International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347- 5552, Volume-1, Issue-2, November, 2013

Proposed Methodology for Secure Image Logging System towards Cyber Forensic

Arun Pratap Srivastava, Rohit Kmar Sharma

Abstract— **In recent years, the importance of cyber forensics (CF) has increased. Meanwhile, society has become considerably digitized, and cybercrime, such as computer attacks or digital data thefts, has increased significantly. Computer forensics is one of the growing concerns in the IT field. Computer forensics is similar to the field of forensics. Police use the science of forensics to scour a crime scene for evidence of what happened, to whom it happened, and who did what to whom. In the case of computer forensics, the crime scene is the machine that was hacked, the victim is the entity to which the computer belongs, and the hacker is the criminal. The evidence in the case of computer forensics is the trail left by the hacker, which is recorded in the log files .log is used as information to investigate the destruction, manipulation, or information leak of digital data and as evidence in the court of law. A log is the general evidence information in a network system and a computing system. Possibility of manipulation or deletion of log information or log file eras ability itself is increasing. Because log files are incriminating evidence against attackers, these files are at risk of attacks. Along with that there is a huge amount of data produced every day. And often it is necessary to store them for a long period of time. Regardless of the type of recorded logs, for reasons of simplicity and convenience, they are usually stored in plain text log files. Both the content type and the storage format suggest that it is possible to significantly reduce the size of log files through lossless data compression. Therefore, a mechanism is needed for reducing the size of log file and to prevent the manipulation and deletion of log info and log files by attackers and maintain the contents of log files .In this paper, implement multi thread server which stores the image files of the web log file after applying lossless compression over web log file at the same time that is recorded and makes log files. We suggest the compressed image log file as evidence about the cyber forensics.**

Keywords— **Cyber forensic, Lossless compression, Log file.**

I. INTRODUCTION

In recent years, the importance of cyber forensics (CF) has increased. Meanwhile, society has become considerably digitized, and cybercrime, such as computer attacks or digital data thefts, has increased significantly [1]. Computer forensics is one of the growing concerns in the IT field [2]. Computer forensics is similar to the field of forensics. Police use the science of forensics to scour a crime scene for evidence of what happened, to whom it happened, and who did what to whom. In the case of computer forensics, the crime scene is the machine that was hacked, the victim is the entity to which the computer belongs, and the hacker is the criminal. The evidence in the case of computer forensics is the trail left by the hacker, which is recorded in the log files [3].log is used as information to investigate the destruction, manipulation, or information leak of digital data and as evidence in the court of law. A log is the general evidence information in a network system and a computing system. A log records information about incidents, such as "time," "id," and "event," as discussed in [4]. By referring to log files, the user or administrator of the system can confirm the active event and the operation event in the system equipment. Relevant data can be collected in multiple places (e.g., network servers, database management systems, user monitoring applications, system services and utilities). In many environments, tracked events can happen very often. As a result, there is a huge amount of data produced this way every day. And often it is necessary to store them for a long period of time. Regardless of the type of recorded events, for reasons of simplicity and convenience, they are usually stored in plain text log files. Both the content type and the storage format suggest that it is possible to significantly reduce the size of log files through lossless data compression, especially if specialized algorithm was used. The smaller, compressed files have the advantages of being easier to handle and saving storage space [12].

The concept of web forensic deals with the process of monitoring access logs, detection of any alteration in log files as well as recovery of those alterations. The significance of web forensic is to investigate web attacks and prevent those in future, using analysis of log file[5]s. In order to carry out a systematic analysis of the hacking Attempt[6], it is advised that the Investigator must investigate all four type of logs namely web server logs, Any third party installed

