

**ANALISIS PERBANDINGAN TOOLS FORENSIK UNTUK
RECOVERY FILE DIGITAL MENGGUNAKAN
METODE NIST**

SKRIPSI

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



disusun oleh

MUHAMAD GUNTUR

18.83.0253

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2022

**ANALISIS PERBANDINGAN TOOLS FORENSIK UNTUK
RECOVERY FILE DIGITAL MENGGUNAKAN
METODE NIST**

SKRIPSI

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



disusun oleh

MUHAMAD GUNTUR

18.83.0253

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2022

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS PERBANDINGAN TOOLS FORENSIK UNTUK
RECOVERY FILE DIGITAL MENGGUNAKAN
METODE NIST**

yang disusun dan diajukan oleh

Muhamad Guntur

18.83.0253

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Oktober 2022

Dosen Pembimbing,

Melwin Syafrizal, S.Kom., M.Eng.

NIK. 190302105

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS PERBANDINGAN TOOLS FORENSIK UNTUK
RECOVERY FILE DIGITAL MENGGUNAKAN
METODE NIST

yang disusun dan diajukan oleh

Muhamad Guntur

18.83.0253

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 November 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Senie Destya, M.Kom.
NIK. 190302312

Muhammad Kopravi, S.Kom., M.Eng.
NIK. 190302454

Rini Indrayani, S.T., M.Eng.
NIK. 190302417

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 November 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 : **Muhamad Guntur**
NIM : **18.83.0253**

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Perbandingan Tools Forensik Untuk Recovery File Digital Menggunakan Metode NIST

Dosen Pembimbing : **Melwin Syafrizal, S.Kom., 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 November 2022

Yang Menyatakan,



Muhamad Guntur

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang mendalam, dengan telah diselesaikannya skripsi ini penulis mempersembahkannya kepada:

1. Ibu, bapak, dan adik yang tidak pernah berhenti mendoakan, memberikan dukungan serta motivasi.
2. Bapak Melwin Syafrizal, S.Kom., M.Eng. selaku Dosen Pembimbing yang senantiasa memberikan arahan dan bimbingan dalam penyelesaian skripsi ini.
3. Keluargaku dan saudaraku yang banyak memberikan bantuan ide maupun semangat.
4. Teman-teman S1 Teknik Komputer angkatan 2018.
5. Semua pihak yang tidak bisa saya sebutkan satu persatu yang telah membantu menyelesaikan skripsi ini.

KATA PENGANTAR

Dengan memanjatkan puja dan puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul “Analisis Perbandingan Tools Forensik Untuk Recovery File Digital Menggunakan Metode NIST”, sebagai salah satu syarat untuk menyelesaikan Program Sarjana (S1) Teknik Komputer Universitas Amikom Yogyakarta.

Penulis menyadari bahwa skripsi ini tidak mungkin terselesaikan tanpa adanya dukungan, bantuan, bimbingan, dan nasehat dari berbagai pihak selama penyusunan skripsi ini. Pada kesempatan ini penulis menyampaikan terima kasih setulus-tulusnya kepada:

1. Ibu, bapak, dan adik yang tidak pernah berhenti mendoakan, memberikan semangat serta dukungan.
2. Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas Amikom Yogyakarta.
5. Bapak Melwin Syafrizal, S.Kom., M.Eng. selaku Dosen Pembimbing yang senantiasa memberikan ide dan arahan dalam penyelesaian skripsi ini.
6. Semua pihak yang tidak bisa saya sebutkan satu persatu yang telah membantu menyelesaikan skripsi ini.

Dalam penulisan skripsi ini masih banyak kekurangan dan kesalahan, karena itu segala kritik dan saran yang membangun akan menyempurnakan penulisan skripsi ini serta bermanfaat bagi penulis dan para pembaca.

