ABSTRACT

AUTOMATED DATA ACQUISITION OF NTFS AND FAT32 FILE SYSTEM FOR DIGITAL FORENSICS

Firzan Irfandi Firman

14/368446/PA/16284

The usage of computers has a big advantage in many sectors; such as education, enterprise, entertainment, engineering, and many more. Technology is like a double edged sword as well. The advantages can be handy for criminals who want to do their heinous acts of crimes. Hence the term cybercrime. Thus to combat cybercrime, search and facts and perpetrators behind, digital forensics is needed.

This research emphasizes on an automated data acquisition on two types of file systems, namely NTFS and FAT, which includes a handful of processes that was based on digital forensic procedures. The program will run on Debian-based Linux. The automated data acquisition program is written in Python programming language by importing the necessary libraries and utilities. A case brief is simulated for this program.

The results show that the program was able to do data acquisition. The program was able to acquire data from a storage. The program was also able to view files, directories and hidden file available within a storage.

Keywords – Digital Forensics, NTFS, FAT, Cybercrime

INTISARI

OTOMASI AKUISISI DATA DARI SISTEM BERKAS NTFS DAN FAT UNTUK FORENSIK DIGITAL

Firzan Irfandi Firman

14/368446/PA/16284

Penggunaan komputer memiliki banyak keuntungan di berbagai sektor; seperti pendidikan, perusahaan, hiburan, keteknikan, dan banyak lagi. Akan tetapi, teknologi ibarat pedang bermata dua. Keuntungannya bisa berguna bagi para penjahat yang ingin melakukan tindakan keji mereka. Hal itu dikenal dengan istilah kejahatan siber. Dengan demikian untuk memerangi kejahatan dunia maya, mencari fakta, serta mencari pelaku di belakangnya, forensik digital diperlukan.

Penelitian ini menekankan pada akuisisi data otomatis pada dua jenis sistem berkas, yaitu NTFS dan FAT, yang mencakup beberapa proses yang didasarkan pada prosedur forensik digital. Program akan berjalan di Linux berbasis Debian. Program akuisisi data otomatis ditulis dalam bahasa pemrograman Python dengan mengimpor perpustakaan dan utilitas yang diperlukan. Studi kasus dibuat untuk menyimulasikan program.

Hasil penelitian menunjukkan bahwa program mampu melakukan akuisisi data. Program dapat memperoleh data dari penyimpanan. Program juga dapat melihat berkas, direktori, dan file tersembunyi yang tersedia dalam penyimpanan.

Keywords – Forensik Digital, NTFS, FAT, Kejahatan Siber.