Manuscript received September 09, 2013.
Arun Pratap Srivastava, Associate Professor, Computer Science & Engineering Department,Vishveshwarya Institute of Engineering & Technology,Dadri, G.B. Nagar,India.(e-mail: arun019@yahoo.com).
Rohit Kmar Sharma, Research Scholar, Computer Science & Engineering Department,Vishveshwarya Institute of Engineering & Technology, Dadri, G.B. Nagar,India (e-mail:rohitzt@gmail.com)

software logs, Operating system logs and client side logs[7][8]. Now we can assume the importance of log files in web forensic. There are many web attacks which are used to alter the integrity of log files like user to root (U2R) attack, in which the intruder exploits some vulnerability associated with the operating system and web server environment of the server machine under attack to perform the conversion from user to root level [9]. In order for computer forensics to be effective, one must have accurate and trust worthy log files. Log files are one of the means available for securing a network against intrusion. Log files record network traffic, taking note of the IP addresses trying to access your network, on which ports access was attempted, time and date of the

attempt, whether or not the attempt was successful, etc. If used correctly log files can be very helpful in maintaining network security and integrity [3]. However, for log files to provide any measure of security logging must be activated and the log file must be checked periodically. Using log files in this manner will provide protection against novice hackers. Liu Jiqiang has proposed security of logs in [10]. In this approach, the security of logs is based upon the security of the systems which the logs were kept in. We bring forwards a system called Secure Audit Logs Server which adopts encryption and dynamic MAC to guarantee the integrity and dependability of the logs. This is important for obtaining effective evidences. Another approach is proposed by Patrick Stahlberg et.al. [11] In which they shows that how to preserve database table storage, the transaction log, indexes, and other system components. Then address the problem of unintended data retention by proposing a set of system transparency criteria and at last apply specific techniques for secure record deletion and log expunction that increase the transparency of database systems, making them more resistant to forensic analysis.

II. LOG FILE

Any specific event that has been taken place within a system or network of an organization is capture by log file as the collection of log entries where these log entries contain the information related to that specific event [13]. Verities of logs file available within an organization to capture records associated with computer security which are generated by many sources including security software's like firewalls, antivirus, intrusion detection and prevention system and many other applications. Regular log analysis is advantageous for recognizing security incidents, strategy violations, fake activity, and functioning problems. Logs are also helpful for performing auditing and forensic analysis, carrying internal investigations; define threshold limit, and recognizing operational fashions and long-term problems [14].

Log file used ASCII code format with .log extension for tracking the operation performed by any user simply by capturing the messages generate by an application, service and operating system or by different functioning logs and alert services. For example Web servers maintain a log files record for every request made to the server [15].

Recently log file are used for analysing network performance, optimizing system and record the action performed by user, and, and make available data useful for examine malicious activity within many of organizations and associations [13]. Were as primarily, log file generally used for troubleshoot problems. . Within an organization, many logs contain records related to computer security; common examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks [18].

III. LOG FILES IN CYBER FORENSIC

Cyber forensics is an significantly derived and proven technique towards the protection, compilation, justification, recognition, investigation, explanation and presentation of cyber evidence consequent from cyber sources for the purpose of facilitate or furthering the reconstruction of events found to be criminal or helping to predict the unconstitutional actions shown to be troublesome to planned operations [19].One important Element of cyber forensics is the reliability of the cyber evidence.

In Cyber forensic, log files are like the black box on an airplane that traces the events happened within an organization's system and networks. Logs are collection of log entries that play a very significant responsibility in facts congregation and each entry contains information related to a precise event that has happened within a system or a network. Log files helps cyber forensic process in probing and seizing computer, obtaining electronic evidence for criminal investigations and maintaining computer records for the federal rules of evidence [20].

IV. LOG MANAGEMENT

The figure of threats against networks and systems have significantly enhanced with the world wide exploitation of network servers, service station and other computing devices. Quantity and diversity of computer security logs and with the revolution of computer security logs, computer security log management is essential [13]. Log management's are required to guarantee that computer security records are stored in satisfactory detail for a suitable period of

time. Log management is the process for creation, broadcasting, storing, examine, and organizing of computer security log data. The elementary problem with log management is successfully balancing a limited quantity of log management resources with a continuous supply of log data. Log creation and storage can be convoluted by numerous factors, as well as high number of log sources; inconsistent log content, formats, and timestamps among sources; and progressively large volumes of log data [13, 16, and 17]. Log management also contains protecting the confidentiality, integrity, and availability of logs. Another problem with log management is ensuring that safety, system, and network administrators regularly perform effective analysis of log data.

