

**METODE STATIC FORENSIC PADA USB MASS STORAGE
MENGUNAKAN FORENSIC TOOLKIT IMAGER**

SKRIPSI



disusun oleh

Pradipta Mahardika Sulaksono

18.83.0191

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

**METODE STATIC FORENSIC PADA USB MASS STORAGE
MENGUNAKAN FORENSIC TOOLKIT IMAGER**

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer Pada
Jenjang Program Sarjana – Program Studi Teknik Komputer



disusun oleh

Pradipta Mahardika Sulaksono

18.83.0191

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

HALAMAN PERSETUJUAN

SKRIPSI

**METODE STATIC FORENSIC PADA USB MASS STORAGE
MENGUNAKAN FORENSIC TOOLKIT IMAGER**

yang dipersiapkan dan disusun oleh

Pradipta Mahardika Sulaksono

18.83.0191

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 9 Oktober 2021

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng

NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

METODE STATIC FORENSIC PADA USB MASS STORAGE MENGUNAKAN FORENSIC TOOLKIT IMAGER

yang dipersiapkan dan disusun oleh

Pradipta Mahardika Sulaksono

18.83.0191

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Maret 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ria Andriani, M.Kom.
NIK. 19030458

SubektiIngsih, M.Kom.
NIK. 190302413

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

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 April 2022

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Pradipta Mahardika Sulaksana
NIM : 18.83.0191

Menyatakan bahwa Skripsi dengan judul berikut :

Metode Static Forensic Pada USB Mass Storage Menggunakan Forensic ToolKit Imager

Dosen Pembimbing : Bano 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, 24 Maret 2022

