

**ANALISIS PERBANDINGAN PERFORMA TOOLS FORENSIK DALAM  
MELAKUKAN DATA RECOVERY DENGAN KAIDAH SNI ISO/IEC**

**27037:2014**

**SKRIPSI**

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



disusun oleh

**REZA ADI RAMADHAN**

**19.83.0433**

Kepada

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

**2023**

**ANALISIS PERBANDINGAN PERFORMA TOOLS FORENSIK DALAM  
MELAKUKAN DATA RECOVERY DENGAN KAIDAH SNI ISO/IEC**

**27037:2014**

**SKRIPSI**

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



disusun oleh

**REZA ADI RAMADHAN**

**19.83.0433**

Kepada

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

**2023**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**ANALISIS PERBANDINGAN PERFORMA TOOLS FORENSIK DALAM  
MELAKUKAN DATA RECOVERY DENGAN KAIDAH SNI ISO/IEC  
27037:2014**

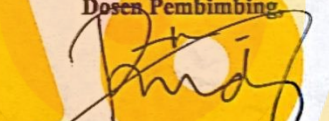
yang disusun dan diajukan oleh

**Reza Adi Ramadhan**

**19.83.0433**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 21 Agustus 2023

Dosen Pembimbing



**M. Rudvanto Arief, S.T., M.T.**  
**NIK. 190302098**

**HALAMAN PENGESAHAN**

**SKRIPSI**

**ANALISIS PERBANDINGAN PERFORMA TOOLS FORENSIK DALAM  
MELAKUKAN DATA RECOVERY DENGAN KAIDAH SNI ISO/IEC  
27037:2014**

yang disusun dan diajukan oleh

**Reza Adi Ramadhan**

**19.83.0433**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 21 Agustus 2023

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**M. Rudyanto Arief, S.T, M.T**  
**NIK. 190302098**

**Jeki Kuswanto, M.Kom**  
**NIK. 190302456**

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

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 21 Agustus 2023

**DEKAN FAKULTAS ILMU KOMPUTER**



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



## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : Reza Adi Ramadhan**  
**NIM : 19.83.0433**

Menyatakan bahwa Skripsi dengan judul berikut:

**Analisis Perbandingan Performa Tools Forensik Dalam Melakukan Data Recovery Dengan Kaidah SNI ISO/IEC 27037:2014**

**Dosen Pembimbing : M. Rudyanto Arief, S.T, M,T**

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.

