
- Reporting: This entails writing a report outlining• the examination process and pertinent data recovered from the overall investigation.

4. THE ABSTRACT DIGITAL FORENSIC MODEL

The abstract digital forensics model [1] proposes a standardized digital forensics process that consists of nine components:

1. Identification: It recognizes an incident from indicators and determines its type.

2. Preparation: Preparation entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support.

3. Approach strategy: It develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.

4. Preservation: Preservation which involves the isolation, securing and preservation of the state of physical and digital evidence.

5. Collection: It entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures.

6. Examination: It involves an in-depth systematic search of evidence relating to the suspected crime.

7. Analysis: Analysis involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found.

8. Presentation: It involves the summary and explanation of conclusions.

9. Returning evidence: It ensures physical and digital property is returned to proper owner.

5. THE INTEGRATED DIGITAL INVESTIGATION MODEL (IDIP)

5.1 Readiness phases

The goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation. It includes two phases:

- Operations Readiness phase
- Infrastructure Readiness phase

5.2 Deployment phases

The purpose is to provide a mechanism for an incident to be detected and confirmed. It includes two phases:

- Detection and Notification phase; where the incident is detected and then appropriate people notified.
- Confirmation and Authorization phase; which confirms the incident and obtains authorization for legal approval to carry out a search warrant.

5.3 Physical Crime Scene Investigation phases

The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident. It includes six phases:-

- Preservation phase; which seeks to preserve the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification.
- Survey phase; that requires an investigator to walk through the physical crime scene and identify pieces of physical evidence.
- Documentation phase; which involves taking photographs, sketches, and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded.
- Search and collection phase; that entails an indepth search and collection of the scene is performed so that additional physical evidence is identified and hence paving way for a digital crime investigation to begin
- Reconstruction phase; which involves organizing the results from the analysis done and using them to develop a theory for the incident.
- Presentation phase; that presents the physical and digital evidence to a court or corporate management.

5.4 Digital Crime Scene Investigation phases

The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes similar phases as the Physical Investigation phases, although the primary focus is on the digital evidence. The six phases are:-

- Preservation phase; which preserves the digital crime scene so that evidence can later be synchronized and analyzed for further evidence.
- Survey phase; whereby the investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location.
- Documentation phase; which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.
- Search and collection phase; whereby an indepth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted files that were used including the dates, duration, log file etc. Low-level time lining is performed to trace a user's activities and identity.
- Reconstruction phase; which includes putting the pieces of a digital puzzle together, and developing investigative hypotheses.
- Presentation phase; that involves presenting the digital evidence that was found to the physical investigative team.

5.5 Review phase

This entails a review of the whole investigation and identifies areas of improvement.
The IDIP model does well at illustrating the forensic process, and also conforms to the cyber terrorism capabilities [6] which require a digital investigation to address issues of data protection, data acquisition, imaging, extraction, interrogation, ingestion/normalization, analysis and reporting. It also highlights the reconstruction of the events that led to the incident and emphasizes reviewing the whole task, hence ultimately building a mechanism for quicker forensic examinations.

6 Computer Intrusion

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

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

ƒ Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

ƒ Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

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

6.1 Computer Forensics

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

ƒ Identity theft, such as stolen credit cards numbers and social security numbers.

ƒ To reveal if trade secrets were stolen from an organization.
ƒ Investigate a hackers attack on a computer system.
ƒ Finding evidence of child pornography.
ƒ For divorce proceedings, evidence of a cheating spouse.

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

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

6.2 Computer Forensics Investigator

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

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

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

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

6.3 Computer Forensics Methodologies

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

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

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

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

model consists of nine phases "identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence".

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

6.4 Computer Forensics and Security Policies

An organization should build their security policy around the event that it is inevitable that computer forensics will be needed in the future. If an enterprise has a plan in place for when an intrusion takes places, it will greatly aid the organization into the forensics process. All employees of an organization should be trained on what to do in the event of 9 an intrusion. Failing to provide employees with training and written procedures can jeopardize a computer forensics investigation. For instance, an employee may think he is aiding in helping to contain an incident and in actuality may be damaging evidence. Along with the typical computer user of the organization, system administrator should also be train. While the system administrator knows a great deal about their system, they may not have the proper training of what to do in the event the computer forensics is needed. For these reason the security policy of an organization should contain what to do in the event that computer forensics is needed.

