

**ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM  
MENGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS***

**SKRIPSI**



disusun oleh

**Nabilla Fatmah**

**18.83.0193**

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

**ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM  
MENGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS***

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Teknik Komputer



disusun oleh

**Nabilla Fatmah**

**18.83.0193**

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

**PERSETUJUAN**

**SKRIPSI**

**ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM  
MENGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS***

yang dipersiapkan dan disusun oleh

**Nabila Fatmah**

**18.83.0193**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 23 Maret 2022

**Dosen Pembimbing,**

**Rini Indrayani, S.T., M.Eng.**

**NIK. 190302417**

**PENGESAHAN**

**SKRIPSI**

**ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM  
MENGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS***

yang dipersiapkan dan disusun oleh

**Nabilla Fatmah**

**18.83.0193**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 23 Maret 2022

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

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

**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 23 Maret 2022

**DEKAN FAKULTAS ILMU KOMPUTER**

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

## PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 23 Maret 2022



Nabilla Fatmah

NIM. 18.83.0193

## MOTTO

“Hatiku tenang karena mengetahui bahwa apa yang melewatkanku tidak akan pernah menjadi takdirku, dan apa yang ditakdirkan untukku tidak pernah melewatkanku”

(Umar bin Khattab)

“Perbanyak bersyukur, kurangi mengeluh. Buka mata, jembarakan telinga, perluas hati. Sadari kamu ada pada sekarang, bukan kemarin atau besok, nikmati setiap momen dalam hidup, berpetualanglah”

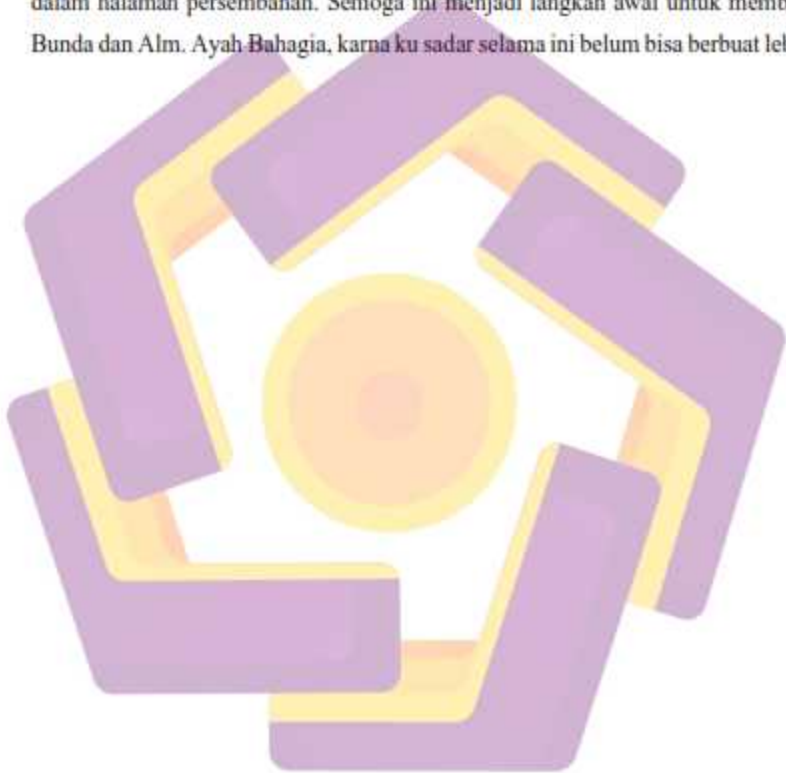
(Ayu Estiningtyas)



## PERSEMBAHAN

Ibunda dan Alm. Ayahanda tercinta,

Sebagai tanda bukti, hormat, dan rasa terimakasih yang tiada terhingga, kupersembahkan karya kecil ini kepada Bunda dan Alm. Ayah yang telah memberikan kasih sayang, dukungan dan cinta kasih yang tiada terhingga dan tidak mungkin dapat ku balas hanya dengan selembar kertas yang bertuliskan kata cinta dalam halaman persembahan. Semoga ini menjadi langkah awal untuk membuat Bunda dan Alm. Ayah Bahagia, karna ku sadar selama ini belum bisa berbuat lebih.



