IT Journal Research and Development (ITJRD)
Vol. 4, No. 2, Maret 2020, pp. 135 – 148, E-ISSN: 2528-4053 |P-ISSN: 2528-4061
DOI : 10.25299/itjrd.2020.vol4(2).4615

Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics

Wisnu Pranoto[1], Imam Riadi[2], dan Yudi Prayudi[3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia[1,3]
Program Studi Sistem Informasi, Fakultas Matematik dan Ilmu Pengetahuan Alam, Universitas Ahmad Dahlan[2]
17917130@student.uii.ac.id[1], imam.riadi@is.uad.ac.id[2], prayudi@uii.ac.id[3]

Article Info

History :
Dikirim 07 Februari 2020
Direvisi 11 Februari 2020
Diterima 28 Februari 2020

Kata Kunci:
Digital Evidence
Live Forensics
Tools Forensics
Solid State Drive NVMe
TRIM

Abstrak

Solid State Drive (SSD) memiliki fitur bernama TRIM. Penelitian ini bertujuan untuk melakukan perbandingan fungsi TRIM disable dan enable, serta membandingkan kemampuan tools forensics dan tools recovery dalam mengembalikan bukti digital pada SSD Non-volatile Memory Express (NVMe) fungsi TRIM. Sistem operasi yang digunakan dalam penelitian ini adalah Windows 10 profesional dengan file system NTFS. Selama ini, teknik akuisisi umumnya digunakan secara tradisional atau static. Oleh karena itu diperlukan teknik untuk mengakuisisi SSD dengan menggunakan metode live forensics tanpa mematikan sistem operasi yang sedang berjalan. Metode live forensics digunakan untuk mengakuisisi SSD NVMe secara langsung pada fungsi TRIM disable dan enable. Tools yang digunakan untuk live akuisisi dan recovery adalah FTK Imager Portable dan Testdisk. Prosentase recovery TRIM disable menggunakan tool Autopsy dan Testdisk 100% sehingga dapat menemukan barang bukti dan menjaga integritas barang bukti, hal ini dibuktikan dengan nilai hash yang sama pada file asli dan file hasil recovery, Sedangkan tool Belkasoft hanya 3%. Sementara pada TRIM enable menggunakan tool Autopsy, Belkasoft, dan Testdisk 0%, file hasil recovery mengalami kerusakan dan tidak dapat di-recovery.

Koresponden:
Wisnu Pranoto
Program Studi Teknik Informatika, Fakultas Teknologi Industri
Universitas Islam Indonesia
Jl. Kaliurang KM.14,5 Sleman, Yogyakarta, Indonesia, 55584
Email : 17917130@students.uii.ac.id

1. PENDAHULUAN

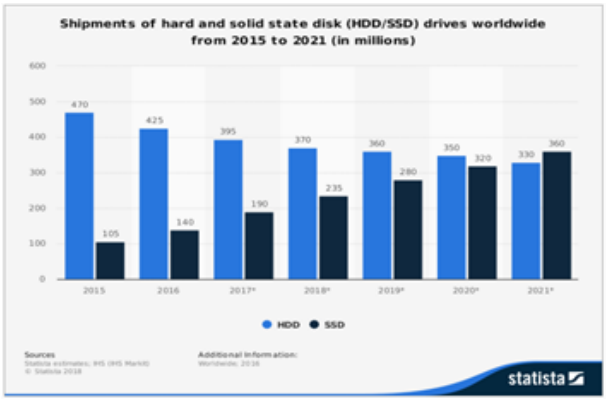
Menurut data penelitian dan laporan pengaduan kejahatan komputer dari ID-CERT [1], tingkat kejahatan komputer semakin meningkat secara signifikan dari tahun ke tahun. Kejahatan komputer itu sendiri merupakan tindakan ilegal yang melibatkan teknologi untuk melakukan manipulasi data digital dan sebagainya [2].

Teknologi komputer menuntut adanya kecepatan akses dalam pengoperasiannya. Hal tersebut dapat dicapai salah satunya dengan media penyimpanan SSD [3]. SSD merupakan kepanjangan dari Solid State Drive. SSD adalah sebuah media yang menyimpan semua data informasi pada chip-chip memory flash [4].

SSD telah meluncurkan teknologi media penyimpanan yaitu SSD Non-volatile Memory Express (NVMe). NVMe adalah sebuah interface yang menggunakan jalur PCIe (Peripheral Component Interconnect express) untuk melakukan perpindahan data secara lebih cepat [5, 6]. Gambar 1 adalah Bentuk fisik SSD NVMe M.2 Key M yang digunakan.

Gambar 1. SSD M.2 NVMe Adata SX6000 Lite

Selain itu, SSD memiliki fitur TRIM. Fitur TRIM adalah sebuah perintah yang berhubungan dengan sistem operasi yang sedang berjalan dan langsung ditujukan kepada firmware dari SSD [7]. TRIM akan menyampaikan block yang dianggap tidak digunakan dan menghapus data yang tersisa secara internal [8, 9]. Oleh sebab itu, penanganan data informasi pada SSD harus dilakukan dengan cepat karena data akan segera hilang jika sistem mati [8]. Gambar 2 menunjukkan perkembangan penggunaan SSD [10].



Gambar 2. Statistik Pengguna SSD

Forensik digital adalah bidang ilmu untuk menyelidiki bukti digital guna mengumpulkan, mengembalikan dan menganalisis bukti digital tersebut. Bukti digital kejahatan komputer terdapat pada perangkat komunikasi seperti smartphone, tablet, laptop atau pengguna komputer lainnya [2, 11, 12]. Bukti digital yang dibutuhkan dapat diperoleh dengan menggunakan teknik live forensics. Live forensics adalah sebuah metode yang digunakan untuk penanganan kejahatan komputer dan data recovery saat sistem komputer sedang berjalan [13]. Teknik live forensics mampu meningkatkan hasil data recovery bukti digital dari fungsi TRIM di SSD NVMe. Teknik ini juga dapat menjamin integritas data tanpa kehilangan bukti digital yang mudah hilang [14, 15].

