Research Paper Engineering

A Super TimeLine Analyzer for Windows

Ranjitha.R

MTech in Computer Science and Engineering with specialization in Cyber Forensics And Information Security ER & DCI-IT, CDAC Campus, Thiruvananthapuram, Kerala

ABSTRACT

Today, there is an increase in crime reporting to the Internet and computers leading to a growing need for computer forensics. Timelines are integral part of forensic analysis. A detailed chronology help the law enforcement to map a suspects' actions to a crime. This project describes a framework "Super TimeLine Analyzer" which primarily focus upon the timeline depth analysis of data sources available on a Windows 8 system. This is an approach to timeline user and application activity so as to automate computer forensic investigations. For intelligence and law enforcement agencies, inspecting metadata can implicitly save concrete time essentially tied to manual analysis. This framework curtail manual processing timeline based log files and automate the classification of both files and network logs.

KEYWORDS

INTRODUCTION

The objective of this paper is to develop a Super TimeLine Analyzer that takes timestamps from registry, and logs as input, makes a timeline of it and perform metadata analysis of its contents. This paper introduce both pertinent information regarding the use and generation of digital forensic timelines as well as the various challenges encompassing them. Also, it provide added information about date/time-based metadata in order to augment circumstantial understanding of transpired events that relate to a given investigation.

In digital forensic investigation, timeline analysis is the combination of timestamps and further event information into an account of what happen on the computer. Information such as timestamps, log, web browser cache, and history is assembled into a super-timeline, with events corroborated from multiple sources.

In the process of conducting a digital forensic investigation, many contingent sources of information are likely available to the investigator. However, many sources of date/time related metadata information are less used by investigators. These sources of information are found all through suspect disk images and are too often neglected for inclusion in a digital forensic timeline. Often times, however, timelines are not even used by investigators as the tendency in the digital forensics community is to refrain their use.

A decisive problem with digital timelines is that even if they appear very simple to assemble based on automatically available date/time-related metadata, much more data is often hidden within the operating system. However, in order to collect a lower level of date/time related metadata, it is imperative to explore for both specific file types and locations that are known to consist of the sought after metadata. Once extracted, the additional metadata may provide the investigator with a more reliable temporal context and frame of reference.

LITERATURE REVIEW

Timestamps are a vital part of metadata that correlate to events that transpired. Arranging these timestamps gives rise to a timeline. However, generating a timeline across composite sources bear several challenges; timestamp explanation is similar sort of metadata that has been largely used in the literature and timestamp analysis has represented a crucial part in digital forensics so far.

The workings [1] of an automatic time line report parsing CLI tool, LogMole. A tool to be used as a means of automating the analysis of log2timeline and mactime body files. An evaluation of [2] the existing tools of timeline analysis and the need for a solid timeline analysis tool. It ease the analysis of computer activity timelines by providing an automatic graphical user interface, modular structure and diverse built-in features to aid the analysts' examination of the data. The [4] approach of assembling the data has been competent in increasing the efficiency of other large data sets, such as intrusion detection databases. The log2timeline, CLI version [5] presents a framework that addresses this problem in an automatic fashion. A framework, built to parse different log files and artifacts and produce a super timeline in an easy automatic fashion to aid investigators in their timeline analysis.

PROPOSED SYSTEM

Proposed system focuses on generating a timeline consisting of timestamps that comes from different sources of a computing system of Windows 8. The Super Timeline analysis occurs on hard drives. The proposed framework, SuperTimeLine Analyzer, a GUI version does timeline analysis and report generation in csv format. The framework provides three implementations for loading the required information necessary for additional processing. The main sources of information analyzed by the software are the timeline CSV file and the mactime-based files provided by the utility tool.

SYSTEM DESIGN

The system uses a tiered architecture as shown in Fig.1 about here. The presentation tier provides Graphical User Interface where the investigator can have two options: Analysis Viewer and Report Viewer. The Logical tier is pulled out from the presentation tier and has its own layer; it controls an application's functionality by performing detailed processing. In this system, the second tier is loading and analysis.

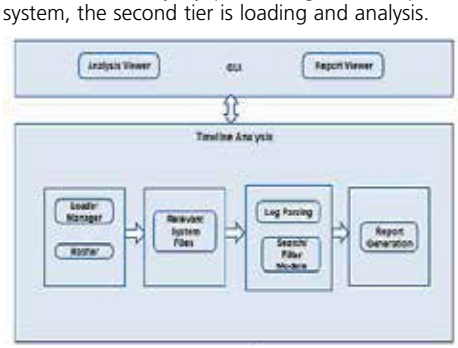

Fig. 1 System Architecture

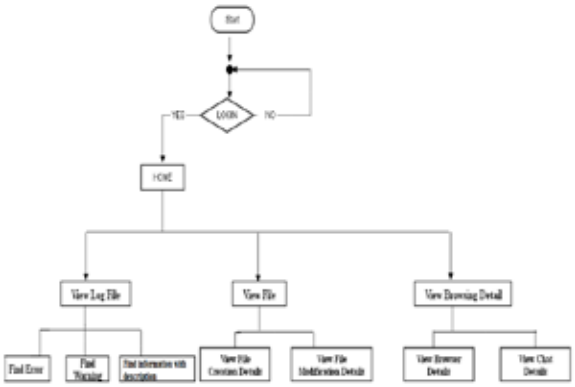

Fig 2 Flow chart diagram for proposed system

Fig. 2 about here represent the flow of control of execution of the application. Initially after logging in, the systems files are given as input, and viewed for different forms like log files, all other files (doc, pdf, image, txt, zip), and browsing, and searching history. After taking this as input, further processing like searching within the image file for required pattern of time stamped changes are obtained.

CONCLUSION AND FUTURE WORK

One of the challenges to digital forensics is the volume of data that needs to be analyzed. There are no tools currently available to parse large amounts of information collected and generated by any tool. If such a tool existed, it could have provided increased information and knowledge based on the underlying nature of artifacts and metadata. Proposed framework reduces the burden of processing timeline-based log files and automating the classification of files. In the world of growing storage, increased time, and resource, automation is key to success. The existing framework is far from being completed as there are always new OS, new files types that contain timestamps that need to be parsed and added to Super TimeLine.

SUMMARY

This paper introduces a time based data forensic and invokes an analysis proposal for Windows operating systems. The designed system indicate interlopers' invidious activity and exposes evidence manipulation by invoking and parsing data in file metadata and the Windows registry.

REFERENCES

[1] Automation of Report and Timeline- file based file and URL analysis by Florian Eichelberger, April 30, 2014.
[2] Enhanced Timeline Analysis for Digital Forensic Investigations by Bartosz Inglota &LuLiua, May 5, 2014. https://github.com/baltek/Zeitline
[3] Automatic Timeline Construction for Computer Forensics Purposes by Yoan Chabot, Aur´elie et al, September 24, 2014.
[4] Computer Forensic Timeline Analysis with Tapestry by Derek Edwards, November 12, 2011
[5] Mastering super timeline log2timeline by Kristinn Guðjónsson. June29, 2010, http://log2timeline.net
[6] Windows.Forensic.Analysis.Toolkit.3rd Edition.
[7] Windows Registry ForensicAdvanced Digital Forensic Analysis of the Windows Registry, Harlan Carvey.
[8] Malware Forensics Field Guide for Windows systems by Cameron H. Malin, Eoghan Casey, James MAquilina.