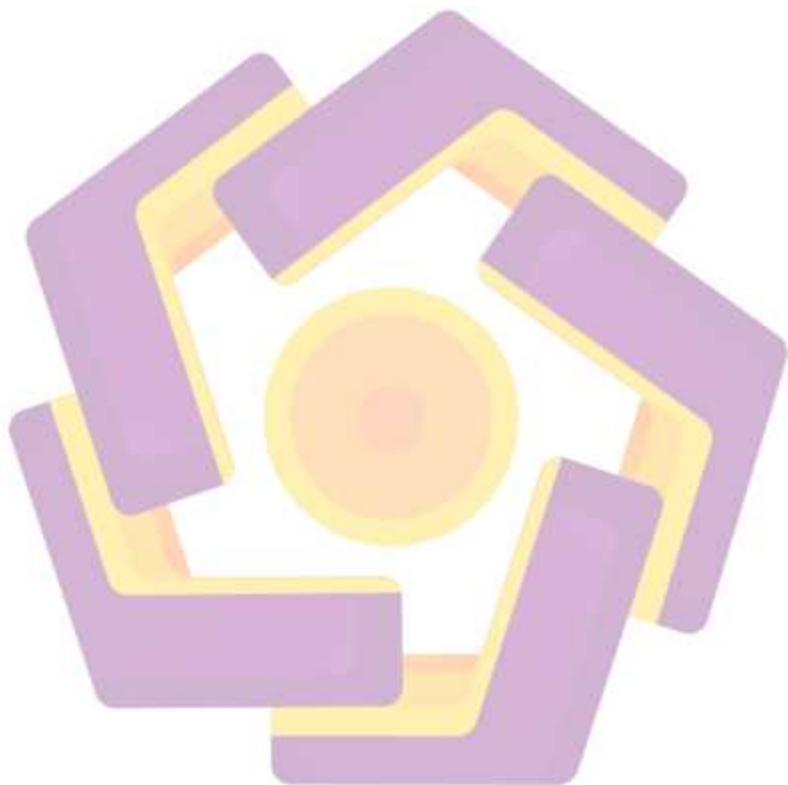
Yang Menyatakan,



Pradipta Mahardika Sulaksana

HALAMAN MOTTO

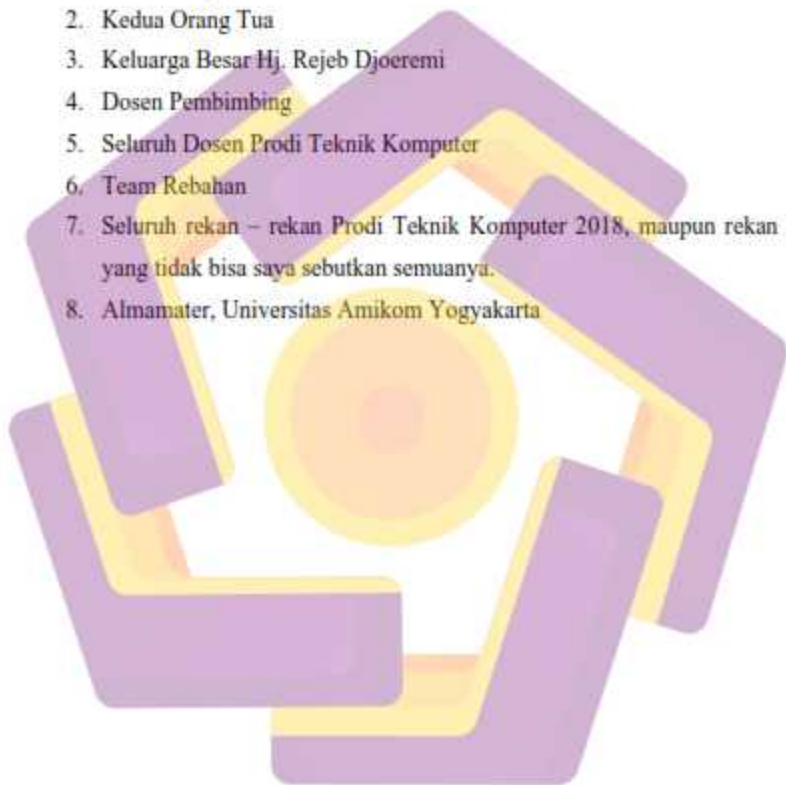
Ngluruk tanpo bolo, menang tanpo ngasorake, sekti tanpo aji, sugih tanpo bondo.



HALAMAN PERSEMBAHAN

Dengan mengucapkan rasa syukur kehadiran Tuhan Yang Maha Esa, peneliti mempersembahkan karya tulis ini kepada :

1. Tuhan Yang Maha Esa
2. Kedua Orang Tua
3. Keluarga Besar Hj. Rejeb Djoeremi
4. Dosen Pembimbing
5. Seluruh Dosen Prodi Teknik Komputer
6. Team Rebahan
7. Seluruh rekan – rekan Prodi Teknik Komputer 2018, maupun rekan lain yang tidak bisa saya sebutkan semuanya.
8. Almamater, Universitas Amikom Yogyakarta



KATA PENGANTAR

Puji syukur dipanjatkan kehadiran Allah SWT dan mengharap ridho yang telah melimpahkan rahmatnya sehingga penulis dapat menyelesaikan penelitian dengan judul “Metode Static Forensic Pada USB Mass Storage Menggunakan Forensic Toolkit Imager”. Penelitian ini disusun sebagai salah satu syarat untuk meraih gelar Sarjana di Program Studi S1 Teknik Komputer Universitas Amikom Yogyakarta. Shalawat serta salam senantiasa disampaikan kepada junjungan kita Nabi Muhammad SAW, Mudah-mudahan kita semua mendapat safaat nya, Aamiin.

