



Penerapan Metode Live Forensics Untuk Akuisisi Pada *Solid State Drive (SSD) NVMe Fungsi TRIM*

Wisnu Pranoto

17917130

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital Program Studi

Informatika Program Magister Fakultas

Teknologi Industri

Universitas Islam Indonesia

2020

Lembar Pengesahan Pembimbing

Penerapan Metode Live Forensics Untuk Akuisisi Pada Solid State Drive (SSD) NVMe Fungsi TRIM

Wisnu Pranoto

17917130



الجامعة الإسلامية
الابستد الاندو

Pembimbing

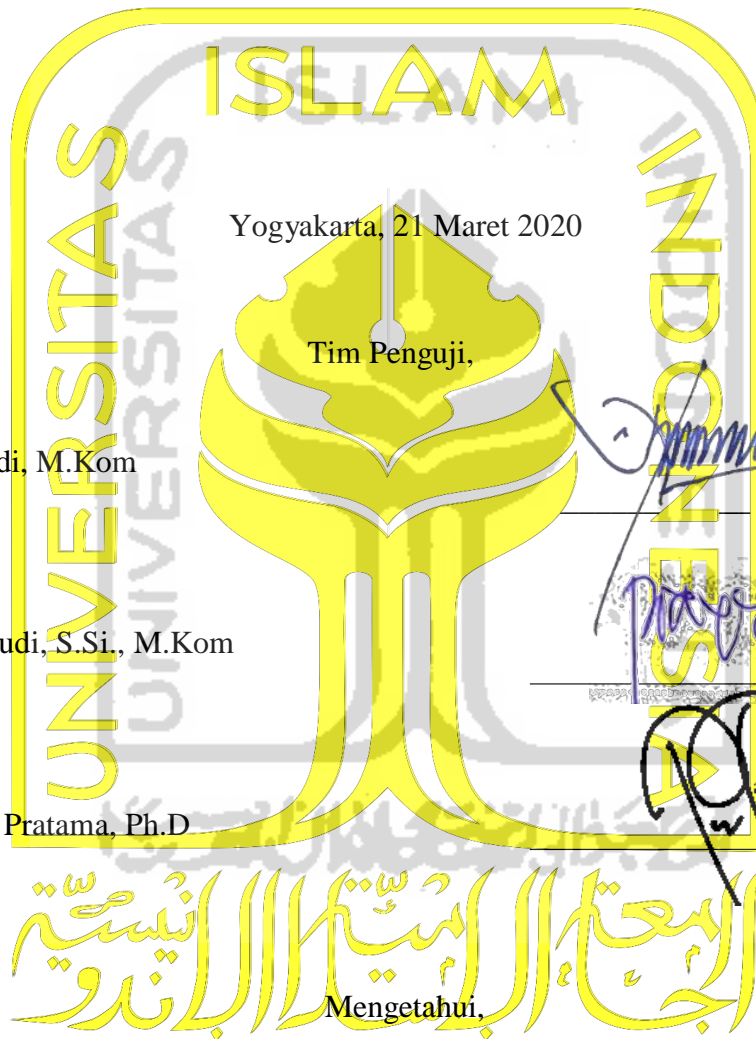
Dr. Imam Riadi, M.Kom

Lembar Pengesahan Penguji

Penerapan Metode Live Forensics Untuk Akuisisi Pada Solid State Drive (SSD)
NVMe Fungsi TRIM

Wisnu Pranoto

17917130



Dr. Imam Riadi, M.Kom
Ketua

Dr. Yudi Prayudi, S.Si., M.Kom
Anggota I

Ahmad Raf'ie Pratama, Ph.D
Anggota II

(Handwritten signatures in blue and black ink over the watermark)

Ketua Program Studi Informatika Program Magister



Universitas Islam Indonesia

Imam Riadi, S.T., M.Sc., Ph.D.

Abstrak

Penerapan Metode Live Forensics Untuk Akuisisi Pada Solid State Drive (SSD) NVMe Fungsi TRIM

Forensik digital sebagai bidang ilmu yang digunakan untuk menyelidiki bukti digital, bertujuan untuk pengumpulan, mengembalikan bukti digital, dan analisis bukti digital tersebut, yang terdapat pada kejahatan komputer melalui perangkat komunikasi seperti smartphone, tablet, laptop atau pengguna komputer lainnya. Pada dekade terakhir, saat ini teknologi komputer dituntut akan kecepatan akses dalam pengoperasiannya, salah satunya yaitu dengan media penyimpanan Solid State Drive. SSD saat ini memiliki teknologi media penyimpanan yang baru yaitu Solid State Drive Non-volatile Memory Express (SSD NVMe). SSD memiliki fitur bernama TRIM. Fitur TRIM memungkinkan sistem operasi untuk memberitahu SSD terkait block mana saja yang sudah tidak digunakan. TRIM berfungsi menghapus block yang telah ditandai untuk dihapus oleh sistem operasi. Akan tetapi dengan adanya fungsi TRIM ini, SSD memiliki efek atau nilai negatif bagi bidang forensik digital untuk menganalisis forensik khususnya pada recovery data. Tujuan penelitian ini melakukan perbandingan fungsi TRIM disable dan enable agar mengetahui kemampuan tools forensics dan tools recovery untuk mengembalikan bukti digital pada SSD NVMe fungsi TRIM. Sistem operasi yang digunakan dalam penelitian ini yaitu 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. Penerapan metode live forensics digunakan untuk mengakuisisi SSD NVMe secara langsung pada kedua fungsi TRIM disable dan enable. Tools yang digunakan untuk live akuisisi dan recovery yaitu FTK Imager Portable, Testdisk, Sleut Kit Autopsy dan Belkasoft Evidence Center. Hasil yang diharapkan adalah berupa tahapan proses analisis untuk mendapatkan barang bukti digital yang telah terhapus permanen dan membandingkan tools yang paling efektif dalam melakukan recovery bukti digital pada SSD NVMe fungsi TRIM.

Kata kunci

SSD NVMe, Bukti Digital, TRIM, Live Forensics, Tools

Abstract

Application of Live Forensics Method for Acquisition of Solid State Drive (SSD) NVMe Features TRIM

Digital forensics as a field of science used to obtain digital evidence, aims to collect or return digital evidence and analysis of digital evidence, found in computer crime through communication devices such as smartphone, tablet, laptop or other computer users. In the last decade computer technology has been demanded for speed of access in its operation, one of which is media the storage of Solid State Drive. SSD currently has a new media storage technology, namely Non-volatile Memory Express Solid State Drive (SSD NVMe) which uses the interface Peripheral Component Interconnect Express (PCIe) which is different from the interface SSD Serial Advanced Technology Attachment (SATA), PCIe can make data transfers faster than the SATA interface. SSD has a feature called TRIM. The TRIM feature allows the operating system to notify SSD which blocks are not used. TRIM removes blocks that have been marked for removal by the operating system. However, with this TRIM feature, SSD have negative effects or values for the digital forensic field for forensic analysis especially in data recovery. The purpose of this study is to compare the function of TRIM disable/enable in order to know the ability of forensics tools and recovery tools to restore digital evidence on SSD NVMe TRIM functions in windows 10 professional system operating with NTFS file system. During this time the acquisition technique is generally used traditionally/static, therefore a technique is needed to acquisition SSD using the live forensics method without shutting down the running operating system. Application of live forensics method to acquisition SSD NVMe directly on both TRIM disable/enable functions. The tool used for live acquisition and recovery is the FTK Imager Portable, Testdisk and tools forensics Sleut Kit Autopsy and Belkasoft Evidence Center. The expected output is a stage of analysis to obtain digital evidence that has been permanently erased and compare the most effective tools for performing digital evidence recovery on the SSD NVMe TRIM function.

Keywords

SSD NVMe, Digital Evidence, TRIM, Live Forensics, Tools

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 21 Maret 2020



Wisnu Pranoto

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dalam penulisan tesis ini

- Pranoto, W., Riadi, I., & Prayudi, Y. (2020). Live forensics method for acquisition on the Solid State Drive (SSD) NVMe TRIM function, DOI:

<https://doi.org/10.22219/kinetik.v0i0.1032>

- Pranoto, W., Riadi, I., & Prayudi, Y. (2020). Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics, DOI:

[https://doi.org/10.25299/itjrd.2020.vol4\(2\).4615](https://doi.org/10.25299/itjrd.2020.vol4(2).4615)

Kontributor	Jenis Kontribusi
Wisnu Pranoto	Mendesain eksperimen (70%) Menulis <i>paper</i> (100%)
Imam Riadi	Memberi ide dan saran (30%) Mereview artikel
Yudi Prayudi	Memberi ide dan saran (30%) Mereview artikel

Halaman Kontribusi

Penelitian ini tidak terlepas dari berbagai saran maupun bimbingan dari berbagai pihak, mulai dari pra penelitian, seminar proposal, seminar progress, hingga seminar pendadaran. Pihak-pihak tersebut, antara lain, Dr. Imam Riadi, M.Kom, Dr. Yudi Prayudi, S.Si., M.Kom, dan Ahmad Raf'ie Pratama, Ph.D.