V. PROBLEM STATEMENT

The aim of this paper is to propose an effective and efficient scheme for cyber forensics to resolve following problems that arise during log file analysis for forensic investigation.

- Digital investigations are becoming more time consuming and complex as the volumes of data required to analysis is large in size therefore lossless compression log file in lossless manner.

- There is possibility of manipulation or deletion of log information. Because log files are incriminating evidence against attackers, these files are at risk of attacks. Therefore, a mechanism is needed to prevent the manipulation and deletion of log info and log files by attackers and maintain the contents of log files that are created at the time of outbreak.

VI. PROPOSED FRAMEWORK

The Details of Proposed framework are as follows:

A. Log Fetching- The first tier contains the client that produces the log data. Some hosts run logging client applications or services that make their log data available through networks to log servers in the second tier. Other hosts make their logs available through other means, such as allowing the servers to authenticate to them and retrieve copies of the log files.

B. Log compression- Log compression is storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents. Log compression is often performed when logs are rotated or archived. .A multi-tiered log file compression solution shall be proposed. Every of the three tiers address one notion of redundancy. The first tier handles the resemblance between neighbouring lines. The second tier handles the global repetitiveness of tokens and token formats. The third tier is general-purpose compressor which handles all the redundancy left after the previous stages. The tiers are not only optional, but each of them is designed in several variants differing in required processing time and obtained compression ratio. This way user with different requirements can find combinations which suit them best. We propose five processing schemes for reasonable ratios of compression time to log file size reduction. A collection of scripts to determine the compression ratios, compression times and decompression times when using data compression was compiled. These scripts were used to run tests on a collection of log files and the obtained statistics recorded.

C. Log Protection-Log files include log entries associated with system and network activity, they need to be protected from breaches of their confidentiality and integrity. For example, logs might intentionally or accidentally record susceptible information such as users' passwords and the content of e-mails. This raise security and isolation concerns containing both the individuals that assessment the logs and others that might be able to access the logs through authorized or unauthorized means. Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party. For example, many root kits are specifically designed to alter logs to remove any evidence of the root kits' installation or execution [21].

To meet data retention requirements, our proposed methodology need capture log entries in image format at server side simultaneously as log entries records by log file in .text format.

VII. METHODOLOGY

Seunghee Yoo, Yilhyeong Mun, Dongsub Cho [22] proposed an methodology having multi thread TCP server which stores the image files of the web URL pages of the same as .text log files makes. As shown in figure 2.