## KATA PENGANTAR

Dengan memanjatkan puji syukur kehadiran ALLAH SWT atas segala nikmat, hidayah dan karunia-Nya. Penulis pada akhirnya dapat menyelesaikan skripsi ini. Penulis meyakini bahwa skripsi ini tidak akan berhasil diselesaikan tanpa pertolongan dan kebaikan Allah. Skripsi ini adalah tugas akhir untuk memenuhi persyaratan akademis guna memperoleh gelar Sarjana Strata Satu (S-1) Ilmu Komputer pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis merasakan kebaikan dan pertolongan Allah melalui banyak pihak yang dengan berbagai cara telah mendukung dan membantu penulis dalam penulisan skripsi ini. Oleh karena itu, penulis menyampaikan ungkapan terima kasih kepada:

1. **Bapak Prof. Dr. Suyanto, MM.** selaku Rektor Universitas Amikom Yogyakarta yang telah memberikan kesempatan kepada penulis untuk menempuh pendidikan di Universitas Amikom Yogyakarta.
2. **Ibu Rini Indrayani, S.T., M.Eng.** selaku dosen pembimbing yang telah memberikan dukungan, arahan dan bimbingan untuk penulis sehingga penulis dapat segera menyelesaikan skripsi ini.
3. **Bapak Hanif Al Fatta, S.Kom., M.Kom.** selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. **Bapak Dony Arlyus, M. Kom.** selaku Ketua Program Studi Teknik Komputer Universitas Yogyakarta yang telah mendukung penulis beserta para mahasiswa prodi Teknik Komputer lainnya selama belajar di Prodi ini.
5. **Para Dosen** di Fakultas Ilmu Komputer Universitas Amikom Yogyakarta, yang telah mengajari, mendidik dan membekali penulis dengan berbagai ilmu pengetahuan selama belajar di Fakultas ini.
6. **Orang tua, adik, sepupu, seluruh keluarga, pacar serta sahabat** yang senantiasa mendukung penulis melalui doa, nasihat dan perhatian.



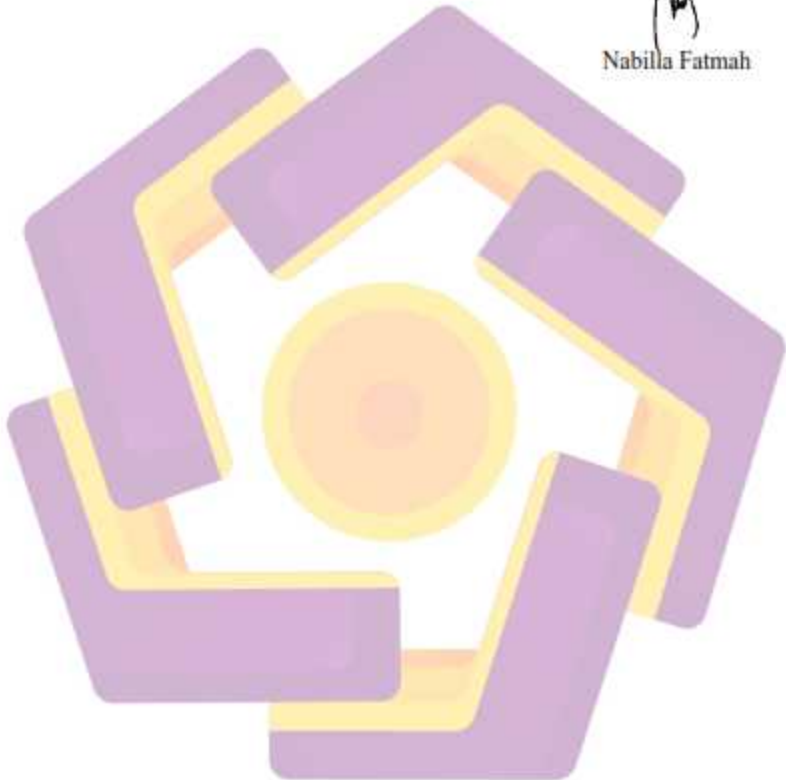
Akhirnya, penulis menyadari bahwa skripsi ini belumlah sempurna. Oleh karena itu, penulis dengan rendah hati menerima segala koreksi, kritik dan saran yang membangun dari pembaca sekalian.

