International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Digital Forensics: Need and Models

R.Selvaprabha

Lecturer, Dept. of Computer Science, K.B.N College (Autonomous), Vijayawada, Andhra Pradesh

rspraba1987@yahoo.com

Abstract---Nowadays, rapid evolution of computers and mobile phones has caused these devices to be used in criminal activities. Providing appropriate and sufficient security measures is a difficult job due to complexity of devices which makes investigating crimes involving these devices even harder. Digital forensic is the procedure of investigating computer crimes in the cyber world. This paper reviews need, importance and some of the fundamental models of this technology.

Keywords: computer crimes, digital forensics, forensics models.

I. INTRODUCTION

Computer forensics is the science of obtaining, preserving, and documenting evidence from digital electronic storage devices, such as computers, PDAs, digital cameras, mobile phones, and various memory storage devices. All must be done in a manner designed to preserve the probative value of the evidence and to assure its admissibility in a legal proceeding. The computer forensics specialist collects and preserves digital evidence. As traditional forensics may involve people with different specialties, computer forensics similarly involves a number of professional specialties working together to gather, preserve and analyse digital evidence.

As computers become smaller, faster and cheaper, computers are increasingly being embedded inside other larger systems which allow information to be created, stored, processed, analyzed and communicated in ways that are unpredicted. Once we gathered digital evidence from monolithic, stand-alone mainframes where as today we have PCs, supercomputers, distributed client-server networks, laptops and smartphones, and LANs and WANs to convey information across the world, each of which is a potential source of digital evidence. Evidences stored in a computer is not unique with regard to relevancy and materiality, but because it can be easily duplicated and modified, often without leaving any traces and is readily available to a miscreant using another computer half a world away and hence, should be constrained by evolving legal standards and constraints to defend privacy issues.

II. THE DIGITAL FORENSIC PROCESS

` For the proper handling of evidence and in order to minimize errors in investigations it is necessary to have a structured way of handling investigations. This structured way is known as the digital forensic process. Moreover, for the credibility of evidence digital forensic experts are usually asked to explain the process they used in collecting evidence in a court of law. This means that the digital forensic examiner should always know the digital forensic process and the appropriate toolsets used in a digital forensic investigation. The digital forensic process can be categorized into four phases namely acquisition, examination, analysis and reporting. The process is common in different fields including mobile and network forensics. The process is used in investigations and has gained recognition in science. The digital forensic process can also be defined as a number of steps from the original incident alert through to reporting of findings. Recall that the authors only focus on the acquisition and analysis phases of the digital forensic process. Hence, the acquisition and analysis phases are discussed in more detail in the following subsections.

A. Acquisition

The acquisition phase describes how data will be acquired from different types of digital information sources. Data has to be acquired in a manner that maintains its integrity and authenticity [10]. The acquired data has to undergo forensic duplication or sector level duplication. A write blocker should be used in creating duplicates. The write blocker ensures that nothing is written to the original hard drive. Software imaging tools can also be used [11]. With imaging either a physical image (bit-by-bit image) can be created of the entire physical device or a logical image can be created which comprises of active directories and files available to the operating system [10].As a way of verifying the integrity of acquired data hashing is used. A digital hash conducts a mathematical algorithm of a device or file and provides a fingerprint that authenticates that the data has not been tampered or altered, and this fingerprint is maintained within the case file.

B. Analysis

The analysis phase describes how the data is processed. A hash analysis search can be conducted using hashing tools such as SHA-1, MD5 or using CRC applications. These tools

conduct a mathematical analysis of a data storage device like a hard drive. By comparing hash values investigators can exclude large numbers of files that have no value to the case and hash comparing can be done between fingerprint and hash values of the data being examined. Enterprise forensic software like FTK and Encase can be used to compare hash values [10].Analysis is mainly about locating digital media and assembling them before interpreting the contents.

III. NEED OF COMPUTER FORENSICS

The purpose of computer forensics is mainly due to the wide variety of computer crimes that take place. In the present technological advancements it is common for every organization to employ the services of the computer forensics experts. There are various computer crimes that occur on small scale as well as large scale. The loss caused is dependent upon the sensitivity of the computer data or the information for which the crime has been committed. The computer forensics has become vital in the corporate world. There can be theft of the data from an organization in which case the organization may sustain heavy losses. For this purpose computer forensics are used as they help in tracking the criminal. The need in the present age can be considered as much severe due to the internet advancements and the dependency on the internet. The people that gain access to the computer systems without proper authorization should be dealt in. The network security is an important issue related to the computer world. The computer forensics is a threat against the wrong doers and the people with the negative mindsets.

The computer forensics is also efficient where in the data is stored in a single system for the backup. The data theft and the intentional damage of the data in a single system can also be minimized with the computer forensics. There are hardware and software that employ the security measures in order to track the changes and the updating of the data or the information. The user information is provided in the log files that can be effectively used to produce the evidence in case of any crime a legal manner. The main purpose of the computer forensics is to produce evidence in the court that can lead to the punishment of the actual. The forensic science is actually the process of utilizing the scientific knowledge for the purpose of collection, analysis, and most importantly the presentation of the evidence in the court of law. The word forensic itself means to bring to the court.The need or the importance of the computer forensics is to ensure the integrity of the computer system. The system with some small measures can avoid the cost of operating and maintaining the security. The subject provides in depth knowledge for the understanding of the legal as well as the technical aspects of computer crime. It is very much useful from a technical stand point, view.

