Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

AKBAR AGUNG BAHAR

17.83.0018

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

AKBAR AGUNG BAHAR

17.83.0018

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

HALAMAN PERSETUJUAN

SKRIPSI

Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST

yang disusun dan diajukan oleh

AKBAR AGUNG BAHAR

17.83.0018

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 7 Mei 2024

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng
NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST

yang disusun dan diajukan oleh

AKBAR AGUNG BAHAR

17.83.0018

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Mei 2024

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Wahid Miftahul Ashari, S.Kom., M.T **NIK. 190302452**	
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	
Banu Santoso, S.T., M.Eng **NIK. 190302327**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Mei 2024

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Akbar Agung Bahar
NIM : 17.83.0018

Menyatakan bahwa Skripsi dengan judul berikut:

Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST

Dosen Pembimbing : Banu Santoso, S.T., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 Mei 2024

Yang Menyatakan,

Akbar Agung Bahar

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Orang tua saya, yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Banu Santoso, S.T., M.Eng Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST”. Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M. Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Joko Dwi Santoso, M.Kom selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyususnan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.

Yogyakarta, <tanggal bulan tahun>
Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
INTISARI xiii
ABSTRACT xiv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
1.6 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 5
2.1 Tinjauan Pustaka 5
2.2 Forensika Digital 7
2.3 Standard Operating Procedure (SOP) 8
2.4 Bukti Digital 8

2.5 Anti Forensic 9
2.5.1 Penyembunyian Data 9
2.5.2 Artifact Wiping 9
2.6 NIST Framework 9
2.6.1 *Collection / Acquisition* 10
2.6.2 *Examination* 10
2.6.3 *Analysis* 11
2.6.4 *Reporting* 11
2.7 Disk Forensic 11
2.8 Hashing 12
2.9 Kebutuhan Tool Investigasi 12
2.9.1 MD5 Checker 12
2.6.4 DD 12
2.6.4 FTK Imager 12
2.6.4 Autopsy 13
2.6.5 Recuva 13
2.6.6 Foremost 13
2.6.7 USB Viewer 14
BAB III METODE PENELITIAN 15
3.1 Gambaran Umum Penelitian 15
3.2 Persiapan Alat dan Bahan Penelitian 16
3.2.1 Lingkungan Simulasi 17
3.2.1 Lingkungan Simulasi 17
3.2.3 Kebutuhan Perangkat Lunak 18
3.3 Skenario dan Simulasi Kasus 18

3.4 Metode Penelitian.....19
3.4.1 Prosedur NIST.....20
3.4.2 One-Shot Case Study.....22
BAB IV HASIL DAN PEMBAHASAN.....23
4.1 Persiapan.....23
4.4.1 Pemasangan Environment dan Tools Investigator.....23
4.1.2 Pemasangan Environment dan Tools Investigator.....24
4.2 Implementasi Skenario File Wiping.....26
4.2.1 File Dihapus.....28
4.2.2 Format USB Flashdisk.....29
4.2.4 File dihapus + overwrite (ditimpa terus menerus).....32
4.2.4 File dihapus + overwrite (ditimpa terus menerus).....33
4.3 Akuisisi Data.....34
4.1.1 Duplikat Hasil Akuisisi (Imaging).....38
4.1 Eksaminasi dan Analisa.....40
4.1.2 Analisa Menggunakan AutoSpy.....41
4.4.2 Analisa menggunakan Recuva.....42
4.1.1 Analisa menggunakan Foremost.....44
4.5 Laporan Akhir Investigasi.....46
4.5.1 Hasil Analisa Menggunakan AutoPsy.....46
4.5.2 Hasil Analisa menggunakan Recuva.....48
4.5.3 Hasil Analisa menggunakan Foremost.....49
4.5.4 Laporan Akhir dari Analisa.....51
BAB V PENUTUP.....53
5.1 Kesimpulan.....53

