ABSTRACT

Malware is software on a computer that is destructive, malware is always developed for special purposes or to harm other parties such as criminal acts and so on. Therefore, it is important to know the files or processes from the memory on our devices so as not to become victims of malware attacks.

Based on the problems above, this final project will design an application that can analyze and classify malware categories in volatile memory processes. In this application, forensic techniques and CLI-based Yara and VirusTotal scanning are used. Forensic techniques were used to perform process analysis on the system's volatile memory and scans were used for method I malware classification and CLI-based VirusTotal scanning for method II malware classification.

After analyzing the memory process, the malware classification process is carried out based on the yara rules or hash values. The process in method I is by checking the string value in the file suspected of being malware and then matching it with the existing yara rules, for method II the hashing process is carried out first and then uses the hash value to start method II. This process is proven not to take long with the test data from 30 trials with 5 memory files, each tested 6 times, the results are 16,053 seconds for method I and 3,516 seconds for method II with an accuracy level of scanning the ID process in memory by 50% for method I and 79%.

Keyword: *Digital Forensics, Malware Forensics, Memory Forensics, VirusTotal, YaraScan*