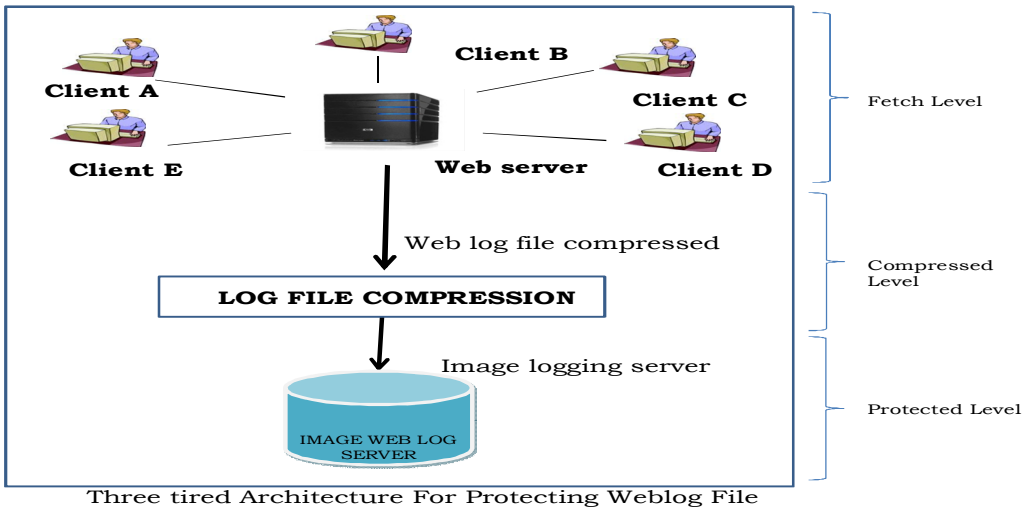

Fig 1: Proposed architecture for protecting Web log File

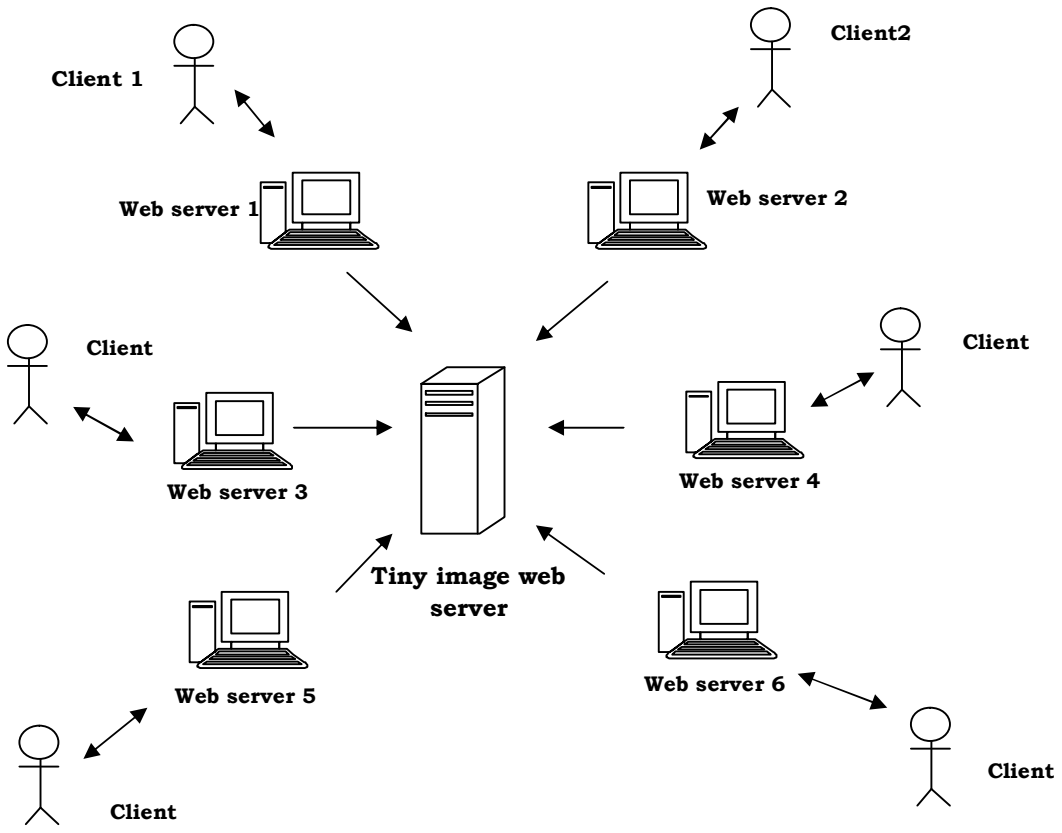

Fig 2: Image logging system

VIII. CONCLUSIONS

In this work the implemented system protect the generated log from illegal tampering by implementing an image logging server that catch .text log file in an image format. Proposed methodology significantly reduce the space requirement at image logging server to hold image of .text log file by applying lossless compression over .text log file before catching it's into image logging server. Transformed image log file ensure all security and log generation requirements like compression, Authenticity, integrity and confidentiality and can be used as authorizes evidence in cyber forensics.

