ANALISIS TEKNIK ANTI-FORENSIK PADA EKSTERNAL STORAGE MENGGUNAKAN FRAMEWORK NIST SP 800-86

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika

disusun oleh

ADHIMAS YUSUF SYAPUTRA

21.11.4536

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

ANALISIS TEKNIK ANTI-FORENSIK PADA EKSTERNAL STORAGE MENGGUNAKAN FRAMEWORK NIST SP 800-86

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

ADHIMAS YUSUF SYAPUTRA

21.11.4536

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS TEKNIK ANTI-FORENSIK PADA EKSTERNAL STORAGE MENGGUNAKAN FRAMEWORK NIST SP 800-86

yang disusun dan diajukan oleh

ADHIMAS YUSUF SYAPUTRA

21.11.4536

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 24 Juni 2025

Dosen Pembimbing,

Subektiningsih, S.Kom., M.Kom.
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS TEKNIK ANTI-FORENSIK PADA EKSTERNAL STORAGE MENGGUNAKAN FRAMEWORK NIST SP 800-86

yang disusun dan diajukan oleh

Adhimas Yusuf Syaputra

21.11.4536

Telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Juni 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Andika Agus Slameto, S.Kom., M.Kom. **NIK. 190302109**	
Muhammad Rudyanto Arief, S.T., M.T **NIK. 190302098**	
Subektiningsih, S.Kom., M.Kom. **NIK. 190302413**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 24 Juni 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Adhimas Yusuf Syaputra
NIM : 21.11.4536

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS TEKNIK ANTI-FORENSIK PADA EKSTERNAL STORAGE MENGGUNAKAN FRAMEWORK NIST SP 800-86

Dosen Pembimbing : Subektiningsih, S.Kom., M.Kom.

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, 24 Juni 2025

Yang Menyatakan,

Adhimas Yusuf Syaputra

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur dan kerendahan hati, skripsi ini dipersembahkan kepada kedua orang tua atas doa dan pengorbanan yang tidak terhingga, kepada keluarga yang senantiasa memberikan doa dan dukungan, kepada dosen pembimbing serta seluruh pengajar yang telah memberikan ilmu yang sangat bermanfaat selama proses studi, serta kepada teman-teman seperjuangan di Universitas Amikom Yogyakarta yang telah memberikan semangat dan dukungan. Semoga karya ini dapat memberikan manfaat dan menjadi langkah awal untuk kontribusi yang lebih besar di masa depan.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "ANALISIS TEKNIK ANTI-FORENSIK PADA EKSTERNAL STORAGE MENGGUNAKAN FRAMEWORK NIST SP 800-86". Skripsi ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan program Sarjana (S1) pada program studi Informatika Universitas Amikom Yogyakarta.

Dalam proses penyusunan skripsi ini, penulis menyadari bahwa terdapat bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Ibu Subektiningsih, M.Kom, selaku dosen pembimbing yang telah banyak meluangkan waktu, memberikan arahan, bimbingan, serta saran dalam penyusunan skripsi ini.
2. Bapak Prof. Dr. M. Suyanto, MM, selaku Rektor Universitas Amikom Yogyakarta.
3. Ibu Prof. Dr. Kusrini, M.Kom, selaku Dekan Fakultas Ilmu Komputer.
4. Ibu Eli Pujastuti, M.Kom, selaku Kepala Program Studi S1 Informatika Universitas Amikom Yogyakarta.
5. Orang tua, adik, dan keluarga yang selalu menjadi sumber doa, semangat, dan ketulusan.
6. Teman-teman seperjuangan, atas motivasi dan kerja sama selama masa studi.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, saran dan kritik yang membangun sangat penulis harapkan untuk perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca serta menjadi referensi dalam penelitian di bidang forensik digital.

