ABSTRACT

One of the anti-forensic activities to secure data is to delete data from storage media, which can make it difficult for law enforcement to collect digital evidence. In practice, there are many methods that can make deleting data completely safe and not easy to recover with various recovery tools, one of which is wiping data. The deletion method with data wiping techniques, in anti-forensic activities is usually used on storage media that stores illegal data related to evidence of crime. If the storage media contains crime data, the owner of the data will try to hide or delete the data, one of which is the data wiping method. includes metadata and tracedata. In an effort to help forensic activities understand data wiping tools, in this final project test six pre-selected sample tools or applications will be taken that can perform data wiping on storage media, with the aim of comparing data wiping results between these tools or applications and then analyzing the advantages and deficiencies for purposes as data for forensic activities. The methods taken for sample tools or applications are the Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M(E), U.S. DoD 5220.22-M (ECE), and Bruce Schneier's Algorithm. These methods can erase and overwrite data so that it cannot be read by unauthorized persons, and can thus be used to prevent disclosure of crimes.

Kata Kunci: Anti Forensic, Data Wiping, Storage Media, Deletion