ACKNOWLEDGMENTS

The research presented in this paper would not have been possible without our college, at VIET, dadri, GB Nagar. We wish to express our gratitude to all the people who helped turn the World-Wide Web into the useful and popular distributed hypertext. We also wish to thank the anonymous reviewers for their valuable suggestions

REFERENCES

[1] Fumiharu Etoh, Kenichi Takahashi ,Yoshiaki Hori, Kouichi Sakurai, "Study of log file dispersion management method" in Annual International Symposium on Applications and the Internet,ieee,2010.

[2] Kessler, M. G. (2006). Kessler's Corner: The growing field of computer forensics. The Kessler Report, 9(1), 7.

[3] Bernie Lantz,Rob Hall,Jason Couraud , "locking down log files: enhancing network security by protecting log files " Issues in Information Systems, Volume VII, No. 2, 2006

[4] NPO The Institute of Digital Forensics 2006, Encyclopedia of Digital Forensics [in Japanese], Dec. 2006

[5] Przemysław Skibiński and Jakub Swacha, "Fast and efficient log file compression" Local Proceedings of ADBIS 2007, pp. 56-69© Technical University of Varna, 2007

[6] Vimal Kumar,Akhilendra Pratap Singh, Anjani K. Rai ,Manoj Wairiya , "Self Alteration Detectable Image Log File for Web Forensics"

[7] Web Forensics, Jess García, http://www.jessland.net

[8] Indian Computer Emergency Response Team, "Web Server Security Guideline," CERT-IN, August, 17, 2004.

[9] Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine, "Threat to privacy in the Forensics Analysis of Database Systems," SIGMOD˝07, Beijing, China, June 12–14, 2007.

[10] Kapil Kumar Gupta, Baikunth Nath, Ramamohanarao Kotagiri," Layered Approach using Conditional Random Fields for Intrusion Detection," IEEE Transaction on Dependable and Secure Computing Vol 7, NO 1,January-March 2010.

[11] Liu Jiqiang Han Zhen Lan Zengwei," Secure Audit Logs Server to Support Computer Forensics in Criminal Investigations," Proceedings of IEEE, TENCOW02

[12] Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine,"Threat to privacy in the Forensics Analysis of Database Systems," SIGMOD˝07, Beijing, China, June 12–14, 2007.

[13] Nikhil Kumar Singh, Deepak Singh Tomar, Bhola Nath Roy, "An approach tounderstand the end user behavior through log analysis" International Journal of Computer Applications (0975 – 8887), August 2010.

[14] Karen Kent and Murugiah Souppaya, "Guide to Computer Security Log Management", Computer Security Division Information
Technology Laboratory National Institute of Standards and Technology Gaithersburg, 2006

[15] Muhammad Kamran Ahmed, Mukhtar Hussain and Asad Raza "An Automated User Transparent Approach to log Web URLs for Forensic Analysis" Fifth International Conference on IT Security Incident Management and IT Forensics 2009.

[16] P. K. Sahoo ,Dr. R. K. Chottaray, "The Role of Audit Logs in Cyber Security" International Journal of Science and Advanced Technology (ISSN 2221-8386) Volume 1 No 7 September 2011

[17] Gary L Palmer "A Road Map for Digital Forensic Research". Technical ReportDTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS), 2001

[18] Rafael Accorsi, Safekeeping Digital Evidence with Secure Logging Protocols:State of the Art and Challenges, University of Freiburg, Germany.

[19] Carrier, B.D., Spafford, E.H "Defining Digital Crime Scene Event Reconstruction" Journal of Forensic Sciences, 49(6). Paper ID JFS2004127,2004

[20] Stephenson. P, "Application Of Formal Methods To Root Cause Analysis of Digital Incidents", International Journal of Digital Evidence, 3(1) ,2004

[21] http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_lr.html.

[22] Seunghee Yoo, Yilhyeong Mun, Dongsub Cho, "Implementation of Image Loging Server for Web Forensic," 978-1-424426249/08, IEEE, 2008.