Yogyakarta, 24 Juni 2025

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.....ix
DAFTAR GAMBAR.....x
DAFTAR ISTILAH.....xii
INTISARI.....xiv
ABSTRACT.....xv
BAB I PENDAHULUAN.....1
1.1 Latar Belakang Masalah.....1
1.2 Rumusan Masalah.....3
1.3 Batasan Masalah.....3
1.4 Tujuan Penelitian.....3
1.5 Manfaat Penelitian.....4
1.6 Sistematika Penulisan.....4
BAB II TINJAUAN PUSTAKA.....5
2.1 Studi Literatur.....5
2.2 Dasar Teori.....14
2.2.1 Forensik Digital.....14
2.2.2 Bukti Digital.....15

2.2.3 File Signature 16
2.2.4 Imaging 16
2.2.5 Hashing 17
2.2.6 Perangkat Penyimpanan 18
2.2.7 Teknik Anti-Forensik 19
2.2.8 Pemulihan Data 20
2.2.9 NIST SP 800-86 21
BAB III METODE PENELITIAN 23
3.1 Objek Penelitian 23
3.2 Alur Penelitian 25
3.3 Identifikasi Masalah 26
3.4 Perancangan Skenario 26
BAB IV HASIL DAN PEMBAHASAN 29
4.1 Penerapan Teknik Anti-Forensik 29
4.2 Penerapan Forensik Digital Menggunakan NIST SP 800-86 37
4.2.1 Forensik Digital Skenario 1: Penghapusan dan Fragmentasi 37
4.2.2 Forensik Digital Skenario 2: Quick Format 49
4.2.3 Forensik Digital Skenario 3: Full Format 54
4.2.4 Forensik Digital Skenario 4: Single-Pass Overwrite 58
4.2.5 Forensik Digital Skenario 5: Random Overwrite 63
BAB V PENUTUP 70
5.1 Kesimpulan 70
5.2 Saran 70
REFERENSI 72
LAMPIRAN 76

DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian 9
Tabel 3.1 Spesifikasi Perangkat Penyimpanan 29
Tabel 3.2 Daftar Skenario 30
Tabel 3.3 Tools yang Digunakan 31
Tabel 4.1 Detail Setiap File 32
Tabel 4.2 Pembahasan Singkat Skenario 33
Tabel 4.3 Nilai Hash File Skenario 34
Tabel 4.4 Detail Barang Bukti 1 43
Tabel 4.5 Detail Barang Bukti 2 43
Tabel 4.6 Nilai Hash dari Image Setiap Media 45
Tabel 4.7 Hasil Perbandingan Hash pada HDD 49
Tabel 4.8 Hasil Perbandingan Hash pada SSD 51
Tabel 4.9 Hasil Penerapan Teknik Anti-Forensik Skenario 1 54
Tabel 4.10 Hasil Pemulihan Data Skenario 1 54
Tabel 4.11 Nilai Hash dari Setiap Image 55
Tabel 4.12 Hasil Perbandingan Hash pada HDD 58
Tabel 4.13 Hasil Penerapan Teknik Anti-Forensik Skenario 2 60
Tabel 4.14 Hasil Pemulihan Data Skenario 2 60
Tabel 4.15 Nilai Hash dari Setiap Image 61
Tabel 4.16 Hasil Penerapan Teknik Anti-Forensik Skenario 3 64
Tabel 4.17 Hasil Pemulihan Data Skenario 3 64
Tabel 4.18 Nilai Hash dari Setiap Image 65
Tabel 4.19 Hasil Penerapan Teknik Anti-Forensik Skenario 4 70
Tabel 4.20 Hasil Pemulihan Data Skenario 4 70
Tabel 4.21 Nilai Hash dari Setiap Image 71
Tabel 4.22 Hasil Penerapan Teknik Anti-Forensik Skenario 5 75
Tabel 4.23 Hasil Pemulihan Data Skenario 5 76
Tabel 4.24 Hasil Penerapan Teknik Anti-Forensik pada Seluruh Skenario 77

