Abstract

The development of anti forensic techniques and the increased of storage media capacity causing the use of traditional forensic techniques become unefficient. To solve these problems, then live forensic techniques is used which have speed in investigation process. Live forensic techniques use volatile data as the evidence which need special treatment to do the forensics. Network forensic is implemented with live forensic techniques because the information have the volatile characteristic. To analyze data in network forensic, the use of appropriate tools is influenced for the evidence which will be processed and investigated in court. Definitely,the deployment of network forensic tools leave the trace in memory, whereas volatile data located in memory. The interface method has major influence to memory usage, so in this final assignment, the interface method will be analyzed to measure the impact to the sistem. The accuracy and elapsed time will be concerned in libe forensic process.

In this final assignment will analyze and test on two tools which have different interface method, i.e TCPView with Graphical User Interface method and Openports with command line method. To measuring the impact to memory using these parameter, i.e memory footprint, library file usage and registry file written, accuracy and elapsed time of these tools.

Based on test result, command line interface method is the best method to implementing live forensic because the usage of memory footprint, file library and registry file written is more less then Graphical User Interface method. The accuracy is as well as the Graphical User Interface method

Keyword: ***traditional forensic, live forensic, network forensic, Graphical User Interface, command line, TCPView, Openports, memory footprint***