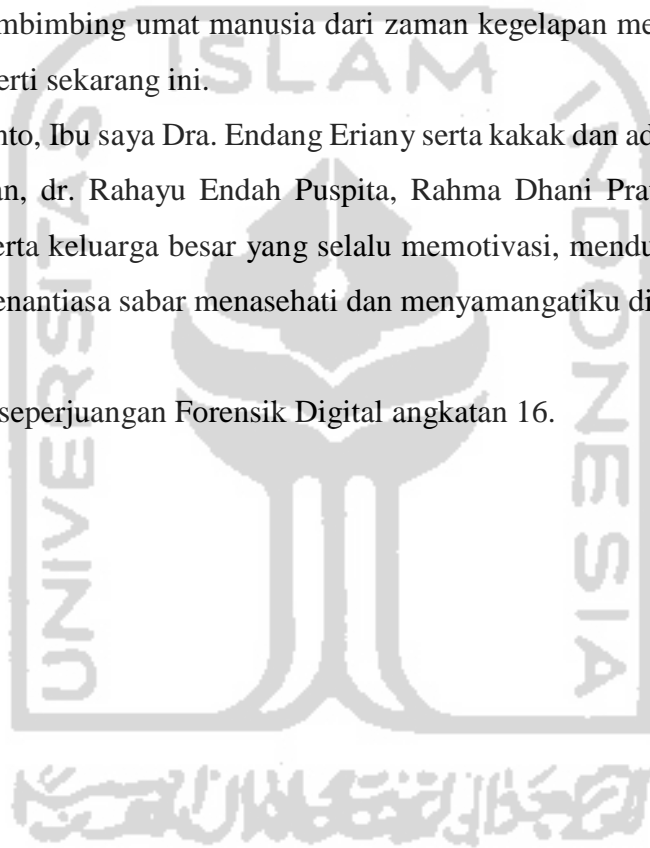


Halaman Persembahan

Bismillahirrahmanirrahim.

Dengan mengucapkan syukur Alhamdulillah, karya penelitian ini saya persembahkan kepada orang-orang yang selama ini telah mendukung, memberikan semangat dan motivasi dalam menyelesaikan pendidikan magister komputer saya ini, secara khususnya kepada :

1. Allah SWT atas rahmat dan hidayahnya serta memberikanku kesehatan sepanjang hidup dan memebrikan kemudahan-kemudahan dari berbagai kesulitan dalam menyelesaikan tugas ini, dan juga kepada Nabi Muhammad SAW, karena beliauah yang telah membimbing umat manusia dari zaman kegelapan menuju zaman terang benderang seperti sekarang ini.
2. Bapak saya Pinto, Ibu saya Dra. Endang Eriany serta kakak dan adik saya dr. Harjinis Taufik Rohman, dr. Rahayu Endah Puspita, Rahma Dhani Pratiwi S.STP, Warid Pranowo. Beserta keluarga besar yang selalu memotivasi, mendukung secara moril, material dan senantiasa sabar menasehati dan menyamangatiku dikala saya lelah dan putus asa.
3. Teman-teman seperjuangan Forensik Digital angkatan 16.



Kata Pengantar

Assalamualaikum Wr. Wb.

Syukur Alhamdulillah, penulis panjatkan kepada Allah SWT atas limpahan dan karunia yang diberikan kepada penulis sehingga dapat menyelesaikan laporan penelitian tesis dengan judul “Penerapan Metode Live Forensics Untuk Akuisisi Pada SSD NVMe Fungsi TRIM”. Adapun maksud dari penulisan laporan penelitian ini adalah sebagai persyaratan dalam mencapai jenjang pendidikan Magister Teknik Informatika konsentrasi Forensika Digital di Fakultas Teknologi Industri, Universitas Islam Indonesia. Dalam proses penyelesaian tesis ini penulis tidak dapat menyelesaikannya bila tidak ada turut serta pihak lain yang juga ikut membantu baik secara langsung maupun tidak langsung dalam menyelesaikan penelitian ini, untuk itu penulis ingin menyampaikan rasa terima kasih kepada beberapa pihak yang telah mendukung dalam penyusunan tesis ini, antara lain:

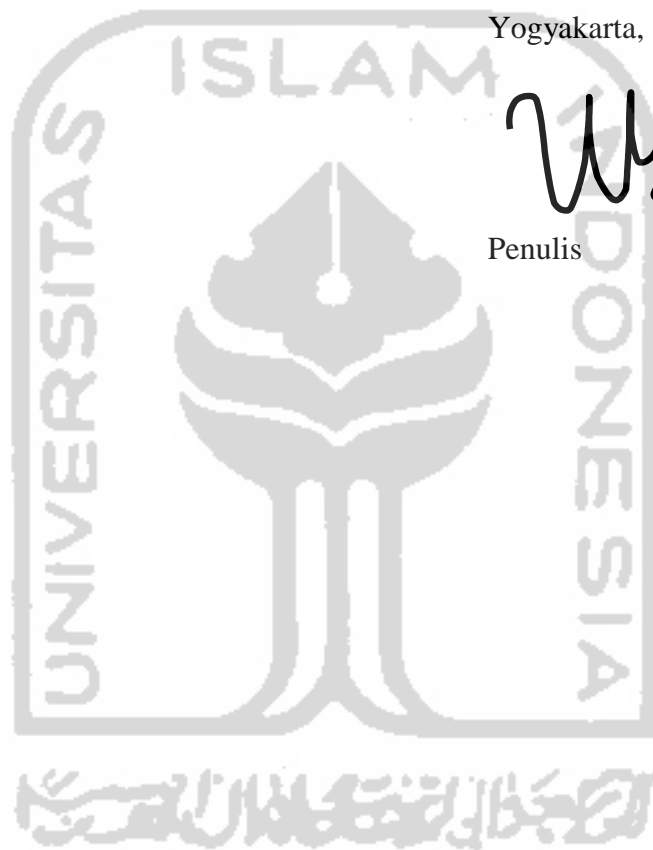
1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D, selaku rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk menimba ilmu di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D, selaku Ketua Program Studi Teknik Informatika Program Magister Fakultas Teknologi Industri, Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Imam Riadi, M.Kom dan Bapak Yudi Prayudi, S.SI., M.Kom, selaku dosen pembimbing yang telah banyak meluangkan waktunya dalam memberikan berbagai saran selama proses bimbingan.
5. Seluruh Dosen, staff administrasi dan civitas Magister Teknik Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama masa studi penulis.
6. Seluruh keluarga baik Bapak, Ibu, dan Kakak yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukungan baik moril maupun materil.
7. Rekan-rekan mahasiswa MTI khususnya konsentrasi Forensika Digital angkatan XVI yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
8. Pihak-pihak lain yang turut membantu dalam menyelesaikan penelitian ini yang tidak dapat disebutkan satu persatu oleh penulis.

Penulis menyadari bahwa laporan penelitian ini masih memiliki kekurangan. Oleh karena itu penulis dengan senang hati menerima setiap saran atau komentar serta kritikan dari pembaca guna penyempurnaan laporan penelitian ini. Akhir kata penulis mengucapkan terima kasih, semoga penyusunan laporan penelitian ini dapat memberikan inspirasi maupun manfaat bagi pembaca, khususnya bagi mahasiswa/mahasiswi Universitas Islam Indonesia. Wassalamu'alaikum Wr. Wb

Yogyakarta, 21 Maret 2020



Penulis



Daftar Isi

Lembar Pengesahan Pembimbing	i
Lembar Pengesahan Penguji.....	ii
Abstrak	iii
Abstract	iv
Pernyataan Keaslian Tulisan	v
Daftar Publikasi	vi
Halaman Kontribusi.....	vii
Halaman Persembahan	viii
Kata Pengantar.....	ix
Daftar Isi	xi
Daftar Tabel.....	xiv
Daftar Gambar	xvi
BAB 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Tujuan Penelitian.....	4
1.4 Batasan Masalah	4
1.5 Manfaat Penelitian	4
1.6 Literatur Review	5
1.7 Metode Penelitian	10
1.8 Sistematika Penulisan	10
BAB 2 Tinjauan Pustaka	12
2.1 Digital Forensik	12
2.2 Investigasi Forensik Digital	13
2.3 SNI 27037:2014.....	19
2.4 <i>Live Forensics</i>	20