DAFTAR GAMBAR

Gambar 3.1 Objek Penelitian 27
Gambar 3.2 Alur Penelitian 28
Gambar 4.1 Jenis File yang Digunakan Dalam Pengujian 32
Gambar 4.2 File Skenario Untuk Fragmentasi 32
Gambar 4.3 Visualisasi Skenario 1 pada HDD 34
Gambar 4.4 Visualisasi Skenario 1 pada SDD 35
Gambar 4.5 Kondisi Penyimpanan SSD dan HDD Hampir Penuh 35
Gambar 4.6 Hasil Pemindaian pada HDD 35
Gambar 4.7 Detail File yang Terfragmentasi pada HDD 36
Gambar 4.8 Detail File yang Terfragmentasi pada SSD 36
Gambar 4.9 Distribusi Blok pada Defraggler 36
Gambar 4.10 Visualisasi Skenario 2 pada HDD 37
Gambar 4.11 Visualisasi Skenario 2 pada SSD 37
Gambar 4.12 Fitur Quick Format pada Windows 37
Gambar 4.13 Visualisasi Skenario 3 pada HDD 38
Gambar 4.14 Visualisasi Skenario 3 pada SSD 38
Gambar 4.15 Fitur Full Format pada Windows 38
Gambar 4.16 Visualisasi Skenario 4 pada HDD 39
Gambar 4.17 Visualisasi Skenario 4 pada SSD 39
Gambar 4.18 Perintah Overwrite Menggunakan dd 39
Gambar 4.19 Visualisasi Skenario 5 pada HDD 40
Gambar 4.20 Visualisasi Skenario 5 pada SSD 40
Gambar 4.21 Random Overwrite Menggunakan dd 41
Gambar 4.22 Alur Proses Investigasi 42
Gambar 4.23 Akuisisi Barang Bukti 1 42
Gambar 4.24 Akuisisi Barang Bukti 2 43
Gambar 4.25 Hasil Imaging HDD pada FTK Imager 44
Gambar 4.26 Hasil Generate Nilai Hash HDD pada Autopsy 44
Gambar 4.27 Hasil Generate Nilai Hash SSD pada Autopsy 44
Gambar 4.28 Hasil Pemulihan dari HDD pada Autopsy 45
Gambar 4.29 Hasil Pemulihan dari SSD pada Autopsy 46
Gambar 4.30 Folder Recycle Bin 46
Gambar 4.31 Signature dari Sistem File NFTS 46
Gambar 4.32 Beberapa File yang Terdeteksi 47
Gambar 4.33 Hasil File Carving Menggunakan Photorec 47
Gambar 4.34 Metadata File JPG yang Berubah 48
Gambar 4.35 Hex Dump File MP4 yang Hanya Berisi 0 50
Gambar 4.36 File MP4 yang Tidak Bisa Dibuka 50
Gambar 4.37 Hasil Pemulihan Menggunakan Photorec 52
Gambar 4.38 Hasil Pemulihan HDD pada Autopsy 55
Gambar 4.39 Folder Recycle Bin 55
Gambar 4.40 Signature dari Sistem File NFTS 56

