ABSTRACT

In the world of digital forensics, data integrity is an important part to attention. In the data analysis process, there are activities that link the file system to the main file system on the operating system or commonly known as mount. Mounting is the stage of linking the file system to the main directory of the operating system so that it can be accessed. One of the processes, the Linux operating system will detect the storage media and mount it to access the file system. On the other hand, the recognition and installation process does not guarantee the integrity of the data on the storage media. This research will analyze and visualize device recognition and empirical test of the effect of installation on data integrity for digital forensic needs. For examiners, an analysis of the device recognition process was carried out based on valid references and empirical tests using the read only method and without read only on the Linux operating system. The test results to visualize device recognition and compare mounting techniques with read only and without read only and its effect on data integrity. Based on the research, a summary of the device recognition process was obtained and the results of the analysis of the two techniques were able to maintain data integrity. The read only mounting technique does not change the partition hash value whereas mounting with read only does not change the partition hash value.

Keywords: mounting, linux, operation system, data integrity, forensic