ABSTRACT

USB FLASH DRIVE DATA ACQUISITION FOR COLLECTING EVIDENCE BY RECOVERING DELETED DATA FROM UNALLOCATED SPACE ACCORDING TO DIGITAL FORENSIC PROCEDURES

Fahreza Lerian

13/344147/PA/15139

The use of flash disk as a data transfer media is very global, yet the use of flash disk can be misused for crimes, such as transactions of a highly confidential personal information, transactions of pornography and others. Files can be erased inside a flash drive or formatting a device could be performed in order to make the criminals untraceable, where the files may contain important information regarding the criminal. Deleting files inside flash drive and emptying the trash bin make files inaccessible for user, recovery is performed in order to gather data from storage. The submission for electronic evidence is accepted to imprison the criminals.

This research includes some processes of investigation: Acquisition by creating bit-by-bit disk image using *dd* command, authenticity verification using MD5 algorithm and analyzing image and files recovery using The Sleuth Kit. The Sleuth Kit (TSK) is an open source tools to investigate the image, the tools can be used to recover deleted file and perform other tasks.

The result of this research informs the acquisition and file recovery of evidence can be done from its image, as long as the files is not overwritten and been through a good formatting process (zeroing the device). The research also informs the result of acquisition and recovery under few circumstances and various type and size of evidence. By using this research implementation, the process can be done with a simple tools and less cost.

Keywords: Digital forensic, USB Flash Drive, Deleted Files, The Sleuth Kit.