Yogyakarta, 24 Maret 2022

Penulis

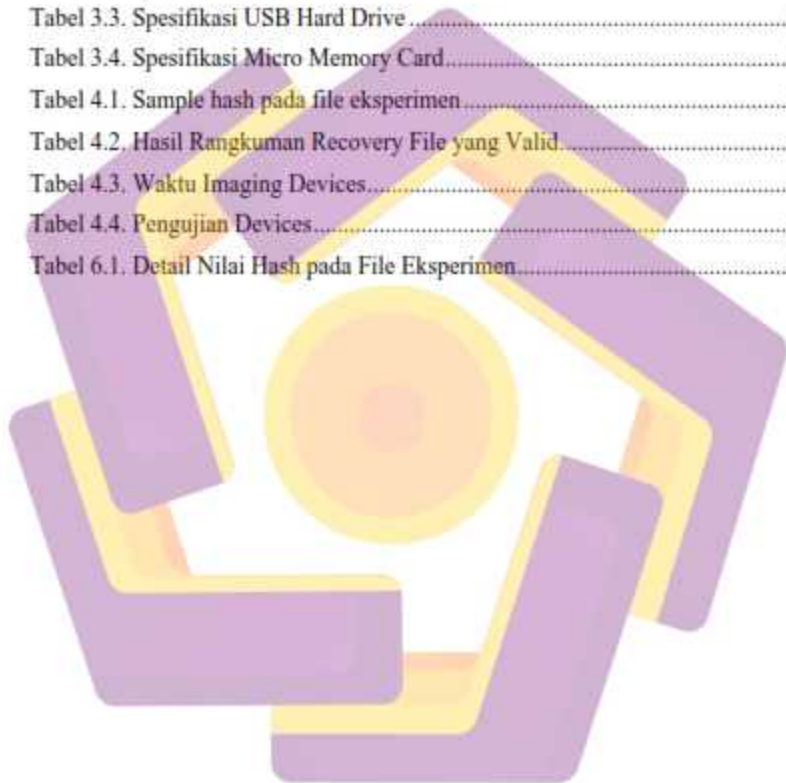
DAFTAR ISI

HALAMAN JUDUL.....	II
HALAMAN PERSETUJUAN.....	III
HALAMAN PENGESAHAN.....	IV
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	V
HALAMAN MOTTO.....	VI
HALAMAN PERSEMBAHAN.....	VII
KATA PENGANTAR.....	VIII
DAFTAR ISI.....	IX
DAFTAR TABEL.....	XI
DAFTAR GAMBAR.....	XII
INTISARI.....	XIV
<i>ABSTRACT</i>	XV
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 METODE PENELITIAN.....	4
1.7 SISTEMATIKA PENULISAN.....	6
BAB II LANDASAN TEORI.....	7
2.1 KAJIAN PUSTAKA.....	7
2.2 DIGITAL FORENSICS.....	10
2.3 COMPUTER FORENSICS.....	12
2.4 DIGITAL EVIDENCE.....	13
2.5 DATA RECOVERY.....	14
2.6 NIST FRAMEWORK.....	14
2.7 USB MASS STORAGE.....	15
2.8 USB FLASH DRIVE.....	16
2.9 HARD DISK DRIVE.....	16
2.10 MICRO MEMORY CARD.....	17

2.11	USB WRITE BLOCKER	18
2.12	ACCESS DATA - FTK IMAGER	18
BAB III METODE PENELITIAN.....		19
3.1	ALAT DAN BAHAN PENELITIAN.....	19
3.2	ALUR PENELITIAN.....	21
BAB IV HASIL DAN PEMBAHASAN		26
4.1	INSTALASI FTK IMAGER	26
4.1.2	DOWNLOAD FTK IMAGER.....	26
4.1.3	PROSES INSTALASI FTK IMAGER	26
4.2	INSTALASI HASH TAB	29
4.2.2	DOWNLOAD HASH TAB.....	29
4.2.3	PROSES INSTALASI HASH TAB	29
4.3	PELAKSANAAN SKENARIO.....	32
4.4	TAHAP KOLEKSI.....	33
4.4.2	DEVICE 1 - USB FLASH DRIVE.....	34
4.4.3	DEVICE 2 - USB HARD DRIVE.....	35
4.4.4	DEVICE 3 - MICRO MEMORY CARD.....	36
4.5	TAHAP EKSAMINASI.....	37
4.5.2	DEVICE 1 - USB FLASH DRIVE.....	38
4.5.3	DEVICE 2 - USB HARD DRIVE.....	38
4.5.4	DEVICE 3 - MICRO MEMORY CARD.....	39
4.6	TAHAP ANALISIS.....	40
4.6.2	DEVICE 1 - USB FLASH DRIVE.....	40
4.6.3	DEVICE 2 - USB HARD DRIVE.....	41
4.6.4	DEVICE 3 - MICRO MEMORY CARD.....	42
4.7	PELAPORAN.....	44
BAB V PENUTUP.....		50
5.1	KESIMPULAN.....	50
5.2	SARAN.....	50
DAFTAR PUSTAKA		51
LAMPIRAN.....		55

DAFTAR TABEL

Tabel 2.1. Daftar Penelitian Terkait.....	9
Tabel 3.1. Spesifikasi Workstation	19
Tabel 3.2. Spesifikasi USB Flash Drive.....	19
Tabel 3.3. Spesifikasi USB Hard Drive.....	20
Tabel 3.4. Spesifikasi Micro Memory Card.....	20
Tabel 4.1. Sample hash pada file eksperimen.....	32
Tabel 4.2. Hasil Rangkuman Recovery File yang Valid.....	44
Tabel 4.3. Waktu Imaging Devices.....	47
Tabel 4.4. Pengujian Devices.....	49
Tabel 6.1. Detail Nilai Hash pada File Eksperimen.....	55



