AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

www.ajcse.info

Asian Journal of Computer Science Engineering 2016; 1(2):20-24

REVIEW ARTICLE

A Review on Recovering and Examining Computer Forensic Evidences

M.Elavarasi[1], N.M.Elango[2*]

[1]*Research Scholar (Part-Time), Bharathiar University, Coimbatore-641 046*
[2]*Associate Professor, School of Information Technology & Engineering, VIT University, Vellore*

Received on: 15/11/2016, Revised on: 13/12/2016, Accepted on: 22/12/2016

ABSTRACT

Digital forensic is the method of acquiring the data's electronically. It is the investigation method of gathering malicious evidence from the target system or on the network. We have to collect the evidence in the way it should be admissible in the court. The forensic investigation can be performed successfully by following the evidence gathering methodologies. Computer forensics is a new field when compare to traditional forensic methods. It is an emerging field due to the increase of cyber crime committed by using the internet. In this paper, we are going to study details of recovering and examining the cyber forensic evidences and the major issues in this field.

Keywords: Cyber-Forensics, Forensic tools, cyber crimes, malicious evidence

INTRODUCTION

In a perfect world the need for deciding out the activity conducted on a network or within a computer would not be necessary; however, this is not a perfect world and there are times when it is extremely important that the activity of a computer be watched. There should be a way for an individual to watch obey valuable things, such a computer or network, in times when possible invasion or bad behavior has happened. For this reason, computer forensic, a newly developed area of computer science, becomes a more and more important aspect daily and will be widely used in the twenty-first century [1].

Digital forensics is the use of examination and analysis ways of doing things to gather and preserve evidence from the appropriate device in a way that is good for presentation in a court of law [2]. The goal of digital forensic is to do a careful investigation while maintaining a chain of evidence to find out exactly what to be found on a appropriate device and who was blamed for it. Digital forensic tools are now used on a daily basis by examiners and analysts. Forensics analyst usually follow a general set of procedures: After physically separating the device in question to make sure it cannot be damaged, investigators make a digital copy of the device's storage media. Once the real media is copied, it has to be sealed in a safe or other secure facility to maintain its original condition. Forensic Analyst use a variety of ways of doing things and recovery software computer programs to examine the copy, searching invisible files and unloaded disk space for copies of deleted or damaged files. Digital forensic is an important tool for solving crimes attached with computers (e.g. phishing and stealing from a bank), as well as for solving crimes against people where evidence may reside on a computer (e.g. hiding illegally-gotten money and child pornography). Memory forensic is a forensic investigation of a computer's memory dump.

Definition of Computer Forensic:

Forensic is the process of using experimental knowledge for collecting, examining, and presenting evidence to the courts. Forensic deals basically with the recovery and analysis of evidence [3]. Evidence can be taken in many forms, for example fingerprints left on a window to DNA evidence found from blood stains to the files on a hard drive. Computer forensic is the method that combines both law and computer science to collect and analyze data from computer, computer networks, wireless transmission devices, and storage devices in a way that is allowed as evidence in a court of law [4]. The three main steps in any computer forensic analysis are

***Corresponding Author:** Dr.N.M.Elango, **Email**: elango.nm@vit.ac.in

acquiring the data, authenticating, and analyzing of the data. Collecting the data mainly involves creating a bit-by-bit copy of the hard drive. Authentication is the making sure of that the copy used to do the analysis is an exact copy of the contents of the original hard drive by comparing the checksums of the copy and the original. If deleted data could not be recovered through the use of common forensic tools, more sensitive equipment can be used to extract the data, but this is rarely done because of the high cost of the instruments. Computer forensic is the process of gathering electronic evidences during an investigation. In order to use this information to litigate a criminal act, evidences must be collected carefully and legally. Computer and Network forensic ways of doing things are used to discover evidence in a variety of crimes ranging from theft of trade secrets. The goal of computer and network forensic is to provide acceptable evidence to allow the criminal to be successfully prosecuted.