Media penyimpanan seperti SSD memiliki jenis penyimpanan non-volatile. Non-volatile adalah jenis penyimpanan yang datanya dapat ditulis dan dihapus, tetapi data tetap ada walau sistem sedang dalam kondisi mati [16]. Penelitian ini menggunakan media penyimpanan jenis non-volatile pada SSD. Ramadhan dkk [4] melakukan penelitian tentang proses forensik data recovery pada SSD SATA dengan menggunakan metode static. Metode static adalah tahapan tradisional untuk mengolah bukti digital secara bit-by-bit image dan taha-

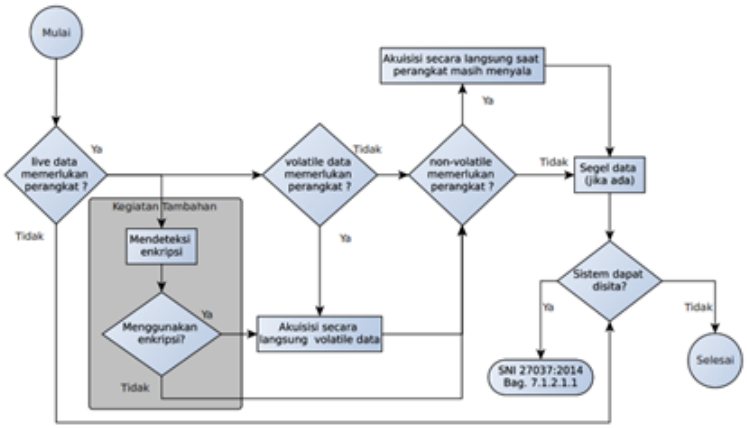
pan proses forensik berjalan pada saat sistem tidak menyala [17, 18, 19]. Hasil penelitian dengan menggunakan teknik tradisional adalah dalam SSD terdapat fitur TRIM disable dan TRIM enable. Penelitian lain yang menggunakan metode static dilakukan oleh Riadi dkk [20] penelitian tersebut meneliti SSD interface NVMe terkait implementasi fungsi TRIM dengan menggunakan freamwork NIJ melalui tahapan Identification, Collection, Examination, Analysis dan Reporting. Penelitian tersebut memperoleh hasil prosentase recovery TRIM disable dengan tool Sluetkit Autopsy 92% dan Recover My File 99% tidak dapat melakukan recovery keseluruhan file yang sudah dihapus, sedangkan TRIM enable dengan tools Sluetkit Autopsy dan Recover My File 0% tidak satupun yang dapat dilakukan recovery pada semua file.

Selain menggunakan metode static, proses file recovery dapat dilakukan dengan teknik forensics menggunakan metode live forensics. Metode live forensics bertujuan agar penanganan investigasi lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan untuk dibaca dan meminimalkan kapasitas imaging memori bila dibandingkan dengan teknik forensik tradisional [21, 22]. Menurut penelitian yang dilakukan oleh Soni dkk [13], metode live forensics diterapkan untuk melakukan data recovery pada saat virtual server sedang berjalan. Proses live forensics virtual server dilakukan seperti menggunakan virtual mesin proxmox yang menyediakan fitur backup. Penelitian tersebut bertujuan untuk melakukan pengembalian data pada saat virtual server sedang berjalan. Tool yang digunakan adalah Sluetkit Autopsy dan Belkasoft. Hasil penelitian tersebut berhasil membaca keseluruhan isi file hasil imaging serta dapat menemukan file yang telah terhapus.

Dalam penelitian ini, peneliti akan menggunakan media penyimpanan SSD interface NVMe dengan fungsi TRIM pada Windows 10 dengan menerapkan metode live forensics untuk recovery file fungsi TRIM.

2. METODE PENELITIAN

Pada penelitian ini, metode akuisisi akan dilakukan dengan menerapkan metode live forensics data non-volatile berdasarkan pedoman dan persyaratan dalam Standar Nasional Indonesia (SNI) 27037:2014 [23]. Tahapan metode live forensics SNI 27037:2014 ditunjukkan pada Gambar 3.



Gambar 3. SNI Acquisition 27037:2014

Beberapa penelitian sebelumnya telah menggunakan prosedur akuisisi live forensics sesuai dengan SNI 27037:2014 [14]. Dalam pedoman SNI 27037:2014, tahapan yang akan digunakan untuk proses akuisisi SSD NVMe, terdiri dari menentukan jenis akuisisi yang akan digunakan, menentukan jenis data yang diperoleh, melakukan prosedur akuisisi, dan menyita hasil akuisisi untuk proses hashing dengan MD5. Gambar 4 berikut ini adalah tahapan pemeriksaan dan analisis yang akan dilakukan untuk menyelesaikan penelitian ini.

Gambar 4. Tahapan Pemeriksaan dan Analisis

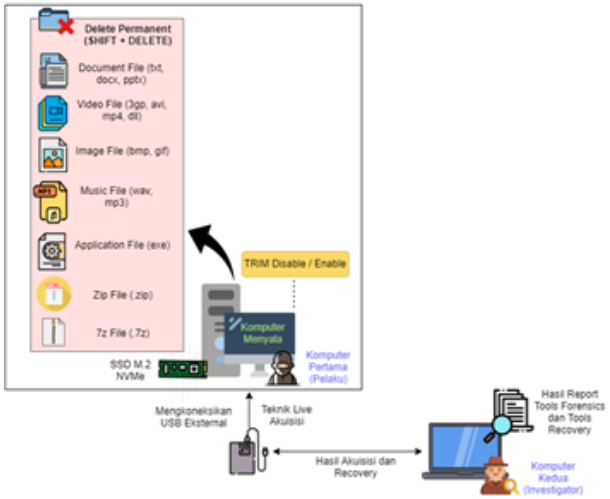
1. Persiapan
   Tahap persiapan dilakukan dengan menyediakan ruang penyimpanan untuk menyimpan data imaging yang akan di-recovery. Tahapan ini dilakukan menggunakan tool FTK Portable Imaging untuk melakukan akuisisi. FTK Imager mendukung live forensics untuk memperoleh file imaging SSD NVMe fungsi TRIM disable dan enable.
2. Ekstraksi
   Dalam tahap ini, dilakukan ekstraksi file imaging dengan mengidentifikasi dan melakukan recovery file yang telah terhapus. Ekstraksi file juga akan mengungkapkan karakterisitik struktur file, data yang telah terhapus, nama file, dan nilai hash md5.
3. Analisis
   Tahap ini menganalisis hasil dari proses ekstraksi yang telah dilakukan sehingga dapat mengukur tingkat efektifitas dari ekstraksi file fungsi TRIM serta memperoleh rekomendasi tools yang tepat untuk recovery file pada penelitian ini.

