

**IMPLEMENTASI DIGITAL FORENSIK PADA *FLASHDRIVE*
DENGAN METODE *NATIONAL INSTITUTE OF JUSTICE*
*FRAMEWORK***

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

Kumara Sakhi Istikmal
18.83.0303

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2023

**IMPLEMENTASI DIGITAL FORENSIK PADA *FLASHDRIVE*
DENGAN METODE *NATIONAL INSTITUTE OF JUSTICE*
*FRAMEWORK***

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

Kumara Sakhi Istikmal

18.83.0303

kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI DIGITAL FORENSIK PADA *FLASHDRIVE* DENGAN
METODE *NATIONAL INSTITUTE OF JUSTICE FRAMEWORK***

yang disusun dan diajukan oleh

Kumara Sakhi Istikmal

18.83.0303

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 September 2022

Dosen Pembimbing,



Senie Destya M.Kom.

NIK. 190302312

HALAMAN PENGESAHAN

SKRIPSI

**IMPLEMENTASI DIGITAL FORENSIK PADA FLASHDRIVE
DENGAN METODE NATIONAL INSTITUTE OF JUSTICE
FRAMEWORK**

yang disusun dan diajukan oleh

Kumara Sakhi Istikmal
18.83.0303

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 September 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Senie Destya, M.Kom
NIK. 190302312



Subektiningsih, M.Kom
NIK. 190302413



Anggit Ferdita Nugraha, S.T., M.Eng
NIK. 190302480



Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Febuari 2023

DEKAN FAKULTAS ILMU KOMPUTER



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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Kumara Sakhi Istikmal
NIM : 18.83.0303

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI DIGITAL FORENSIK PADA FLASHDRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE FRAMEWORK

Dosen Pembimbing : Senie Destya, 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, 21 Febuari 2023

Yang Menyatakan.



Kumara Sakhi Istikmal

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur dan bahagia telah menyelesaikan laporan tugas akhir ini yang tak luput dari doa-doa dan dukungan dari orang-orang tercinta yang selalu memberikan support. Dengan rasa bangga dan syukur saya haturkan rasa syukur dan terimakasih saya kepada:

1. Allah SWT karena hanya atas izin dan karunianya lah skripsi ini dapat dibuat dan selesai pada waktunya.
2. Bapak Ibu saya, yang telah memberikan dukungan moral maupun materi serta doa yang tiada henti untuk kesuksesan saya, karena tiada kata sindah lantunan doa dan tiada doa yang paling khusyuk selain doa yang terucap dari orang tua.
3. Bapak serta Ibu Dosen prodi Teknik Komputer
4. Sindri Fera Kusuma selaku teman terbaik saya yang selalu memberi dukungan terhadap saya
5. Teman-teman Teknik Komputer 03 yang telah berjuang bersama.
6. Diri saya sendiri yang telah berjuang dan semangat sampai di titik ini.

KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kepada ALLAH SWT atas rahmat dan karunianya yang telah senantiasa dalam menyelesaikan penulisan tugas akhir ini. Skripsi ini ditulis dengan tujuan sebagai salah satu syarat untuk mencapai gelar sarjana Komputer Jurusan Teknik Komputer di Universitas Amikom Yogyakarta.

Skripsi ini ditulis merupakan bagian implementasi dari ilmu yang telah diperoleh di bangku perkuliahan. Penulisan skripsi ini tentu tidak akan berjalan lancar tanpa ada bantuan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Dosen Pembimbing Ibu Senie Destya, M.Kom.
2. Bapak Anggit Ferdita Nugraha, S.T., M.Eng.
3. Ibu Subektiningsih, M.Kom.
4. Dan semua pihak yang terkait dalam penyelesaian tugas akhir termasuk Keluarga, Sahabat dan Teman-teman.

Penulis berharap dengan adanya penulisan laporan tugas akhir ini dapat memberikan manfaat ataupun referensi bagi siapapun yang membutuhkan dan bisa dijadikan sebagai pengetahuan yang berguna dalam mempelajari ilmu forensik.