2.5	<i>Solid State Drive (SSD)</i>	20
2.6	Arsitektur <i>Solid State Drive (SSD)</i>	21
2.6.1	Connector Fisik M.2 SATA.....	23
2.6.2	Connector Fisik M.2 NVMe.....	23
2.6.3	TRIM	24
BAB 3 Metode Penelitian		25
3.1	Tinjauan Pustaka.....	25
3.2	Persiapan Sistem Mesin dan Tools	25
3.3	Skenario dan Simulasi Kasus.....	26
3.4	Akuisisi SSD NVMe menggunakan Metode <i>Live Forensic</i>	28
3.4.1	Tahapan Akuisisi TRIM <i>Disable</i>	30
3.4.2	Tahapan Akuisisi TRIM <i>Enable</i>	31
3.5	Pemeriksaan dan Analisis Output SSD NVMe	32
3.6	Hasil Pembahasan dan Laporan.....	34
BAB 4 Hasil dan Pembahasan		35
4.1	Tinjauan Pustaka.....	35
4.2	Persiapan Tools.....	36
4.3	Skenario dan Simulasi	37
4.4	Tahapan Akuisisi SSD NVMe.....	41
4.4.1	Tahapan Fungsi TRIM <i>Disable</i>	42
4.4.2	Teknik Akuisisi TRIM <i>Disable</i>	46
4.4.3	Tahapan Fitur TRIM <i>Enable</i>	48
4.4.4	Teknik Akuisisi TRIM <i>Enable</i>	52
4.5	Pemeriksaan dan Analisis Output.....	55
4.5.1	Pemeriksaan dan Analisis TRIM <i>Disable</i> Menggunakan Autopsy.....	55
4.5.2	Pemeriksaan dan Analisis TRIM <i>Disable</i> Menggunakan Belkasoft	59
4.5.3	Pemeriksaan dan Analisis TRIM <i>Disable</i> Menggunakan Testdisk.....	63
4.5.4	Pemeriksaan dan Analisis TRIM <i>Enable</i> Menggunakan Autopsy	67

4.5.5	Pemeriksaan dan Analisis TRIM <i>Enable</i> Menggunakan Belkasoft	73
4.5.6	Pemeriksaan dan Analisis TRIM <i>Enable</i> Menggunakan Testdisk	78
BAB 5 Kesimpulan dan Saran		89
5.1	Kesimpulan	85
5.2	Saran	86
Daftar Pustaka.....		88



Daftar Tabel

Tabel 1.1 Rangkuman <i>Review</i> Penelitian	7
Tabel 1.2 Rangkuman <i>Review</i> Penelitian (Lanjutan)	8
Tabel 1.3 Rangkuman <i>Review</i> Penelitian (Lanjutan)	9
Tabel 2.1 Barang Bukti Digital dan Elektronik	12
Tabel 3.1 Status Storage <i>Disable/Enable</i> serta Nilai Hash	33
Tabel 3.2 Hasil Pengembalian Data Status TRIM <i>Disable</i>	33
Tabel 3.3 Hasil Pengembalian Data Status TRIM <i>Enable</i>	34
Tabel 4.1 Spesifikasi penggunaan Hardware dan Software	36
Tabel 4.2 Keaslian Nama File Ganjil, Nilai Hashing, dan Ektensi File (TRIM <i>Disable</i>)... 45	
Tabel 4.3 Keaslian Nama File Genap, Nilai Hashing dan Ektensi File (TRIM <i>Enable</i>).... 51	
Tabel 4.4 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Sleuth Kit Autopsy 57	
Tabel 4.5 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Autopsy (Lanjutan)... 58	
Tabel 4.6 Daftar File Ganji Hasil Analisis TRIM <i>Disable</i> dengan Autopsy (Lanjutan).... 59	
Tabel 4.7 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Belkasoft Evidence 61	
Tabel 4.8 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Belkasoft (Lanjutan).. 62	
Tabel 4.9 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Belkasoft Lanjutan) ... 63	
Tabel 4.10 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Testdisk	65
Tabel 4.11 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Testdisk (Lanjutan).. 66	
Tabel 4.12 Daftar File Ganjil Hasil Analisis TRIM <i>Disable</i> dengan Testdisk (Lanjutan).. 67	
Tabel 4.13 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Autopsy	69
Tabel 4.14 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Autopsy (Lanjutan) .. 70	
Tabel 4.15 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Autopsy (Lanjutan) .. 71	
Tabel 4.16 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Autopsy (Lanjutan) .. 72	
Tabel 4.17 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Autopsy (Lanjutan) .. 73	
Tabel 4.18 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Autopsy (Lanjutan) .. 74	
Tabel 4.19 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Belkasoft	76
Tabel 4.20 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Belkasoft (Lanjutan). 77	
Tabel 4.21 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Belkasoft (Lanjutan). 78	
Tabel 4.22 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Belkasoft (Lanjutan). 80	
Tabel 4.23 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Testdisk	83
Tabel 4.24 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Testdisk (Lanjutan) .. 84	
Tabel 4.25 Daftar File Genap Hasil Analisis TRIM <i>Enable</i> dengan Testdisk (Lanjutan) .. 85	

Tabel 4.26 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Testdisk (Lanjutan) .. 86

Tabel 4.27 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Testdisk (Lanjutan) .. 87



Daftar Gambar

Gambar 1.1 Pengaduan Per Kategori Kejahatan Komputer	1
Gambar 1.2 Statistik Perkembangan Penggunaan SSD.....	2
Gambar 1.4 Alur Metode Penelitian.....	10
Gambar 2.1 <i>Digital Forensic Investigation Process</i> (SNI 27037:2014).....	14
Gambar 2.2 Anatomi <i>Solid State Drive</i> (SSD).....	21
Gambar 2.3 Arsitektur <i>Solid State Drive</i>	22
Gambar 2.4 Connector SSD M.2 Slot SATA.....	23
Gambar 2.5 Connector SSD M.2 Slot NVMe.....	24
Gambar 3.1 Metodologi Penelitian.....	25
Gambar 3.2 Tahapan Skenario SSD NVMe Live Forensik <i>Recovery</i>	27
Gambar 3.3 Tahapan Simulasi	28
Gambar 3.4 Tahapan Investigasi SSD NVMe.....	29
Gambar 3.5 Prosedur Akuisisi Perangkat dalam Kondisi Menyala SNI 27037:2014.....	30
Gambar 3.6 Tahapan Akuisisi TRIM <i>Disable</i>	31
Gambar 3.7 Tahapan Akuisisi TRIM <i>Enable</i>	31
Gambar 3.8 Tahapan Pemeriksaan dan Analisis	32
Gambar 4.1 SSD SATA 2.5” (atas) dengan SSD SATA M.2 (bawah).....	35
Gambar 4.2 SSD M.2 NVMe Adata XPG SX6000 Lite	36
Gambar 4.3 Converter SSD M.2 NVMe Adata XPG SX6000 Lite	37
Gambar 4.4 Barang Bukti Elektronik	38
Gambar 4.5 Mengkoneksikan USB Penyimpanan Eksternal	38
Gambar 4.6 Perangkat Usb Eksternal.....	39
Gambar 4.7 Perangkat Komputer Investigator	39
Gambar 4.8 Tahapan Simulasi	40
Gambar 4.9 Tahapan Teknik Akuisisi SSD NVMe	41
Gambar 4.10 Flowchart Tahapan Fitur TRIM SSD	43
Gambar 4.11 Perintah Comment Pengecekan Fungsi TRIM	43
Gambar 4.12 Perintah Comment TRIM <i>Disable</i> /Nonaktif	44
Gambar 4.13 Perintah Pengecekan Ulang Fungsi TRIM	44
Gambar 4.14 Daftar Sebelum Keseluruhan File Ganjil Dihapus Permanen	46
Gambar 4.15 Tahapan Teknik Akuisisi TRIM <i>Disable</i>	46
Gambar 4.16 Hasil Output Akuisisi TRIM <i>Disable</i> Menggunakan FTK Imager Portable. 47	

