Advanced Computer Forensics
Ruiyang Liu 85C576
Conference Paper Summary – Group #4

Paper selected: Computer Forensic Timeline visualization tool
Paper author: Jens Olsson*, Martin Boldt
Word count: 671 words

Computer forensics is intended to assist investigators in locating evidence of computer crimes more effectively. A computer forensic visualization tool can be beneficial in presenting evidence in a straightforward and effective manner. The timeline visualization tool described in this work is introduced. Users are able to execute forensics activities more quickly, more reliably, and with fewer errors as a result of using this timeline visualization tool, according to the results of an extensive set of tests. For example, the history of emails and chats has a large number of timestamps. By examining their timestamps, you may learn important information about them, such as when they were first created and when they were transported, among other things. With the use of a time visualization tool, the investigator can go back and forth in time in order to locate the answers. They will also be able to zoom in and out in order to see exactly what happened at a specific time.

According to the findings of this study, the author has developed a prototype program called CFTL (Cyber Forensic TimeLab) that can scan a disk image for timestamps and display them. In addition, the author introduces a number of recent forensics tools. To give an example, the FTK (Forensic Toolkit) developed by AccessData has the ability to look through large amounts of evidence in a short period of time. The ILook investigator can assist in browsing files in a variety of categories, which allows for picture production in complex systems if necessary. Furthermore, using the Sleuth kit tool can aid in the analysis of a variety of file systems, as well as the recovery of accidentally deleted files, among other things. Its ability to make evidence visualization possible in a coherent manner, on the other hand, makes the CFTL more competitive in this regard.

CFTL may be broken into two sections: Scanner and Viewer. Scanner is the first of these two parts. The scanner is the primary executable component, and it includes a data controller as well as a number of handlers for various file types. In addition, the scanner can create an XML file for use with Viewer. The XML files generated by Scanner can be imported into the Viewer.

There is a graphical user interface for the Viewer to use in order to conduct the timeline. Also discussed is how to increase the efficiency of the Viewer, according to the author. When the scrollbar comes to a stop, the viewer can begin loading the data, indicating that the entire file is no longer required to be loaded previously.

CFTL and FTK are compared in order to evaluate the prototype, and the results are presented in this paper. The tests are based on fictitious scenarios that have been created. The results of the tests reveal that CFTL provides relative advantages for the individuals when time analysis is used. In addition, the author created a survey for all of the people who took part in this experiment. They were all successful in completing the survey connected to the CFTL.

The author then presents a prototype tool that he calls the CFTL command line interface. FAT32, FAT16, and NTFS are among the file systems that CFTL is capable of handling. Apart from that, CFTL can be used to scan emails, instant messages, browser history, and other data types, among other things. After conducting an examination, the results of the test demonstrate that the inclusion of a timeline in digital forensic tools increases the efficiency and accuracy of investment decisions. When CFTL is utilized to do the task at hand, it takes approximately one-third the time of the state-of-the-art tool. Finally, the author discusses future work that will be done in connection with the CFTL. There will be a seamless integration with the currently installed applications. Additionally, automatic pattern finding will be available.