2.1. Pengumpulan Data

Alat dan bahan yang dibutuhkan untuk mendapatkan bukti digital dalam penelitian ini adalah laptop tipe ASUS X455LN dengan sistem operasi Windows 10 Education dengan arsitektur 64-bit dan USB SSD eksternal yang digunakan untuk penyimpanan live acquisition. Tools forensics yang akan digunakan untuk acquisition SSD NVMe adalah FTK Portable Imager untuk imaging. Selanjutnya, analisis dan recovery bukti digital dilakukan menggunakan tools Sluetkit Autopsy, Belkasoft Evidence dan Testdisk.

2.1.1. Skenario

Penelitian ini membutuhkan skenario untuk mendapatkan bukti digital. Tahapan skenario mencakup semua kegiatan yang dijalankan pada SSD NVMe fungsi TRIM. Tahapan skenario pada SSD NVMe digunakan sebagai pedoman penghapusan permanen (shift+delete) beberapa file yang akan di-recovery dan dianalisis. Untuk mempermudah penghapusan file, penamaan file dibedakan berdasarkan ganjil-genap. TRIM disable adalah file nama ganjil, sedangkan TRIM enable adalah file nama genap. Nilai hash dari beberapa file ganjil-genap dapat dilihat pada Tabel 1 di bawah ini. Gambar 5 adalah skenario yang akan pada penelitian ini.



Gambar 5. Skenario SSD NVMe Live Forensics Recovery

Tahapan yang dilakukan terhadap pelaku :

1. Pelaku menggunakan SSD NVMe dengan sistem operasi Windows 10 Professional dan file system NTFS.

2. Pelaku membagi dua partisi C: dan D:Ṗartisi D: digunakan untuk kebutuhan penyimpanan file yang akan dimanipulasi.
3. Pelaku menerapkan fungsi TRIM disable dan enable.
4. Pelaku menghapus permanen (shift+delete) file label ganjil-genap pada SSD NVMe di bagian partisi D:\.

Tahapan yang dilakukan terhadap investigator :

1. Investigator mengkoneksikan USB SSD SATA eksternal ke komputer Pelaku untuk menyimpan hasil acquisition dan recovery file.
2. Investigator melakukan acquisition SSD NVMe secara langsung pada komputer Pelaku menggunakan USB SSD SATA eksternal dengan tool FTK Portable Imager dan tools recovery Testdisk.
3. Komputer investigator digunakan untuk melakukan pemeriksaan dan analisis hasil imaging menggunakan Sleutkit Autopsy dan Belkasoft.

Tabel 1. Daftar Beberapa Sample File Label Ganjil-Genap dan Nilai Hash

File Type	Nama File Asli	Nilai MD5
Document	D:\DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c
	D:\DOCX 2.docx	6db984ae2628503104cb46fab8b9ef8c
	D:\XLSX 1.xlsx	56c424725531715f142e77ccc5cee774
	D:\XLSX 2.xlsx	56c424725531715f142e77ccc5cee774
	\D:TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c
	D:\TXT 2.txt	6bb11f42a5b591be9ec1a0e95a5cd00c
Video	D:\3GP 1.3gp	cd5f422a723609bff58c699704f91d88
	D:\3GP 2.3gp	cd5f422a723609bff58c699704f91d88
	D:\AVI 1.avi	72562d25302f0698c19040a6d50ceb0c
	D:\AVI 2.avi	72562d25302f0698c19040a6d50ceb0c
Image	D:\GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb
	D:\GIF 2.gif	ed28cc871584230543b5a2d8a386a2cb
Music	D:\MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb
	D:\MP3 2.mp3	d004ad9c716fbb7262d09fcd812b7bdb
Application	D:\MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c
	D:\MASTER 2.exe	562f2ea6e41020fd7bf5426bd77cd59c
Zip	D:\ZIP 1.zip	47cf035aa29599823cce99bef2467330
	D:\ZIP 2.zip	47cf035aa29599823cce99bef2467330
7z	D:\7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876
	D:\7Z 2.7z	e2d9c0b0a82113ce52d5334ffd24a876

Untuk dilakukannya simulasi kasus pada penelitian live forensics dan recovery SSD NVMe ini, peneliti melakukan simulasi yaitu penghapusan file dengan perintah SHIFT+DELETE dan kemudian file didalam partisi ke-dua tersebut akan dilakukan recovery data. Gambar 6 berikut ini adalah tahapan simulasi dari skenario penelitian.

3. HASIL DAN PEMBAHASAN

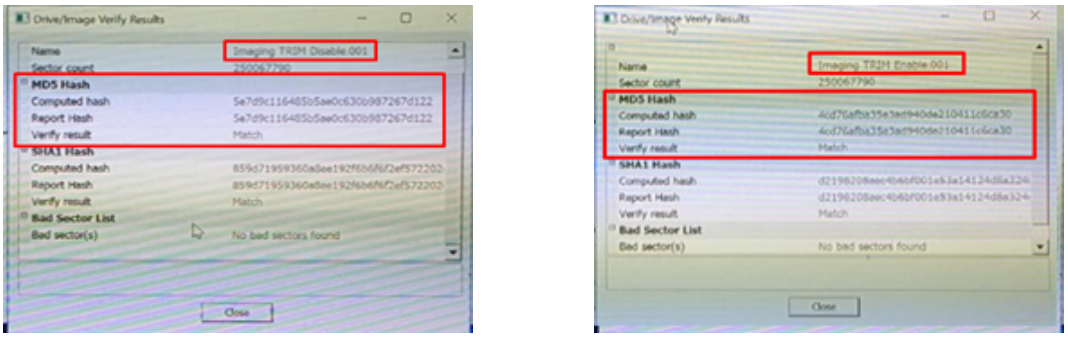
3.1. Hasil

Penelitian ini dilakukan dengan metode live forensics menggunakan USB SSD eksternal untuk melakukan live acquisition SSD NVMe fungsi TRIM. Hal ini dilakukan untuk menghindari kerusakan dan kehilangan bukti digital pada SSD NVMe fungsi TRIM. Berdasarkan skenario yang telah dibuat, Investigator melakukan ekstraksi dari hasil imaging SSD NVMe fungsi TRIM disable dan enable menggunakan tools Autopsy, Belkasoft Evidence, dan Testdisk.

