Resent Trends in Digital & Computer Forensics

Ms.N.D.Sonwane [1], Mr.S.P.Taley [2], Ms.P.K.Karmore [3]

[1] *Assistant Professor, Computer Science & Engineering, DBACER, Maharashtra, India*
[2] *Assistant Professor, Information Technology, DBACER, Maharashtra, India*
[3] *Assistant Professor, Computer Science & Engineering, DBACER, Maharashtra, India*

ABSTRACT

Digital forensics is the science of identifying, extracting, analysing and presenting the digital evidence that has been stored in the digital devices. Various digital tools and techniques are being used to achieve this. Our paper explains forensic analysis steps in the storage media, hidden data analysis in the file system, network forensic methods. Digital evidence can be useful in a wide range of criminal investigations including homicides, sex offenses, missing persons, child abuse, drug dealing, fraud, and theft of personal information. Also, civil cases can hinge on digital evidence, and electronic discovery is becoming a routine part of civil disputes.

Keyword: - *Digital Forensic Tool, Network Forensic Tool, Packet Sniffer tool, Dynamic link libraries*

1. INTRODUCTION

A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in the Cyber space or digital world. The investigation process is as follows (As per National Institute of Standards and Technology) [1].

Collection phase: The first step in the forensic process is to identify potential sources of data and acquire forensic data from them. Major sources of data are desktops, storage media, Routers, Cell Phones, Digital Camera etc. A plan is developed to acquire data according to their importance, volatility and amount of effort to collect [2].

Examination: Once data has been collected, the next phase is to examine it, which involves assessing and extracting the relevant pieces of information from the collected data [2].

Analysis: Extracted and relevant data has been analysed to draw conclusions. If additional data is sought for detail investigation will call for in depth data collection.

Reporting: This is the process of preparing and presenting the outcome of the Analysis phase. Computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored as data or magnetically encoded information. To effectively combat cybercrime, greater emphasis must be placed in the computer forensic field of study, including but not limited to financial support, international guidelines and laws, and training of the professionals involved in the process, as well as the following subject matter:

Computer crime
The computer forensic objective
The computer forensic priority
The accuracy versus speed conflict
The need for computer forensics
The double tier approach

1.1 COMPUTER FORENSICS SERVICES

A computer forensics professional does more than turn on a computer, make a directory listing, and search through files. Your forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case. For example, they should be able to perform the following services:

1) Data seizure
2) Data duplication and preservation
3) Data recovery
4) Document searches
5) Media conversion
6) Expert witness services
7) Computer evidence service options

1.2 BENEFITS OF PROFESSIONAL FORENSICS METHODOLOGY

Protection of evidence is critical. A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that

1) No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer

2) No possible computer virus is introduced to a subject computer during the analysis process

3) Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage

4) A continuing chain of custody is established and maintained

No matter how careful they are, when people attempt to steal electronic information (everything from customer databases to blueprints), they leave behind traces of their activities. Likewise, when people try to destroy incriminating evidence contains on a computer (from harassing memos to stolen technology), they leave behind vital clues. In both cases, those traces can prove to be the smoking gun that successfully wins a court case. Thus, computer data evidence is quickly becoming a reliable and essential form of evidence that should not be overlooked.

2. TYPES OF MILITARY COMPUTER FORENSIC TECHNOLOGY

The U.S. Department of Defense (DoD) cyber forensics includes evaluation and in-depth examination of data related to both the trans- and post-cyber-attack periods. Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and assessment of the intent and identity of the perpetrator. Real-time tracking of potentially malicious activity is especially difficult when the pertinent information has been intentionally hidden, destroyed, or modified in order to elude discovery. The information directorate's cyber forensic concepts are new and untested. The directorate entered into a partnership with the National Institute of Justice via the auspices of the National Law Enforcement and Corrections Technology Centre (NLECTC) located in Rome, New York, to test these new ideas and prototype tools. The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership. This first of- a-kind event represents a new paradigm for transitioning cyber forensic technology from military research and development (R&D) laboratories into the hands of law enforcement. The experiment used a realistic cybercrime scenario specifically designed to exercise and show the value added of the directorate-developed cyber forensic technology.