6.5 Intrusion Detection Systems

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

ƒ Misuse intrusions, where well-defined attacks are aimed at known weak points of a system. Due to the fact that these attacks have been experienced before and are therefore well defined/documented, very often a purely rule based detection system encapsulating the known information about the attack is applied.

ƒ Anomaly intrusion. These are harder to quantify and are based on observations of normal system usage patterns, and detecting deviation from this norm. There are no fixed patterns that can be monitored and as a result a more "fuzzy approach is often required.

Anomaly-based IDS's uses a typically statistical profile of activity to decide whether the occurrence of a particular component event or event pattern is normal or anomalous. If normal, then the activity is considered to be harmless and thus legitimate. On the other hand, if it is anomalous then it is potentially unauthorized and harmful. Signature-based IDS's attempts to match a sequence of observed events with a known pattern of events which is characteristic of an attack of some sort, such as a buffer overflow attack and password guessing. If no match is found with any of the known attack event patterns (signatures), then the activity under scrutiny is considered to be harmless and thus legitimate. Solely signature-based IDS cannot recognize a new or previously unknown type of attack; anomaly-based IDS on the other hand cannot categorically identify a sequence of events as an attack

.

6.6 Intrusion Detection Systems and a View to Its Forensic Applications

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

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

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

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

7 Software Tools

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

7.1 Hard Drive Tools

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

7.2 Network Tools

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

7.3 Tools to Search and Recover Files

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

7.4 All Purpose Tools

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

8 Summary

A survey of the field of computer intrusion forensics is given in this paper. To reiterate computer forensics deals with the preservation, identification, extraction, documentation and interpretation of computer data [Kruse II

and Heiser 2002]. The paper explored a wide-range of areas dealing with computer forensics. The legal issues surrounding an investigation were discussed. Next, the skills need to be possessed by the investigator were examined. After that, the computer forensics methodologies were discussed along with incorporating forensics into an organization security policy. Subsequently, a basic overview of intrusion detection systems and how they relate and aid in computer forensics was discussed. Furthermore, some basic steps need to preserve, recover and examine data were discussed. Last, a wide-range of software tools were examined that can aid in the investigation process. One of the most important parts of computer security is being prepared. While it important for an organization to take the normal security precautions such as having a firewall, anti-virus software and patching the operating system regularly for known vulnerabilities, it is also important that an organization is prepared for the inevitable event of an intrusion. An organization should include in their security policy what to do in the event of an intrusion and methods to be used in a computer forensics investigation. There are many things that an organization can do that will aid in the forensics process after an intrusion. First, an enterprise should use an Intrusions detection system, so the intrusion can be noticed and contained as quickly as possible limiting the damage caused. Next, an organization could also use a program such as tripwire to compare the hash values on a system to detect if any files have been changed. Also, the organization should store the log file of a computer in a remote location. Last, the most important thing is to educate the user of what to do in the event of an intrusion. The birth of the Computer has brought about, what is known as the "Information Revolution". Never before has such a wealth of data, both public and private, been so accessible and obtainable. With this revolution have come certain undesirable elements, being the underworld of computer fraud and crackers, who quite often achieve their aims by breaking into compute systems and impersonating legitimate system users. Many methods preventing intrusions into computer systems have been implemented, but these will always be imperfect.

References

[1] Mark Reith, Clint Carr and Gregg Gunsch, (2002) an Examination of Digital Forensic Models International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3.

[2] Michael Noblett, Mark.M.Pollitt and Lawrence Presley, (2000) Recovering and Examining Computer Forensic Evidence, Forensic Science Communications, Volume 2, Number 4.

[3] Brian Carrier and Eugene H Spafford,(2003) Getting Physical with the Investigative Process International Journal of Digital Evidence. Fall 2003, Volume 2, Issue 2.

[4] Gary L Palmer. (2001). A Road Map for Digital Forensic Research. Technical Report DTR-T0010- 01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

[5] M. M. Pollitt, An ad hoc review of digital forensic models, In Systematic Approaches to Digital Forensic Engineering, 2007, pages 43{54. University of Central Florida, USA, IEEE, April 10- 12, 2007 2007.

[6] National Institute of Justice. (2002). Results from Tools and Technology Working Group, Governors Summit on Cybercrime and Cyberterrorism, Princeton NJ.

[7] Lindsey, T. Challenges in Digital Forensics. 2006 Available from: http://www.dfrws.org/2006/proceedings/Lindseypres.pdf.

[8] Dr. Yong Guan, Digital Forensics: Research Challenges and Open Problems December 4, 2007