Computer Forensics Needs to the present World

The need for computer forensic has become more with the increase in the number of computer crimes and lawsuits in which large organizations are involved. It has become a need for organizations to either employ the services of a computer forensic agency or hire a computer forensic expert in order to protect the organization from computer events or solve cases involving the use of computers and related technologies [5].

The financial lose caused as a result of computer crimes have also added to a renewed interest in computer forensic. Computer forensic offers the following benefits to organizations:

- It ensures the integrity and makes sure of the overall performance and continued existence of an organization's computer system and network infrastructure.
- Helps the organization take by force important information if their computer systems or networks are damaged.
- Extracts, processes, and explains the actual evidences in order to prove the attacker's actions and the organization's innocence in court.
- It helps to finds computer criminals and terrorists from different parts of the world. Computer criminals and terrorists that use the Internet as a communication medium can be found and their plans known. IP addresses play a very important role in finding out the locations of the position of terrorists.
- Saves the organization money and valuable time. Many managers set apart and distribute a large amount of their IT budget for computer and network security.
- Tracks complicated cases such as child pornography and e-mail spamming.
- A computer forensics expert secures of that the following rules are identified as correct during an investigation:
- No possible evidence damaged, destroyed, or came to agreement by the forensic procedures used to investigate the computer evidences.
- No possible computer harmful programs or apps is introduced to the computer being installed during the analysis process evidences.

In a crime involving the use of technology, the evidences so furnished will also be in some electronic form. At times it becomes very hard to test the truthfulness of such evidences, in presence of expert. Here comes the role of computer forensic [6]. Forensic generally means the use of science and technology to establish facts in courts of law. When prefixed by the word computer, it obviously means the relation with computer space. We term them as 'electronic evidence'. They are commonly defined as collection, preservation, and analysis and court presentation of computer related evidences.

The main objectives of computer forensics

The overall goal of all computer forensic phases' preservation, identification, extraction, and documentation is to detect a computer event, identify the intruder, and prosecute the criminal in a court of law. With an increase in computer crime events ranging from theft of intellectual property rights to computer terrorism, the goals of computer crimes are becoming more widespread in nature.

The main goals of computer forensic can be summarized as follows:

- To recover, carefully study, and preserve the computer and related materials in a manner that can be presented as evidence in a court of law
- To identify the evidence in a short amount of time, guess the possible result of the malicious activity on the victim, and

evaluate the intent and identity of the criminal.

Methodologies used in computer forensics

Computer forensic tools and ways of doing things are major components of an organization's disaster recovery and play a clear role in overcoming and handling computer evidences. Due to the growing of computers the criminal activity also grown, there should be a proper set of ways of doing things to use in an investigation. The evidence which is received from computers is delicate and breakable and can be easily erased or changed, and the taken computer can be damaged if not handled using proper ways of doing things. The methodology involved in computer forensic may differ depending upon the procedures, resources available and also the target company.

Forensic tools enable the forensic examiner to recover deleted files, hidden files, and also the temporary data that the user may not locate.

A forensic investigator must focus on basic areas such as standalone computers, workstations, servers, and online channels. Investigation of standalone PC's and workstations and other removable media can be simple. Investigation of servers and online channels, however, it is little bit complicated and tricky [7].

During investigation, logs are often not examined or audited. The investigator must understand that logs files play an important role during the investigation. They must be given due importance, as they could provide a lead in the case.

Computer forensic ways of doing things consist of the following basic activities:

- **Preservation:** The forensic investigator must preserve the integrity and integrity of the originally collected evidence. The original evidence should not be altered or damaged. The forensic examiner must make an image or a copy of the original evidence and then he should do the analysis on that image or copy. The examiner must also compare the copy with the original evidence to identify any changes or damage.
- **Identification:** Before commencing the investigation , the forensic investigator must identify where the evidence is present and its location. For example, evidence may be contained in internal hard disks, removable storage media, or log files. Every forensic examiner must understand the difference between actual evidence and the evidence containers. Locating and identifying information and data is a challenge for the digital forensic investigator. Different examination processes such as keyword searches, log file analyses, and system checks help an investigation.
- **Extraction:** After identifying the evidences, the forensic examiner must extract data from it. Since dangerous and unstable data can be lost at any point, the forensic investigator must extract this data from the copy made from the original evidence. This extracted data's must be compared with the original evidence and carefully studied.
- **Interpretation:** The most important role a forensic examiner plays during investigation is to understand what he or she has actually found. The inspection and analysis of the evidence must be understood and also explained in a clear manner.
- **Documentation:** From the beginning of the investigation until the end evidence is presented before a court of law, forensic examiners must maintain documentation relating to the evidence. The documentation contains the chain of custody of the evidences gathered and documents relating to the evidence analysis.

Testing the Evidences:

After the evidence is collected, investigators do general tests on the evidence to decide the following:

1. Authenticity: The investigator must figure out the source of the evidence.
2. Reliability: The investigator must find out the evidence is reliable and perfect.

Steps Involved in Forensic Investigation

These are the following steps which are followed in forensic investigation they are explained below

1. The investigation process is started at the moment of computer crime was suspected
2. Immediately the investigator should gather the preliminary evidences which includes taking photograph of the scene and also marking the evidence
3. A legal court warrant should be obtained be seizure of the data's
4. Investigator has performed first responder procedures.

5. Evidences which are captured from the crime scene are numbered and secured safely
6. The gathered evidence should be taken carefully to the forensic laboratory
7. The evidences are created into two bit stream copies. The original disk should not be tampered
8. An hashing algorithm is used to generate checksum of the disk images
9. A report of chain of custody has o be maintained. If any change to this chain the evidence is questionable at the time of admissibility in court.
10. Original evidence has to be kept safe and secured preferably it can be kept in a location of which it cannot be accessed easily.
11. We have to analyze the image copy for evidence.
12. A detailed forensic report has to be prepared. Which includes the forensic methodology and recovery tools used?
13. The report has to be submitted to the client.
14. If it is needed the forensic investigator may attend the court and he/she has to testify as a witness.

Computer forensic tools for acquiring the data:

Many Digital tools are available during a digital investigation, some are specific toward forensic. The different phases from the digital forensic investigation process explained below. There are many hardware and software tools were used in forensic investigation for collecting and analyzing the data [8].

Encase Forensic Suite:

This is windows based tool and also court-validated computer forensic software. The functionalities of Encase are explained below [9]:

1. Analyzing the file signatures.
2. Conditions and queries are filtered.
3. Finding deleted files and file fragments from slack space.
4. Recovering the deleted folders.
5. Analysis of log file and event log.
6. Searching file type.
7. External file viewer and registry viewer.

Forensic Tool Kit(FTK):

Forensic Toolkit, or FTK, is computer forensic software made by Access Data. It scans a hard drive looking for different information. It can for example locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encrypted code [10].

The toolkit also includes a standalone disk imaging program called FTK Imager. The FTK Imager is a simple but well-said tool. It saves an image of a hard disk in one file or in parts that may be later on rebuilt. It calculates MD5 hash values and confirms the integrity of the data before closing the files. The result is an image file that can be saved in multiple formats, including DD raw

Win Hex Tool:

It is a universal Hex editor tool which is mainly used in computer forensics for data recovery, low level editing of data. The main functionalities are explained below

1. Cloning and imaging of disk
2. Hex view of the file
3. Calculating mass Hash value of the files (MD5,SHA,SHA-1,SHA 4,MD4,RipeMD….)
4. Gathering free space, inter partition space and slack space and generic texts from images and drives
5. Creating files and directory for all computer media
6. Unifying and dividing even and odd words/bytes
7. Concatenating and splitting up of the files
8. Comparing and analyzing the files
9. Search and replacing the functions
10. Detection of NTFS and Alternate data streams(ADS)
11. Physical and logical search done at a time

Digital Forensics Framework:

Digital forensic framework is another popular platform dedicated to digital forensic. The tool is open source and comes under GPL License. It can be used either by professionals or non-professionals without any trouble. This tools is used for maintaining the digital chain of custody, to access the remote or local devices, forensic of Windows or Linux OS, recovery hidden of deleted files, quick search for files' meta data, and different other things.