Yogyakarta, 22 November 2022

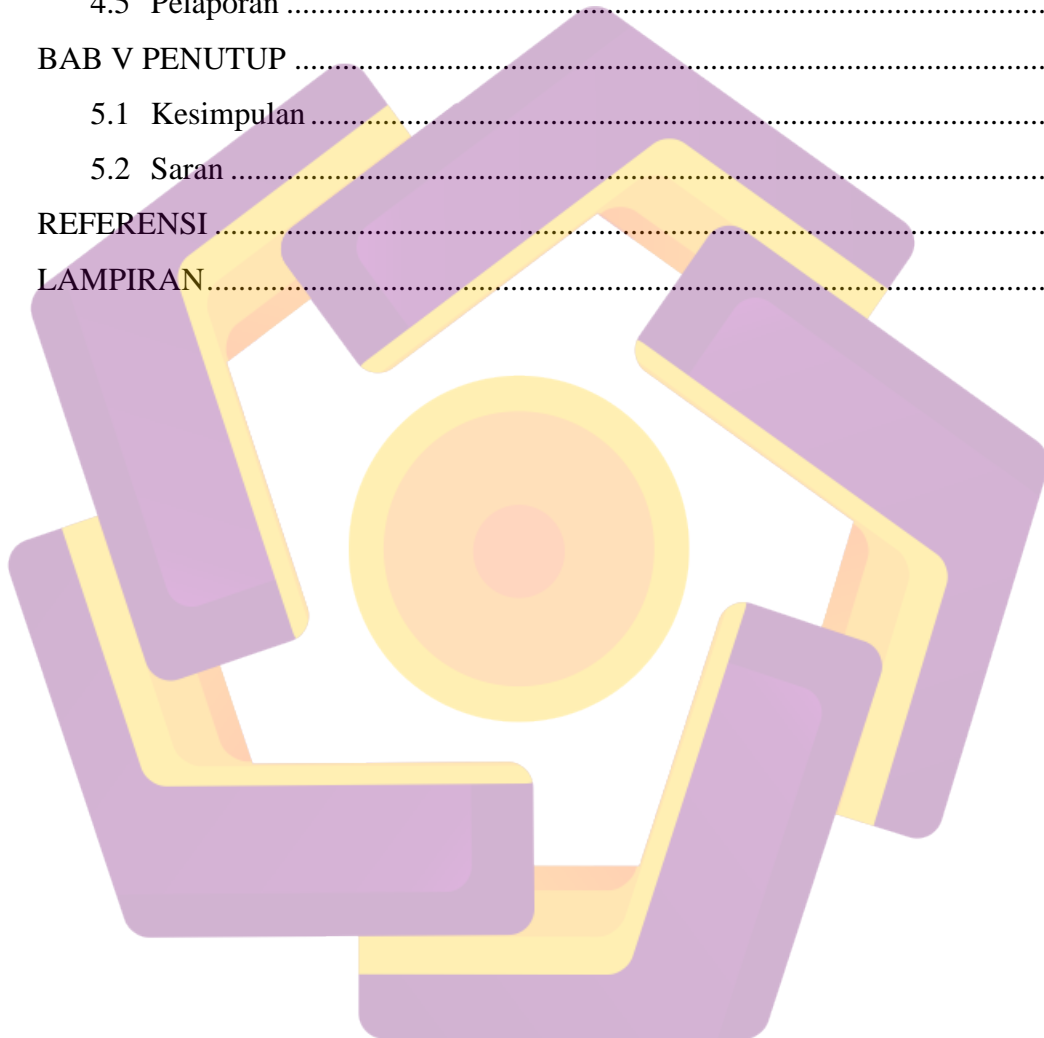
Penulis

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.....	x
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN.....	xiii
DAFTAR LAMBANG DAN SINGKATAN	xiv
INTISARI	xv
ABSTRACT.....	xvi
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	5
2.1 Studi Literatur	5
2.2 Dasar Teori	11
2.2.1 Forensik Digital	11
2.2.2 Data Recovery	11
2.2.3 NIST	12
2.2.4 Sampling.....	13
2.2.5 USB Flash Drive.....	13
2.2.6 Hard Disk Drive.....	13