Gambar 6. Tahapan Simulasi

3.1.1. Persiapan

Pada tahapan ini, akuisisi bukti digital yang terdapat dalam SSD NVMe dilakukan dengan menggunakan tools yang mendukung teknik live forensics seperti FTK Portable Imager. Tahapan teknik live forensics dilakukan untuk mendapatkan file yang sudah dihapus permanen dalam SSD NVMe fungsi TRIM disable dan enable. Tools live forensics yang digunakan dalam penelitian ini adalah FTK Portable Imager. Karena FTK Portable Imager dapat mengambil data dan informasi file yang sudah terhapus, FTK Portable Imager dapat mendukung teknik live forensics. Gambar 7 berikut ini adalah hasil potret kamera dokumentasi proses live forensics imaging TRIM disable dan TRIM enable menggunakan FTK Portable Imager. Tabel 2 menunjukkan hasil proses imaging dan nilai hash MD5. Tujuan dari proses imaging adalah untuk menghindari kerusakan pada bukti digital asli yang terkandung di dalam SSD NVMe ketika proses analisis dilakukan.



(a) (b)

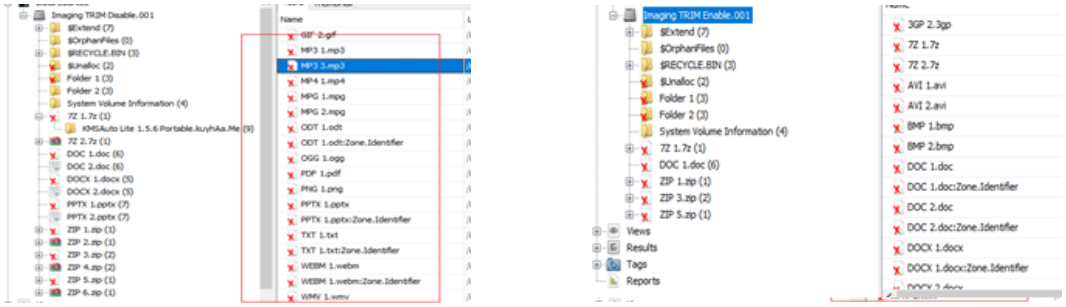
Gambar 7. Hasil Imaging (a) TRIM Disable, (b) TRIM Enable

Tabel 2. Hasil Akuisisi SSD NVMe fungsi TRIM menggunakan FTK Portable Imager

Nama Imaging	Nilai MD5	Proses Akuisisi (Time)
TRIM Disable	5e7d9c116485b5ae0c630b987267d122	50 menit 46 detik
TRIM Enable	4cd76afba35e3ad940de210411c6ca30	50 menit 44 detik

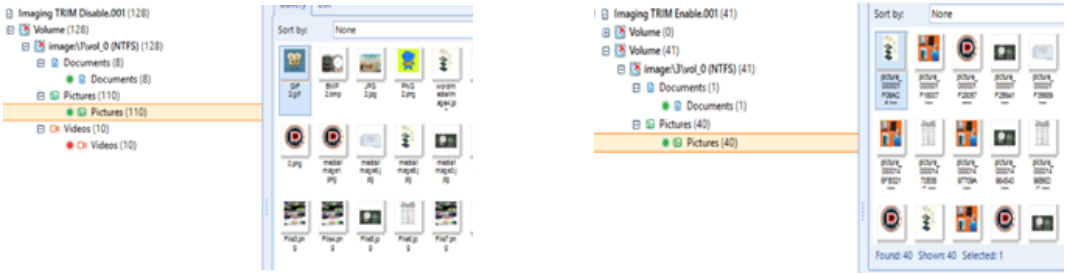
3.1.2. Ekstraksi Perbandingan Tools

Pada tahapan ini, peneliti melakukan ekstraksi file imaging. Proses ini bertujuan untuk melakukan ekstraksi hasil imaging guna menjaga integritas dan keaslian barang bukti. Hasil imaging yang akan diekstraksi adalah salinan dari hasil imaging. Tools untuk membantu proses ekstraksi pemeriksaan dan analisis imaging adalah Autopsy, Belkasoft, dan Testdisk. Gambar 8, Gambar 9, dan Gambar 10 menunjukkan bukti digital yang terhapus.



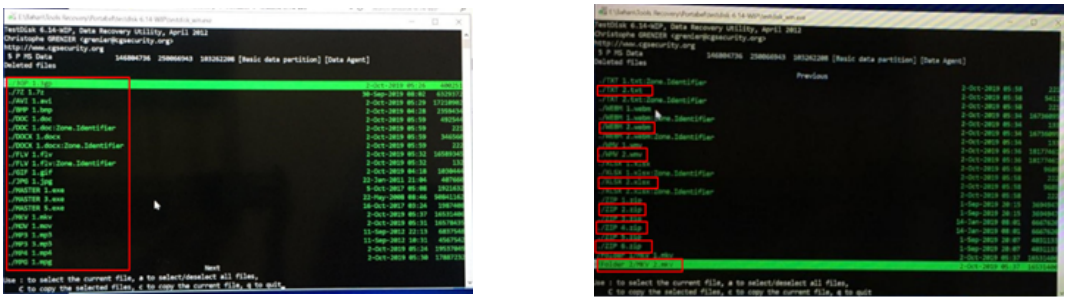
(a) (b)

Gambar 8. Pemeriksaan Tool Sluetkit Autopsy (a) TRIM Disable, (b) TRIM Enable



(a) (b)

Gambar 9. Pemeriksaan Tool Belkasoft (a) TRIM Disable, (b) TRIM Enable



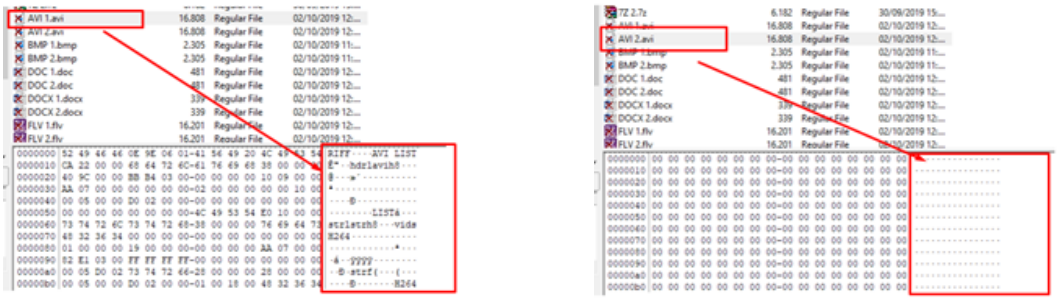
(a) (b)

Gambar 10. Pemeriksaan Tool Testdisk (a) TRIM Disable, (b) TRIM Enable

3.1.3. Analisis Perbandingan Tools

Pada tahapan ini, analisis hasil akuisisi dilakukan menggunakan FTK imager. Di tahap ini ditemukan nilai signature file yang sudah terhapus pada fungsi TRIM disable dan enable. Signature file adalah suatu nilai

informasi data yang digunakan untuk mengidentifikasi isi dalam data [24, 25] [24][25]. Gambar 11 (a) menunjukkan signature pada file label ganjil tidak mengalami kerusakan. Dengan demikian, bisa disimpulkan bahwa file label ganjil dapat dibaca dan di-recovery. Sementara itu, Gambar 11 (b) menunjukkan bahwa signature pada file label genap mengalami kerusakan atau berubah sehingga file tersebut tidak dapat di-recovery.



