Digital Forensic a Novel Way to Investigate E-Crime

Dr. P. K. Sahoo
Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science & Technology. Yamnampet, Ghatkesar, RR DIST, Hyderabad, TS

Nikhila Vinjamuri
B. Tech 4th Year Student, Sreenidhi Institute of Science & Technology Yamnampet, Ghatkesar, RR DIST, Hyderabad, TS

Abstract - The society is facing a serious security problem because of the increasingly dependence over the Internet for e-commerce, business, education etc. This leads to a situation where hackers are actively exploits individuals, organization and the society as a whole by taking advantages of the new cyber threats and information security issues. Now a day's Viruses, Worm attacks, Denial of Service attacks and Phishing attacks becoming the news headlines. Every day there are reports of loss of critical data, cyber attacks, hacking of systems and web sites etc. The numbers of computer crimes are increasing exponentially day by day. In this scenario digital forensic is a novel way to investigate and to protect the vital documents from cyber attacks. This paper presents the digital forensic methodology to investigate and to protect individuals, industries and the society as a whole form computer related crimes. The proposed methodology uses log files as the main source of evidence for investigation. The solution proposed here greatly simplifies the process of log analysis by centralizing the logging process from all the devices present in the network and also provide a secured storage for the log data which is very essential for forensic investigation.

Keywords: cyber security, cyber forensic, Forensic Tools, cyber attacks, log files.

I. INTRODUCTION

There are continuous reports of internet security problems due to the increased dependency over the Internet by organizations and individuals to carry out critical business processes. As society grows increasingly dependent on the Internet for commerce, banking, and mission-critical applications, the ability to detect and neutralize network attacks is becoming increasingly significant [1]. As the world becomes more interconnected through the Internet and more government agencies and businesses moving their assets to the Internet, cyber crimes are getting more sophisticated, more organized and on the exponential rise. The computer crimes affect our daily lives and national security deeply, especially in this information epoch, the expanding wave of Internet connectivity and digital technologies bring us a lot of convenient, at the same time they also offer criminals more chance to commit crime [2]. The number of cyber attacks increased by 93 percent from 2009 to 2010, reports security vendor Symantec. The company said 286 million new threats were reported last year, including attacks on corporate systems and those that occurred via social networks [3]. For governments, cyber crimes threaten national security. For businesses, cyber crimes damage profit and shake the trust of consumers. Unlike traditional crimes, cyber crimes operate in a different domain space – posing new and challenging problems. Cyber Crime is increasing at an alarming rate. The number of Cyber Crimes in India may touch a humongous figure of 3, 00,000 in 2016, almost double the level of last year. The study revealed that in the past attacks have been mostly initiated from the countries such as US, Turkey, China, Brazil, Pakistan, Algeria, Turkey, Europe, and the UAE, and with the growing adoption of internet and Smartphone. India has emerged as one of the most favorite countries among cyber criminals.

1.1 GROWTH OF CYBER CRIME CASES IN INDIA (2011 – 2015)

The statistics that have been demonstrated and observed show the seriousness of Cyber Crimes in India. The country has registered 107% of CAGR (Common Annual Growth Rate) in the number of Cyber Crimes registered in last few

years. Nearly 13,301 Cyber Crime cases were registered in 2013 by Mahindra. The number increased by almost 50 percent in the following year, reaching 22,601 . The statistics of 2014 shows the unexpected increase; making the count of cyber crime cases reach 71,708 . Surprisingly, in 2015 the number of cases registered under Cyber Crime laws increased by more than 100% to 1, 49,254.It further stated that mobile frauds have also become an area of concern for companies as 35-40 percent of financial transactions are done via mobile devices these days and this number is expected to grow to 55-60 percent by 2016.

