IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

An Implementation of Time Line Events Visualization Tool Using Forensic Digger Algorithm

Priyanka Khatik[1*] and Preeti Choudhary[2]

[1*,2]*Department of CSE, Infinity Management & Engineering College, Sagar, M.P., India*

www.ijcseonline.org

Received: 09/03/2014 Revised: 24/03/2014 Accepted: 17/04/2014 Published: 30/04/2014

Abstract— Introduction should lead the reader to the importance of the study; tie-up published literature with the aims of the study and clearly states the rationale behind the investigation. It should state the purpose and summarize the rationale for the study and gives a concise background. Use references to provide the most salient background rather than an exhaustive review. The last sentence should concisely state your purpose for carrying out the study.

Index Term—Server Time Line Analysis, Server Log, Event Log, Web Analysis

I. INTRODUCTION

This project explores visualizations for forensic investigations, using web history analysis as an example area in much need of visual tools. A web visualization tool called "Server Events & Time Line" was created and its effectiveness evaluated against a non-visual tool, Net Analysis. Many of the problems Net Analysis has are common to forensic tools – the dataset is large and Cluttered because it is presented in one large table. The program provides very little to help the investigator analyze the results, so a large amount of time is spent filtering the table into a more digestible size. The table format also makes it difficult to explain results to those not familiar with the software, such as police officers.

As the prevalence and usage of networked computer systems increases, the chances of these computer systems being involved with criminal behavior logically also increases. The field of digital forensics has grown rapidly over the last decade due to the rise of the internet and the associated crimes, and although the ideas are well established, the discipline of digital forensics is still new and developing Data visualization is often an area neglected by programmers because it requires more skills and time to do properly, and does not seemingly add any new functions to the software since it just shows the resultant data in a new way. This research will explore using visualizations for forensic investigations, using web history analysis as an example area in much need of visual tools. This project will create a visual tool called timeline visualization tool, and evaluate its effectiveness against pre existing non-visual tools.

II. RELATED WORKS

Formal frameworks for the reconstruction of digital crime scenes are discussed by Stephenson [1] and Gladyshev et al. [2]. Stephenson uses a Petri Net approach to model worm attacks in order to identify the root cause of an attack. Gladyshev et al. present a state machine approach to model digital events. Their approach uses a generic event reconstruction algorithm and a formal methodology for reconstructing events in digital systems.

A work has proposed neural networks for automated event reconstruction [3]. However, the approach in this paper searches for patterns of events in the low-level timeline based on predetermined rules. A significant challenge in digital forensics is to achieve automated evidence analysis and automated event reconstruction. Stallard and Levitt [4] [5] have proposed an expert system using a decision tree to search for violations of known assumptions about data relationships, and Abbott et al. [6] have proposed a framework for scenario matching in forensic investigations based on transaction logs with automated recognition of event scenarios based on a stored event database. These approaches do not suggest replaying the scenarios on a testbed, but the output of their systems could be used as a basis for realistic testing in ViSe. This would provide a far more thorough analysis and a more convincing case in court. Elseasser and Tanner [7] have proposed an automated diagnosis system that generates possible attack sequences based on profiles of the victim host configuration and of the unauthorized access gained by the attacker. The hypothesized attack sequences are simulated on a model of the victim network, and a successful simulation indicates that the attack sequence could feasibly lead to unauthorized access.

Neuhaus and Zeller [8] have recently proposed a method for automatically isolating processes that are necessary for an intrusion to occur. In the approach proposed by Olsson and Boldt et. al [18] improved upon file metadata based timelines with the Cyber Forensic Time Lab (CFTL). Also, log2timeline in Guðjónsson, 2010 [10], with the time-scanner enhancement can automatically and recursively examine files and directories. If an appropriate 'input module' is available for a file, times are extracted and added to a timeline. Reference (Guðjónsson, 2010) also hints at the possibility of grouping events that are part of the same

Corresponding Author: *Priyanka Khatik*
Dept. of CSE, Infinity Management & Engineering Institute, Sagar, M.P., India

activity when describing the potential future use of the 'super event' table in the SQLite output format. A more detailed review of available timeline software is available in Carbone et. al. [13] but the examples in this sub-section demonstrate that there are a number of benefits to using an 'enhanced' timeline in addition to improving the richness of the timeline, i.e. increasing the number of events. As discussed in [9], a tool such as Time stamp could be used to clear file system times, but this would not affect timing within files. Even if not overwritten maliciously, file access times can be updated in bulk by anti-virus products [10] or the updating of them disabled by default in modern operating systems or by altering a Registry key.

