ABSTRACT

Millenials like now have a lot of cyber crime, and it's growing rapidly. One of the cyber crimes that concerns is to use malware. Currently malware has begun to enter into smartphones with an intermediary of applications. To anticipate the entry of malware into the smartphone, the need for an analysis process with the right method and easy to use. One of the methods used is by using reverse engineering method that is to search for information about hidden malware. To support reverse engineering methods there is an operating system called remnux which is one of the distro of linux. Inside the operating system remnux there are tools that can analyze malware in the form of apk, xml and dex. namely androguard. From the results of testing that has been done that the Android application analysis system can analyze the application permissions, package names, main activities and program codes of each class. There are 3 fake version application samples that were analyzed and then compared with 3 application samples obtained from the Google Play Store. The final result obtained from this test is the detection of malware on the program code from 3 fake version applications and knowing how the malware works.

Keywords: Malware, Remnux, Analysis, Reverse Engineering