2.2.7	FTK Imager	14
2.2.8	Autopsy.....	14
2.2.9	Recuva	15
2.2.10	EaseUS Data Recovery Wizard	15
2.2.11	HashTab	16
2.2.12	SAFE Block	16
2.2.13	Microsoft Windows	16
BAB III METODE PENELITIAN		18
3.1	Gambaran Umum Penelitian.....	18
3.2	Analisis Masalah.....	18
3.3	Solusi Permasalahan	18
3.4	Alur Penelitian	19
3.5	Alat dan Bahan Penelitian.....	22
BAB IV HASIL DAN PEMBAHASAN		23
4.1	Skenario	23
4.2	Koleksi.....	25
4.2.1	Flash Drive	27
4.2.2	Hard Disk.....	29
4.3	Eksaminasi	31
4.3.1	Flash Drive	32
4.3.1.1	Autopsy	32
4.3.1.2	Recuva.....	33
4.3.1.3	EaseUS Data Recovery Wizard	34
4.3.2	Hard Disk.....	35
4.3.2.1	Autopsy	35
4.3.2.2	Recuva.....	36
4.3.2.3	EaseUS Data Recovery Wizard	37
4.4	Analisis	38
4.4.1	Flash Drive	38
4.4.1.1	Autopsy	38
4.4.1.2	Recuva.....	39

4.4.1.3 EaseUS Data Recovery Wizard	41
4.4.2 Hard Disk.....	42
4.4.2.1 Autopsy	42
4.4.2.2 Recuva.....	44
4.4.2.3 EaseUS Data Recovery Wizard	45
4.5 Pelaporan	46
BAB V PENUTUP	50
5.1 Kesimpulan	50
5.2 Saran	50
REFERENSI	51
LAMPIRAN.....	54