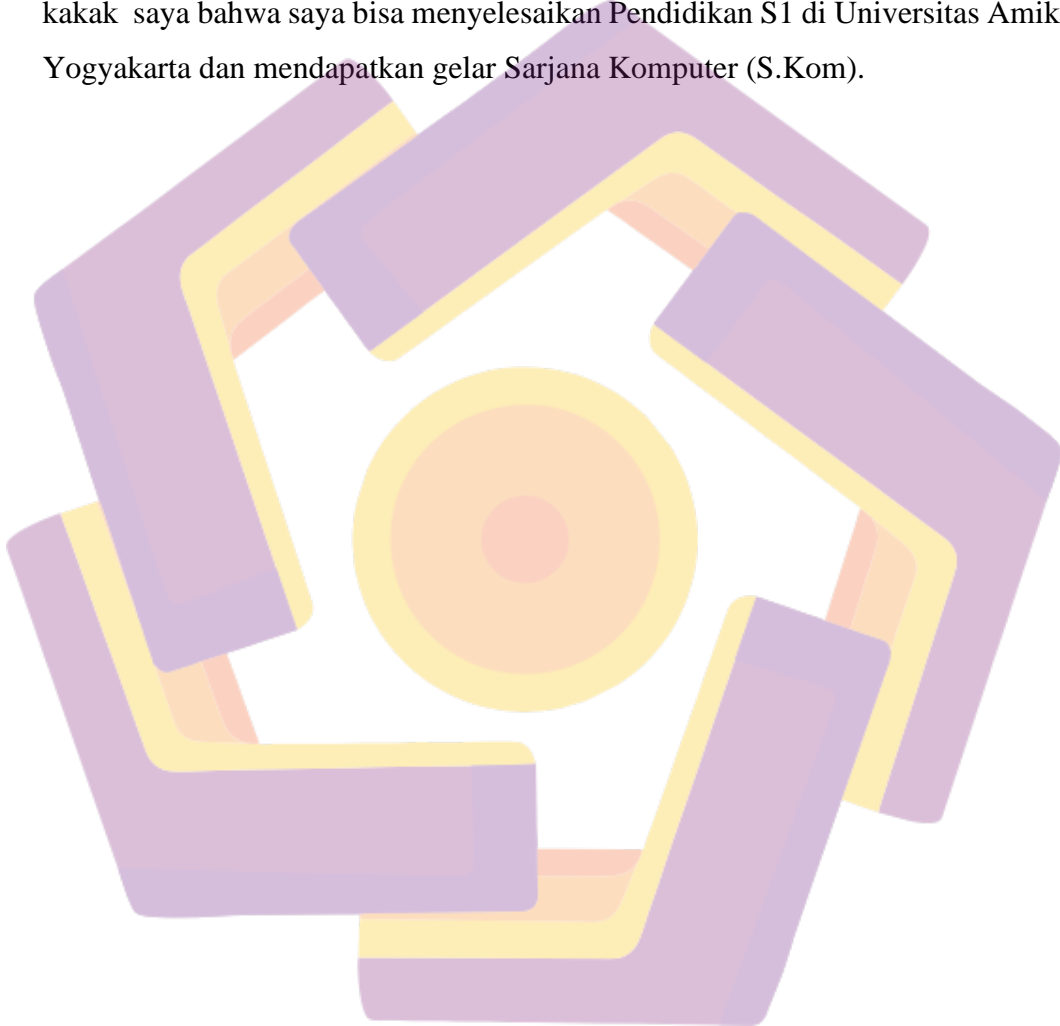
Yogyakarta, 21 Agustus 2023



Reza Adi Ramadhan

## **HALAMAN PERSEMBAHAN**

Saya persembahkan skripsi ini khusus untuk kedua orang tua dan kakak-kakak saya, dimana yang telah membiayai saya selama saya berkuliah. Ini menjadi motivasi bagi saya sendiri untuk membuktikan kepada kedua orang tua dan kakak-kakak saya bahwa saya bisa menyelesaikan Pendidikan S1 di Universitas Amikom Yogyakarta dan mendapatkan gelar Sarjana Komputer (S.Kom).



## KATA PENGANTAR

Puji syukur saya panjatkan kehadirat Allah SWT yang telah memberikan hidayah-Nya sehingga saya bisa menyelesaikan skripsi dengan judul “Analisis Perbandingan Performa Tools Forensik Dalam Melakukan Data Recovery Dengan Kaidah SNI ISO/IEC 27037:2014”.

Penyusunan skripsi ini tidak lepas dari dukungan dari berbagai pihak, oleh karena itu saya ucapkan **terimakasih** kepada mereka diantaranya :

1. Ayah Bambang Supriono (Alm), Ibu Ni Ketut Netri dan keluarga saya yang selalu mendoakan dan memberikan dukungan kepada saya untuk menyelesaikan skripsi ini.
2. Bapak M. Rudyanto Arief, S.T, M.T. selaku dosen pembimbing saya yang telah membimbing dan memberikan banyak masukan untuk saya melakukan penelitian ini hingga skripsi ini bisa terselesaikan.
3. Bapak dan Ibu Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu pengetahuan yang sangat bermanfaat pada saat perkuliahan.
4. Teman-teman saya dari Teknik Komputer 19 yang memberikan saya masukan untuk mengerjakan skripsi

Penulis menyadari masih banyak kekurangan dalam penulisan skripsi ini. Untuk itu, penulis sangat mengharapkan saran yang membangun agar tulisan ini dapat berkembang dan berguna kedepannya.

