

PENERAPAN METODE NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PEMULIHAN BARANG BUKTI YANG DIHAPUS

Dini Wulan Suci

(190441100122)

Dosen Pembimbing

1. Wahyudi Agustiono, S.Kom., M.Sc., Ph.D.
2. Novi Prastiti, S.Kom., M.Kom.

ABSTRAK

Perkembangan teknologi informasi tidak hanya berdampak positif, namun juga negatif bagi masyarakat, salah satunya adanya peningkatan kejahatan *cybercrime*. Diantara jenis *cybercrime*, yang menjadi fokus pada penelitian ini adalah kejahatan *carding* atau pembobolan identitas kartu kredit orang lain secara *illegal*. Kejahatan ini memanfaatkan media penyimpanan *flashdisk* dan *harddisk* untuk menyimpan data hasil *carding*. Namun, pelaku berusaha menghilangkan bukti kejahatannya dengan menghapus seluruh data bukti. Oleh sebab itu, adanya penelitian ini bertujuan untuk menemukan bukti digital terkait kasus *carding*.

Penelitian ini menghasilkan prosedur digital forensik dalam melakukan investigasi pada media penyimpanan guna memulihkan barang bukti berupa *file*. Sehingga penelitian ini menggunakan *tools* FTK Imager dan Autopsy, serta metode *National Institute of Standards and Technology Special Publication 800-86* (NIST SP 800-86) yang memiliki empat tahapan yaitu Pengumpulan, Pemeriksaan, Analisis, dan Pelaporan sebagai acuan dalam proses akuisisi serta pengolahan bukti digital.

Penelitian ini dilakukan dengan mengakuisisi data pada bukti elektronik menggunakan FTK Imager, dan didapatkan rata-rata waktu yang untuk menyalin data pada *flashdisk* dengan *storage* 8GB yaitu 8 menit, sedangkan pada *harddisk* dengan *storage* 80GB diperlukan waktu 43 menit. Selanjutnya, hasil pemulihan data pada penelitian ini menunjukkan bahwa FTK Imager dan Autopsy mampu memulihkan barang bukti yang dihapus (Shift+Delete), dengan presentase keberhasilan 100%. Sebaliknya, kedua alat forensik tersebut tidak dapat memulihkan data yang dihapus dengan cara pemformatan pada bukti elektronik, sehingga presentase keberhasilan 0%. Hal tersebut terbukti dari hasil pengujian terhadap bukti elektronik yang telah dilakukan oleh peneliti sebanyak 5 kali pengujian dalam kurun waktu 8 minggu.

Kata Kunci: *Cybercrime*, FTK Imager dan Autopsy, NIST SP 800-86.

ABSTRACT

The development of information technology not only has positive impacts, but also negative impacts on society, one of which is an increase in cybercrime crimes. Among the types of cybercrime, the focus of this research is the crime of carding or illegally breaking into someone else's credit card identity. This crime uses flash disk and hard disk storage media to store carding data. However, the perpetrator tried to eliminate evidence of his crime by deleting all evidence data. Therefore, this research aims to find digital evidence related to carding cases.

This research produces digital forensic procedures for conducting investigations on storage media to recover evidence in the form of files. So this research uses the FTK Imager and Autopsy tools, as well as the National Institute of Standards and Technology Special Publication 800-86 (NIST SP 800-86) method which has four stages, namely Collection, Examination, Analysis and Reporting as a reference in the acquisition and processing process. digital evidence.

This research was carried out by acquiring data on electronic evidence using FTK Imager, and it was found that the average time for copying data on a flash disk with 8GB storage was 8 minutes, whereas on a hard disk with 80GB storage it took 43 minutes. Furthermore, the data recovery results in this study show that FTK Imager and Autopsy are able to recover deleted evidence (Shift+Delete), with a success percentage of 100%. On the other hand, these two forensic tools cannot recover data deleted by formatting electronic evidence, so the success rate is 0%. This is proven by the results of testing on electronic evidence which was carried out by researchers 5 times over a period of 8 weeks.

Keywords: *Cybercrime, FTK Imager and Autopsy, NIST SP 800-86.*