5.2 Saran 54

DAFTAR PUSTAKA .....**Error! Bookmark not defined.**

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu 6

Tabel 2. 2 Penelitian yang Diusulkan

Tabel 3. 1 Spesifikasi EC2 Instance Victim

Tabel 3. 2 Detail Spesifikasi USB Flashdisk

Tabel 3. 3 Kebutuhan Perangkat Lunak Investigator

Tabel 3. 4 Implementasi Teknik Anti Forensic File Wiping

Tabel 4. 1 Implementasi Teknik Anti Forensic File Wiping

Tabel 4.3 Hasil Akuisisi Physical USB Flashdisk

Tabel 4.4 MD5 Hash Dari Hasil Imaging

Tabel 4.5 Informasi File Asli yang Dilakukan Tindakan File Wiping

Tabel 4.6 Hasil Analisa Anti Forensic Skenario Pertama menggunakan Autopsy

Tabel 4.7 Hasil Analisa Anti Forensic Skenario Kedua menggunakan Autopsy

Tabel 4.8 Hasil Analisa Anti Forensic Skenario Ketiga menggunakan Autopsy

Tabel 4.10 Hasil Analisa Anti Forensic Skenario Pertama menggunakan Recuva

Tabel 4.11 Hasil Analisa Anti Forensic Skenario Kedua menggunakan Recuva

Tabel 4.12 Hasil Analisa Anti Forensic Skenario Ketiga menggunakan Recuva

Tabel 4.13 Hasil Analisa Anti Forensic Skenario Keempat menggunakan Recuva

Tabel 4.14 Hasil Analisa Anti Forensic Skenario Pertama menggunakan Foremost

Tabel 4.15 Hasil Analisa Anti Forensic Skenario Kedua menggunakan Foremost

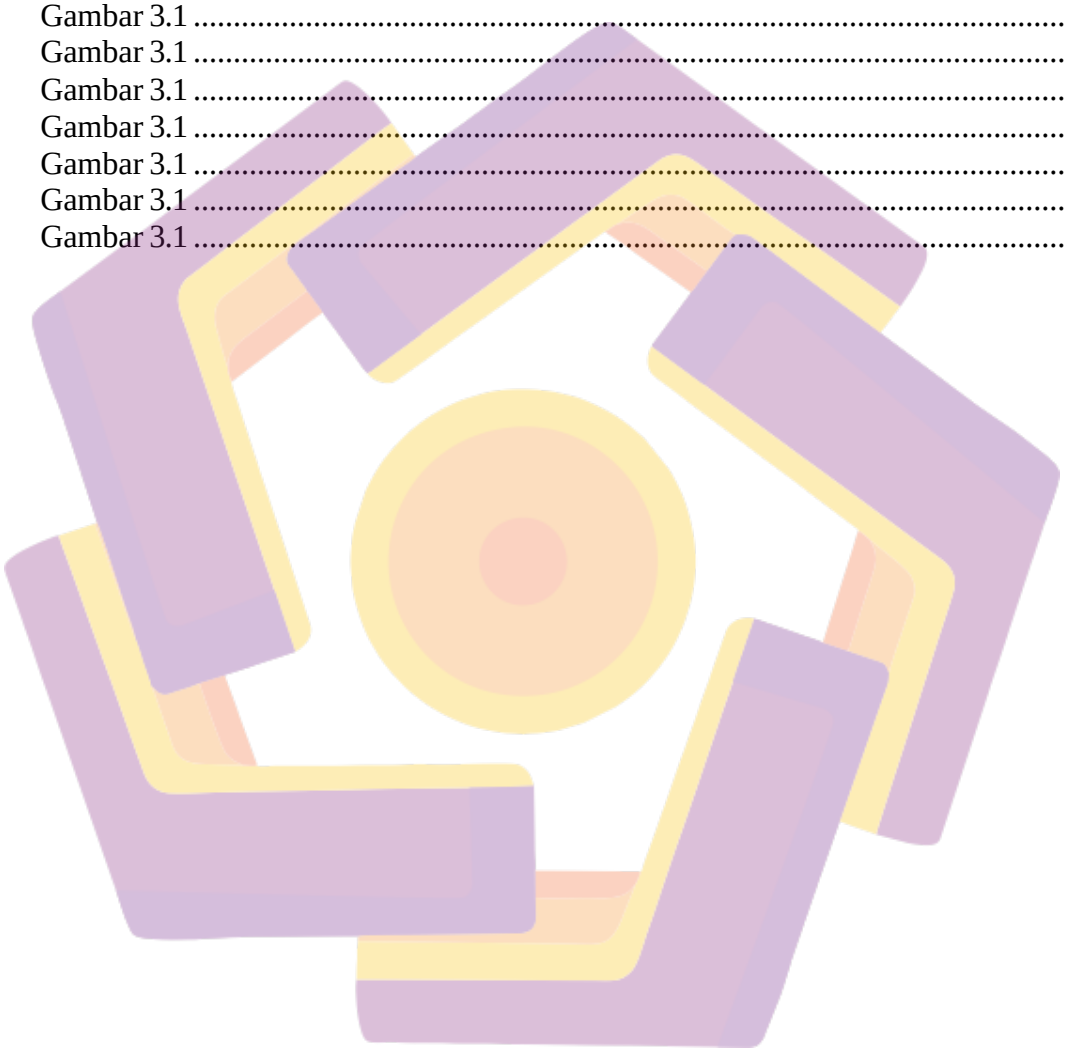
Tabel 4.16 Hasil Analisa Anti Forensic Skenario Ketiga menggunakan Foremost