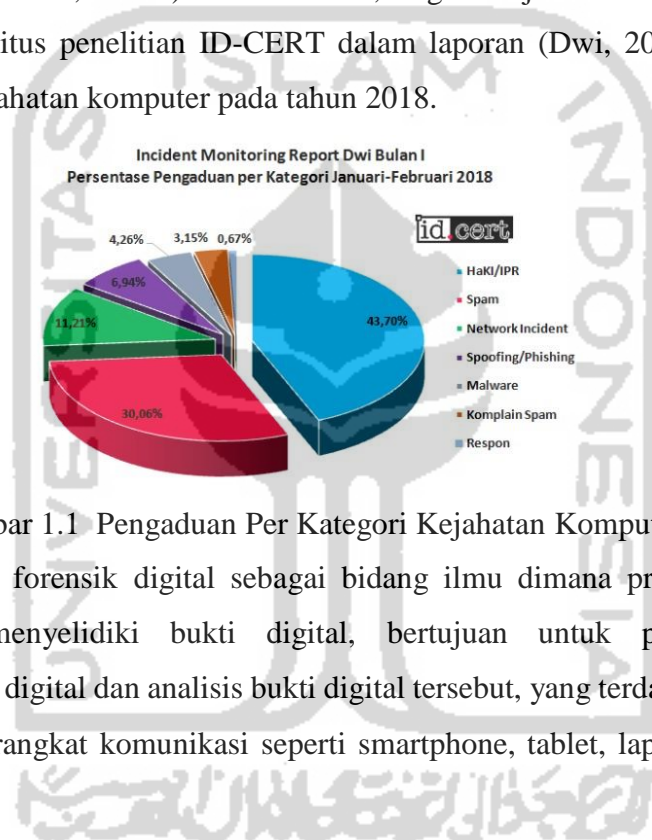
Gambar 4.17 Proses dan Hasil Output <i>Recovery</i> TRIM <i>Disable</i> Menggunakan Testdisk..	48
Gambar 4.18 Flowchart Tahapan Fitur TRIM SSD	49
Gambar 4.19 Perintah Comment Pengecekan Fungsi TRIM	49
Gambar 4.20 Perintah Comment TRIM <i>Enable</i> /Aktif	50
Gambar 4.21 Perintah Comment Pengecekan Ulang Fungsi TRIM <i>Enable</i>	50
Gambar 4.22 Daftar Sebelum Keseluruhan File Genap Dihapus Permanen.....	52
Gambar 4.23 Tahapan Teknik Akuisisi TRIM <i>Enable</i>	52
Gambar 4.24 Hasil Output Akuisisi TRIM <i>Enable</i> Menggunakan FTK Imager Portable ..	53
Gambar 4.25 Proses dan Hasil Output <i>Recovery</i> TRIM <i>Enable</i> Menggunakan Testdisk...	54
Gambar 4.26 Pemeriksaan TRIM <i>Disable</i> dengan Sleuth Kit Autopsy	56
Gambar 4.27 Daftar File <i>Recovery Ganjil</i> TRIM <i>Disable</i> dengan Sleuth Kit Autopsy.....	56
Gambar 4.28 Pemeriksaan TRIM <i>Disable</i> dengan Belkasoft Evidence Center	59
Gambar 4.29 Daftar File Setelah Pemeriksaan TRIM <i>Disable</i> dengan Belkasoft	60
Gambar 4.30 Daftar File <i>Recovery</i> TRIM <i>Disable</i> dengan Belkasoft Evidence Center	60
Gambar 4.31 Proses <i>Recovery</i> TRIM <i>Disable</i> Menggunakan Testdisk	64
Gambar 4.32 Daftar File <i>Recovery</i> TRIM <i>Disable</i> dengan Testdisk	64
Gambar 4.34 Daftar File Genap Setelah Pemeriksaan TRIM <i>Enable</i> dengan Autopsy.....	68
Gambar 4.35 Daftar File <i>Recovery</i> TRIM <i>Enable</i> dengan Sleuth Kit Autopsy	68
Gambar 4.36 Pemeriksaan TRIM <i>Enable</i> dengan Belkasoft Evidence Center	73
Gambar 4.37 Daftar File Setelah Pemeriksaan TRIM <i>Enable</i> dengan Belkasoft Evidence	74
Gambar 4.38 Daftar File <i>Recovery</i> TRIM <i>Enable</i> dengan Belkasoft Evidence Center	74
Gambar 4.39 Proses <i>Recovery</i> TRIM <i>Enable</i> Menggunakan Testdisk	78
Gambar 4.40 Daftar File <i>Recovery</i> TRIM <i>Enable</i> dengan Testdisk.....	79

BAB 1

Pendahuluan

1.1 Latar Belakang

Seiring perkembangan teknologi yang pesat, banyak hal telah terjadi. Penyalahgunaan pengguna yang bertujuan demi mendapatkan keuntungan pribadi maupun merugikan orang lain, salah satu bentuk kejahatan komputer. Kejahatan komputer merupakan tindakan ilegal yang melibatkan teknologi dengan modus pencurian, manipulasi data digital dan lain sebagainya (Nuh Al-Azhar, 2012a). Pada saat ini, tingkat kejahatan komputer meningkat signifikan, menurut situs penelitian ID-CERT dalam laporan (Dwi, 2018) diperoleh data terkait pengaduan kejahatan komputer pada tahun 2018.



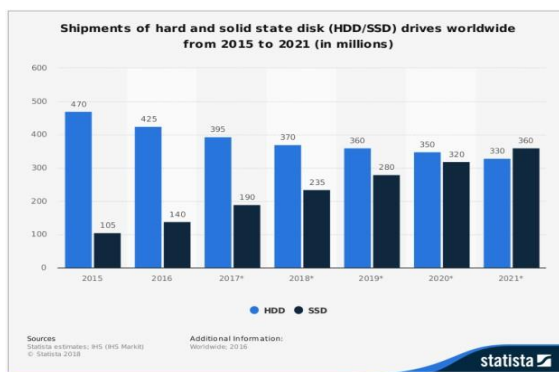
Gambar 1.1 Pengaduan Per Kategori Kejahatan Komputer

Pada saat ini, forensik digital sebagai bidang ilmu dimana proses ilmu tersebut digunakan untuk menyelidiki bukti digital, bertujuan untuk pengumpulan atau mengembalikan bukti digital dan analisis bukti digital tersebut, yang terdapat pada kejahatan komputer melalui perangkat komunikasi seperti smartphone, tablet, laptop atau pengguna komputer lainnya.

Perkembangan teknologi komputer dituntut akan kecepatan akses dalam pengoperasiannya salah satunya yaitu dengan media penyimpanan SSD. SSD adalah kepanjangan dari *Solid State Drive*, prinsip SSD sama seperti HDD yaitu untuk menyimpan data. Tetapi informasi pada data tidak disimpan pada piringan magnetis layaknya HDD. Sedangkan SSD menyimpan semua data informasi pada *chip-chip memory flash*¹. SSD merupakan memori yang bersifat *non-volatile*. Pada saat ini perusahaan beralih menggunakan SSD karena performa SSD tersebut sangat tinggi, ukuran yang baik dari segi fisik, dan efisiensi konsumsi daya sebagaimana yang disebutkan oleh (Ramadhan, Prayudi,

¹ <https://www.it-jurnal.com/pengertian-ssd/>

& Sugiantoro, 2016). Berikut ini merupakan survei mengenai perkembangan *Solid State Drive* diseluruh dunia yang diterbitkan oleh statista.com.



Gambar 1.2 Statistik Perkembangan Penggunaan SSD

Gambar 1.3 adalah perkembangan SSD, SSD saat ini memiliki teknologi media penyimpanan yang baru yaitu *Solid State Drive Non-volatile Memory Express* (SSD NVMe) yang menggunakan interface PCIe (*Peripheral Component Interconnect Express*) yang berbeda dengan *interface* SSD SATA, dimana PCIe dapat melakukan perpindahan data yang lebih cepat dibandingkan dengan *interface* SATA.

Solid State Drive memiliki fitur bernama TRIM. Fitur TRIM memungkinkan Sistem Operasi untuk memberitahu SSD terkait block mana saja yang sudah tidak digunakan. Ketika akan melakukan proses *write*, tidak perlu melakukan proses penghapusan. Menurut (Geier, 2015) TRIM berfungsi menghapus blok yang telah ditandai untuk dihapus oleh sistem operasi. Sehingga fitur TRIM membantu menjaga agar performa *write* di *drive* SSD terjaga lebih baik². Sistem Operasi Windows 10 saat ini sudah terpasang secara *default* fungsi TRIM dengan *mode enable*, fungsi TRIM secara otomatis akan menghapus data lama pada sektor sebelum ditempatkan data baru, Sehingga SSD akan melakukan proses *write* data secara optimal. Akan tetapi dengan adanya fitur TRIM ini, SSD memiliki efek atau nilai negatif bagi bidang forensik digital untuk analisis forensik khususnya pada *recovery* data.

Dalam penelitian sebelumnya, terdapat beberapa penelitian tentang teknik *forensic* pada HDD. Pada proses tersebut dilakukan akuisisi pada mesin virtual *server* menggunakan metode *live forensic*. *Live forensic* adalah sebuah proses forensik dilakukan dengan cara mengumpulkan informasi, menganalisis dan mempresentasikannya menggunakan *tools forensic* pada saat sistem sedang berjalan (on) (Riadi & Rauli, 2019). Dengan metode *live forensic* tersebut berhasil melakukan akuisisi tanpa mengganggu sistem operasi yang lain, mengangkat file yang ada dalam partisi tersebut, dapat dibaca oleh *software forensic* yaitu

² <https://harry.sufehmi.com/2015/10/07/tentang-ssd-di-server/>

belkasoft dan *autopsy* serta beberapa file yang telah dihapus dapat ditemukan kembali (Soni, Sudyana, Prayudi, Mukhtar, & Sugiantoro, 2019).

Kemudian, terdapat beberapa penelitian tentang teknik *forensic* yang menggunakan SSD SATA. SSD SATA yang terfrozen dijadikan barang bukti digital dengan metode *static forensic*, penelitian tersebut menggunakan *tools Recovery my file, Belkasoft, Forensic toolkit (FTK)* dan *Encase*. Kemudian hasil pemeriksaan dari SSD SATA yang ter-frozen tidak semua file dapat diperoleh dari 85 file yang *recovery* hanya 28,7 % (Riadi, Umar, & Nasrulloh, 2018). Selain itu terdapat *interface* lain SSD SATA yaitu NVMe melakukan uji coba antrian perintah (*command*), *queuing interface*, perbandingan *power* dan sifat pada SSD SATA dan NVME (Sivashankar, Scholar, & S, 2015).

