ABSTRACT

Malware is a piece of software or software created to infiltrate or damage a computer system. The spread of malware is currently so easy either through certain advertisements on websites, usb flash drives, and other media. Everything is very closely related to crimes such as file theft, internet banking, credit cards and so on. In this regard, there is a field that deals with crimes, namely digital forensics. One of the stages in digital forensics is analyzing digital evidence, in this case malware. To prove a software is said to be malware is to know how the program works on a computer system. The Dynamic Analysis Malware method is a suitable method for analyzing how malware works.

In this Final Project, the Malware Dynamic Analysis method is used to analyze 5 available malware samples, namely Poison Ivy, Gen Variant Johnnie 97338, Trojan GenericKD 40427213, Dropped:Trojan.AgentWDCR. PZW, 32.Trojan.Raasmd. Auto and Gen:Variant.Strictor.171520. The test method used for the 6 samples is by using Regshot and Wireshark. From this test it can be found that in the Regshot method there were the most Registry changes by Dropped:Trojan.AgentWDCR.PZW of 163 Registry. Whereas in the Wireshark Method, the malware that sent the most protocols was Gen:Variant.Strictor. 171520 with 1993 protocols.

Keywords — Digital Forensics; Malware Analysis; Dynamic Analysis; Trojans; Gen; Poison Ivy; Wireshark; Regshot; Protocols.