DAFTAR TABEL

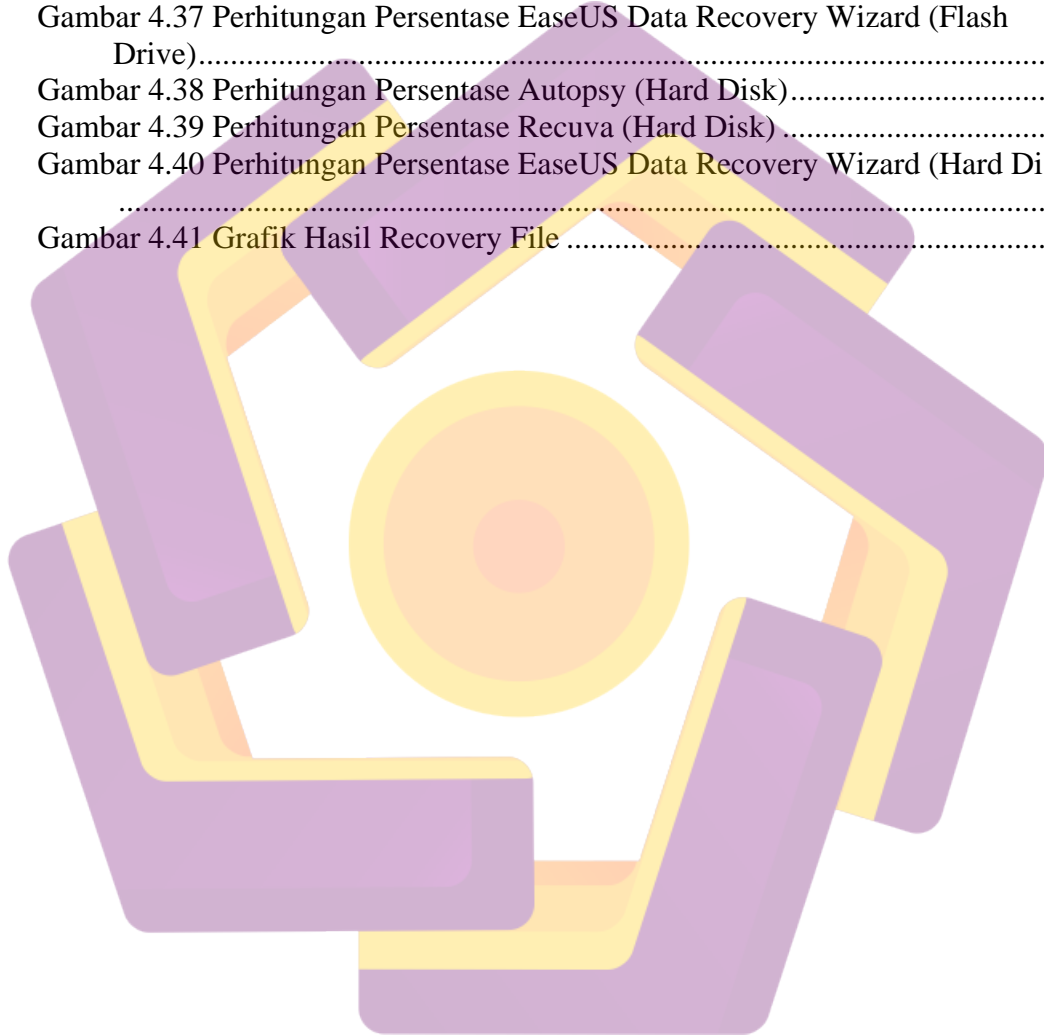
Tabel 2.1 Keaslian Penelitian	7
Tabel 3.1 Hardware.....	22
Tabel 3.2 Software	22
Tabel 4.1 Sampel File dan Hash	23
Tabel 4.2 Validasi Hash Recovery Autopsy (Flash Drive).....	38
Tabel 4.3 Validasi Hash Recovery Recuva (Flash Drive)	40
Tabel 4.4 Validasi Hash Recovery EaseUS Data Recovery Wizard (Flash Drive)	41
Tabel 4.5 Validasi Hash Recovery Autopsy (Hard Disk).....	43
Tabel 4.6 Validasi Hash Recovery Recuva (Hard Disk)	44
Tabel 4.7 Validasi Hash Recovery EaseUS Data Recovery Wizard (Hard Disk).....	46
Tabel 4.8 Hasil Recovery File	47