2.1 TYPES OF LAW ENFORCEMENT COMPUTER FORENSIC TECHNOLOGY

Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information (data). Often the computer evidence was created transparently by the computer's operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and, thus, special forensic software tools and techniques are required to preserve, identify, extract, and document the related computer evidence. Computer forensics tools and techniques have proven to be a valuable resource for law enforcement in the identification of leads and in the processing of computer related evidence. Computer forensics tools and techniques have become important resources for use in internal investigations, civil lawsuits, and computer security risk management. Forensic software tools and methods can be used to identify passwords, logons, and other information that is automatically dumped from the computer memory as a transparent operation of today's popular personal computer operating systems. Such computer forensic software tools can also be used to identify backdated files and to tie a diskette to the computer that created it. Law enforcement and military agencies have been involved in processing computer evidence for years. This section touches very briefly on issues dealing with Windows NTR, WindowsR 2000, XP and 2003 and their use within law enforcement computer forensic technology.

2.2 SPECIALIZED FORENSICS TECHNIQUES

A computer forensics specialist has many duties and responsibilities relating to computer systems analysis, such as:

• Protecting the computer system from any tampering, data corruption, damage, or viruses
•Ensuring that the computer system is not destroyed or damaged in any way
•Discovering all hidden, deleted, encrypted, or password protected files
•Recovering as much as possible about the deleted files and accessing the protected or encrypted files

Before the investigation starts, it is vital that the computer is handled with care so that no evidence is destroyed or damaged, no computer virus may infect the system, and no evidence is destroyed by mechanical or electromagnetically influences. It is also crucial that the evidence is always kept in custody and that none of the confidential information on the suspect's system is misused. After the expert discovers all hidden files, recovers all deleted files and access all encrypted files, they create an overall analysis in which an overview of the computer system is given and every conspicuous pattern is displayed. The electronic investigations also show which files have been deleted or protected. The computer forensic expert will then assist in the investigation or litigation as a consultant. When computer investigators arrive at a crime scene, they first unplug the computer in case it is running a file-erasure program that could potentially destroy evidence. An image backup (a byte-by-byte copy of a computer's hard drive) is made and used for all examination of the data so that there is no chance of damage to the original drive. The backup will include all active and deleted files, fragments of data not completely overwritten; swap files, embedded data and metadata, and much more. Because of the volatile nature of electronic evidence, simple tasks such as booting up a computer or saving a document can alter data or other files. A computer forensics expert is able to make an image backup without damaging or tampering with potential evidence, which is critical in the legal system. Next, the mirror image is taken to the lab for retrieval and analysis. Some criminals use encryption programs to make their files unreadable, but experts are able to recover encrypted or password protected documents during the retrieval process. A forensics expert can also recover deleted computer files and email, identify what websites have been visited and what files have been downloaded, and find any attempts to conceal or destroy evidence.

3. CONCLUSIONS

Since then, computer forensics has become a popular topic in computer security circles and in the legal community. Like any other forensic science, computer forensics deals with the application of law to a science. In this case, the science involved is computer science, and some refer to it as forensic computer science. Computer forensics has also

been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyse the various levels at which computer data is stored after the fact. Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence.

4. REFERENCES

[1] K. Kent, S. Chevaller, T. Grance and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST SP800-86 Notes 2006.

[2] S. K. Brannon and T. Song, "Computer Forensics: Digital Forensic Analysis Methodology," Computer Forensics Journal, Vol. 56, No. 1, 2008, pp. 1-8.

[3] N. Meghanathan, S. R. Allam and L. A. Moore, "Tools and Techniques for Network Forensics," International Journal of Network Security & Its Applications, Vol. 1, No. 1, 2009, pp. 14-25.

[4] John R. Vacca. *Computer Forensics: Computer Crime Scene Investigation, Second Edition,*ISBN: 1-58450-389-0 ,ISBN-13: 978-1-58450-389-7

[5] Daphyne Saunders Thomas, Karen A. Forch "LEGAL METHODS OF USING COMPUTER FORENSICS TECHNIQUES FOR COMPUTER CRIME ANALYSIS AND INVESTIGATION "Issues in Information Systems, Volume V, No 2, 2004