Abstract

Write prevention is the act of blocking write operations on a storage medium. This activity has its own challenges when storage media began to use USB technology. This challenge needs to be considered because in digital forensics, write prevention to storage media is necessary to maintain data integrity when the cloning process is performed. Cloning is a data acquisition process to make an exact copy of the digital data from the storage media that the data will be copied to. Currently, hardware-based write blocker devices tend to be expensive. While this tool is very much needed and there are still many police officers and forensic labs in Indonesia that do not have it. In previous research, an open source linux write blocker was developed in 2017. The gap from this research is the limitation of the tool in terms of its old development year, so that the USB connector technology and supporting operating system need to be updated again, which at that time still used USB 2.0 and was supported by Linux Kernel 4.10. To overcome this, modifications are needed to the linux write blocker so that the system can keep up with existing technological developments. The modified linux write blocker implementation is installed on the raspberrypi kernel which functions as a storage media container to take a copy of the data using the cloning command and still maintain the integrity of the data. The modified linux write blocker can be implemented on raspberrypi using the current kernel. Hardware write blockers can perform the cloning process on both storage media with USB 2.0 and 3.0 connectors. To maintain data integrity, a comparison of the hash obtained at the beginning before the cloning operation with the hash after the cloning operation is carried out, and produces the same value in both hashes. With this research, it is expected to be able to make an initial design of hardware write blocker at a relatively low cost and can be implemented on its own in various places that require write blocking activities.

Keywords: write blocker, acquisition, data integrity, storage media, USB