Dari beberapa penelitian sebelumnya terdapat permasalahan yang terjadi pada SSD yaitu permasalahan tentang fitur TRIM. Fitur TRIM memiliki nilai negatif pada analisis *forensic* khususnya untuk *recovery data*. Hal ini mengakibatkan penyidik sulit mendapatkan data yang dibutuhkan. Fungsi TRIM akan membersihkan secara otomatis setiap sektor data yang tidak terpakai, sehingga dalam proses *recovery data* dengan *tools forensic* seperti *belkasoft* dan *autopsy* akan sulit mendapatkan data yang telah terhapus, karena sistem *controller* memori pada SSD telah memutuskan kapan dan berapa banyak blok ditandai untuk penghapusan (Ramadhan et al., 2016). Dengan menerapkan metode *live forensic* nantinya akan mampu meningkatkan hasil *recovery data* dari fungsi TRIM pada SSD NVMe. Sehingga membantu penyidik dalam mendapatkan informasi yang dibutuhkan.

Dari permasalahan tersebut maka perlu dilakukan penelitian untuk melakukan pengujian pada SSD NVMe dengan menerapkan metode *live forensic* untuk mengetahui sejauh mana penerapan teknik akuisisi *recovery data* SSD NVMe fitur TRIM. Harapannya adalah dengan mengangkat bukti digital atau informasi maka akan berguna untuk kepentingan penyidik. Pada penelitian ini, solusi yang akan ditawarkan terkait kebutuhan *recovery data* dalam proses teknik akuisisi menggunakan SSD NVMe dengan fitur TRIM yaitu menerapkan metode *live forensic* dan *tools forensic* seperti *Belkasoft, Forensic toolkit (FTK), Autopsy* dan *tools recovery Testdisk*.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka yang menjadi rumusan masalah adalah sebagai berikut:

- a. Bagaimana penerapan metode *live forensic* untuk akuisisi SSD NVMe dengan fitur TRIM ?
- b. Bagaimana proses pemeriksaan dan analisis pada SSD NVMe dengan fitur TRIM ?
- c. Apakah hasil imaging dari fitur TRIM dapat dibaca oleh tool forensik dan dapat merecovery file yang telah terhapus ?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan penelitian ini adalah sebagai berikut:

- a. Menerapkan metode *live forensic* untuk mengakuisisi dan *recovery* SSD NVMe.
- b. Untuk proses pemeriksaan dan analisis pada SSD NVMe dengan fitur TRIM
- c. Untuk mengetahui hasil imaging dari fitur TRIM sehingga dapat dibaca oleh tool forensik dan dapat merecovery file yang telah terhapus

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini meliputi:

- a. Sistem Operasi yang digunakan pada penelitian ini adalah Windows 10 file system NTFS.
- b. Tools yang digunakan dalam kebutuhan *recovery* file adalah *Forensic toolkit Portable (FTK)*, *Autopsy*, *Belkasoft* dan *tools recovery Testdisk*.
- c. *Solid State Drive Non-volatile Memory Express* (SSD NVMe) yang digunakan dalam penelitian ini adalah SSD M.2 Adata NVMe dengan kapasitas 128GB
- d. Implementasi fitur TRIM pada SSD NVMe yang sudah terdapat pada sistem operasi Windows 10.
- e. Proses *live* akuisisi *recovery file* dilakukan melalui perangkat USB SSD SATA eksternal.
- f. Bentuk data yang akan diakuisisi hanya data *non-volatile*.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain:

- a. Dengan adanya penelitian ini, diharapkan dapat mengetahui sejauh mana kemampuan tools dalam proses *recovery* file pada SSD NVMe.
- b. Dengan adanya penelitian ini juga mempelajari dan mengetahui tingkat efektivitas dari masing-masing tools yang digunakan dalam *live* akuisisi *recovery* SSD NVMe.

1.6 Literatur Review

Storage SSD merupakan tantangan baru dalam digital *forensic*. Dalam penyelesaian kasus-kasus yang berhubungan dengan digital *forensic* membutuhkan sebuah eksperimen untuk membantu dan mempermudah investigasi pengumpulan barang bukti digital. Telah banyak penelitian dalam digital *forensic* yang membahas tentang *storage*.

Untuk mengkaji masalah tentang *storage* ada beberapa penelitian salah satunya yang dilakukan oleh (Ramadhan et al., 2016) yaitu proses forensik *recovery* data menggunakan metode static pada penelitian ini menganalisa terkait *recovery* data dan melakukan perbandingan karakteristik *Solid State Drive* dengan *Hard Disk* konvensional, dengan menerapkan SSD fungsi TRIM pada komputer fisik *operating system* Microsoft Windows 7. Penelitian ini menunjukkan tahapan-tahapan akuisisi SSD *forensic* mulai dari penghapusan *file*, hingga *file* yang telah terhapus *direcovery* kembali menggunakan *tools forensic*. Dengan metode yang sama penelitian tentang SSD juga dilakukan oleh (Nisbet, Lawrence, & Ruff, 2013) tentang komparasi implementasi *forensic* digital pada fitur TRIM yang diaktifkan lalu melakukan praktik *recovery file* pada *file system* NTFS dan Ext4. Setelah mendapatkan hasil dari beberapa fitur TRIM, akan dilakukan proses analisa secara konvensional dan bisa ditarik kesimpulan *recovery* data pada fitur TRIM menggunakan metode static tidak sepenuhnya data bisa *direcovery*. Dengan metode yang sama penelitian tentang SSD SATA juga dilakukan oleh (Riadi et al., 2018) SSD SATA dengan *software* pembeku (*shadow defender*) untuk pengembalian bukti digital menggunakan metode *static, framework* yang digunakan adalah NIJ dan format file sistem SSD adalah NTFS. Penelitian tersebut menggunakan tools forensik seperti *FTK Imager, OSForensic, Autopsy, Winhex*. Hasil *recovery* file pada *software* pembeku akan sangat sulit untuk melakukan *recovery*, keberhasilan *recovery* file adalah 28,7%. Hasil dan metode yang sama diperoleh dari (Hadi & Riadi, Imam, 2019) penelitian tentang SSD interface NVMe implementasi fungsi TRIM menggunakan framework NIST dengan tahapan Collection, Examination, Analysis, dan Reporting. Hasil *recovery* yang diperoleh dengan fungsi TRIM disable, sebagian data yang dihapus dapat *direcovery*. Sedangkan TRIM enable, data yang dihapus tidak dapat *direcovery*.

Selain menggunakan metode *static* proses *recovery* data bisa dilakukan menggunakan metode *live forensic* seperti penelitian dilakukan (Soni et al., 2019) melakukan analisis tahapan-tahapan prosedur akuisisi berdasarkan standar SNI 27037:2014 dari *Virtual Machine Proxmox* jenis *Server* dengan melakukan teknik-teknik akuisisi dan menerapkan metode *live forensic* untuk melakukan pengembalian data saat virtual server sedang berjalan, akuisisi tersebut menggunakan *tools Autopsy* dan *Belkasoft*. *Tools* forensik untuk mempermudah proses analisis barang bukti digital *Proxmox*. Untuk *operating system* yang digunakan mesin virtual adalah *Ubuntu 16.04* dan *Microsoft Windows 10*. Penelitian untuk melakukan perbandingan antara *method static forensic* dan *live forensic* yang dilakukan oleh (Rafique & Khan, 2013) tujuannya untuk menerapkan metode yang efektif dengan *tools* forensik yang sesuai dari permasalahan yang ada. Sehingga dengan banyaknya melakukan perbandingan metode dalam setiap permasalahan dapat mencari kelemahan dan dapat menghubungkan dari masing-masing metode terkait.



Tabel 1.1 Rangkuman *Review* Penelitian

Paper Utama	Isu	Metode	Storage yang digunakan			OS		Tools yang digunakan	Target
			HDD	SSD SATA	SSD NVMe	Windows	Ubuntu		
(Kaur, Singh, 2012)	Penjabaran teknik pada proses digital forensik dalam penggunaan tools	Melakukan analisis dan perbandingan tools	-	-	-	√	√	<i>FTK, Encase, Autopsy</i>	HDD
(Rafique & Khan, 2013)	Implementasi <i>live forensic</i> dan static	Membandingkan teknik dan penjabaran terkait static forensic dan <i>live forensic</i>	-	-	-	-	-	-	Bukan penelitian eksperimental
(Nisbet et al., 2013)	Analisis akuisisi SSD multi platform	Analisis <i>recovery</i> data dengan skenario eksperimen	-	√	-	√	√	-	SSD File Sistem : Windows (NTFS), linux (Ext4), Mac Os (HFS+)
(Sivashankar et al., 2015)	Melakukan uji coba antrian perintah (command), queuing interface, perbandingan power	-	√	√	√	-	-	-	Bukan penelitian experimental

Tabel 1.2 Rangkuman *Review* Penelitian (Lanjutan)