DAFTAR GAMBAR

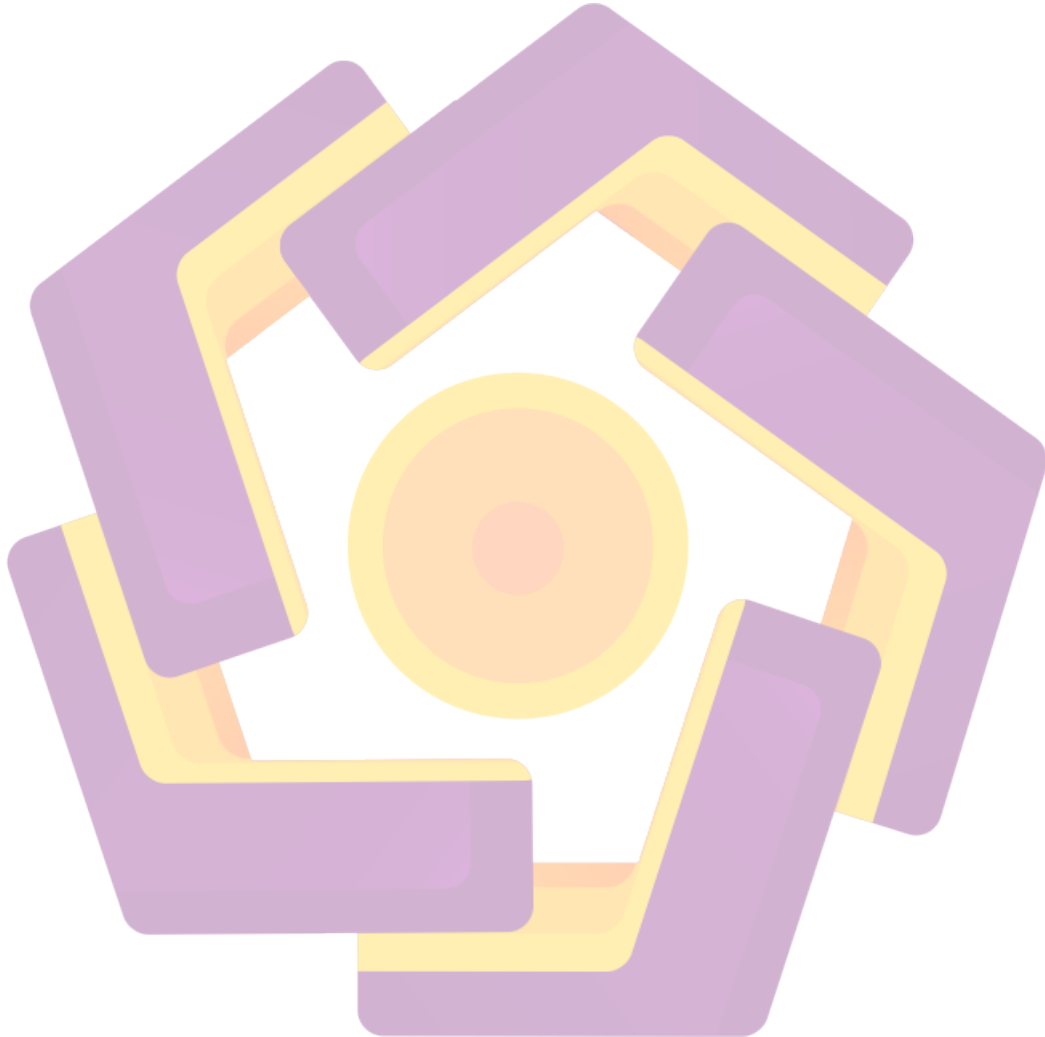
Gambar 1.1 Statistik Kasus Cybercrime di Indonesia Tahun 2021	1
Gambar 2.1 Tahapan Digital Forensic dari NIST	12
Gambar 2.2 USB Flash Drive	13
Gambar 2.3 Hard Disk Drive	14
Gambar 2.4 AccessData	14
Gambar 2.5 Autopsy	15
Gambar 2.6 Recuva	15
Gambar 2.7 EaseUS	16
Gambar 2.8 HashTab	16
Gambar 2.9 ForensicSoft	16
Gambar 2.10 Microsoft	17
Gambar 3.1 Alur Penelitian	19
Gambar 3.2 Flowchart Skenario	20
Gambar 4.1 Sampel pada Flash Drive	24
Gambar 4.2 Sampel pada Hard Disk	24
Gambar 4.3 Quick Format pada Flash Drive	25
Gambar 4.4 Quick Format pada Hard Disk	25
Gambar 4.5 Bukti Flash Drive dan Hard Disk	26
Gambar 4.6 Tampilan SAFE Block	26
Gambar 4.7 Setup SAFE Block	27
Gambar 4.8 Tampilan FTK Imager	27
Gambar 4.9 Write Protection pada Flash Drive	28
Gambar 4.10 Labeling Flash Drive	28
Gambar 4.11 Hasil Verifikasi Image Flash Drive	29
Gambar 4.12 Write Protection pada Hard Disk	29
Gambar 4.13 Labeling Hard Disk	30
Gambar 4.14 Hasil Verifikasi Image Hard Disk	30
Gambar 4.15 Mount Image To Drive (Flash Drive)	31
Gambar 4.16 Mount Image To Drive (Hard Disk)	31
Gambar 4.17 Pencarian File pada Autopsy (Flash Drive)	32
Gambar 4.18 Penemuan File pada Autopsy (Flash Drive)	32
Gambar 4.19 Pencarian File pada Recuva (Flash Drive)	33
Gambar 4.20 Penemuan File pada Recuva (Flash Drive)	33
Gambar 4.21 Pencarian File pada EaseUS Data Recovery Wizard (Flash Drive)	34
Gambar 4.22 Penemuan File pada EaseUS Data Recovery Wizard (Flash Drive)	34
Gambar 4.23 Pencarian File pada Autopsy (Hard Disk)	35
Gambar 4.24 Penemuan File pada Autopsy (Hard Disk)	35
Gambar 4.25 Pencarian File pada Recuva (Hard Disk)	36
Gambar 4.26 Penemuan File pada Recuva (Hard Disk)	36
Gambar 4.27 Pencarian File pada EaseUS Data Recovery Wizard (Hard Disk)	37
Gambar 4.28 Penemuan File pada EaseUS Data Recovery Wizard (Hard Disk)	37
Gambar 4.29 Perbandingan Hash Recovery Autopsy (Flash Drive)	38
Gambar 4.30 Perbandingan Hash Recovery Recuva (Flash Drive)	39