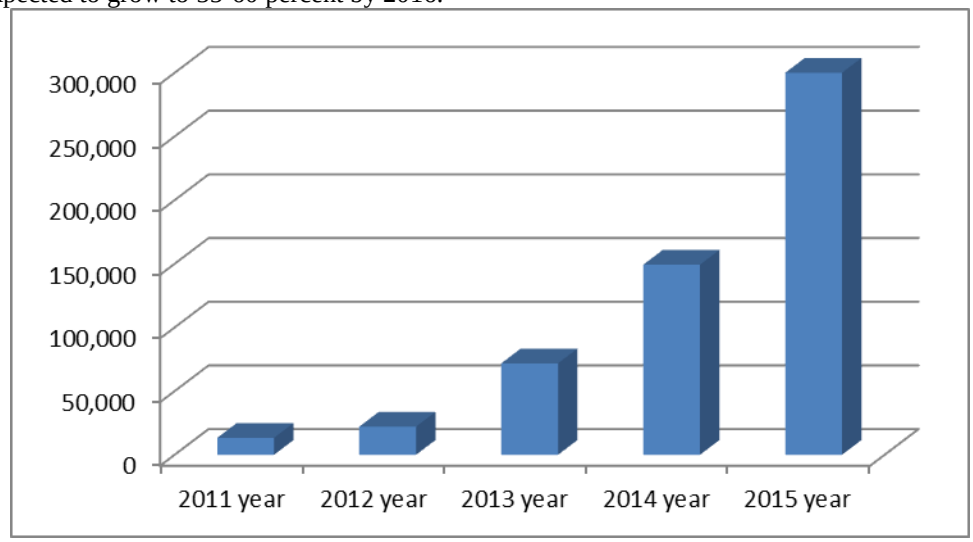

Fig:1 The statistics collected by Assocham-Mahindra SSG Study from 2011 to 2015 in India.

Breaches of personally identifiable information have increased dramatically over the past few years and have resulted in the loss of millions of records, which creates a serious security problem both for the individuals and organizations [4]. Security and privacy become great concern for this new world. To meet this challenge, Cyber Trust Program at National Science Foundation has adjusted its research funding directions [5]. Current Web browsers are plagued with vulnerabilities, providing hackers with easy access to computer systems via browser-based attacks [6]. Computer and network attacks are the product of an attackers understanding of the strengths and weaknesses in the operating systems, features of popular software, networking protocols and programming languages [7]. In the recent development stated above, security log data are very useful as security device logs that trace possible attacks from the attackers and record the day-to-day activity of system users. In recent years, it has become important for researchers, security incident responders and educators to share network logs and many log tools and techniques have been developed to sanitize this sensitive data source in order to enable more collaboration. Unfortunately, many more attacks have been created, in parallel that try to exploit weakness in the process [8]. In most of companies or organizations, logs play important role in information security [9]. Logs are one of the most fundamental resources to any security professional. It is widely recognized by the government and industry that it is both beneficial and desirable to share logs for the purpose of security research [10]. Today log traces are widely used to identify and prevent violations of corporate information systems [11].

II. DIGITAL FORENSIC

Digital forensic is a scientifically proven method to investigate computer related crime. The use of scientific methods towards the collection, preservation, analysis, Interpretation, documentation and presentation of digital evidence derived from digital sources is an excellent way of investigation of digital crime. A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in the Cyber space or digital world [12]. Digital forensic techniques are basically used to trace the user's IP address, DNS and other details. Digital forensic examination may focus on identifying transactions within a database system or application that indicate evidence of wrong doing, such as fraud [13]. Hence forth identifying who, when and how modified or tampered the data. Digital forensic usually performs in six steps as given below: -

1. Identification
2. Collection

3. Preservation
4. Examination
5. Analysis
6. Presentation/report.

The three main steps in any computer forensic investigation are acquiring, authenticating, and analyzing of the data. Acquiring the data mainly involves creating a bit-by-bit copy of the hard drive. Authentication is the ensuring that the copy used to perform the investigation is an exact replica of the contents of the original hard drive by comparing the checksums of the copy and the original. Analysis of the data is the most important part of the investigation since this is where incriminating evidence may be found. Data recovery is another important aspect of the forensics investigation. Tracking the hacking activities within a compromised system is also important. With any system that is connected to the Internet, hacker attacks are as certain as death and taxes. Although it is impossible to completely defend against all attacks, as soon as a hacker successfully breaks into a computer system the hacker begins to leave a trail of clues and evidence that can be used to piece together.