Gambar 4.41 Hasil Pemulihan File Carving pada HDD 56
Gambar 4.42 Hasil Pemulihan SSD pada Autopsy 56
Gambar 4.43 Hasil File Carving pada SSD 57
Gambar 4.44 Hasil Pemulihan File Carving pada HDD 57
Gambar 4.45 Metadata File PDF yang Berubah 58
Gambar 4.46 Hasil Pemulihan Menggunakan Autopsy 61
Gambar 4.47 Signature dari Sistem File NFTS 62
Gambar 4.48 Hasil File Carving pada Kali Linux 62
Gambar 4.49 Hasil Pemulihan pada SSD 63
Gambar 4.50 Hasil Pemulihan Menggunakan Photorec 63
Gambar 4.51 Autopsy Tidak Dapat Mendeteksi Tipe dari Sistem File 66
Gambar 4.52 Hasil Pemulihan Photorec pada HDD 66
Gambar 4.53 Hasil pemulihan Photorec pada SSD 67
Gambar 4.54 Proses Pengaturan Ulang pada HDD 68
Gambar 4.55 Proses Pengaturan Ulang pada SSD 68
Gambar 4.56 Disk yang Harus Diformat 69
Gambar 4.57 Autopsy Mendeteksi High Entropy 71
Gambar 4.58 Hasil File Carving pada HDD 72
Gambar 4.59 File yang Dapat Dipulihkan pada HDD 72
Gambar 4.60 File yang Dapat Dipulihkan pada SSD 72
Gambar 4.61 Hasil Analisis Menggunakan Utility File pada Kali Linux 73
Gambar 4.62 File MOV yang Tidak Dapat Diputar 74
Gambar 4.63 File DBX yang Tidak Dapat Dibuka 74
Gambar 4.64 Hasil Analisis Menggunakan Utility File 74

DAFTAR ISTILAH

Forensik Digital	Cabang ilmu forensik yang berfokus pada identifikasi, pengumpulan, analisis, dan pelaporan bukti digital dari perangkat elektronik.
Anti-Forensik	Teknik atau upaya yang dilakukan untuk menghapus, menyembunyikan, atau mempersulit proses identifikasi dan pemulihan bukti digital.
Jejak Digital	Informasi atau data yang secara tidak langsung ditinggalkan oleh pengguna selama aktivitas digital yang dapat dianalisis untuk tujuan investigasi.
NIST SP 800-86	Dokumen panduan dari *National Institute of Standards and Technology* (NIST) yang memberikan kerangka kerja sistematis dalam investigasi forensik digital, meliputi tahapan *collection, examination, analysis*, dan *reporting*.
TRIM	Perintah pada sistem operasi yang memberi tahu SSD untuk menghapus blok data yang tidak lagi digunakan sehingga meningkatkan efisiensi dan mempercepat kinerja.
Bukti Digital	Informasi dalam bentuk digital yang dapat digunakan di pengadilan sebagai bagian dari proses hukum atau investigasi.
Cybercrime	Tindakan kriminal yang melibatkan penggunaan teknologi komputer atau jaringan sebagai sarana atau target kejahatan.
Imaging	Proses pembuatan salinan bit-per-bit dari media penyimpanan digital untuk keperluan analisis forensik tanpa memodifikasi data asli.
Hash	Nilai unik yang dihasilkan dari proses algoritma tertentu untuk merepresentasikan data dalam bentuk string alfanumerik tetap.

File Carving	Teknik pemulihan data yang mencari dan mengekstrak file dari media penyimpanan berdasarkan pola *file signature*, tanpa bergantung pada struktur sistem file.
Metadata	Data yang menjelaskan informasi tentang data lain, seperti waktu pembuatan file, ukuran, atau lokasi penyimpanan.
Sistem File	Struktur logis yang digunakan sistem operasi untuk mengatur, menyimpan, dan mengakses data pada media penyimpanan.
Master File Table	Komponen utama pada sistem file NTFS yang berisi informasi metadata setiap file dan direktori dalam volume.
Chain of Custody	Dokumentasi yang mencatat riwayat kepemilikan, pengendalian, transfer, dan analisis barang bukti digital untuk menjamin keabsahannya di pengadilan.
Hearsay	Pernyataan atau informasi yang tidak diperoleh secara langsung oleh penyidik atau saksi dan tidak dapat dijadikan alat bukti yang sah menurut hukum, kecuali termasuk dalam pengecualian.
File Signature	Pola byte tertentu pada awal file (*header*) yang digunakan untuk mengidentifikasi jenis file, sering digunakan dalam proses file carving.
Garbage Collection	Proses pada SSD yang menghapus blok data yang tidak lagi digunakan untuk menjaga performa dan memperpanjang umur perangkat.
Bad Sector	Bagian dari media penyimpanan yang rusak dan tidak dapat diakses atau digunakan untuk menyimpan data.
Utility	Perangkat lunak atau alat bantu yang dirancang untuk melakukan tugas khusus dalam pengelolaan sistem atau media penyimpanan.
Hex Dump	Representasi data dalam format heksadesimal, sering digunakan dalam analisis forensik untuk memeriksa konten biner file secara langsung.