Yogyakarta, 23 Maret 2022

Penulis



Nabilla Fatmah

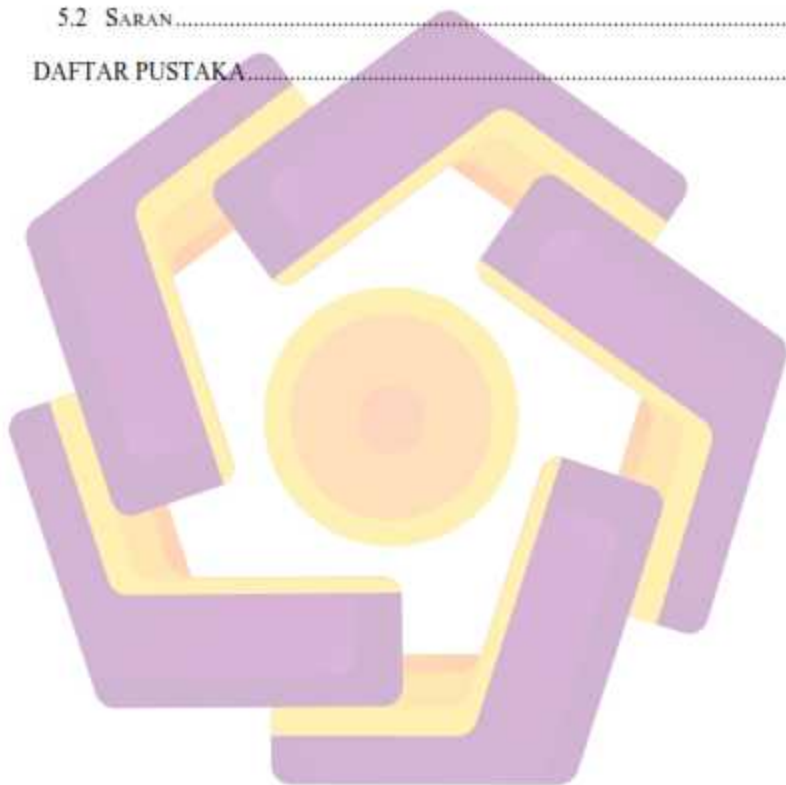


## DAFTAR ISI

JUDUL .....	i
PERSETUJUAN.....	ii
PENGESAHAN .....	iii
PERNYATAAN .....	iv
MOTTO .....	v
PERSEMBAHAN .....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI .....	ix
DAFTAR TABEL .....	xii
DAFTAR GAMBAR.....	xiii
INTISARI .....	xv
<i>ABSTRACT</i> .....	xvi
BAB I PENDAHULUAN .....	1
1.1 LATAR BELAKANG .....	1
1.2 RUMUSAN MASALAH.....	3
1.3 BATASAN MASALAH .....	3
1.4 MAKSUD DAN TUJUAN PENELITIAN.....	4
1.5 MANFAAT PENELITIAN .....	5
1.6 METODE PENELITIAN.....	5
1.6.1 Metode Pengumpulan Data .....	5
1.6.2 Metode Analisis.....	5
1.7 SISTEMATIKA PENULISAN.....	6
BAB II LANDASAN TEORI.....	8
2.1 KAJIAN PUSTAKA .....	8

