ANALISIS FORENSIK RECOVERY DATA PADA SERVER SISTEM INFORMASI DENGAN METODE NATIONAL INSTITUTE OF JUSTICE

Noka Arievaldy Hendyatoro
Program Studi Sistem Informasi, Fakultas Sains & Teknologi
Universitas Teknologi Yogyakarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail : noka.hendyantoro@student.uty.ac.id

ABSTRACT

Along with technological advances, the era of digitalization is an era where cyber crime cases are increasing. Cyber crime cases relate to criminals who erase evidence of criminal records. Forensic data resides on storage media can be SSD NVMe and HDD. The storage media has different characteristics that can affect the results of data recovery during the data forensic process. Data deleted in digital forensics can be done with normal delete and secure delete scenarios. The normal delete scenario works by marking the old deleted data space so that it can be occupied with new data, whereas in the secure delete scenario the deleted data cannot be returned. The research was conducted based on the National Institute of Justice method by designing scenarios for normal and secure delete data deletion on storage media, imaging processes, validating images according to the hash of the original file record, and data recovery processes using the Recuva application. The results of the study are file recovered from each scenario and storage media. The average percentage of files that can be recovered in both storage media with normal delete scenario is 49%, while in the secure delete scenario, no files can be found and recovered.

Keywords : Digital Forensics, SSD NVMe, HDD, National Institute of Justice