(a) (b)

Gambar 11. Tahapan Analisis (a) TRIM Disable Label Ganjil, (b) TRIM Enable Label Genap

Tahapan analisis hasil recovery file yang dirangkum pada Tabel 3 dan Tabel 4 menunjukkan hasil dari analisis proses recovery file TRIM disable dan enable yang dilakukan menggunakan tools Sleutkit Autopsy.

Tabel 3. Analisis Hasil Recovery TRIM Disable Label Ganjil Tool Sleutkit Autopsy

Hasil Nama File Recovery	Nilai MD5	Informasi
DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
XLSX 1.xlsx	56c424725531715f142e77ccc5cee774	Successful recovery
TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
3GP 1.3gp	cd5f422a723609bff58c699704f91d88	Successful recovery
AVI 1.avi	72562d25302f0698c19040a6d50ceb0c	Successful recovery
MPG 1.mpg	293a2b5b3a18b1f283bcc2cbda358e0b	Successful recovery
GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb	Successful recovery
MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb	Successful recovery
MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c	Successful recovery
ZIP 1.zip	47cf035aa29599823cce99bef2467330	Successful recovery
7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876	Successful recovery

Hasil analisis TRIM disable file label ganjil menunjukkan bahwa dengan melihat keaslian barang bukti dari file tersebut berdasarkan analisis file menggunakan Autopsy, dapat diasumsikan bahwa keseluruhan file label ganjil mempunyai nilai hash MD5 yang identik atau dengan kata lain, integritas barang bukti terjaga. Ditemukan 11 barang bukti file dari 11 file asli. Hasil prosentase recovery menggunakan tools Autopsy label ganjil 100%.

Ditemukan semua file dengan label ganjil 10 dari 11 file berhasil di-recovery dengan baik tanpa ada kerusakan. Sedangkan file label genap ditemukan 0 dari 11 file, tidak satu pun yang dapat di-recovery sehingga file tersebut mengalami kerusakan. Pada file label ganjil yang sudah terhapus sebelumnya pada fungsi TRIM disable dapat dilakukan recovery dengan sempurna. Dengan demikian, dapat disimpulkan bahwa ketika penghapusan file label ganjil dilakukan dalam keadaan disable, maka recovery dapat dilakukan dengan sempurna. Sementara itu, karena file label genap dihapus pada saat TRIM enable, file label genap tersebut tidak dapat di-recovery seluruhnya. Hasil prosentase recovery menggunakan tools Autopsy label ganjil 99% sedangkan label genap 0%.

Tabel 5 dan Tabel 6 menunjukkan hasil dari proses analisis dan recovery file TRIM disable dan enable yang telah dilakukan dengan tool Belkasoft.

Tabel 5 ditemukan 3 barang bukti dari 11 file asli yang memiliki nilai hash MD5 yang sama, sehingga barang bukti tersebut tidak rusak. Sedangkan 9 dari 11 file asli mempunyai struktur data yang rusak dengan

Tabel 4. Analisis Hasil Recovery TRIM Enable Label Genap Tool Autopsy

Hasil Nama File Recovery	Nilai MD5	Informasi
DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
DOCX 2.docx	821d1ae6d9543f57e95a82c26fcbcbb6	Corrupted file
XLSX 1.xlsx	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
XLSX 2.xlsx	c4e4f86f732fd5873e050500e18bb414	Corrupted file
TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
TXT 2.txt	9ba601b1c111c9ebc50b523d09ea5f21	Corrupted file
3GP 1.3gp	cd5f422a723609bff58c699704f91d88	Successful recovery
3GP 2.3gp	299e23fd97392eae859b7117dfb91634	Corrupted file
AVI 1.avi	72562d25302f0698c19040a6d50ceb0c	Successful recovery
AVI 2.avi	a13a97acca90cce38197742e79ebd152	Corrupted file
MPG 1.mpg	-	Corrupted file
MPG 2.mpg	-	Corrupted file
GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb	Successful recovery
GIF 2.gif	-	Corrupted file
MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb	Successful recovery
MP3 2.mp3	255f0e8c535c187b3e13adb241eae315	Corrupted file
MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c	Successful recovery
MASTER 2.exe	a6e1964dd6a7e6d0498522db4c157335	Corrupted file
ZIP 1.zip	47cf035aa29599823cce99bef2467330	Successful recovery
ZIP 2.zip	9ba7bb2ab23acedeedb3b9207f51d2c0	Corrupted file
7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876	Successful recovery
7Z 2.7z	d184ed7759220cb6d86fae5cb6965174	Corrupted file

Tabel 5. Analisis Hasil Recovery TRIM Disable Label Ganjil Tool Belkasoft

Hasil Nama File Recovery	Nilai MD5	Informasi
DOCX 1.docx	-	Corrupted file
XLSX 1.xlsx	-	Corrupted file
TXT 1.txt	-	Corrupted file
3GP 1.3gp	-	Corrupted file
AVI 1.avi	-	Corrupted file
MPG 1.mpg	-	Successful recovery
picture_00000414A000.jpg	d4fc57bddd2ed31d53f00002791a245d	Corrupted file
picture_000003F52000.gif	7ac62754ea19fc0fede4f2f902a9be94	Successful recovery
picture_000014A33000.png	ecec4d4b31f17d5123552f4e4cb25edd	Successful recovery
picture_00001F640000.bmp	8cad97ecf36337caebedd53fd81258dd	Corrupted file
MP3 1.mp3	-	Corrupted file
MASTER 1.exe	-	Corrupted file
ZIP 1.zip	-	Corrupted file
7Z 1.7z	-	Corrupted file

ukuran file menjadi 0, sehingga file tersebut rusak. Hasil prosentase recovery menggunakan tools Belkasoft label ganjil 3%.

