ABSTRACT

MALWARE ANALYSIS IN ANDROID OPERATING SYSTEM USING MEMORY FORENSICS BASED ON API

By

RIFYANDARU WIBISONO

1202150088

Malware is a program that is on an operating system and can endanger the affected operating system. In the development of the internet there are many types of malware that can be found on the internet such as Android malware. Android malware is malware that makes a negative influence on the Android operating system. Malware has the purpose of harming users of the affected operating system. Therefore malware analysis is used to identify malware. Malware analysis is a way to get information from malware to deal with attacks on infected victims. In doing analysis malware can be used several ways to detect malware such as detecting based on memory usage. In detecting malware based on memory you can use forensic memory to detect it. After getting the results of malware detection a method will be used to make an impact on malware based on API. In using memory forensics tools used volatility to get the results of malware analysis and use reverse engineering with APKtools tools to find out malicious activity based on the use of the API from the application. In this study 10 malware were used to analyze the use of volatility and APK tools to have an impact on using the results of analysis and also based on malicious activity from the API. So from the results of this study are the impacts related to the API and the results of analysis.

Keyword : *malware, malware analysis, memory, memory forensics.*