The importance of computer forensics is evident in tracking the cases of the child pornography and email spamming. The computer forensics has been efficiently used to track down the terrorists from the various parts of the world. The terrorists using the internet as the medium of communication can be tracked down and their plans can be known. There are many tools that can be used in combination with the computer forensics to find out the geographical information and the hide outs of the criminals. The IP address plays an important role to find out the geographical position of the terrorists. The security personnel deploy the effective measures using the computer forensics. The Intrusion Detecting Systems are used for that purpose.

IV. DIGITAL FORENSICS MODELS

The number of suggested and proposed investigation models is not small, as such; it would be quite a daunting exercise to review them all. We have indeed, selected the models to be reviewed based on the chronological order, ensuring at least one proposed model per year. We are not suggesting that the selected models are better or superior than the other models that were also introduced in the same year. Our objective is to identify and extract the phases in the investigation models rather than selecting which model is the best.

4.1 Computer Forensic Investigative Process (1984)

Pollitt has proposed a methodology for dealing with digital evidence investigation so that the results with be scientifically reliable and legally acceptable. It comprises of 4 distinct phases.

1. Acquisition 2.Identification 3. Evaluation 4.Admission

In Acquisition phase, evidence was acquired in acceptable manner with proper approval from authority. It is followed by Identification phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human.

The Evaluation phase comprise of the task to determine whether the components indentified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence. In the final phase, Admission, the acquired & extracted evidence is presented in the court of law.

4.2. DFRWS Investigative Model (2001)

The first Digital Forensics Research Workshop (DFRWS) proposed a general purpose digital forensics investigation process. It comprises of 6 phases. Identification b) Preservation c) Collection d) Examination e) Analysis

f) Presentation

DFRWS Investigative model started with an Identification phase, in which profile detection, system monitoring, audit analysis, etc, were performed. It is immediately followed by Preservation phase, involving tasks such as setting up a proper case management and ensuring an acceptable chain of custody. This phase is crucial so as to ensure that the data collected is free from contamination. The next phase is known as Collection, in which relevant data are being collected based on the approved methods utilizing various recovery techniques.

Following this phase are two crucial phases, namely, Examination phase and Analysis phase. In these two phases, tasks such as evidence tracing, evidence validation, recovery of hidden/encrypted data, data mining, timeline, etc, were performed. The last phase is Presentation. Tasks related to this phase are documentation, expert testimony, etc.

4.3. Abstract Digital Forensics Model (ADFM) (2002)

Inspired by DFRWS investigative model, Reith, Carr &Gunsch, proposed an enhanced model known as Abstract Digital Forensic Model. In this model, the author introduced three additional phases, thus expanding the number of phases to nine.

a)Identification b)Preparation c)Approach Strategy d)Preservation e)Collection f)Examination g)Analysis h)Presentation i)Returning Evidence

The 3 significant phases introduced in this model were Preparation, Approach Strategy and Returning Evidence. In Preparation phase, activity such as preparing tools, identify techniques and getting management support, were done. Approach Strategy was introduced with the objective to maximize the acquisition of untainted evidence and at the same time to minimize any negative impact to the victim and surrounding people. In order to ensure that evidences are safely return to the rightful owner or properly disposed, the Returning Evidence phase was also introduced.

The firest phase in ADFM is Identification phase. In this phase, the task to recognize and determine type of incident is performed. Once the incident type was ascertained, the next phase, Preparation, is conducted, followed by Approach Strategy phase. Physical and digital data acquired must be properly isolated, secured and preserved. There is also a need to pay attention to a proper chain of custody. All of these tasks are performed under Preservation phase. Next is the Collection phase, whereby, data extraction and duplication were done. Identification and locating the potential evidence from the collected data, using a systematic approach are conducted in the next following phase, known as Examination phase. The task of determining the significant of evidence and drawing conclusion based on the evidence found is done in Analysis phase. In the following phase, Presentation phase, the findings are summarized and presented. The investigation processes is completed with the carrying out of Returning Evidence phase.

V. CONCLUSION

The rapid development of computing devices requires new methods or tools to be used by the digital forensic investigators to obtain the evidences as a legally acquired evidence to be presented in the court. With the complexity of networking, computing environment and the advancement of mobile devices, the digital forensic investigators also need to be advanced in their tools and methodologies to obtain the evidences legally without affecting the user's privacy to the court. There are many tools and methodologies newly developed to assist digital forensic investigators in the digital evidence acquisition process and analyze the evidences. This paper provides the importance and basic models of this technology. The future work will include the tools and methodologies of digital forensic technology.

VI. REFERENCES

[1] M.Cross,SceneoftheCyberCrime,2rded.Syngress.2008.p500
[2] A.J.Marcellaand .S.Greenfield.Cyberforensics,London.AuerbachPublications
[3] K.J.Jones,R.Bejtlichand C.W.Rose.RealDigitalForensics,NewYork
[4] .J.Vacca,Digitalforensics–computer Crime Scene Investigation, CharlesRiverMedia
[5] E.Casy.DigitalEvidenceandComputerCrime-ForensicScience,Computers andtheInternet,2rded,Academic Press
[6] M.Solomon, G.Barett,D.Broom, N,Computer_Forensics London.Sybex
[7] E.Casey, DigitalEvidenceandComputerCrime,2rded, Elsevier
[8] http://www.accessdata.com
[9] http://www.paraben.com
[10] .http://www.guidencesoftware.com