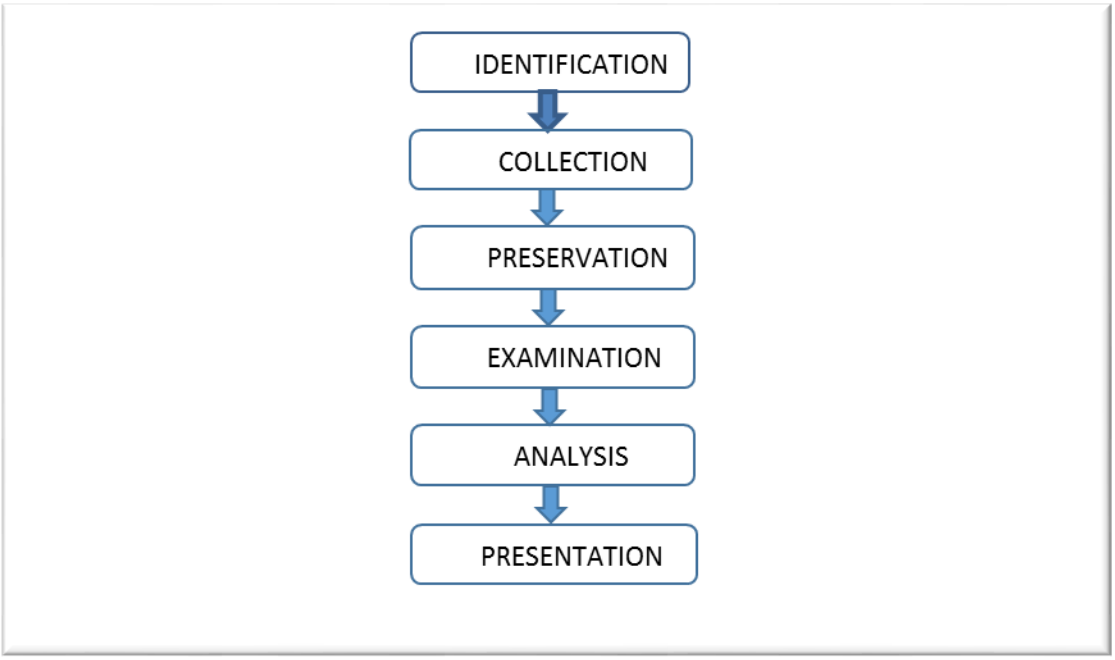

Fig 1: Shows the various steps in digital forensic.

Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis. The first step is to identify the evidence that is related suspect data. The digital evidence can be of any form such as CD, floppy disk, hard disk, pen drive and so on. Next step is to preserve this evidence in a safe storage. Then next step is to examine these collected evidences. The examination of suspect data determines the details such as origin and content of the evidence. Here examination pays attention to various factors related to crime such as who used it and why? Then analysis is followed, which analyses the digital evidence without modifying the data. Digital evidence is extremely volatile; once the evidence is contaminated it cannot be decontaminated. After collecting various proofs and following the steps of digital forensic there is the need of documenting or making a report of the chain of the custody which is the roadmap followed for collection of digital evidence is to be documented and shown to jury during the course of investigation.

2.1 TOOLS USED IN DIGITAL FORENSIC

- EnCase: EnCase is a fully-featured commercial application tool, which enables an investigator to examine the data from hard disks, removable media (such as floppy disks and CDs) and even Palm PDAs (Personal

Digital Assistants) and also to prepare a image. This simple tool allows forensic examiners to write small programs, or scripts, which can perform highly customized searching and filtering of the data which has been imaged.

- Vogon Forensic Software: The Vogon is imaging software used to create an exact replica of the data on a drive, which can then be indexed by the processing software to allow fast searching by the investigation committee. Vogon's also offers similar functionality to that of EnCase by simplifying the process of data imaging and search operation for the examiner with a little less cost.

- SafeBack: SafeBack is another commercial computer forensics tool commonly used by law enforcement agencies throughout the world. It is primarily used to store the original data used in the investigation process and it one of the best tool for preserving the digital information. It has no capability to do analysis.

III. LOG FILES, THE PRIME SOURCE FOR DIGITAL FORENSIC

Log file is a computer generated file which contains information about the user access to the system or data manipulation done by the user. Log file contains list of events, which have been logged by a computer. The best way to investigate crime using digital forensic by taking the help of the log files with the help of forensic tool. Log files are often created or generated during software installations and are created by web servers. Most of the log files are saved in the plain text format, which minimizes their file size and allows them to be viewed in a basic text editor. Log file don't have standard format. It is the biggest challenge to have a uniform log file format to communicate with all the log sources. To make the log file understandable to everyone and to have a uniform log format, some consortiums came forward to suggest some standards for log files. There are two well known log formats available as explained in table 1 and 2.

1) W3C extended format.
2) Web star format.

Table 1: Web Star Log's Major Attributes

DATE	Date of request.
URL	The requested item. Same as **CS-URI** and **CS-URI-STEM**.
HOSTNAME	Name or IP address of the requesting computer.
TIME	Time of request.
BYTES	Bytes sent, same as **BYTES_SENT**. Required for all of the Bytes related columns in various reports.
SC-STATUS	It is same as a STATUS field.
REFERRER	Site and page that referred the visitor to your site

Table 2 W3C Extended Log's Major Attributes

DATE	Date of the request.
CS-URI	The requested item
C-IP	Client IP addresses.
TIME	Time of request.
BYTES	Bytes sent.
SC-STATUS	Result code.
CS(REFERER)	Site and page that referred the visitor to your site.

A) Different Types of Log Data

1. Network device logs.
2. Firewall logs.
3. Web server log files.
4. System log files.

1. *Network Device Logs*: For communication in the network there is a need of various internetworking device like routers, hubs, switches etc., in which most of the devices maintain their own log files. So these log files are called as the networking device logs. These logs data maintain or contain the information of the network traffic.