DAFTAR GAMBAR

Gambar 2.1. NIST Framework.....	14
Gambar 2.2. USB Flash Drive	16
Gambar 2.3. Hard Disk Drive	17
Gambar 2.4. Micro Memory Card	18
Gambar 3.1 Alur Penelitian.....	21
Gambar 3.2 Flowchart Tahap Skenario	21
Gambar 3.3 Flowchart Tahap Koleksi	22
Gambar 3.4 Flowchart Tahap Eksaminasi	23
Gambar 3.5 Flowchart Tahap Analisis	24
Gambar 4.1 Instalasi FTK Imager 1.....	26
Gambar 4.2 Instalasi FTK Imager 2.....	27
Gambar 4.3 Instalasi FTK Imager 3.....	27
Gambar 4.4 Instalasi FTK Imager 4.....	28
Gambar 4.5 Menu pada FTK Imager	28
Gambar 4.6 Instalasi HashTab 1	29
Gambar 4.7. Instalasi HashTab 2	30
Gambar 4.8. Instalasi HashTab 3	30
Gambar 4.9. Instalasi HashTab 4	31
Gambar 4.10. File Hashes pada HashTab	32
Gambar 4.11. Evidence Bag Device 1	33
Gambar 4.12. Evidence Bag Device 2	34
Gambar 4.13. Evidence Bag Device 3	34
Gambar 4.14. Labeling USB Flash Drive	35
Gambar 4.15. Hasil Verifikasi Image Device 1	35
Gambar 4.16. Labeling USB Hard Drive.....	36
Gambar 4.17. Proses Labeling MMC	36
Gambar 4.18. Proses Imaging MMC	37
Gambar 4.19. Hasil Verifikasi Image Device 3	37
Gambar 4.20. Evidence Image USB Flash Drive	38

Gambar 4.21. Folder Eksperimen dengan Berisi Files	38
Gambar 4.22. Evidence Image USB Hard Drive	39
Gambar 4.23. Folder pada Evidence Image MMC	39
Gambar 4.24. File pada Evidence Image MMC	40
Gambar 4.25. Metadata pada File USB Flash Drive.....	40
Gambar 4.26. Komparasi Hash pada file di USB Flash Drive	41
Gambar 4.27. Metadata Pada file di USB Hard Drive	42
Gambar 4.28. Komparasi Hash pada File di USB Hard Drive	42
Gambar 4.29. Metadata pada file MMC	43
Gambar 4.30. Komparasi Hash pada file di MMC	43
Gambar 4.31. <i>Chain Of Custody</i> Device 1.....	45
Gambar 4.32. <i>Chain Of Custody</i> Device 2.....	46
Gambar 4.33. <i>Chain Of Custody</i> Device 3.....	46
Gambar 4.34. Perhitungan Akurasi Device 1.....	47
Gambar 4.35. Perhitungan Akurasi Device 2.....	47
Gambar 4.36. Perhitungan Akurasi Device 3.....	47
Gambar 4.37. Grafik Imaging Devices	48
Gambar 4.38. Grafik Recovery Bukti Digital.....	48

INTISARI

Peningkatan penggunaan perangkat penyimpanan USB cenderung massif & eksponensial disebabkan berbagai aspek, salah satunya ukuran dan harga perangkat penyimpanan USB yang terjangkau. Saat ini kualitas penanganan *cybercrime* di Indonesia masih minim, dimulai dengan masalah pengumpulan barang bukti cenderung tidak lengkap, kesalahan saat proses akuisisi barang bukti hingga yang paling parah hilang serta rusaknya barang bukti tersebut.

Static Forensics merupakan salah satu jenis metode dari forensik digital yang memperoleh bukti digital dengan melakukan ekstraksi serta analisis setelah insiden terjadi, ataupun setelah sistem komputer dimatikan (*post-incident*). NIST Framework merupakan sebuah acuan proses pengambilan serta pengolahan bukti digital, yang dikembangkan oleh Lembaga National Institute of Standards and Technology.

Hasil yang diperoleh dari analisis recovery bukti digital metode static forensics dipadu dengan framework NIST dapat diterapkan dengan baik dan optimal. Dilakukan 20 kali pengujian, dengan hasil akurasi recovery bukti digital mencapai 100% pada ketiga devices.

Kata Kunci : Perangkat Penyimpanan USB, Static Forensics, NIST Framework

ABSTRACT

The increase in the use of USB Mass Storage tends to be massive & exponential due to various aspects, one of which is the size and affordable price of USB storage devices. Currently, the quality of handling cybercrime in Indonesia is still minimal, starting with the problem of collecting evidence that tends to be incomplete, errors during the process of acquiring evidence to the most severe loss and damage to the evidence.

Static Forensics is one type of digital forensics method that obtains digital evidence by extracting and analyzing it after the incident has occurred, or after the computer system has been turned off (post-incident). The NIST Framework is a reference for digital evidence retrieval and processing, which was developed by the National Institute of Standards and Technology.

The results obtained from the analysis of digital evidence recovery using static forensics methods combined with the NIST framework can be applied properly and optimally. The test was carried out 20 times, with the results of the digital evidence recovery accuracy reaching 100% on the three devices.

Keyword: USB Mass Storage, Static Forensics, NIST Framework