Yogyakarta, 10 Agustus 2023

Reza Adi Ramadhan

## 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 LAMPIRAN .....	xi
DAFTAR LAMBANG DAN SINGKATAN.....	xii
DAFTAR ISTILAH .....	xiii
INTISARI.....	xiv
ABSTRACT .....	xv
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah .....	3
1.4 Tujuan Penelitian .....	4
1.5 Manfaat Penelitian .....	4
1.6 Sistematika Penulisan .....	5
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>6</b>
2.1 Studi Literatur.....	6
2.2 Dasar Teori Pemulihan Data.....	11
2.3 Landasan Teori .....	11
2.3.1 Digital Forensik .....	11
2.3.2 Komputer Forensik .....	12
2.3.3 Statik Forensik .....	12
2.3.4 Live Forensik .....	12
2.3.5 Data Recovery .....	13



2.3.6	MD5 Hash .....	13
2.3.7	Bukti Digital .....	13
2.3.8	USB Flash Drive .....	13
2.3.9	SNI ISO/IEC 27037:2014 .....	13
<b>BAB III METODE PENELITIAN .....</b>		<b>18</b>
3.1	Objek Penelitian.....	18
3.2	Alur Penelitian .....	18
3.3	Penjelasan Alur Penelitian .....	19
3.3.1	Skenario .....	19
3.3.2	Standar SNI ISO/IEC 27037:2014 .....	20
3.3.3	Analisis perbandingan data recovery .....	21
3.4	Alat dan Bahan.....	22
3.5	Sampel Data Penelitian.....	22
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>		<b>24</b>
4.1	Skenario .....	24
4.2	SNI ISO/IEC 27037:2014.....	26
4.3	Hasil Dan Pembahasan Tools FTK Imager .....	27
4.4	Hasil Dan Pembahasan Tools Autopsy.....	29
4.5	Hasil Dan Pembahasan Tools Disk Drill .....	32
4.6	Hasil Dan Pembahasan Tools Foremost.....	35
4.7	Hasil Dan Pembahasan Tools PhotoRec.....	37
4.8	Hasil Dan Pembahasan Tools WinHex.....	39
4.9	Analisis Perbandingan Data Recovery .....	42
<b>BAB V PENUTUP.....</b>		<b>45</b>
5.1	Kesimpulan .....	45
5.2	Saran .....	45
<b>REFERENSI.....</b>		<b>46</b>
<b>LAMPIRAN .....</b>		<b>48</b>