Tabel 4.17 Hasil Analisa Anti Forensic Skenario Keempat menggunakan Foremost

Tabel 4.18 Hasil Efektifitas Keberhasilan Recovery Data dari Ketiga Tool pada Skenario Anti Forensic Pertama

DAFTAR GAMBAR

Gambar 1.1 15
Gambar 2.1 15
Gambar 3.1 19
Gambar 3.1 19
Gambar 3.1 19
Gambar 3.1 19
Gambar 3.1 19
Gambar 3.1 19
Gambar 3.1 19
Gambar 3.1 19
Gambar 3.1 1



INTISARI

Data digital memegang peranan penting dalam semua kegiatan digitalisasi. USB Flashdisk sebagai media penyimpanan data yang paling banyak digunakan memiliki kemungkinan terjadinya kehilangan data. Banyaknya cara kriminal yang dilakukan untuk menghapus jejak jejak data digital menjadi tantangan tersendiri bagi investigator. Untuk itu perlu dilakukan tindakan forensik komputer khususnya data recovery terhadapnya agar dapat merestore data ke media lain dengan aman sekaligus menjadikan temuan data sebagai bukti di persidangan. Pada penelitian ini dilakukan uji anti forensik (menghilangkan jejak data) dengan mengikuti skenario pengujian yang telah dirancang, kemudian diamati, direkam, dan dianalisis. Hasil pengujian dan analisis hasil pengujian menunjukkan kemampuan berbagai teknik dan tool dalam mengupayakan pengembalian data yang sudah dihapus.

Kata kunci: Forensik Digital, Forensik Disk, Anti Forensik.

ABSTRACT

Digital data plays an important role in all digitization activities. USB flash drives as the most widely used data storage media have the possibility of data loss. The many criminal methods used to erase digital data traces are a challenge for investigators. For this reason, it is necessary to carry out computer forensic measures, especially data recovery on them so that they can safely restore data to other media while at the same time making data findings as evidence in court. In this study, an anti-forensic test was carried out (removing data traces) by following the test scenarios that had been designed, then recorded, recorded, and analyzed. The test results and the analysis of the test results show the ability of various techniques and tools to recover data that has been deleted.

Keyword: Digital Forensic, Disk Forensic, Anti Forensic.