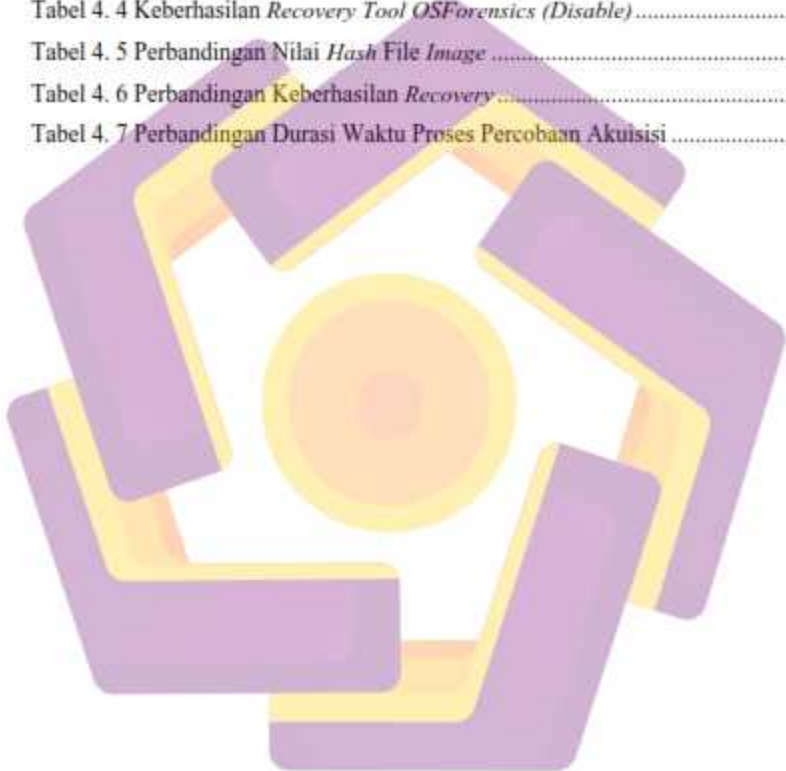
2.2	DASAR TEORI .....	11
2.2.1	Digital Forensik .....	11
2.2.2	Penggelapan Dana .....	12
2.2.3	<i>Solid State Drive (SSD)</i> .....	13
2.2.4	TRIM .....	14
2.2.5	<i>AccessData FTK Imager</i> .....	14
2.2.6	<i>Sleuth kit Autopsy</i> .....	15
2.2.7	<i>OSForensics</i> .....	15
2.2.8	SNI 27037:2014.....	16
2.2.9	<i>Microsoft Windows</i> .....	17
<b>BAB III METODE PENELITIAN .....</b>		<b>18</b>
3.1	ALUR PENELITIAN .....	18
3.2	TINJAUAN PUSTAKA .....	18
3.3	ALAT DAN BAHAN PENELITIAN .....	19
3.4	RANCANGAN SKENARIO .....	20
3.4.1	Skenario Kasus .....	20
3.4.2	Simulasi Kasus .....	21
3.5	AKUISISI DAN <i>RECOVERY</i> .....	23
3.5.1	Akuisisi dan <i>Recovery SSD NVMe TRIM Enable</i> .....	24
3.5.2	Akuisisi dan <i>Recovery SSD NVMe TRIM Disable</i> .....	25
3.6	PEMERIKSAAN DAN ANALISIS.....	26
3.7	KESIMPULAN .....	26
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>28</b>
4.1	PENERAPAN RANCANGAN SKENARIO .....	28
4.3.1.	Penerapan Skenario Kasus .....	28
4.3.2.	Penerapan Simulasi Kasus.....	29
4.2	AKUISISI DAN <i>RECOVERY</i> .....	35
4.4.2	Akuisisi dan <i>Recovery SSD NVMe TRIM Enable</i> .....	37
4.4.2.1	<i>TOOL AUTOPSY (TRIM ENABLE)</i> .....	37
4.4.2.2	<i>TOOL OSFORENSICS (TRIM ENABLE)</i> .....	40
4.4.3	Akuisisi dan <i>Recovery SSD NVMe TRIM Disable</i> .....	43

4.4.3.1	<i>TOOL AUTOPSY (TRIM DISABLE)</i> .....	43
4.4.3.2	<i>TOOL OSFORENSICS (TRIM DISABLE)</i> .....	46
4.5	PEMERIKSAAN DAN ANALISIS.....	49
4.6	KESIMPULAN .....	57
BAB V PENUTUP .....		61
5.1	KESIMPULAN .....	61
5.2	SARAN.....	61
DAFTAR PUSTAKA.....		63



## DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu dan Usulan Penelitian.....	9
Tabel 3. 1 Alat dan Bahan Penelitian .....	19
Tabel 4. 1 Keberhasilan <i>Recovery Tool Autopsy (Enable)</i> .....	39
Tabel 4. 2 Keberhasilan <i>Recovery Tool OSForensics (Enable)</i> .....	42
Tabel 4. 3 Keberhasilan <i>Recovery Tool Autopsy (Disable)</i> .....	46
Tabel 4. 4 Keberhasilan <i>Recovery Tool OSForensics (Disable)</i> .....	49
Tabel 4. 5 Perbandingan Nilai <i>Hash File Image</i> .....	50
Tabel 4. 6 Perbandingan Keberhasilan <i>Recovery</i> .....	59
Tabel 4. 7 Perbandingan Durasi Waktu Proses Percobaan Akuisisi .....	59



## DAFTAR GAMBAR

Gambar 1. 1 Statistik Penggunaan SSD (Sumber : statista.com) .....	2
Gambar 2. 1 SSD NVMe M.2 (Sumber : www.transcend-info.com) .....	13
Gambar 2. 2 Proses Digital Forensik SNI 27037:2014 Bag. 7.1.2.1.1 .....	16
Gambar 3. 1 Alur Penelitian .....	18
Gambar 3. 2 Laptop Lenovo seri Ideapad 320S-14IKB .....	19
Gambar 3. 3 Solid State Drive (SSD) M.2 NVMe .....	20
Gambar 3. 4 Ilustrasi Rancangan Skenario .....	21
Gambar 3. 5 Alur Simulasi Kasus .....	22
Gambar 3. 6 <i>Flowchart</i> Tahapan Fungsi TRIM pada SSD NVMe M.2 .....	23
Gambar 3. 7 <i>Flowchart</i> Akuisisi Perangkat dalam Keadaan Mati .....	24
Gambar 3. 8 Alur Akuisisi pada SSD TRIM <i>Enable</i> .....	25
Gambar 3. 9 Alur Akuisisi pada SSD TRIM <i>Disable</i> .....	26
Gambar 4. 1 Laporan Keuangan Sebagai Barang Bukti .....	28
Gambar 4. 2 File Bukti Transaksi diduga Palsu .....	29
Gambar 4. 3 Perintah Pengecekan Fungsi TRIM <i>enable</i> .....	30
Gambar 4. 4 Perintah TRIM <i>Enable</i> /Aktif .....	31
Gambar 4. 5 Perintah Pengecekan Ulang Fungsi TRIM <i>enable</i> .....	31
Gambar 4. 6 Daftar File yang dihapus Permanen pada Fungsi TRIM <i>Enable</i> .....	32
Gambar 4. 7 Perintah Pengecekan Fungsi TRIM <i>disable</i> .....	33
Gambar 4. 8 Perintah TRIM <i>Disable</i> /Nonaktif .....	34
Gambar 4. 9 Perintah Pengecekan Ulang Fungsi TRIM <i>Disable</i> .....	34
Gambar 4. 10 Daftar File yang dihapus Permanen pada Fungsi TRIM <i>Disable</i> .....	35
Gambar 4. 11 Nilai <i>Hash</i> Hasil <i>Imaging</i> SSD NVMe M.2 TRIM <i>Enable</i> .....	36
Gambar 4. 12 Nilai <i>Hash</i> Hasil <i>Imaging</i> SSD NVMe M.2 TRIM <i>Disable</i> .....	36
Gambar 4. 13 Metadata File <i>Image</i> Hasil Akuisisi <i>Tool Autopsy</i> (TRIM <i>Enable</i> ) .....	38
Gambar 4. 14 <i>Deleted Files</i> pada Hasil Akuisisi SSD TRIM <i>Enable</i> <i>Tool Autopsy</i> .....	38
Gambar 4. 15 Hasil <i>Recovery</i> SSD TRIM <i>Enable</i> <i>Tool Autopsy</i> .....	39