CAINE:

CAINE (Computer Aided Investigative Environment is the Linux based tool created for digital forensic. It offers an atmosphere to join together an existing software tools as software modules in a user friendly manner. This tool is an open source.

List of Forensic Tools

No	Name of the Software	Website
1	X ways Forensics 16.3 Integrated computer forensics Software	www.X-ways.net.
2	WinHex 16.3 : Computer Forensics & Data Recovery software ,Hex Editor & Disk Editor	www.X-ways.net.
3	Forensic Tool Kit - FTK is the industry-standard in computer forensics software used by government agencies and law enforcement for digital investigations.	http://accessdata.com /products/computerforensics/ftk
4	Encase forensics V 7	http://www.guidance software.com
5	S tools (Stegnography tool) : text files hiding inside images.	http://www.spychecker.com/program/stools.html.
6	Camouflage - hide your files inside a jpeg image!	http://freesoftwareproject.weebly.com/free-filecamouflage.html.
7	Slueth Kit + Autopsy Browser – Forensic Tool Set	http://www.sleuthkit.org.
8	Passware Kit: Password Cracking	http://www.lostpassword.com/kitenterprise.htm.
9	History viewer (Show all browser as well as user activities)	http://www.historyviewer.net/index.html.
10	Child Key logger/ family Key logger – Storing key strokes	http://www.familykeylogger.com/.
11	Stegnos privacy suite -2012 provide secret safe. Deposit all your important documents, private photos and videos in Steganos Safe 2012 – out of reach for others and highly secure	http://www.steg
12	Email Tracker pro – Email tracing and Spam filtering	http://www.emailtrackerpro.com.

CONCLUSION

It is quite important achievement for police and law enforcing officers that India has kept pace with the changing towards the technology and introduced very important changes in its laws to be controlled by the demands of technology. The only thing which needs a special and extremely important attention is the training communicated to the putting into use people in charge so that the provisions are well enough enforced. Hopefully in years to come this problem will also be redressed and the country will witness a totally new, refreshed and technically sound legal and enforcement framework.

With the help of these few popular digital forensic tools used by different law enforcing agencies using in performing crime investigation. In this paper, I added all kind of tools like higher price/higher cost, free, open source, computer forensic, mobile forensic and others. If you are going to start learning digital forensic, you can download or buy these tools and start working on those. It will help you in better understanding the whole process and tools. With the increasing use of digital data and mobile phones, digital forensic has become more important. Computer crimes are also increasing day by day. So companies are also trying to launch more powerful version of the tools, and you need to be in touch of latest digital forensic news to know about recent releases.

REFERENCES

1. Ramesh Babu CH. Computer Intrusion Forensics. International Journal of Emerging Technology in Computer Science & Electronics. 2014; 11(1): 15-17.
2. John JL. Digital Forensics and Preservation. DPC Technology Watch Report.2012; P:1-66.
3. Kaur M, Kaur N, Khurana S. A Literature Review on Cyber Forensic and its Analysis tools. International Journal of Advanced Research in Computer and Communication Engineering. 2016; 5(1):23-28.
4. "Computer Forensics", US-CERT, 2008.
5. EC-Council. Computer Forensics: Investigation Procedures and Response (CHFI). Cengage Learning, 2016. P:1-208.
6. Samarth. Cyber Forensics & Electronic Evidences: Challenges In Enforcement & Their Admissibility. 2012.
7. Investigation Procedures and Response EC-Council | Press.2010.P:1-171.
8. Sindhu KK, Mesh ram BB. Digital Forensic Investigation Tools and Procedures.I.J. Computer Network and Information Security, 2012;4: 39-48.
9. http://www.WinHex.com
10. CTI Reviews. Investigating High-Tech Crime. Cram101 Textbook Reviews, 26-Sep-2016 - Education - 29 pages.