Yogyakarta, 21/4/2023

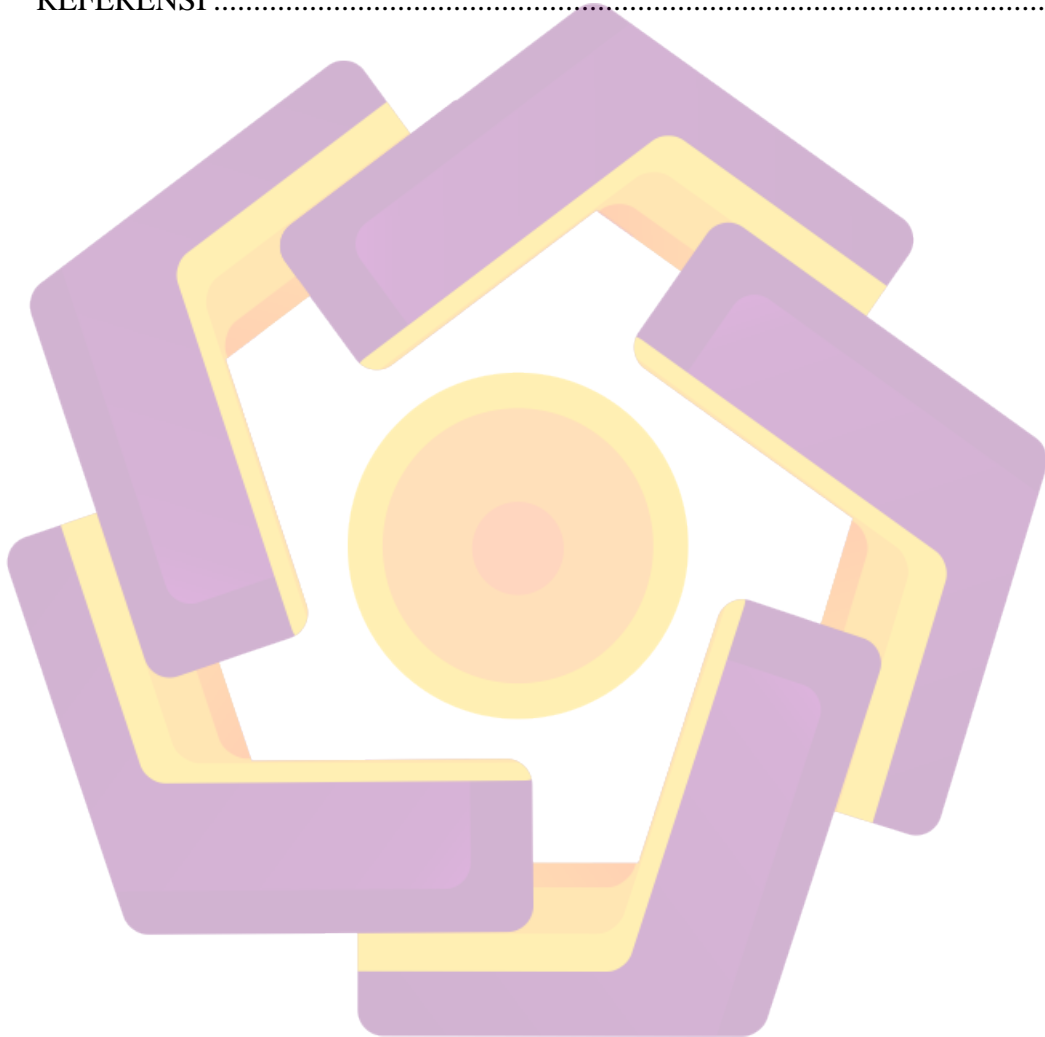


Kumara Sakhi Istikmal

DAFTAR ISI

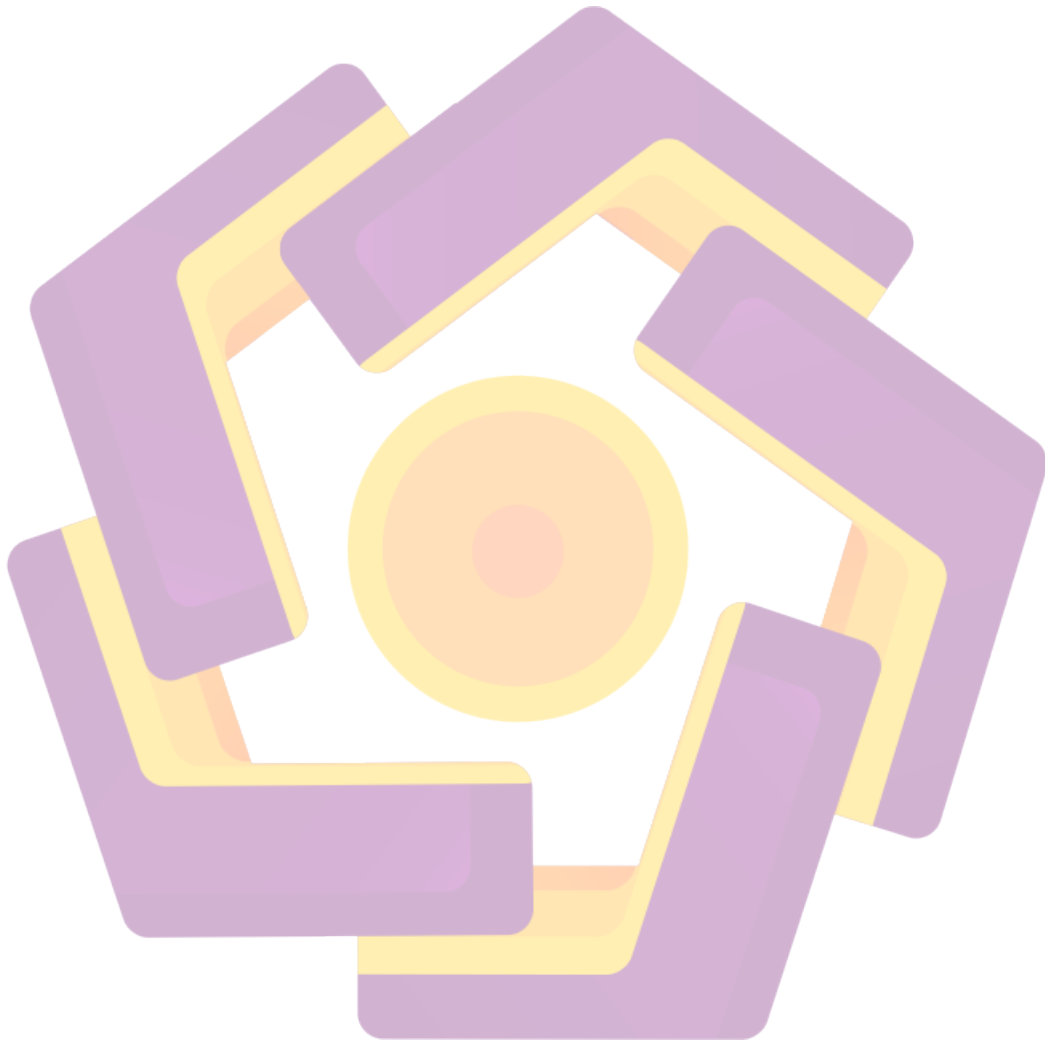
HALAMAN JUDUL	ii
DAFTAR ISI.....	iii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
INTISARI	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
2.1 Studi Literatur	6
2.2 Dasar Teori	9
2.2.1 Digital Forensik.....	9
2.2.2 Bukti Digital.....	9
2.2.3 Framework NIJ.....	9
2.2.4 Prinsip Forensik.....	11
2.2.5 Hashing.....	12
2.2.6 Imaging.....	13
2.2.7 <i>Autopsy</i>	13
2.2.8 <i>Hex Editor Neo</i>	13
2.2.9 Steganografi.....	13
BAB III METODE PENELITIAN	14
3.1. Objek Penelitian.....	14
3.2. Alur Penelitian	14
3.3. Alat dan Bahan.....	17
3.4. Langkah Penelitian	17
3.5. Menyusun Skenario	19
BAB IV HASIL DAN PEMBAHASAN	21
4.1 Implementasi Skenario	21
4.2 Proses Digital Forensik Dengan Metode NIJ	23
4.2.3 Examination.....	24
4.2.3.1 Extraction	25

4.2.3.2 Analysis Proses Menemukan pesan mencurigakan pada <i>tools Hex editor Neo</i>	27
4.2.3.3 <i>MD5 Hashing</i>	30
4.2.4 <i>Documenting dan Reporting</i>	32
BAB V PENUTUP	34
5.1 Kesimpulan	34
5.2 Saran	34
REFERENSI	35



DAFTAR TABEL

Tabel 2.1. Penelitian Penulis	7
Tabel 3.1. Alat Dan Bahan Penelitian	17
Tabel 4.1. Informasi Media File	26