Gambar 4.31 Perbandingan Hash Recovery EaseUS Data Recovery Wizard (Flash Drive).....	41
Gambar 4.32 Perbandingan Hash Recovery Autopsy (Hard Disk)	42
Gambar 4.33 Perbandingan Hash Recovery Recuva (Hard Disk).....	44
Gambar 4.34 Perbandingan Hash Recovery EaseUS Data Recovery Wizard (Hard Disk)	45
Gambar 4.35 Perhitungan Persentase Autopsy (Flash Drive).....	47
Gambar 4.36 Perhitungan Persentase Recuva (Flash Drive)	47
Gambar 4.37 Perhitungan Persentase EaseUS Data Recovery Wizard (Flash Drive).....	48
Gambar 4.38 Perhitungan Persentase Autopsy (Hard Disk).....	48
Gambar 4.39 Perhitungan Persentase Recuva (Hard Disk)	48
Gambar 4.40 Perhitungan Persentase EaseUS Data Recovery Wizard (Hard Disk)	48
Gambar 4.41 Grafik Hasil Recovery File	49

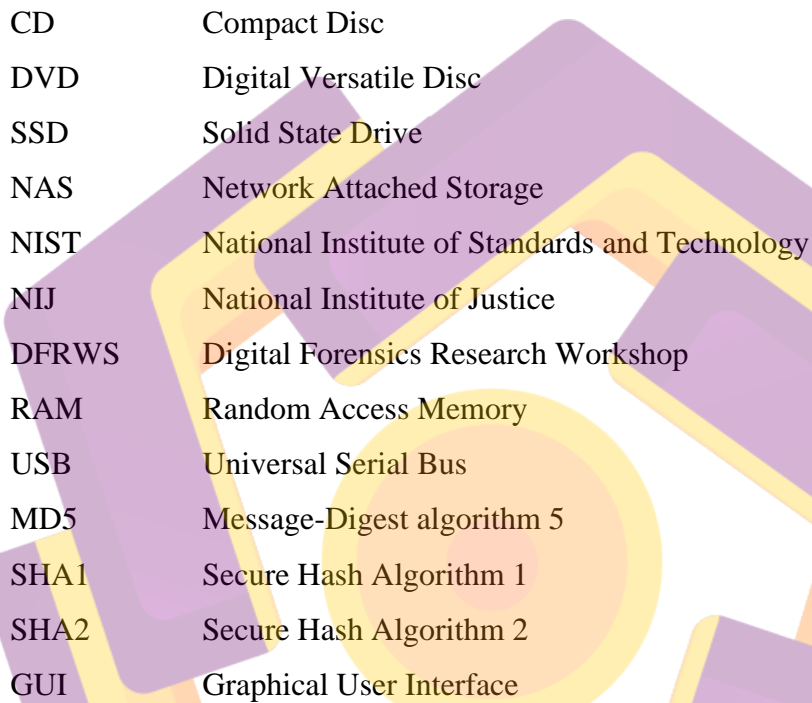


DAFTAR LAMPIRAN

Lampiran 1. Sampel File dan Hash.....	54
---------------------------------------	----