## DAFTAR TABEL

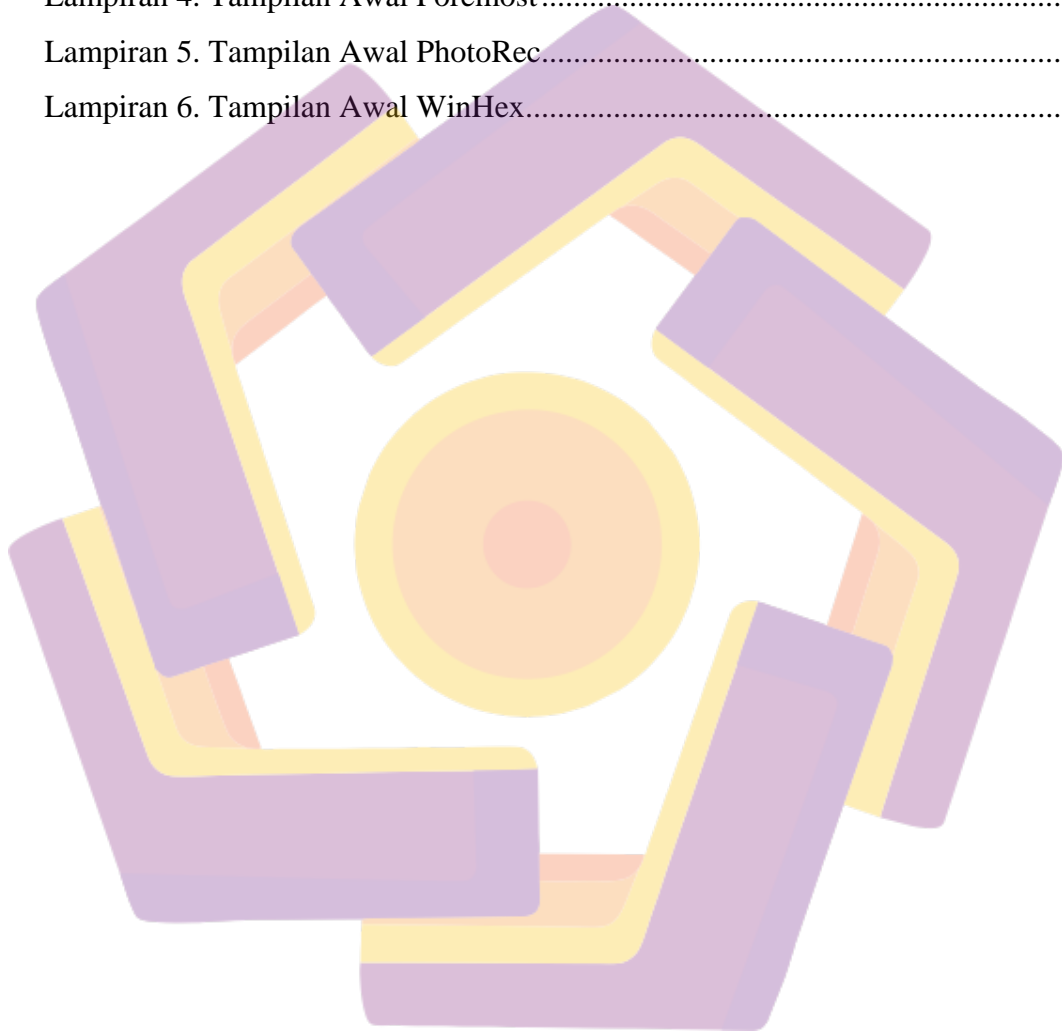
Tabel 2.1 Keaslian Penelitian .....	8
Tabel 3.1 Alat dan Bahan.....	22
Tabel 3.2 Data Sampel Penelitian dengan tipe data.....	22
Tabel 4.1 Data Penelitian dengan tipe data.....	24
Tabel 4.2 Hasil Perbandingan Nilai MD5 dan Penamaan File FTK.....	28
Tabel 4.3 Hasil Perbandingan Nilai MD5 dan Penamaan File Autopsy.....	31
Tabel 4.4 Hasil Perbandingan Nilai MD5 dan Penamaan File Disk Drill .....	33
Tabel 4.5 Hasil Perbandingan Nilai MD5 dan Penamaan File Foremost .....	36
Tabel 4.6 Hasil Perbandingan Nilai MD5 dan Penamaan File PhotoRec.....	38
Tabel 4.7 Hasil Perbandingan Nilai MD5 dan Penamaan File WinHex.....	40
Tabel 4.8 Hasil Perbandingan Data Recovery menggunakan Tools.....	42
Tabel 4.9 Hasil Persentase Kinerja Keseluruhan .....	44

## DAFTAR GAMBAR

Gambar 3.1 Alur Penelitian .....	18
Gambar 3.2 Simulasi Kasus .....	19
Gambar 3.3 Kerangka SNI ISO/IEC 27037:2014 .....	20
Gambar 3.4 Data Sampel Penelitian .....	23
Gambar 4.1 Simulasi Penyelesaian Kasus .....	26
Gambar 4.2 Kerangka SNI ISO/IEC 27037:2014.....	26
Gambar 4.3 Hasil Imaging Menggunakan FTK Imager .....	27
Gambar 4.4 Hasil Bukti Digital Yang Ditemukan Dengan FTK Imager.....	28
Gambar 4.5 Hasil Imaging Menggunakan Autopsy.....	30
Gambar 4.6 Hasil Bukti Digital Yang Ditemukan Autopsy .....	30
Gambar 4.7 Hasil Imaging Menggunakan Disk Drill .....	32
Gambar 4.8 Hasil Bukti Digital Yang Ditemukan Dengan Disk Drill .....	33
Gambar 4.9 Hasil Imaging Menggunakan Foremost.....	35
Gambar 4.10 Hasil Bukti Digital Yang Ditemukan Dengan Foremost .....	35
Gambar 4.11 Hasil Imaging Menggunakan PhotoRec.....	37
Gambar 4.12 Hasil Bukti Digital Yang Ditemukan Dengan PhotoRec.....	38
Gambar 4.13 Hasil Imaging Menggunakan WinHex.....	40
Gambar 4.14 Hasil Bukti Digital Yang Ditemukan Dengan WinHex.....	40