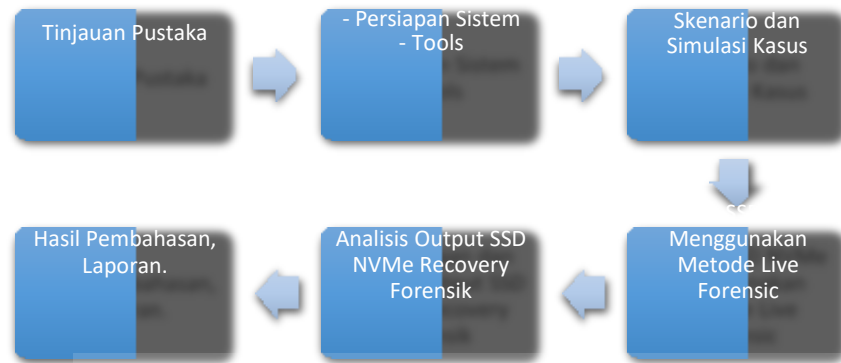
Paper Utama	Isu	Metode	Storage yang digunakan			OS		Tools yang digunakan	Target
			HDD	SSD SATA	SSD NVMe	Windows	Ubuntu		
(Shah, Mahmood, & Slay, 2015)	Akuisisi beberapa merk SSD	Analisis pengembalian data		√		√			SSD, Garbage Collection, TRIM, Encryption & Compression
(Soni et al., 2019)	Menerapkan Freamwork SNI untuk Akuisisi virtual mesin server	Metode <i>Live forensics</i>	√				√	<i>Belkasof, Autopsy</i>	<i>Recovery</i> HDD : file type .docx, .zip, .jpg, .xlsx.
(Ramadhan et al., 2016)	Implementasi forensik digital pada fitur TRIM	Metode Static		√		√		<i>FTK, Autopsy, Belkasoft</i>	<i>Recovery</i> SSD file sistem NTFS : TRIM support, file type : .mkv, .rar, .mp3, .exe,
(A. Faiz & Imam, 2017)	Melakukan analisis storage yang dibekukan pada windows XP	Metode Static	√				√	<i>DC3DD, Autopsy, WinHex, Photorec, Foremost</i>	HDD : Deep Freeze. File dokument digital, gambar, log history, log file

Tabel 1.3 Rangkuman *Review* Penelitian (Lanjutan)

Paper Utama	Isu	Metode	Storage			OS		Tools yang digunakan	Target
			HDD	SSD SATA	SSD NVMe	Windows	Ubuntu		
(Riadi et al., 2018)	Menerapkan freamwork NIJ dan software pembeku pada komputer.	Metode Static		✓		✓		<i>OSForensics, Autopsy, WinHex,</i>	SSD : Shadow Defender. <i>Recovery</i> file dokument, file gambar, file multimedia, file aplikasi, file log, history internet
(Sudyana & Lizarti, 2019)	Menerapkan freamwork SNI dan sistem IAAS cloud computer	Metode Live Forensics	✓			✓	✓	<i>Autopsy</i>	HDD : server proxmox, extensi file :.xlsx, .jpg, .pdf, .docx
(Hadi & Riadi, Imam, 2019)	Menerapkan freamwork NIST untuk akuisisi fitur TRIM	Metode Static			✓	✓		<i>Autopsy dan Recovery MyFile</i>	SSD : file dokumen, file multimedia, file gambar
Usulan Penelitian	Menerapkan Metode Live Forensic Untuk Akuisisi Pada <i>Solid State Drive</i> (SSD) NVMe Fitur TRIM	Penerapan Metode Live Forensics			✓	✓		<i>Belkasoft, FTK Portable Imager, Autopsy dan tools recovery, Recovery, Testdisk.</i>	SSD : TRIM <i>enable/disable</i> . <i>Recovery</i> file : .3gp, .exe, .avi, .bmp, .gif, .flv, .mpg, .webm, .jpg, .xlsx, .pptx, .doc, .docx, .mov, .mp3, .mp4, .ogg, .odt, .pdf, .png, .txt, .7z, .zip, .mww
		Penelitian yang akan dilakukan adalah melakukan penelitian terkait <i>forensic storage</i> menggunakan <i>Solid State Drive NVMe</i> . Dengan menerapkan metode <i>live forensic</i> dan variasi <i>tools forensic recovery</i> untuk akuisisi SSD NVMe fitur TRIM ini diharapkan menjadi solusi dan acuan investigator dalam mengakuisisi saat menggunakan SSD NVMe sesuai dengan permasalahan yang ada.							

1.7 Metode Penelitian

Langkah-langkah yang ditempuh untuk melakukan penelitian ini adalah sebagai berikut :



Gambar 1.3 Alur Metode Penelitian

1.8 Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut:

BAB I Pendahuluan

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II Kajian Teori

Pada Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

BAB III Metodologi Penelitian

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antar muka aplikasi yang akan dibuat.

BAB IV Pembahasan

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

BAB V Penutup

Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam

mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.



BAB 2

Tinjauan Pustaka

2.1 Digital Forensik

Forensik digital merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer yang digunakan dalam kepentingan pembuktian hukum, untuk melakukan pembuktian kejahatan dengan menggunakan teknologi atau komputer secara ilmiah hingga mendapatkan bukti digital yang digunakan untuk menjerat pelaku kejahatan (Nuh Al-Azhar, 2012b).

Menurut (Prayudi, 2014) dalam jurnal Seminar Nasional Sains dan Teknologi Informasi-ISSN : 2355-536X yang berjudul *Problema dan Solusi Digital Chain of Custody Dalam Proses Investigasi Cybercrime*, salah satu faktor penting dalam forensik digital untuk proses investigasi yaitu barang bukti. barang bukti tersebut memiliki dua istilah yang hampir sama, yaitu barang bukti digital dan barang bukti elektronik. Barang bukti digital adalah barang bukti yang diekstrak dari barang elektronik (email, sms, file, video, log, teks, gambar). Sedangkan barang bukti elektronik adalah barang bukti yang bersifat fisik (*handphone, hardisk, radio, komputer, kamera digital, dan lain-lain*).

Tabel 2.1 Barang Bukti Digital dan Elektronik

NO	Barang Bukti Elektronik	Barang Bukti Digital
1	Komputer PC	Logical file
2	Laptop/notebook, netbook, tablet	Deleted file
3	Handphone, smartphone	Lost file
4	Flashdisk/thumb drive	File slack
5	Floppydisk	Log file
6	Harddisk	Encrypted file
7	CD/DVD	Steganography file
8	Router, switch, hub	Office file
9	Kamera video, cctv	Audio file
10	Kamera digital	Video file
11	Digital recorder	Image file
12	Music/video player, dan lain-lain	Email
13		User ID dan password
14		Short message service
15		Call logs

Forensik digital merupakan salah satu bidang spesialis pemahaman komputer yang sangat luas. Forensik digital menjadi salah satu bentuk spesialisasi untuk melakukan investigasi yang berhubungan dengan kejahatan komputer. Forensik digital mengacu pada proses akuisisi, pelestarian, analisis, dan penyajian bukti digital yang dihasilkan dari kejahatan terkait digital (Sant, 2014). Forensik digital akan melakukan pemeriksaan setiap barang bukti elektronik dalam rangka mencari data-data digital yang berkaitan dengan kasus kejahatan dan pelakunya.

Dalam ilmu forensik digital, seorang ahli dalam bidang forensik digital harus memahami prinsip-prinsip dasar. Hal ini menjadi dasar seorang ahli forensik digital dalam melakukan investigasi kejahatan komputer. Menurut (ACPO, 2012), prinsip-prinsip dasar forensika digital adalah :

- a. Sebuah lembaga hukum atau petugasnya dilarang mengubah data-data digital yang tersimpan dalam media penyimpanan yang selanjutnya akan dibawa ke pengadilan.
- b. Untuk seorang yang merasa perlu mengakses data digital yang tersimpan dalam media penyimpanan barang bukti, maka orang tersebut harus jelas kompetensi, relevansi, dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
- c. Terdapat catatan teknik dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan dan analisis berlangsung. Jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut akan mendapatkan hasil yang sama.
- d. *Person in charge* dari investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan juga analisis dan dapat memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

2.2 Investigasi Forensik Digital

Investigasi Forensik Digital atau *Digital Forensics Investigation* (DFI) merupakan sebuah upaya penyelidikan, pengusutan, pemeriksaan, pencarian, pengumpulan data, informasi dan temuan lainnya. Berdasarkan tahapan-tahapan prosedur ilmiah dan teknik khusus digunakan untuk mendapatkan barang bukti digital agar diterima dalam pengadilan (Kohn, Eloff, & Eloff, 2013).

Siklus investigasi forensik digital yang diterbitkan oleh (Nasional, 2014) ada 4 tahapan yaitu identifikasi, pengumpulan, akuisisi, dan preservasi. Siklus tersebut dijelaskan pada gambar 2.1.