Pada tahapan pemeriksaan dan analisis recovery dengan tools Belkasoft, recovery file yang terhapus permanen dengan fungsi TRIM disable dapat dilakukan terhadap file dengan jenis ekstensi .jpg, .png, dan .bmp. Namun, label nama berubah menjadi picture_00000414A000.jpg, picture_000003F52000.gif, picture_-000014A33000.png, dan picture_00001F640000.bmp. Ditemukan bahwa hanya file jenis docx dan bmp yang dapat di-recovery tercatat hanya ada 2 file dari 23 dan dapat di-recovery dengan sempurna. Sementara itu, pada TRIM enable file label ganjil tidak satupun dapat direcovery dengan sempurna. Hasil prosentase recovery

Tabel 6. Analisis Hasil Recovery TRIM Enable Label Genap Tool Belkasoft

Hasil Nama File Recovery	Nilai MD5	Informasi
document_000001F02000.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
MKV 1. mkv	081988e8c44e575b84cda8934058e9b	Corrupted file
XLSX 1.xlsx	-	Corrupted file
XLSX 2.xlsx	-	Corrupted file
TXT 1.txt	-	Corrupted file
TXT 2.txt	-	Corrupted file
3GP 1.3gp	-	Corrupted file
3GP 2.3gp	-	Corrupted file
AVI 1.avi	-	Corrupted file
AVI 2.avi	-	Corrupted file
MPG 1.mpg	-	Corrupted file
MPG 2.mpg	-	Corrupted file
picture_000003F52000.gif	7ac62754ea19fc0fede4f2f902a9be94	Corrupted file
picture_00001F640000.bmp	8cad97ecf36337caebedd53fd81258dd	Successful recovery
MP3 1.mp3	-	Corrupted file
MP3 2.mp3	-	Corrupted file
MASTER 1.exe	-	Corrupted file
MASTER 2.exe	-	Corrupted file
ZIP 1.zip	-	Corrupted file
ZIP 2.zip	-	Corrupted file
7Z 1.7z	-	Corrupted file
7Z 2.7z	-	Corrupted file

menggunakan tools Belkasoft label ganjil 2% sedangkan label genap 0%.

Tabel 7 dan Tabel 8 menunjukkan hasil dari proses analisis dan recovery file TRIM disable dan enable yang telah dilakukan dengan tool Testdisk.

Tabel 7. Analisis Hasil Recovery TRIM Disable Label Ganjil Tool Testdisk

Hasil Nama File Recovery	Nilai MD5	Informasi
DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
XLSX 1.xlsx	56c424725531715f142e77ccc5cee774	Successful recovery
TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
3GP 1.3gp	cd5f422a723609bff58c699704f91d88	Successful recovery
AVI 1.avi	72562d25302f0698c19040a6d50ceb0c	Successful recovery
MPG 1.mpg	293a2b5b3a18b1f283bcc2cbda358e0b	Successful recovery
GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb	Successful recovery
MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb	Successful recovery
MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c	Successful recovery
ZIP 1.zip	47cf035aa29599823cce99bef2467330	Successful recovery
7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876	Successful recovery

Tabel 7 ditemukan 11 barang bukti dari 11 file asli yang memiliki nilai hash MD5 yang sama, sehingga barang bukti tersebut tidak rusak. Hasil prosentase recovery TRIM disable menggunakan tools Autopsy label ganjil 100%.

Tabel 8 ditemukan semua file dengan label ganjil 11 dari 11 file berhasil di-recovery dengan baik tanpa ada kerusakan. Sedangkan file label genap ditemukan 0 dari 11 file, tidak satu pun yang dapat di-recovery dan nilai ukuran file 0, sehingga file tersebut mengalami kerusakan. Pada file label ganjil yang sudah terhapus sebelumnya pada fungsi TRIM disable dapat dilakukan recovery dengan sempurna. Dengan demikian, dapat disimpulkan bahwa ketika penghapusan file label ganjil dilakukan dalam keadaan disable, maka recovery dapat dilakukan dengan sempurna. Sementara itu, karena file label genap dihapus pada saat TRIM enable, file label

Tabel 8. Analisis Hasil Recovery TRIM Enable Label Genap Tool Testdisk

Hasil Nama File Recovery	Nilai MD5	Informasi
DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
DOCX 2.docx	821d1ae6d9543f57e95a82c26fcbcbb6	Corrupted file
XLSX 1.xlsx	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
XLSX 2.xlsx	c4e4f86f732fd5873e050500e18bb414	Corrupted file
TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
TXT 2.txt	9ba601b1c111c9ebc50b523d09ea5f21	Corrupted file
3GP 1.3gp	cd5f422a723609bff58c699704f91d89	Successful recovery
3GP 2.3gp	299e23fd97392eae859b7117dfb91634	Corrupted file
AVI 1.avi	72562d25302f0698c19040a6d50ceb0c	Successful recovery
AVI 2.avi	a13a97acca90cce38197742e79ebd152	Corrupted file
MPG 1.mpg	293a2b5b3a18b1f283bcc2cbda358e0b	Successful recovery
MPG 2.mpg	0a74c90b47733e0551b55012f4889ca2	Corrupted file
GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb	Successful recovery
GIF 2.gif	320ed11a909004095b8cf26c25767f62	Corrupted file
MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb	Successful recovery
MP3 2.mp3	255f0e8c535c187b3e13adb241eae315	Corrupted file
MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c	Successful recovery
MASTER 2.exe	a6e1964dd6a7e6d0498522db4c157335	Corrupted file
ZIP 1.zip	47cf035aa29599823cce99bef2467330	Successful recovery
ZIP 2.zip	9ba7bb2ab23acedeedb3b9207f51d2c0	Corrupted file
7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876	Successful recovery
7Z 2.7z	d184ed7759220cb6d86fae5cb6965174	Corrupted file

genap tersebut tidak dapat di-recovery seluruhnya. Hasil prosentase recovery menggunakan tools Testdisk label ganjil 100% sedangkan label genap 0%.

3.2. Pembahasan

SSD memiliki beberapa fitur diantaranya fitur TRIM disable maupun enable. Fitur TRIM berfungsi untuk menyampaikan block yang dianggap tidak digunakan dan menghapus data yang tersisa secara internal. Fitur TRIM menyebabkan tantangan bagi investigator dalam mendapatkan bukti digital. Ada beberapa penelitian yang meneliti tentang fitur TRIM diantaranya melakukan akusisisi pada SSD fungsi TRIM menggunakan metode static. Tujuan dari penelitian tersebut untuk mendapatkan bukti digital yang sudah terhapus permanen saat fitur TRIM disable maupun enable. Penelitian tersebut memperoleh hasil, bahwa penerapan fungsi TRIM disable tidak dapat melakukan recovery keseluruhan file yang sudah dihapus permanen dengan tool Sluetkit Autopsy dan membutuhkan waktu pemeriksaan 12 jam lebih 24 menit, sedangkan TRIM enable tidak dapat melakukan recovery semua file dengan tools Sluetkit Autopsy dan membutuhkan waktu 13 jam lebih 25 menit [4].