## DAFTAR LAMPIRAN

Lampiran 1. Tampilan Awal FTK Imager .....	48
Lampiran 2. Tampilan Awal Autopsy.....	48
Lampiran 3. Tampilan Awal Disk Drill .....	48
Lampiran 4. Tampilan Awal Foremost.....	49
Lampiran 5. Tampilan Awal PhotoRec.....	49
Lampiran 6. Tampilan Awal WinHex.....	49



## DAFTAR LAMBANG DAN SINGKATAN

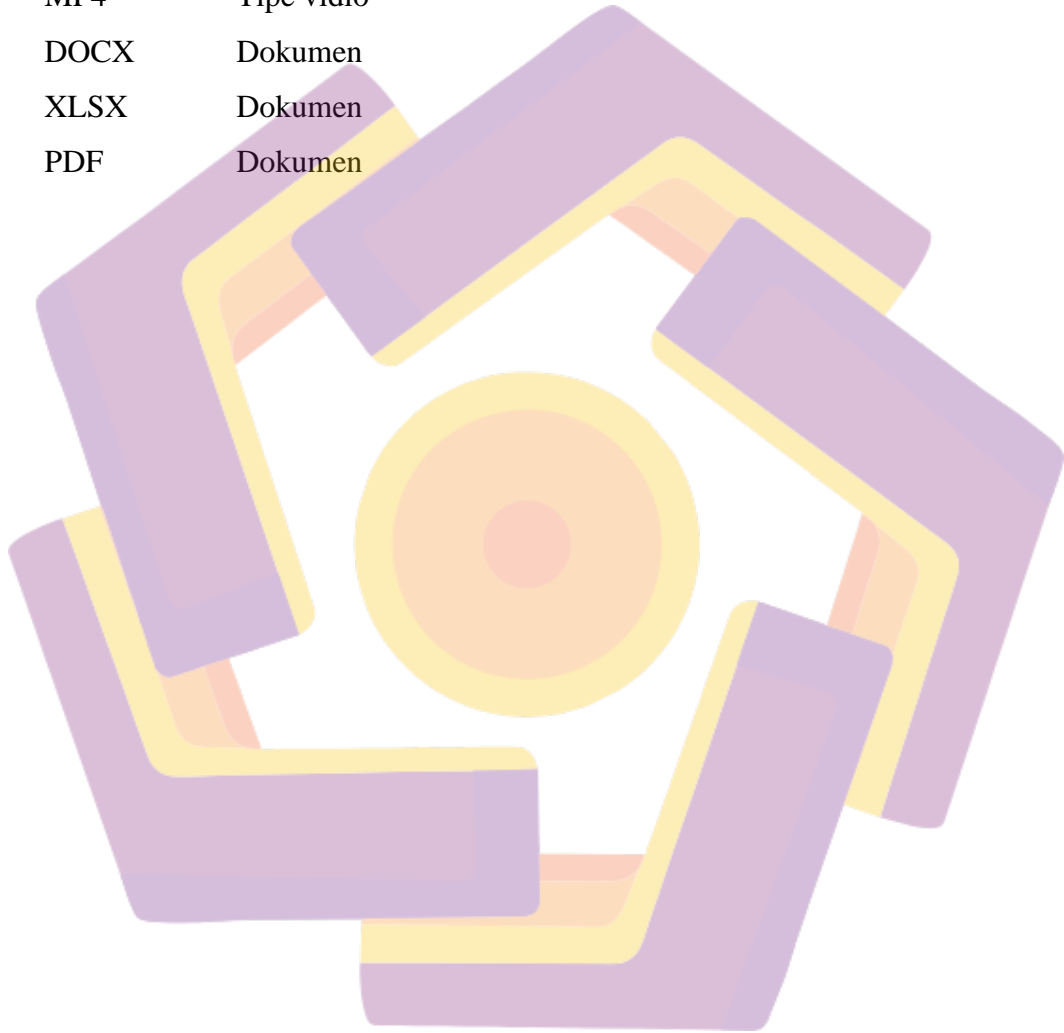
- P      Artinya Persentase (%)
- $\sum dr$     Artinya jumlah data yang di recovery
- $\sum dv$     Artinya jumlah data asli yang valid pada bukti digital





