ABSTRACT

The mode of operation in the world of cyber crime is increasingly numerous and varied. The technique used by the perpetrators of the crime are increasingly sophisticated. One of them uses malware. Malware has been designed as sophisticated as possible to create a gap in the security system. Even today malware getting easy entry into a computer via an intermediary file and can also be through a website containing malware. In anticipation of the entry of malware into the computer, the need for the detection process with the right methods and easy to use. One easy method is to use a reverse engineering method is a method to search for a hidden information. To support reverse engineering methods are called REMnux operating system which is a distribution of Linux. In an operating system REMnux there are tools that can detect malware that are in the form of exe file that is execscan, there is also analyze.pdf and pdf id which can detect malware in the form of pdf files, and can also detect malicious website address or containing malware. With the detection of malware using the method of reverse engineering on REMnux can allow an analyst to carry out detection of malware and also makes an analyst to get information about malware that is useful to be reported to antivirus developers as a reference for the future.

Keywords: Malware, reverse engineering