There is also some work that discusses the visualisation of digital forensic timelines. For example, EnCase's visualisation is mentioned in [11]. Buchholz and Falk [12] developed Zeitline, which is a GUI based tool that allows file system times to be imported from The Sleuth Kit and other sources (using Import Filters). This tool provides searching and filtering of events. It also introduces the concepts of atomic events and complex events, where the former are "events that are directly imported from the system" and the latter are "comprised of atomic events or other complex events". Zeitline [12] allows an investigator to manually combine atomic events into complex events. Aftertime (Netherlands Forensic Institute (NFI Labs), 2010) is a Java based application that not only performs enhanced timeline generation from a disk image, but also visualises the results as a histogram, with time on the x-axis against numbers of different events on the y-axis.

Lerche and Koziol give the overview of visualization of forensic data. Basic and fundamental visualization was explained in his work. How different techniques could be used in forensic process also discuss. Also they focus how visualization helps to detect anomalies and attack in network forensics [15].

Cluster based groping of similar data of different density in analysis of log files. Choose candidate outlier and compute the distance between candidate point and non candidate cluster. They found to be for then it is anomaly, this approach is presented in [14].

After studying all the major exiting techniques and tools for forensic analysis, we found that there is still an open space for the development and research on automated forensic timeline analysis tool, that can be compatible enough to handle the web log files as well firewall log files with the advanced correlation strategy.

III. SERVER TIME LINE APPROACH TOOL

In this section author address of solution/need/importance of the study problem statement/objectives

In this paper, we present server timeline tool for analysing of the web servers for the forensic analysis. In the proposed system, we have developed tools that assist the server administrator and web administrator to improve their website by determining occurred link connections in the website. Firstly, we have obtained access log files, which are recorded in web server. The obtained log files were analysed by proposed methodology. So, raw log files were pre-processed and the path analysis technique was used to investigate the web log files of URL information concerning access to electronic sources. The input to the proposed system is a log file, which is maintained and managed by the web server system that stores the information of the users and web contents. It basically manages the records consist of several parameters.

In figure 1, the algorithm of the proposed forensic algorithm "Forensic Digger" is presented. The reconstruction time line analysis supports many of the proposed solutions for automated forensic analysis, and it would be interesting to integrate some of these approaches with our work. It generates hypotheses before executing the process of reconstruction experiments and the problem of performing automated comparison of the results with the digital evidence.

The work proposed here in this paper will focus on the analysis of events with visualizations for the web access log files events or simply web log file events. The proposed technique for the web server time line analysis will perform the following actions that provides support to the investigators.

First, the experts will take the log files and by using the proposed tool for log files visualization and analysis starts drawing an action plan. They may perform the following steps for investigating the crime scene.

Step1- Analyse the dates and day based on occurrence of event. (Reported by the server administrator)

Step2- Integrate the log files as per the need.

Step3- Identify the parameters for analysis, that helps to collect the evidences of malicious activity like (IP ADDRESS, DATE, MAC ADDRESS etc.)

Step4- In the integrated log files, search the activity for frequent visitors with their ip addresses, file access, byte transferred etc.

Step5- Confirm the IP address of the malicious user, by analysing the behaviour.

Step6- Reconstruct the event timeline hypothesis by analysing the evidences and log file entries.

Step7- Generate the reports as the evidences.

Step8- Present all the reports to the courts, that supports the prosecution to convince the court against the accused.

