ABSTRACT

IMPLEMENTATION AND ANALYSIS OF DIGITAL FORENSICS SYSTEM ON LINUX VULNERABLE MACHINE USING FORENSICS ZACHMAN FRAMEWORK

By
Leonardo Taufan Sontani
1202160380
(Bachelor Program in Information System)

As technology develops, more methods of hacking develop, and the number of hackings increases. In 2022, BSSN found 976 million hacking detected entering Indonesia's network. Based on Government Regulations, owners of electronics system must have a system to prevent and analyze any hacking attempts to their system. Therefore, digital forensics requires a proper strategy and software to accelerate the examination of a case.

This research analyzes system logs from a Linux Vulnerable Machine for its ability to log a hacking event. This research also compares the performance between three free or trial-license of digital forensic software (Autopsy, FTK Imager, OSForensics) to look for digital evidence. This experiment is done by doing a penetration testing on a Linux Vulnerable Machine following a walkthrough which then analyzed using a forensics framework.

From this experiment, it is found that access.log should be prioritized to be analyzed. Access.log logs many activities that show the timeline when the server was being attacked, such as the IP address and the timestamp. And based on its ability to create an image file, data analysis, and finding deleted data, FTK Imager is better compared to the others for executing digital forensics.

Keywords: framework, FORZA, Typhoon, log.