Gambar 2.1 *Digital Forensic Investigation Process* (SNI 27037:2014)

1. Identifikasi

a. Perencanaan Investigasi

Perencanaan investigasi ini diatur oleh SNI pada bagian 6.7.2. Perencanaan dilakukan untuk menyusun strategi terkait investigasi yang akan dilakukan. Mulai dari perencanaan tools yang digunakan, perencanaan teknis investigasi, dan hal terkait lainnya.

b. Persiapan dan pengarahan *team*

Persiapan dan pengarahan *team* diatur oleh SNI pada bagian ke 6.7. Persiapan dilakukan dengan mempersiapkan seluruh kebutuhan baik itu hal administrasi maupun hal teknis untuk proses investigasi. Pengarahan *team* dilakukan untuk memastikan seluruh anggota *team* investigasi paham dengan kasus yang akan ditangani, apa yang harus dilakukan dan tidak dilakukan selama investigasi, dan meningkatkan untuk selalu menjaga integritas barang bukti.

c. Penilaian resiko keamanan TKP

Hal ini diatur dalam SNI pada bagian ke 6.2.2. Penilaian resiko dilakukan untuk menjaga keamanan *team* investigasi dan barang bukti. Sebagai contoh untuk menilai apakah di TKP terdapat senjata atau material yang dapat menyebabkan kerusakan fisik.

d. Pengamanan TKP

Hal ini diatur dalam SNI pada bagian ke 6.2.1. Pengamanan TKP dilakukan untuk melindungi barang bukti. Pengamanan juga dilakukan untuk membatasi tidak semua orang bisa masuk ke TKP dan hanya orang-orang yang telah diizinkan oleh *team*.

e. Pencarian barang bukti

Hal ini diatur dalam SNI pada bagian ke 5.4.2. Pencarian barang bukti merupakan proses dimulainya melihat keseluruhan TKP dan mencari apa saja yang berpotensi barang bukti.

f. Identifikasi barang bukti

Hal ini diatur dalam SNI pada bagian ke 5.4.2. Melakukan identifikasi baik itu dari sisi jenis, bentuk, dan fungsinya terhadap barang bukti yang ditemukan dari hasil pencarian apakah bisa menjadi barang bukti yang berpotensi. Identifikasi juga

melakukan pengecekan terhadap status barang bukti yang ditemukan semisal apakah dalam keadaan menyala atau tidak.

g. Menentukan prioritas barang bukti

Hal ini diatur dalam SNI pada bagian 6.8. Memberikan prioritas terhadap barang bukti yang ditemukan terhadap aspek kerentanan data tersebut. Barang bukti yang mudah hilang seperti data dalam RAM yang hilang jika komputer mati harus diberikan prioritas. Sehingga barang bukti dengan prioritas tinggi diberikan tindakan yang lebih.

h. Dokumentasi

Hal ini diatur dalam SNI pada bagian ke 6.6. Segala aktivitas terkait penemuan barang bukti harus didokumentasikan. Dan dokumentasi disini juga mencakup keseluruhan aspek proses yang dilakukan mulai tahapan identifikasi sampai tahapan akhir investigasi yang harus selalu didokumentasikan. Dokumentasi dilakukan untuk menjaga integritas barang bukti.

i. Pencatatan barang bukti (*Chain of Custody*)

Hal ini diatur dalam SNI pada bagian 6.1. *Chain of custody* merupakan catatan rantai perjalanan barang bukti. Jika ketika barang bukti ditemukan, harus dicatat informasinya dan selanjutnya kemana saja barang bukti tersebut berpindah atau apa saja yang dilakukan terhadap barang bukti harus dicatat di *form chain of custody*. Hal ini juga dilakukan untuk menjaga integritas barang bukti.

2. Pengumpulan

a. Menentukan barang bukti disita atau diakuisisi di TKP

Hal ini diatur dalam SNI pada bagian 6.8 dan 7.1.1.3. Dari hasil pemberian prioritas barang bukti, akan ditentukan apakah barang bukti yang ditemukan dapat langsung disita atau harus diakuisisi di TKP terkait datanya yang mudah hilang.

b. Melakukan penyitaan barang bukti

Hal ini diatur dalam SNI pada bagian ke 7.1.2. Penyitaan barang bukti dibagi menjadi dua tahapan yaitu prosedur penyitaan perangkat dalam keadaan menyala dan dalam keadaan mati.

(1) Barang bukti dalam keadaan menyala

- Menganalisis apakah membutuhkan data *volatile* dari perangkat.

Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Analisis dilakukan untuk menentukan apakah dari perangkat yang menyala tersebut membutuhkan data *volatile* yang akan hilang apabila perangkat dimatikan.

- Jika butuh lakukan prosedur *live* akuisisi.

Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Jika hasil analisis menyimpulkan dibutuhkan data *volatile*, maka lakukan prosedur *live* akuisisi terhadap perangkat.

- Jika tidak butuh lakukan pemeriksaan aspek keamanan dan kerentanan data terhadap listrik.

Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Jika tidak butuh data *volatile*, atau proses *live* akuisisi telah selesai, lakukan pemeriksaan aspek keamanan data apakah data akan rusak apabila perangkat langsung dimatikan. Jika ternyata data akan rusak jika perangkat langsung dimatikan, lakukan prosedur *shutdown* secara sistem normal.

- Melakukan prosedur *shutdown* perangkat.

Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Jika data stabil atau tidak bermasalah apabila perangkat langsung dimatikan, cabut secara langsung kabel power untuk mematikan perangkat.

(2) Barang bukti dalam keadaan mati

- Cabut semua kabel yang terkoneksi dan baterai (jika ada baterai)

Hal ini diatur dalam SNI pada bagian ke 7.1.2.2. Cabut semua kabel dan amankan kabel tersebut, lalu label seluruh *port* yang terkoneksi dengan kabel untuk memudahkan proses rekonstruksi. Setelah prosedur ini selesai, maka lakukan prosedur selanjutnya yaitu memberikan label barang bukti.

c. Memberikan label barang bukti

Hal ini diatur dalam SNI pada bagian ke 7.1.2. Label seluruh barang bukti untuk memudahkan proses rekonstruksi dan memudahkan mengenali barang bukti tersebut.

d. Mempacking barang bukti

Hal ini diatur dalam SNI bagian 7.1.2. proses pengemasan barang bukti dengan memasukkan barang bukti ke dalam alat pembungkus barang bukti. Perhatikan aspek keamanan barang bukti ketika akan dikemas. Sebagai contoh, perangkat yang terkoneksi ke jaringan *wireless* seperti *smartphone* harus dikemas dalam alat pembungkus khusus yang dapat menetralkan sinyal tersebut.

e. Mengumpulkan keterangan verbal dari saksi-saksi

Hal ini diatur dalam SNI pada bagian ke 7.1.1.2. untuk mendapatkan petunjuk lebih dari mencari informasi terkait barang bukti yang ditemukan. Sebagai contoh menanyakan *password* sistem yang ditemukan dalam barang bukti.

3. Akuisisi

a. Pemeriksaan aspek keamanan barang bukti

Hal ini diatur dalam SNI pada bagian ke 7.1.1.1. Pemeriksaan aspek keamanan untuk memastikan bahwa proses akuisisi yang dilakukan tidak akan merusak barang bukti.

b. Penentuan model akuisisi yang dilakukan

Hal ini diatur dalam SNI pada bagian ke 7.1.3. Proses akuisisi terbagi menjadi 3 jenis yaitu akuisisi pada perangkat menyala, akuisisi pada perangkat yang tidak menyala dan partial akuisisi. Penentuan model akuisisi yang digunakan sesuai hasil identifikasi yang telah dilakukan terhadap barang bukti.

(1) Akuisisi pada perangkat yang menyala

- Lakukan prosedur *live* akuisisi untuk mendapatkan data *volatile*.

Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Data *volatile* akan dapat hilang apabila perangkat digitalnya dimatikan, oleh karena itu *live* akuisisi dilakukan ketika perangkat digitalnya dimatikan, oleh karena itu *live* akuisisi dilakukan ketika perangkat masih dalam keadaan menyala. Beberapa contoh data *volatile* yaitu data di RAM, data proses yang berjalan, data koneksi jaringan. Petugas harus berkompentensi dan menggunakan *tools* yang valid untuk melakukan prosedur ini.

- Jika data *non volatile* juga dibutuhkan saat itu, lakukan juga prosedur akuisisi pada data *non volatile*.

Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Lakukan juga prosedur *live* akuisisi jika data *non volatile* seperti data yang tersimpan di *logical* juga dibutuhkan.

- Jika perangkat bisa disita, lakukan prosedur pengumpulan barang bukti.

Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Jika setelah proses akuisisi pada data *volatile* selesai dan perangkat dapat disita lakukan prosedur pengumpulan barang bukti. Perangkat yang tidak dapat disita sebagai contoh komputer *server* yang sangat krusial terhadap sistem yang sedang berjalan.

(2) Akuisisi pada perangkat yang tidak menyala

- Lakukan prosedur *static* akuisisi dengan melakukan imaging terhadap media penyimpanan data.

Hal ini diatur dalam SNI pada bagian ke 7.1.3.2. Proses *static* akuisisi dijalankan dengan melakukan *bitstream copy*.

(3) *Partial* akuisisi

- Dapat dilakukan dengan menggunakan perpaduan prosedur *live* dan *static* akuisisi.