DAFTAR GAMBAR

Gambar 3. 1 Alur penelitian.....	15
Gamabr 3. 2 Metode <i>National Institute of Justice</i>	17
Gambar 4. 1 ascii to biner [18]	21
Gambar 4. 2 Penyisipan pada file dengan ekstensi .jpg.....	22
Gambar 4. 3 Penyisipan pada file dengan ekstensi .mp3.....	22
Gambar 4. 4 Penyisipan pada file dengan ekstensi .mp4.....	22
Gambar 4. 5 Pembuatan Informasi <i>case</i>	23
Gambar 4. 6 <i>Optional Information</i>	23
Gambar 4. 7 <i>Select Type of data</i>	24
Gambar 4. 8 Tampilan hasil Akuisisi.....	24
Gambar 4. 9 Tab Tipe Data.....	25
Gambar 4. 10 Tipe File	25
Gambar 4. 11 Hasil Akuisisi	25
Gambar 4. 12 <i>Extract File</i>	26
Gambar 4. 13 Hasil dari Extract File	27
Gambar 4. 14 Menemukan Pesan mencurigakan JPG	27
Gambar 4. 15 <i>View</i>	28
Gambar 4. 16 Pesan Mencurigakan C0D3.....	28
Gambar 4. 17 Menemukan Pesan mencurigakan MP3.....	28
Gambar 4. 18 view pesan mp3.....	29
Gambar 4. 19 Pesan Mencurigakan m'sCoWURusIA	29
Gambar 4. 20 Menemukan Pesan mencurigakan MP4.....	29
Gambar 4. 21 View pada file mp4.....	30
Gambar 4. 22 Pesan Mencurigakan Nam3Pesan Mencurigakan Nam3	30
Gambar 4. 23 Proses awal <i>Hashing</i>	31
Gambar 4. 24 Proses <i>Hashing</i> pada file jpg.....	31
Gambar 4. 25 Proses <i>Hashing</i> pada file mp3.....	32
Gambar 4. 26 Proses <i>Hashing</i> pada file mp4.....	32

INTISARI

Perkembangan digital forensik saat ini semakin penting dengan beberapa insiden keamanan informasi yang rentan dan terus – menerus bertambah. Pada dasarnya perubahan yang berkembang pesat ini terjadi dibidang perangkat lunak (*Software*) dan perangkat keras (*Hardware*). Akuisis dilakukan untuk tahap yang penting dalam proses analisis namun tetap merujuk pada metode yang ada. Metode yang digunakan dalam melakukan penelitian untuk menangani bentuk kejahatan dengan barang bukti media *Flashdrive* adalah metode national institute of justice (NIJ).

Penelitian ini bertujuan untuk menemukan barang bukti digital berupa file media gambar (JPG), audio (MP3), dan video (MP4) terdapat pesan tersembunyi yang disisipkan oleh pelaku menggunakan steganografi end of file. Pelaku melakukan format data pada *flashdrive* untuk menghilangkan barang bukti digital tersebut.

Proses penelitian ini menggunakan tools forensik Autopsy dan Hex Neo Editor serta *NIJ framework* sebagai simulasi penyelidikan pada kasus kriminal Steganografi End of file. Hasil dari penelitian ini berupa data recovery pada *flashdrive* yang dilakukan proses *Acquisition* dan *Examination* untuk menemukan integritas file media gambar (JPG), audio (MP3), dan video (MP4). Data yang direcovery pada *flashdrive* dapat dijadikan sebagai barang bukti yang terjaga integritasnya pada proses persidangan kasus *cybercrime*.

Kata kunci : *NIJ*, Digital Foresik, Autopsy, steganografi, *end of file*

ABSTRACT

The development of Digital Forensic is currently increasingly important with several information security incidents that are vulnerable and constantly increasing. Basically, this rapidly growing change occurs in the field of software (Software) and hardware (Hardware). Acquisition is carried out for an important stage in the analysis process but still refers to the existing method. The method used in conducting research to deal with forms of crime with Flashdrive media evidence is the national institute of justice (NIJ) method.

This study aims to find digital evidence in the form of image media files (JPG), audio (MP3), and video (MP4) containing hidden messages inserted by the perpetrator using end of file steganography. The perpetrator formatted the data on the flash drive to destroy the digital evidence.

This research process uses Autopsy forensic tools and Hex Neo Editor as well as the NIJ framework as a simulation of investigations into End of file Steganography criminal cases. The results of this study are in the form of data recovery on a flash drive which is carried out by the Acquisition and Examination processes to find the integrity of image (JPG), audio (MP3), and video (MP4) media files. Data recovered on a flash drive can be used as evidence that proves its integrity in cybercrime cases.

Keyword: NIJ, Forensic Digital, Autopsy, End of file, Steganography