2. *Firewall Logs*: Firewall is the combination of both software and hardware. It is installed in the network in order to monitor the network's incoming and outgoing traffic. Firewall follows some predefined rules by following these set of rules allows the information or disallows based on the rules. These logs reveal a lot of information about the security threat attempts on the network and on the nature of the traffic coming in and going out of the firewall. It provides real time information to the administrators on the security threat attempts so that they can swiftly initiate any action.

3. *Web Server Logs*: A web server log file is a log file or these are several log files created and maintained by the server. Web server's uses log files to record data about website visitors. This information includes the IP address of each visitor, time of visit and other details. This data can be processed by the website statistics software, which can display the information in a user friendly format.

4. *System log files*: System log files manage the information generated by the kernel and system utilities. Detailed information about the various activities of the operating system is captured in these system log files.

IV. CONCLUSION

Security- related threats are becoming headlines in news papers and magazines because of the damage they made to the individuals and the society. As the internet grows due to the increasing demand by organizations and individuals, the attackers are taking advantages of the vulnerabilities of the host and networks and are able to access the vital data. Hence protecting the very significant data of the society is a challenge of the hour. This paper discusses the issues in cyber security and information security and suggests way to investigate various computer related attacks. No doubt in this scenario digital forensic play a significant role in the process of detection and identification of the crime by using sophisticated forensic tools. Even though there are many forensic tools available, but tools such as EnCase and Safeback are widely popular because of their efficiency. This paper uses log as the main digital source to do forensic investigation.

REFERENCES

[1] David Watson, Matthew Smart and G. Robert Malan, "Protocol Scrubbing: Network Security Transparent Flow Modification", IEEE/ACM transactions on Networking, vol. 12, no. 2, April 2004.

[2] Virginiah Sekgwathe , Mohammad Talib, "Cyber Forensics: Computer Security and Incident Response", International Journal on New Computer Architectures and Their Applications (IJNCAA) (ISSN 2220-9085) , Vol. 2, Pages 127-137, 2012.

[3] Lee Garber, IEEE International Journal on computer and reliability societies, July/August 2011.

[4] National Institute of Standards and Technology Special Publication 800-122(Draft), 58 pages, January 2009.

[5] Dr. David H.C. Du,"Cyber Security: An Obtainable Goal", the 28th IEEE workshops on International Conference on Distributed Computing Systems, 2008.

[6] Grier, C. Shou Tang King , "Secure Web Browsing with OP Web Browser", IEEE Symposium on Security and Privacy, pages 402-416, May 2008.

[7] McCray, J., "A Roadmap to becoming security conscious", IEEE International workshop on Man and Cybernetics Society, pages 1-9, June 2003.

[8] Honolulu, Hawaii, Proceedings of the 2009 ACM symposium on Applied Computing, pages 1286-1293, 2009.

[9] Ya-Ting Fan Shiuh-Jeng Wang "Intrusion Investigations with Data-Hiding for Computer Log-File Forensics", Proceedings of the IEEE 5th International Conference on Future Information Technology, pages 1-6, May 2010.

[10] Slagell A., Yurcik W., "Sharing computer network logs for security and privacy: a motivation for new methodologies of anonymization", IEEE 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, pages 80-89, September 2005.

[11] Forte, D.V. Maruti, C. Vetturi, M.R. Zambelli "SecSyslog: an approach to secure logging based on covert channels", IEEE first International workshop on Systematic Approaches to Digital Forensic Engineering, Pages 248, November 2005.

[12] K. K. Sindhu and B. B. Meshram, "Digital Forensics and Cyber Crime Data mining," The *Journal of Information Security*, Vol. 3 No. 3, doi: 10.4236/jis.2012.33024., pp. 196-201, 2012.

[13] Shweta Tripathi , Bandu Baburao Meshram, "Digital Evidence for Database Tamper Detection", Journal of Information Security, Vol. 3, Pages 113-12, 2012.

[14] I-Long Lin Hong-Cheng Yang Guo-Long Gu Lin, A.C., "A study of information and communication security forensic technology capability in Tajwan", Proceedings of IEEE International Conference on Security Technology, October 2003, pages 386.

[15] Tian Yue; Li Xiaobin; Yang Zhengqiu, IEEE International Symposium on Computer Science and Computational Technology, Volume 2, Page(s):694 – 697, December 2008.

[16] Takada T, Koike H, "Information visualization system for monitoring and auditing computer logs", Proceedings of IEEE International Conference on Information Visualization, pages 570-576, 2002.

[17] C. Viecco and J. Camp, "A Life or Death of InfoSec Sub-version, "IEEE security and Privacy, vol. 6, no. 5, pp. 74-76, 2008.