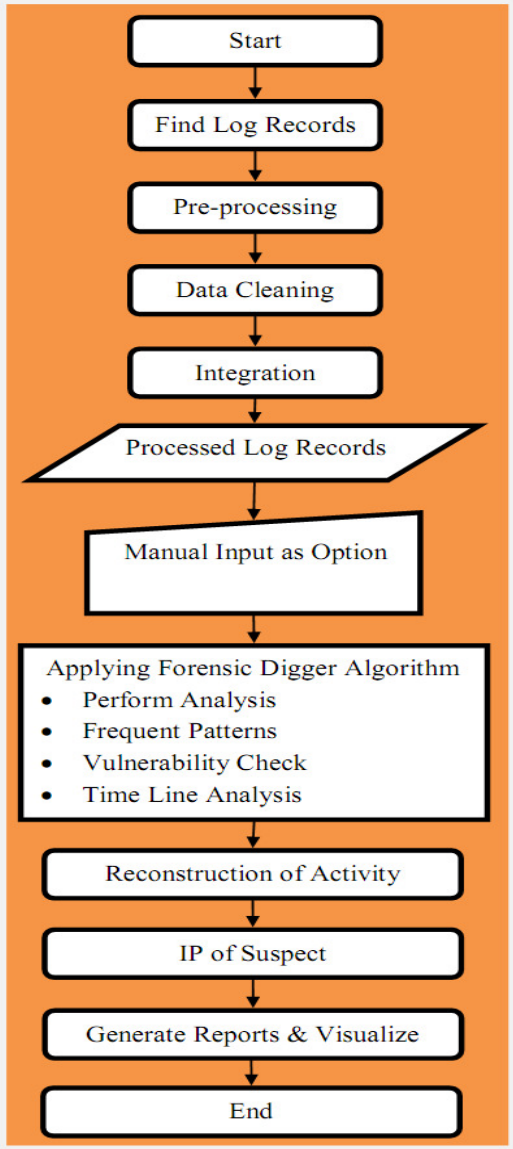

Figure 1: Forensic Digger Algorithm

The proposed server timeline analysis and visualisation tool presented in this paper supports many of the proposed solutions for automated forensic analysis, and it would be interesting to integrate some of these approaches with our work. It generates hypotheses before executing the process of reconstruction experiments and the problem of performing automated comparison of the results with the digital evidence.

IV. IMPLEMENTATION & RESULTS

The proposed scheme implemented by developing a web application, using Microsoft .Net Framework 4.0, Visual Studio 2010. Which is tested on windows 8 environment with IIS 6.0. Which is one of the best combination for creating data driven sites. Since both efforts are collaborative in nature, there's always plenty of support from documentation and mailing lists. Bugs are fixed rapidly, and requests for features are always heard, evaluated, and if feasible, implemented. The Chart controls enable you to create ASP.NET pages or Windows Forms applications with simple, intuitive, and visually compelling charts for complex statistical or financial analysis.

This section has highlighted thematic areas where novel digital technologies may bring improvement to the forensic process. It underlines the fact that, until recently, three-dimensional forensic reconstruction techniques have been used (along with other multimedia technologies) mainly to present forensic evidence in the courtroom. The technologies have been targeted in this area due to their success in communicating highly complex, technical spatial and temporal evidential information to the general public. Modern systems for creating visualisations have evolved to the extent that non-experts can create meaningful representations of their data. However, the process is still not easy enough, mainly because the visual effects of processing, realising and rendering data are well-understood by the user.

