International Journal of Engineering Technology, Management and Applied Sciences

IJETMAS

www.ijetmas.com February 2016, Volume 4, Issue 2, ISSN 2349-4476

Need for a Computer Forensics in Crime Evidence

Miss.P.Sumathi, Mrs.G.Saktheeswari, Mrs.C.Kuyin ,

Asst.Prof in B.Com(CA)

Jayaraj Annapackiam College For Women (Autonomous)

Periyakulam

ABSTRACT

The Internet is growing explosively, as is the number of crimes committed against or using computers. As a response to the growth of computer crime, the field of computer forensics has emerged. Computer forensics involves carefully collecting and examining electronic evidence that not only assesses the damage to a computer as a result of an electronic attack, but also to recover lost information from such a system to prosecute a criminal. With the growing importance of computer security today and the seriousness of cyber crime, it is important for computer professionals to understand the technology that is used in computer forensics. It promotes the idea that the competent practice of computer forensics and awareness of applicable laws is essential for today's organizations. This paper will discuss the need for computer forensics to be practiced in an effective and legal way.

Key Words: Digital Forensics, Data recovery, Crime Evidence, Finger prints

INTRODUCTION

Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.

CHARACTERISTICS OF COMPUTER FORENSICS

- Identifying
- Preserving
- Analyzing
- Presenting

NEEDS OF COMPUTER FORENSICS

- To Produce evidence in the court that can lead to the punishment of the actual
- To ensure the integrity of the computer system.
- To focus on the response to hi-tech offenses, started to intertwine.

HISTORY OF COMPUTER FORENSICS

The history of computer forensics can be traced to back to the 1970s when military investigators started finding instances of computer-related criminal activity and needed a more comprehensive approach for solving these technical crimes. Many computer forensics degree and training programs now include a History of Computer Forensics course so that students can learn about how this industry developed, and what types of security breaches and cybercrimes have affected individuals and businesses over time. This field did begin in the United States as government personnel realized that they would need investigative protocol to solve cybercrimes and criminal activities related to computers.

GOALS OF COMPUTER FORENSICS

The main goal of computer forensic experts is not only to find the criminal but also to find out the evidence and the presentation of the evidence in a manner that leads to legal action of the criminal.

CYBER CRIME AND EVIDENCE

Cyber Crime occurs when information technology is used to commit or conceal an offence.

DIGITAL EVIDENCE

Any data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or understand by a person or a computer system or other similar device. It includes a display, print out or other output of that data.

- Latent as fingerprint or DNA
- Fragile and can be easily altered, damaged, or destroyed.
- Can be Time Sensitive.

RULES OF EVIDENCE

- **Admissible**
  Must be able to be used in court or elsewhere.
- **Authentic**
  Evidence related to incident in relevant way.
- **Complete**
  Exculpatory evidence for alternative suspects.
- **Reliable**
  No questions about authencity & veracity.
- **Believable**
  Clear, easy to understand and believable by a jury.

TOP 10 LOCATIONS FOR EVIDENCE

- Internet History Files
- Temporary Internet Files
- Slack/Unallocated Space
- Buddy lists, personal chat room records, P2P, others saved areas
- News groups/club lists/posting
- Settings, folder structure, file names
- File storage Dates
- Software/Hardware added
- File Sharing ability
- E-mails

International Journal of Engineering Technology, Management and Applied Sciences

IJETMAS

www.ijetmas.com February 2016, Volume 4, Issue 2, ISSN 2349-4476

COMPUTER FORENSICS METHODOLOGY

- Shut down the computer
- Document the hardware configuration to the system
- Transport the computer system to a secure location
- Make Bit Stream Backups of Hard disk and Floppy disk
- Mathematically verify data on all storage devices
- Document the system date and time
- Make a list of key search words
- Evaluate unallocated Space(Erased files)
- Identify file, program and storage anomalies.
- Evaluate Program functionalities.

APPLICATIONS OF COMPUTER FORENSICS

- Financial fraud detection
- Criminal prosecution
- Civil litigation
- Corporate Security Policy and Acceptable use and violations.

SKILLS REQUIRED FOR COMPUTER FORENSICS APPLICATION

- Programming or Computer-related experience
- Broad understanding of operating systems and applications
- Strong analytical skills
- Strong Computer science fundamentals
- Strong System administrative skills
- Knowledge of cryptography and steganography
- Strong Understanding of the rules of evidence and evidence handling
- Ability to be an expert witness in a court of law

USES OF COMPUTER FORENSICS

More recently, commercial organizations have used computer forensics to their benefit in a variety of cases such as:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the work place
- Regulatory compliance

CONCLUSION

The role of computer forensics will play a large role in society as computer technology emerges. It is an extremely hot topic and is used widely among all industries. Corporations and government agencies hire computer forensics specialists whenever they need a computer-related crime investigated. The specialists gather evidence from various media and present the evidence to whoever has ordered it or in some cases, in a court of law. With the growing importance of computer security today and the seriousness of cyber crime, it is important for computer professionals to understand the technology that is used in computer forensics.

REFERENCES

- *Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence". Retrieved 26 July 2010.*
- *Leigland, R (September 2004). "A Formalization of Digital Forensics"*
- *A Yasinsac; RF Erbacher; DG Marks; MM Pollitt (2003). "Computer forensics education". IEEE Security & Privacy. CiteSeerX: 10.1.1.1.9510.*
- *Warren G. Kruse; Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5. Retrieved 6 December 2010.*
- *Gunsch, G (August 2002). "An Examination of Digital Forensic Models"*
- *Adams, R. (2012). "'The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice".*
- *Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier. ISBN 0-12-163104-4.*
- *Various (2009). Eoghan Casey, ed. Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 0-12-374267-6. Retrieved 27 August 2010.*
- *Garfinkel, S. (August 2006). "Forensic Feature Extraction and Cross-Drive Analysis"*
- James Wardell and G. Stevenson Smith, " Recovering Erased Digital Evidence from CD-*RW Discs in a Child* Exploitation Investigation", International Journal of Digital Forensics & Incident Response".
- *www.wikipedia.com*
- *www.computerforensics.in*
- *http://www.forensics-research.com/index.php/computer-forensics/computer-forensics-history/*
- *http://forensicswiki.org/wiki/Websites*
- *http://www.computerforensics.com/expert-in-your-corner.html*
- *https://forensiccontrol.com/resources/beginners-guide-computer-forensics/*