## DAFTAR ISTILAH

JPG	Tipe file gambar
JPEG	Tipe file gambar
PNG	Tipe file gambar
MP4	Tipe vidio
DOCX	Dokumen
XLSX	Dokumen
PDF	Dokumen



## INTISARI

Semakin pesat perkembangan teknologi munculnya sisi negative dari penggunaan teknologi yang mengarah pada tindakan cyber crime. Cyber crime menjadikan komputer sebagai alat untuk meretas jaringan, mencuri informasi, menghapus informasi, menyembunyikan informasi dan merusak informasi. Pelaku cyber crime akan menghapus dan memformat data yang dikumpulkan untuk menghilangkan jejak. Pada ilmu forensik digital kehilangan data bisa dikembalikan dengan recovery menggunakan tools-tools forensik digital. Penelitian ini bertujuan melakukan recovery data pada device flasdisk dengan 6 tools forensik dan menggunakan 3 parameter yaitu kecepatan proses pemulihan, jumlah file yang berhasil dipulihkan, dan kebenaran file yang dipulihkan. Peneliti menggunakan metode statik forensik, yang dimana statik forensik merupakan metode forensik yang digunakan untuk memperoleh bukti digital dengan melakukan ekstraksi serta analisis setelah insiden terjadi. Dengan kaidah SNI ISO/IEC 27037:2014 sebagai acuan melakukan penanganan bukti digital. Hasil penelitian ini menghasilkan Disk Drill memiliki kinerja tertinggi yaitu sebesar 100%, lalu PhotoRec memiliki kinerja sebesar 100% dikarenakan proses recovery lebih lama dari pada Disk Drill, FTK Imager memiliki kinerja sebesar 91,6%, Autopsy memiliki kinerja sebesar 33,3%, WinHex memiliki kinerja sebesar 33,3% dan Foremost memiliki kinerja sebesar 25%.

**Kata kunci:** Cyber Crime, Statik Forensik, ISO/IEC 27037:2014, Tools Forensik

## ABSTRACT

*The rapid development of technology has led to the emergence of the negative side of the use of technology that leads to cyber crime. Cyber crime uses computers as a tool to hack into networks, steal information, delete information, hide information and damage information. Cyber criminals will delete and format the data collected to eliminate traces. In digital forensics, data loss can be restored by recovery using digital forensic tools. This research aims to recover data on a flasdisk device with 6 forensic tools and uses 3 parameters, namely the speed of the recovery process, the number of files successfully recovered, and the correctness of the recovered files. Researchers use the static forensic method, where static forensics is a forensic method used to obtain digital evidence by extracting and analyzing it after an incident occurs. With the rules of SNI ISO / IEC 27037: 2014 as a reference for handling digital evidence. The results of this study indicate that Disk Drill has the highest performance of 100%, then PhotoRec has a performance of 100% because the recovery process is longer than Disk Drill, FTK Imager has a performance of 91.6%, Autopsy has a performance of 33.3%, WinHex has a performance of 33.3% and Foremost has a performance of 25%.*

**Keyword:** *Cyber Crime, Forensic Statics, ISO/IEC 27037:2014, Forensic Tools*