INTISARI

Penyelidikan forensik digital sering kali menghadapi tantangan dari teknik anti-forensik yang diterapkan oleh pihak yang berniat menyembunyikan jejak digital mereka. Dalam upaya menghilangkan jejak, pelaku dapat menggunakan perangkat lunak untuk menghapus data secara permanen atau melakukan perusakan fisik terhadap media penyimpanan agar data tidak dapat dipulihkan. Hal ini menyebabkan jejak-jejak digital yang dapat menjadi bukti sulit atau bahkan tidak dapat dikumpulkan.

Penelitian ini bertujuan untuk menganalisis pengaruh teknik anti-forensik terhadap proses pemulihan data dari dua jenis perangkat penyimpanan eksternal, yaitu SSD portabel dan HDD portabel. Pengujian dilakukan dengan menerapkan beberapa teknik anti-forensik *disk wiping* yang mencakup penghapusan, fragmentasi, *formatting*, dan *overwriting* pada kedua jenis perangkat, diikuti oleh proses pemulihan data menggunakan metode pemulihan konvensional dan metode file carving. Seluruh proses pengujian forensik digital dilakukan menggunakan kerangka kerja NIST SP 800-86, yang mencakup *collection*, *examination*, *analysis*, dan *reporting* sebagai panduan analisis.

Teknik-teknik anti-forensik yang hanya menghapus data pada sistem file, seperti penghapusan, fragmentasi, dan *quick format*, masih memungkinkan pemulihan data. Namun, hal ini hanya berlaku pada HDD, karena pada SSD terdapat fitur TRIM. Di sisi lain, teknik-teknik anti-forensik yang menghapus data asli pada disk, seperti *full format*, *single-pass overwrite*, dan *random overwrite*, tidak memungkinkan pemulihan data. Hasil penelitian diharapkan dapat memberikan pemahaman mengenai pengaruh teknik anti-forensik terhadap proses pemulihan data pada perangkat penyimpanan eksternal. Penelitian selanjutnya dapat mengembangkan ruang lingkup teknik anti-forensik yang diuji.

Kata kunci: Forensik Digital, Teknik Anti-Forensik, NIST SP 800-86, Pemulihan Data, Perangkat Penyimpanan.

ABSTRACT

Digital forensic investigations often face challenges from anti-forensic techniques used by individuals trying to conceal their digital traces. In an effort to eliminate evidence, perpetrators may use software to permanently delete data or physically damage storage media to make recovery impossible. As a result, digital traces that could serve as evidence may become inaccessible.

This study aims to analyse the impact of anti-forensic techniques on the data recovery process from two types of external storage devices, namely portable SSD and portable HDD. The testing involves applying several disk-wiping anti-forensic techniques, namely deletion, fragmentation, formatting, and overwriting on both types of devices. These are followed by data recovery attempts using conventional recovery methods and file carving technique. The entire forensic testing process is conducted using the NIST SP 800-86 framework, which includes the phases of collection, examination, analysis, and reporting.

Anti-forensic techniques that operate only at the file system level, such as deletion, fragmentation, and quick format, still allow data recovery. However, this is only applicable to HDDs, as SSDs contain the TRIM feature. On the other hand, techniques that delete the actual data on disk, such as full format, single-pass overwrite, and random overwrite leave no recoverable data on either device type. This research is expected to contribute to a better understanding of how anti-forensic techniques affect the data recovery process on external storage devices. Future research may expand the scope of tested anti-forensic techniques.

Keyword: *Digital Forensics, Anti-Forensic Techniques, NIST SP 800-86, Data Recovery, Storage Media.*