Oleh sebab itu, metode live forensics akan mampu meningkatkan hasil recovery data dari fungsi TRIM disable. Penanganan data pada SSD harus dilakukan dengan cepat karena data akan segera hilang jika sistem mati. Hasil yang diperoleh dari permasalahan fungsi TRIM disable pada penelitian ini adalah secara keseluruhan file dapat di-recovery menggunakan tools Sluetkit Autopsy dengan sempurna dan tidak merubah nilai hash pada file. Live acquition TRIM disable menggunakan tools FTK Portable Imager membutuhkan waktu 50 menit 46 detik. Sedangkan untuk permasalahan fungsi TRIM enable, file tersebut dapat di-recovery seluruhnya dengan tools Sluetkit Autopsy, tetapi file tersebut mengalami kerusakan dan nilai hash pada file tersebut tidak identik. Live acquisition TRIM enable menggunakan tools FTK Portable Imager membutuhkan waktu 50 menit 44 detik. Hasil recovery pada SSD NVMe fungsi TRIM menggunakan ketiga tools forensics memiliki hasil yang berbeda, untuk TRIM disable menggunakan Autopsy dan Testdisk 100% file dapat di-recovery, sedangkan tools Belkasoft hanya 3% file yang dapat di-recovery. Sementara pada TRIM enable menggunakan tools

Autopsy, Belkasoft, dan Testdisk 0% file tidak dapat di-recovery, file hasil recovery mengalami kerusakan dan tidak dapat di-recovery. Berikut rangkuman hasil recovery file SSD NVMe dengan metode live forensics pada Tabel 9.

Tabel 9. Sampel Hasil Perbandingan Recovery Tools Forensics.

		Hasil Recovery Tools Forensics					
Jenis File	Ekstensi File	Autopsy		Belkasoft		Testdisk	
		TRIM Disable	TRIM Enable	TRIM Disable	TRIM Enable	TRIM Disable	TRIM Enable
Dokument	.docx	✓	x	x	x	✓	x
	.xlsx	✓	x	x	x	✓	x
	.txt	✓	x	x	x	✓	x
Video	.3gp	✓	x	x	x	✓	x
	.mpg	✓	x	x	x	✓	x
	.avi	✓	x	x	x	✓	x
Gambar	.gif	✓	x	x	x	✓	x
	.jpg	✓	x	✓	x	✓	x
	.png	✓	x	✓	x	✓	x
	.bmp	✓	x	P	x	✓	x
Musik	.mp3	✓	x	x	x	✓	x
Aplikasi	.exe	✓	x	x	x	✓	x
Zip	.zip	✓	x	x	x	✓	x
7Z	.7z	✓	x	x	x	✓	x

Berdasarkan informasi yang dikumpulkan dan dijabarkan berdasarkan metode dan skenario yang di-implementasikan pada penelitian ini, terbukti bahwa fungsi TRIM menyebabkan masalah dan tantangan bagi investigator digital forensics. Hal ini dikarenakan fungsi TRIM memiliki pengaruh negatif yaitu TRIM dapat berpengaruh untuk melakukan recovery data ketika TRIM enable pada sistem operasi. Akibatnya fungsi TRIM melakukan penghapusan data yang dianggap tidak digunakan dan menghapus data yang tersisa secara internal. Teknologi pada media penyimpanan SSD memiliki nilai negatif, khususnya pada analisis forensik untuk menemukan informasi dan memahami data yang tersimpan pada media penyimpanan SSD. Hal itu adalah fakta bahwa SSD menjadi tantangan untuk analisis forensik [26].

4. KESIMPULAN

Berdasarkan hasil penelitian, teknik live forensics dapat diterapkan untuk akuisisi SSD NVMe fungsi TRIM pada sistem operasi Windows 10 profesional. Proses pemeriksaan dan analisis pada SSD dilakukan baik dengan fungsi TRIM disable maupun enable. Hasil prosentase recovery TRIM disable menggunakan tools Autopsy 100%, Belkasoft 3%, dan Testdisk 100%. Sementara prosentase recovery TRIM enable menggunakan tools Autopsy label ganjil 99% dan label genap 0%, Belkasoft label ganjil 2% dan label genap 0%, Testdisk label ganjil 100% dan label genap 0%. Penelitian ini menemukan bahwa dalam proses recovery, TRIM disable dapat menjaga integritas barang bukti. Hal ini dibuktikan dengan nilai hash yang sama pada file asli dan file hasil recovery. Sementara pada TRIM enable, file hasil recovery mengalami kerusakan dan tidak dapat di-recovery. File tersebut juga tidak identik dengan file aslinya sehingga integritas barang bukti tidak terjamin.

Bagi penelitian selanjutnya, disarankan untuk melakukan pengujian implementasi fungsi TRIM dalam sistem operasi lainnya seperti MacOs, Linux dan Virtual Mesin, menggunakan file sistem yang berbeda seperti ExFat, ReFS dan lain sebagainya, eksplorasi metode penghapusan, metode penanganan SSD, serta tools yang digunakan untuk melakukan recovery file dalam bidang forensik digital.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimah kasih atas bantuan semua pihak selama proses penyusunan penelitian ini. Terimah kasih kepada dosen pembimbing Dr. Imam Riadi, M.Kom dan Dr. Yudi Prayudi, S.Si., M.Kom atas arahan dan bimbinganya selama proses penyusunan penelitian ini dan terimah kasih pula kepada seluruh staf Program Studi Teknik Informatika Program Magister atas bantuannya. Terima kasih kepada kedua orang tua dan keluarga atas bantuan moril dan materi selama menyelesaikan studi. Dan tidak lupa terimah kasih kepada rekan-rekan seperjuangan yang telah memberikan bantuan dan semangat serta dukungan dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