Gambar 4. 16 Metadata File <i>Image</i> Hasil Akuisisi Tool <i>OSForensics</i> (TRIM <i>Enable</i> ) .....	41
Gambar 4. 17 <i>Deleted Files</i> pada Hasil Akuisisi SSD TRIM <i>Enable Tool OSForensics</i> .....	41
Gambar 4. 18 Hasil <i>Recovery</i> SSD TRIM <i>Enable Tool OSForensics</i> .....	42
Gambar 4. 19 Metadata File <i>Image</i> Hasil Akuisisi Tool <i>Autopsy</i> (TRIM <i>Disable</i> ) .....	44
Gambar 4. 20 <i>Deleted Files</i> pada Hasil Akuisisi SSD TRIM <i>Disable Tool Autopsy</i> .....	45
Gambar 4. 21 Hasil <i>Recovery</i> SSD TRIM <i>Disable Tool Autopsy</i> .....	45
Gambar 4. 22 Metadata File <i>Image</i> Hasil Akuisisi Tool <i>OSForensics</i> (TRIM <i>Disable</i> ) .....	47
Gambar 4. 23 <i>Deleted Files</i> pada Hasil Akuisisi SSD TRIM <i>Disable Tool OSForensics</i> .....	48
Gambar 4. 24 Hasil <i>Recovery</i> SSD TRIM <i>Disable Tool OSForensics</i> .....	48
Gambar 4. 25 Perbandingan File Bukti Transaksi 1 .....	51
Gambar 4. 26 Perbandingan File Bukti Transaksi 2 .....	52
Gambar 4. 27 Perbandingan File Bukti Transaksi 3 .....	53
Gambar 4. 28 Perbandingan File Bukti Transaksi 4 .....	54
Gambar 4. 29 Perbandingan File Bukti Transaksi 5 .....	55
Gambar 4. 30 Perbandingan File Bukti Transaksi 6 .....	56
Gambar 4. 31 Perbandingan File Bukti Transaksi 7 .....	56
Gambar 4. 32 Laporan Keuangan yang Sudah Dimanipulasi .....	57

## INTISARI

Kegiatan kejahatan yang melibatkan sebuah perangkat komputer kemungkinan besar akan terekam pada media penyimpanan sistem komputer. Salah satu media penyimpanan utama komputer saat ini selain *harddisk* (HDD) adalah *Solid State Drive* (SSD). Belakangan ini banyak sekali perusahaan yang beralih ke SSD untuk mendapatkan kinerja yang lebih tinggi, ukuran fisik yang baik, dan efisiensi energi. Survei yang dipublikasikan oleh *statista.com* tentang perkembangan *Solid State Drive* diseluruh dunia menunjukkan bahwa penggunaan SSD semakin meningkat setiap tahunnya berbanding terbalik dengan penggunaan HDD yang terus menurun setiap tahunnya. SSD memiliki fungsi TRIM yang merupakan suatu fitur pada SSD yang berhubungan dengan sistem operasi. Fungsi TRIM tersebut memiliki efek negatif pada analisis forensik dan persistensi data setelah dilakukan penghapusan tidak dapat lagi dijamin karena pengontrol penyimpanan SSD memutuskan kapan dan berapa banyak blok yang ditandai untuk dihapus. Metode analisis yang digunakan pada penelitian ini adalah SNI *Acquisition* 27037:2014, yaitu salah satu tahapan dari SNI 27037:2014 yang memiliki beberapa proses yang perlu dilakukan seperti menyelidiki aspek keamanan barang bukti, menentukan model akuisisi, melakukan akuisisi dan meninjau hasil akuisisi.

Fokus dari penelitian ini adalah untuk melakukan percobaan akuisisi dan *recovery* dengan tool *Autopsy* dan tool *OSForensics* pada SSD NVme M.2 fungsi TRIM *enable* dan *disable*. Proses investigasi diawali dengan melakukan *imaging* menggunakan tool *AccessData FTK Imager* dengan fungsi TRIM *enable* dan *disable* yang diatur menggunakan *command prompt* yang sudah tersedia pada sistem operasi *Windows 10 Pro*, kemudian dilakukan penghapusan permanen (*SHIFT+DELETE*) file target yang akan menjadi objek *recovery*, kemudian dilakukan akuisisi file *image* SSD dan dilanjutkan dengan *recovery* data menggunakan tool *Autopsy* dan tool *OSForensics*.