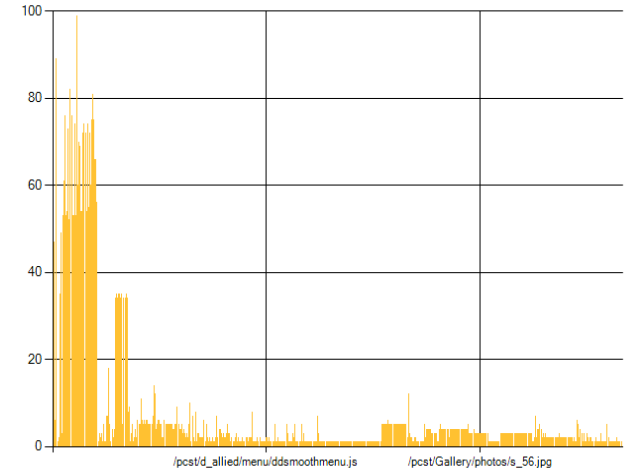

Figure 2: Graph for the page count

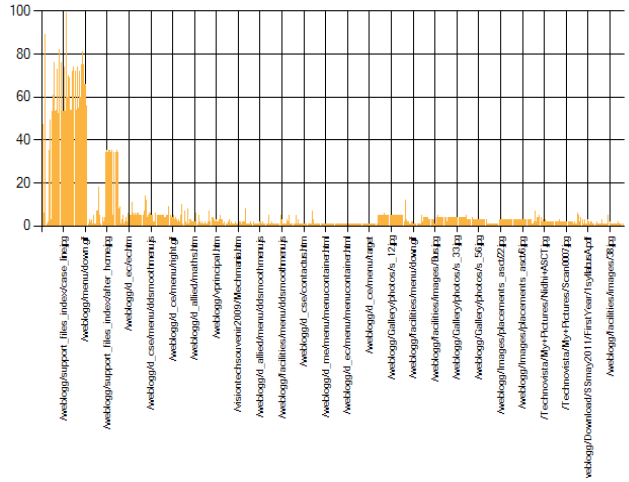

Figure 3: popularity of the web page

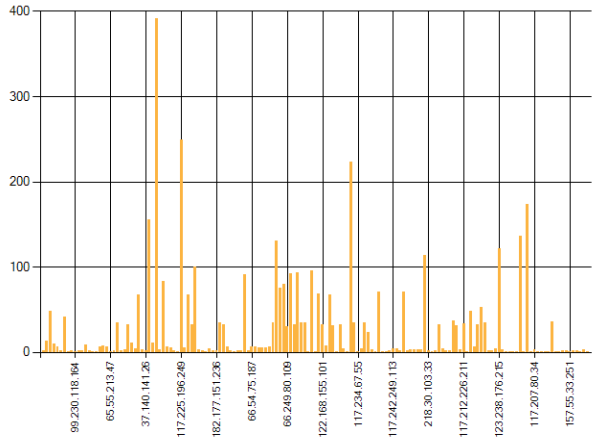

Figure 4 : Graph specifying the frequent visitors with ip-addresses

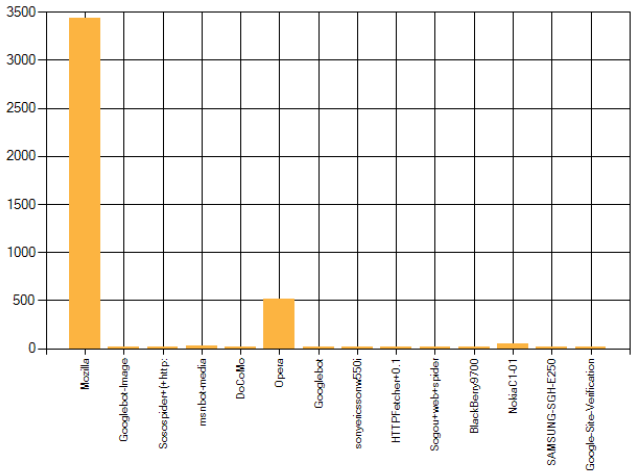

Figure 5: Unique browser usage

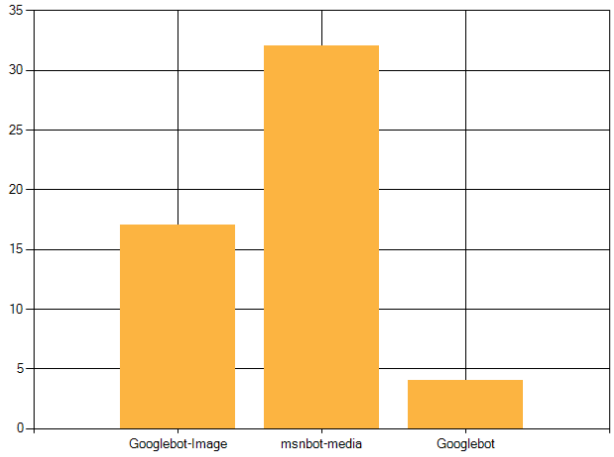

Figure 2: Bots used for web crawling

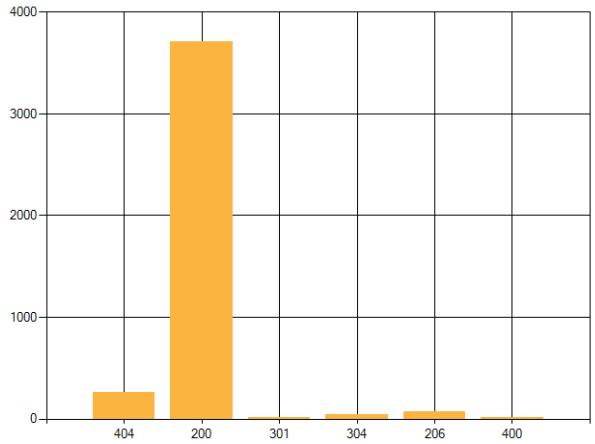

Figure 7: Visualization of DOS attacks

User testing was carried out to test the hypothesis that visualisations would indeed help forensic investigators. The proposed server time line tool was tested against Webscavator and Net Analysis, the most commonly used forensic web history analysis program. Which results the proposed tool is easy to operate and doesn't required any extra training or program to understand.

V. CONLUSION & FUTURE WORK

Digital forensics involves the application of tools and technologies to prove the truth of a past event. The discipline of digital forensics has developed methods to enhance the identification, correlation, and characterization of digital information. As with other forensic disciplines, technology is used to increase information symmetries so that recreations of past events more probably reflect the true event, and justice is served.

Timelines are excellent ways of reaching a conclusion. One need to collect log entries that show a distinct, clear chain of events that culminate in the incident, As it is a giant step towards proving your case. In addition, the timelines analysis are often considered as circumstantial because of the ease with which logs can be altered and file times spoofed. Therefore, we further need to support the field of providing security to log files. Future work on understanding the effects of anti-forensic tools on a reconstruction will add value to the approach.

REFERENCES

[1]. Stephenson, P.: Formal modeling of post-incident root cause analysis. Int. J. Digit. Evid. 2 (2003)