[1] Dwi, "Laporan dwi bulan i 2014," *Incid. Monit. Rep*, pp. 1–9,.
[2] M.Al-Azhar, "Digital forensic practical guildelines for computer investigation."
[3] I.Riadi, R.Umar, and I.Nasrulloh, "Analisis forensik digital pada frozen solid state drive dengan metode national institute of justice (nij," *Elinvo (Electronics, Informatics, Vocat. Educ*, vol.3, no.1, pp. 70–82,.
[4] R.Ramadhan, Y.Prayudi, and B.Sugiantoro, "Implementasi dan analisis forensika digital pada fitur trim solid state drive (ssd."
[5] B.Nikkel, "Nvm express drives and digital forensics," *Digit. Investig*, vol.16, pp. 38–45,.
[6] Q.Xu, "Performance analysis of nvme ssds and their implication on real world databases," in *SYSTOR 2015 - Proc. 8th ACM Int. Syst*. Storage Conf.
[7] R.Hubbard, "Forensics analysis of solid state drive (ssd," pp. 1–11,.
[8] F.Geier, "The differences between ssd and hdd technology regarding forensic investigations," pp. 67,.
[9] R.Chaurasia and P. Sharma, "Solid state drive (ssd) forensics analysis : A new challenge," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* ©, vol.6, no.2, pp. 1081–1085,.
[10] Statista, "Shipments of hard and solid state disk (hdd/ssd) drives worldwide from 2015 to 2021," available:. [Online]. Available: https://www.statista.com/statistics/285474/hdds-and-ssds-in-pcs-global-shipments-2012-2017/.
[11] M.Al-Azhar, "The essentials of digital forensic."
[12] Y.Prayudi, "Problema dan solusi digital chain of custody," senasti - semin," *Nas. Sains dan Teknol. Inf.*
[13] D.Soni, Y.Prayudi, H.Mukhtar, and B.Sugiantoro, "Server virtualization acquisition using live forensics method," *Adv. Eng. Res*, vol. 190, pp. 18–23,.
[14] D.Sudyana and N.Lizarti, "Digital evidence acquisition system on iaas cloud computing model using live forensic method," *Sci. J. Informatics*, vol.6, no.1, pp. 125–137,.
[15] I.Riadi and M.Rauli, "Live forensics analysis of line app on proprietary operating system," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol.4, no.4, pp. 305–314,.
[16] J.Arulraj and A.Pavlo, "How to build a non-volatile memory database management system," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, vol. Part F1277, pp. 1753–1758,.
[17] M.Rafique and M. Khan, "Exploring static and live digital forensics: Methods, practices and tools," *Int. J. Sci. Eng. Res*, vol.4, no.10, pp. 1048–1056,.
[18] A.Nisbet, S.Lawrence, and M.Ruff, "A forensic analysis and comparison of solid state drive data retention with trim enabled file systems," *Aust. Digit. Forensics Conf*, pp. 10,.
[19] A.Faiz and R.Imam, "Forensic analysis of 'frozen' hard drive using deep freeze method," March.
[20] I.Riadi and A.Hadi, "Analisis bukti digital ssd nvme pada sistem operasi proprietary menggunakan metode static forensics," *CoreIt*, vol. 3321, no.2, pp. 1–8,.
[21] D.Yudhistira, "Metode live forensics untuk analisis random access memory pada perangkat laptop."
[22] S.Rahman and M.Khan, "Review of live forensic analysis techniques," *Int. J. Hybrid Inf. Technol*, vol.8, no.2, pp. 379–388,.
[23] B.Nasional, "Teknologi informasi – teknik keamanan – pedoman identifikasi, pengumpulan akuisisi, dan preservasi bukti digital," in *SNI 27037:2014*, Jakarta.
[24] D.Jeong and S.Lee, "Forensic signature for tracking storage devices: Analysis of uefi firmware image, disk signature and windows artifacts," *Digit. Investig*, vol.29, pp. 21–27,.
[25] K.Gary, "File signature," available:. [Online].
[26] Y.Gubanov and O.Afonin, "Recovering evidence from ssd drives: Understanding trim, garbage collection, and exclusions."

BIOGRAFI PENULIS

Wisnu Pranoto lahir di Pekanbaru 4 September 1992, memperoleh gelar serjana Teknik Informatika dari Universitas Islam Riau pada tahun 2016, dan menempuh Program Magister Teknik Informatika pada Fakultas Teknologi Industri di Universitas Islam Indonesia pada tahun 2017. Bidang keminatan penelitian di bidang Forensics Digital dan Teknologi Informasi. Memiliki lisensi dan sertifikasi internasional Certified Ethical Hacker (CEH) dan Computer Hacking Forensic Investigator (CHFI). Penulis dapat dihubungi melalui email : 17917130@students.uii.ac.id.

Imam Riadi memperoleh gelar serjana Pendidikan Teknik Elektro tahun 2001 di Universitas Negeri Yogyakarta, Magister Ilmu Komputer di Universitas Gadjah Mada pada tahun 2004, dan Doktor Ilmu Komputer di Universitas Gadjah Mada pada tahun 2014. Saat ini sebagai Dosen pada Universitas Ahmad Dahlan, selain itu aktif juga melakukan penelitian berbagai bidang Embedded System, Computer Network, Network Security, Digital Forensics, Mobile Forensics. Memiliki lisensi dan sertifikasi Cisco Networking Academy Program (CNAP), Computer Hacking Forensic Investigator (CHFI), Certified Incident Handler (CIH), Certified Ethical Hacker (CEH), Mikrotik Certified Network Associate (MTCNA). Penulis dapat dihubungi melalui email : imam.riadi@is.uad.ac.id.

Yudi Prayudi memperoleh gelar serjana Ilmu komputer pada tahun 1993 di Universitas Gadjah Mada, Magister Komputer di Institut Teknologi Sepuluh November 2001 dan Doktor Ilmu Komputer di Universitas Gadjah Mada pada tahun 2020, saat ini sebagai Dosen pada Universitas Islam Indonesia, selain itu sebagai Kepala Pusat Studi Forensik Digital dan Director Center For Digital Forensics Studies. Selain itu akfif juga melakukan berbagai penelitian internasional maupun nasional di bidang Digital Forensics, Digital Evidence, Steganography, E-learning, Security, juga aktif sebagai praktisi hingga membantu konsultasi dan menangani kasus kejahatan dunia maya oleh penegak hukum atau lembaga lain. Memiliki lisensi dan sertifikasi Computer Hacking Forensics Investigator (CHFI) dan Oxygen Certified Examiner (OCE), Encase Forensics, Enscript Programming. Penulis dapat dihubungi melalui email : prayudi@uii.ac.id.