Review:Computer Forensics Technology

Prof.Nutan Sonwane
Department of Computer Science & Engineering
DBACER,Nagpur
Nagpur India

Prof. Saurabh Taley
Department of Information Technology
SDMP,Nagpur
Nagpur,India

Abstract

Computer Forensics World is a growing community of professionals involved in the digital forensics industry. It is an open resource, free for all to access and to use. Digital investigations and crime regularly cross international and language borders today. Open database connectivity technology is now providing access to a wide range of database technologies, such as neural networks and pattern recognition databases, which are being used to analyze shoe prints and tool marks. These new Computer-aided analysis tools can link and chart case information, allowing the investigator to question the data and pose scenarios as well as suggest and follow possible investigative paths.

Keywords—*Forensics, recognition, investigation*

I. INTRODUCTION

Computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored stored as data or magnetically encoded information. The fascinating part of the science is that the computer evidence is often transparently created by the computer's operating system without the knowledge of the computer operator. The information may actually be hidden from view. To find it, special forensic software tools and techniques are required. Most law enforcement agencies, especially those in large cities, are understaffed when it comes to having trained computer forensics experts. Industry, on the other hand, has been taking computer forensics seriously for several years. Sadly, it took a number of embarrassing computer break-ins by teenage hackers to put the spotlight on it. The problem is, industry doesn't know which computer forensics issues to focus on. The biggest issue surrounding the computer forensics conundrum is a shortage of technologists who have a working knowledge of computer forensics. Academics are teaching the subjects, but most lack real-world experience, which is critical when training students. Also, many academics are not current with forensics trends and tools.

II. TYPES OF COMPUTER FORENSICS TECHNOLOGY

Defensive information technology will ultimately benefit from the availability of cyber forensic evidence of malicious activity. Criminal investigators rely on recognized scientific forensic disciplines, such as medical pathology,
to provide vital information used in apprehending criminals and determining their motives. Today, an increased opportunity for cyber crime exists, making advances in the law enforcement, legal, and forensic computing technical arenas imperative. As previously explained, cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime. Cyber forensics focuses on real-time, online evidence gathering rather than the traditional offline computer disk forensic technology.
Two distinct components exist in the emerging field of cyber forensics technology. The first, computer forensics, deals with gathering evidence from computer media seized at the crime scene. Principal concerns with computer forensics involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes.

A. Military Computer Forensics Technology

The U.S. Department of Defense (DoD) cyber forensics includes evaluation and indepth examination of data related to both the trans- and post-cyberattack 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 Center (NLECTC) located in Rome, New York, to test these new ideas and prototype tools.

B. Law enfourcement Computer Forensics Technology

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.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.

C. Business Computer Forensics Technology

Today, many computer forensics workshops have been created to familiarize investigators and security personnel with the basic techniques and tools necessary for a successful investigation of Internet and computer-related crimes. So many workshops have been created that it is beyond the scope of this chapter to mention them all. However, throughout the book, a number of them will be mentioned in detail. Workshop topics normally include: types of computer crime, cyber law basics, tracing email to its source, digital evidence acquisition, cracking passwords, monitoring computers remotely, tracking online activity, finding and recovering hidden and deleted data, locating stolen computers, creating trackable files, identifying software pirates, and so on.

Conclusion

As compare among all available technology the hybrid technologies are good response technologies. Hybrid *technology* is an approach to enterprise computing where organizations provide and manage some information resources in-house while using cloud-based services for others. Organizations are able to maintain a centralized approach to Information Technology governance while also experimenting with cloud computing. This has led to the term "hybrid IT," which is often used interchangeably with "hybrid cloud."*Emerging technologies* can be defined as radically novel and fast-growing technologies that are persistent over time, and with the potential to exert a considerable impact on the socio-economic domain. They span a variety of industries from Agriculture, Aviation, and Entertainment to Electronics, Displays, and Information Technology.

References

[1]. Pankaj Gupta, Jaspal Singh, Anterpreet Kaur Arora, "Digital Forensics- A Technological Revolution in Forensic Sciences" ISSN 0971-0973, April-June 2011

[2]. John R Vacca " Computer Forensics ,computer forensics scene investigation" Second edition.

[3]. Nathan Balon ,Ronald Stovall ,Thomas Scaria "Computer Intrusion Forensics" CIS 544