Hasil dari proses percobaan akuisisi dan *recovery* menunjukkan bahwa tool *OSForensics* memiliki durasi waktu proses akuisisi yang lebih cepat, yaitu 228 menit dengan TRIM *enable* dan 231 menit pada TRIM *disable* sedangkan pada tool *Autopsy* 323 menit pada TRIM *enable* dan 334 menit pada TRIM *disable*. Namun pada proses *recovery*, tool *Autopsy* menunjukkan fitur yang sangat memudahkan penggunaannya yaitu bisa melakukan *recovery* file secara kolektif, sedangkan pada tool *OSForensics* versi Trial harus melakukan *recovery* file satu-persatu secara manual. Persentase tingkat keberhasilan tool *Autopsy* dalam melakukan *recovery* pada *Solid State Drive* (SSD) NVMe M.2 dengan fungsi TRIM *enable* sebesar 0% sedangkan dengan fungsi TRIM *disable* 100%. Hasil yang sama juga didapatkan oleh tool *OSForensics* dimana *recovery* yang dilakukan pada *Solid State Drive* (SSD) NVMe M.2 dengan fungsi TRIM *enable* sebesar 0% sedangkan dengan fungsi TRIM *disable* 100%.

**Kata Kunci:** *Autopsy, OSForensics, SSD Fungsi TRIM, Akuisisi, Recovery*



## ABSTRACT

Crime activities involving a computer device are likely to be recorded on computer system storage media. One of the main storage media for computers today besides the hard disk (HDD) is the Solid State Drive (SSD). Recently, many companies are turning to SSD for higher performance, good physical size, and energy efficiency. A survey published by *statista.com* on the development of Solid State Drives around the world shows that the use of SSD is increasing every year, inversely proportional to the use of HDD which continues to decline every year. SSD have a TRIM function which is a feature on SSD related to the operating system. The TRIM function has a negative effect on forensic analysis and data persistence after deletion can no longer be guaranteed as the SSD storage controller decides when and how many blocks are marked for deletion. Live forensic is one of the forensic methods that is carried out while the system is running (active). The analytical method used in this study is SNI Acquisition 27037:2014, which is one of the stages of SNI 27037:2014 which has several processes that need to be carried out such as investigating the security aspects of evidence, determining the acquisition model, making acquisitions and reviewing the acquisition results.

The focus of this research is to conduct acquisition and recovery experiments with Autopsy tool and OSForensics tool on NVMe M.2 SSDs enable and disable TRIM functions. The investigation process begins with imaging using the AccessData FTK Imager tool with the TRIM enable and disable functions which are set using the command prompt that is already available on the Windows 10 Pro operating system, then permanent deletion (SHIFT+DELETE) of the target file will be the object of recovery, then SSD image file acquisition was carried out and continued with data recovery using the Autopsy tool and the OSForensics tool.

The results of the acquisition and recovery processes show that the OSForensics tool has a faster acquisition process time duration. The results of the acquisition and recovery experiment show that the OSForensics tool has a faster acquisition process time duration, which is 228 minutes with TRIM enabled and 231 minutes on TRIM disabled, while the Autopsy tool is 323 minutes on TRIM enabled and 334 minutes on TRIM disabled. However, in the recovery process, the Autopsy tool shows features that make it very easy for users, namely being able to collectively recover files, while the Trial version of the OSForensics tool has to manually recover files one by one. The percentage of the Autopsy tool's success rate in performing recovery on an NVMe M.2 Solid State Drive (SSD) with the TRIM function enabled is 0% while the TRIM function disabled is 100%. The same result is also obtained by the OSForensics tool where the recovery is performed on the NVMe M.2 Solid State Drive (SSD) with the TRIM function enabled at 0% while the TRIM function disabled is 100%.

**Keyword:** Autopsy, OSForensics, TRIM Function SSD, Acquisition, Recovery