DAFTAR LAMBANG DAN SINGKATAN



<i>P</i>	Persentase keberhasilan
<i>R</i>	Jumlah file yang berhasil di-recovery
<i>S</i>	Jumlah file yang sebenarnya
CD	Compact Disc
DVD	Digital Versatile Disc
SSD	Solid State Drive
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
NIJ	National Institute of Justice
DFRWS	Digital Forensics Research Workshop
RAM	Random Access Memory
USB	Universal Serial Bus
MD5	Message-Digest algorithm 5
SHA1	Secure Hash Algorithm 1
SHA2	Secure Hash Algorithm 2
GUI	Graphical User Interface

INTISARI

Perkembangan teknologi media penyimpanan telah memudahkan para pengguna komputer. Saat ini, banyak pilihan media penyimpanan seperti *flash drive*, *hard disk*, *solid state drive*, *memory card* dan lainnya. Tetapi dari banyaknya pilihan tersebut, media penyimpanan kerap kali ditemukan sebagai barang bukti kejahatan. Berbagai kasus tentang *cybercrime* sering kali menjadi sorotan, mulai dari pengumpulan barang bukti yang cenderung tidak lengkap, kesalahan saat proses akuisisi, bahkan rusaknya barang bukti. Akibat masalah tersebut diperlukan forensik digital. Saat ini banyak *tools* forensik yang dapat digunakan untuk *recovery file* yang telah terhapus maupun terformat. Dari banyaknya *tools* tersebut diperlukan salah satu *tools* yang paling efektif agar proses *recovery file* dapat berjalan maksimal.

Penelitian ini membandingkan *tools* forensik antara Autopsy, Recuva dan EaseUS Data Recovery Wizard pada *flash drive* dan *hard disk* untuk *recovery file*. Penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST) yang terdiri dari 4 tahapan yaitu *collection*, *examination*, *analysis*, dan *reporting*.

Hasilnya penelitian ini dari 30 sampel *file* yang diuji pada *flash drive* dan *hard disk*, *tools* Autopsy mendapatkan persentase keberhasilan 80%, *tools* Recuva mendapatkan persentase keberhasilan 53,33% dan *tools* EaseUS Data Recovery Wizard mendapatkan persentase keberhasilan 50%. Hal ini menunjukkan bahwa *tools* Autopsy lebih efektif untuk *recovery file* dibandingkan Recuva dan EaseUS Data Recovery Wizard.

Kata kunci: *flash drive*, *hard disk*, *cybercrime*, forensik, NIST.

ABSTRACT

The development of storage media technology has made it easier for computer users. Currently, there are many choices of storage media such as flash drives, hard disks, solid state drives, memory cards and others. But of the many choices, storage media is often found as evidence of a crime. Various cases of cybercrime are often in the spotlight, starting from the collection of evidence which tends to be incomplete, errors during the acquisition process, and even damage to evidence. As a result of these problems digital forensics is needed. Currently there are many forensic tools that can be used to recover deleted files. Of the many tools, one of the most effective tools is needed so that the file recovery process can run optimally.

This study compares the forensic tools between Autopsy, Recuva and EaseUS Data Recovery Wizard on flash drives and hard disks for file recovery. This study uses the National Institute of Standards and Technology (NIST) method which consists of 4 stages, namely collection, examination, analysis, and reporting.

The results of this research are from 30 sample files that were tested on flash drives and hard disks, the Autopsy tools get a success percentage of 80%, the Recuva tools get a success percentage of 53,33% and the EaseUS Data Recovery Wizard tools get a success percentage of 50%. This shows that the Autopsy tool is more effective for file recovery than Recuva and EaseUS Data Recovery Wizard.

Keyword: *flash drive, hard disk, cybercrime, forensic, NIST.*