[2]. [2]. Gladyshev, P., Patel, A.: Finite state machine approach to digital event reconstruction. Digit. Invest. 1 (2004)

[3]. Khan M, Chatwin C, Young R. A framework for post-event timeline reconstruction using neural networks. Digital Investigation 2007;4: 146–57.

[4]. Stallard, T.B.:Automated analysis for digital forensic science. Master's thesis, University of California, Davis (2002)

[5]. Stallard,T.,Levitt,K.N.:Automated analysis for digital forensic science: Semantic integrity checking. In: ACSAC 160–169 (2003)
[6]. Abbott, J., Bell, J., Clark, A., Vel, O.D., Mohay, G.: Automated recognition of event scenarios for digital forensics. In: SAC '06: Proceedings of the 2006 ACM symposium on applied computing pp. 293–300.ACMPress,NewYork (2006)
[7]. Elsaesser, C., Tanner, M.C.: Automated diagnosis for computer forensics. Technical report, The MITRE Corporation (2001)
[8]. Neuhaus, S., Zeller, A.: Isolating intrusions by automatic experiments. In: Proceedings of the 13th annual network and distributed system security symposium. pp. 71–80 (2006)
[9]. Olsson J, Boldt M. Computer forensic timeline visualization tool. Digital Investigation 2009;6(S1):S78–87.
[10]. Guðjónsson K. Mastering the super timeline with log2timeline. SANS Reading Room; 2010.
[11]. Bunting. EnCE study guide; 2008. pp. 235–237.
[12]. Buchholz F, Falk C. In: DFRWS, editor. Design and implementation of Zeitline: a forensic timeline; 2005
[13]. Carbone R, Bean C. Generating computer forensic super-timelines under Linux; 2011.
[14]. Sutapat Thiprungsri. Miklos A. Vasarhelyi, Cluster Analysis for Anomaly Detection in Accounting Data: An Audit Approach, The International Journal of Digital Accounting Research,pp 69-84,2011.
[15]. Gerald Schrenk, Rainer Poisel, "A Discussion of Visualization Techniques for the Analysis of Digital Evidence", International Conference on Availability, Reliability and Security,pp758-763,2011.

AUTHORS PROFILE

Priyanka Khatik, is currently pursuing M.Tech from Infinity Management & Engineering College, Sagar, M.P and herArea of interest are web security and Forensics.