Hal ini diatur dalam SNI pada bagian ke 7.1.3.4. *Partial* akuisisi dilakukan untuk perangkat yang krusial dan tidak dimungkinkannya melakukan akuisisi terhadap keseluruhan data seperti dikarenakan jumlah data yang sangat besar.

c. Pelaksanaan akuisisi

Setelah proses penentuan metode akuisisi dipilih, berikutnya adalah dilaksanakan proses akuisisi sesuai dengan metode akuisisi yang telah ditentukan sebelumnya.

d. Verifikasi hasil akuisisi

Hal ini diatur dalam SNI pada bagian ke 7.1.4. Verifikasi dilakukan untuk memastikan data hasil akuisisi identic dengan data aslinya. Verifikasi dapat dilakukan dengan menggunakan fungsi hash.

4. Preservasi

a. Memberikan segel barang bukti

Hal ini diatur dalam SNI pada bagian ke 6.9.2. Barang bukti yang telah dipacking, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya dan berguna menjaga integritas barang bukti.

b. Pemeriksaan aspek keamanan pemindahan barang bukti

Hal ini diatur dalam SNI pada bagian ke 6.9.2. Pemeriksaan aspek keamanan dilakukan untuk memastikan barang bukti aman selama proses pemindahan barang bukti dari TKP ke tempat penyimpanan ataupun laboratorium. Pemeriksaan aspek keamanan mencakup pemeriksaan pengemasan barang bukti untuk menjaga pengemasan yang dilakukan tidak merusak barang bukti.

c. Pemindahan barang bukti

Hal ini diatur dalam SNI pada bagian ke 6.9.2. Selama proses pemindahan barang bukti, petugas harus berhati-hati dan selalu memperhatikan keamanan barang bukti. Selain itu juga harus melakukan update di *form chain of custody*.

d. Penyimpanan barang bukti

Hal ini diatur dalam SNI pada bagian ke 6.9.2. Barang bukti harus disimpan dalam tempat penyimpanan yang memiliki fasilitas keamanan yang baik dan fasilitas penyimpanan yang memiliki fasilitas kemanan yang baik dan fasilitas penyimpanan yang baik. Sebagai contoh harus memiliki fasilitas untuk menjaga suhu ruangan penyimpanan tdak terlalu panas atau tidak terlalu dingin sehingga dapat menyebabkan kerusakan barang bukti.

2.3 SNI 27037:2014

SNI 27037:2014 yang berjudul Teknologi Informasi – Teknik keamanan – Pedoman identifikasi, pengumpulan akuisisi, dan preservasi bukti digital merupakan standar forensik digital yang keseluruhan isi dokumennya diadopsi dari ISO 27037:2012 dengan metode *republikasi-reprint*. SNI 27037:2014 merupakan standar nasional yang membahas tentang panduan spesifik terlibat aktivitas investigasi forensik digital. Aktifitas tersebut meliputi identifikasi, pengumpulan, akusisi, dan preservasi bukti digital telah mengatur prinsip dasar penanganan bukti digital, adapun prinsip dasar tersebut adalah :

- a. *Minimize handling of the original digital device or potential digital evidence,*
- b. *Account for any changes and document actions taken,*
- c. *Comply with the local rules of evidence,*
- d. *The DEFR and DES should not take actions beyond their competence.*

Digital Evidence First Responder (DEFR) yaitu seseorang yang memiliki wewenang, terlatih dan memenuhi persyaratan khusus sebagai pihak pertama yang bertindak di tempat kejadian perkara mengkoneksi dan mengakuisisi barang bukti digital sesuai dengan tanggung jawabnya. Sedangkan *Digital Evidence Specialist* (DES) adalah seseorang yang dapat melakukan tugas-tugas dari DEFR dan memiliki spesialisasi pengetahuan, keterampilan dan kemampuan untuk menangani berbagai masalah teknis forensik digital.

Berikut adalah langkah-langkah yang harus dilakukan DEFR dan DES dalam menangani bukti digital atau barang bukti digital :

- a. Mendokumentasikan semua aktifitas.
- b. Menentukan dan menerapkan metode yang akurat dan handal dalam proses penyalinan barang bukti digital berpotensi dari sumber aslinya.
- c. Menyatakan bahwa usaha penjagaan barang bukti digital yang berpotensi aman dari pihak-pihak yang tidak berwenang.

Semua proses ini merupakan proses penting yang harus dilakukan secara teliti dan hati-hati untuk tetap menjaga integritas barang bukti. Metodologi yang digunakan dalam pengumpulan barang bukti digital akan berpengaruh terhadap diterima atau tidaknya barang bukti tersebut di pengadilan. Selain membahas barang barang bukti digital, SNI juga membahas tentang panduan umum tentang bagaimana mengumpulkan non-digital *evidence*. Karena selain barang bukti digital, barang bukti yang tidak digital juga berpotensi memberikan petunjuk terkait investigasi sebuah kasus kejahatan (Nasional, 2014).

2.4 *Live Forensics*

Menurut (Rafique & Khan, 2013) digital forensik dibagi menjadi dua metode, yaitu live forensics dan static forensics. *Live forensics* merupakan proses forensik dilakukan dengan cara mengumpulkan data volatile (mudah hilang) dan menganalisis informasi barang bukti digital pada saat sistem sedang running (*on*). Live forensics bertujuan untuk melakukan analisa barang bukti tanpa mempengaruhi fungsionalitas sistem, sehingga keseluruhan fungsi yang dijalankan sistem tidak akan terganggu selama proses analisis digital dilakukan. Sedangkan static forensics menggunakan pendekatan konvensional yaitu barang bukti elektronik diolah menjadi bit-by-bit image untuk dilakukan proses forensik. Proses forensiknya sendiri berjalan pada sistem yang tidak running (*off*). Secara konvensional *static forensics* digunakan untuk investigasi hasil imaging dan menganalisis isi dari bukti digital, seperti file yang dihapus, history web browser, berkas fragmen, koneksi jaringan, file yang diakses, history login user.

Teknik *live forensics* telah berkembang dalam dasawarsa terakhir, seperti analisis konten memory untuk mendapatkan gambaran dan informasi yang lebih baik mengenai proses aplikasi yang sedang berjalan (Rahman & Khan, 2015). Teknik *live forensics* juga diterapkan pada Random Access Memory (RAM). Metode live forensic bertujuan agar penanganan investigasi lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan bisa dibaca dan kapasitas memori yang lebih minim apabila dibandingkan dengan teknik forensik tradisional (Yudhistira, 2018). Data pada RAM bersifat data volatile (data sementara) jika komputer mati maka data itu akan hilang. Data volatile ini berisi data penting seperti username dan password dalam suatu akun seperti email (M. N. Faiz, Umar, & Yudhana, 2017).

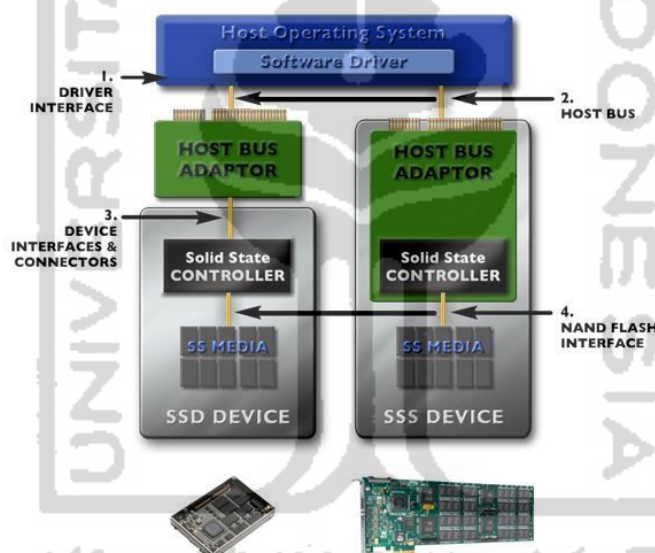
Kemudian menurut (Adelstein, 2006) teknik live forensics bisa dilakukan dengan cara mengumpulkan data ketika sistem yang terkena serangan dan sistem masih berjalan (*running*). Bukti digital forensik yang dikumpulkan melalui sistem yang berjalan tersebut dapat memberikan bukti yang tidak dapat diperoleh dari forensik konvensional (*static disk image*). Bukti digital yang dikumpulkan tersebut merupakan data yang bisa berubah-ubah dari sistem yang dinamis dan tidak mungkin untuk diproduksi ulang pada waktu berikutnya.

2.5 *Solid State Drive (SSD)*

SSD, atau dikenal *Solid State Drive* merupakan salah satu media penyimpanan selain Hardisk. Penyimpanan SSD menggunakan *non volatile memory* yaitu *memory* yang datanya dapat ditulis dan dihapus, tetapi data tetap ada walaupun dalam kondisi mati (*off*) karena

SSD tidak menggunakan disk magnetis seperti Hardisk tradisional. Berbeda dengan *volatile memory* yaitu datanya dapat ditulis dan dihapus, tetapi hilang saat kondisi mati (*off*) misalnya RAM.

SSD merupakan media penyimpanan data yang menggunakan *Integrated Circuit* (IC) yang dirakit sebagai memori untuk menyimpan data secara presenten³. Sedangkan HDD menggunakan magnetic disk atau komponen elektromekanis platter yang berputar, dan head yang akan bergerak untuk membaca dan menulis pada *disk* dengan menggunakan elektromagnetik yang berdampak oksidasi pada HDD meningkat. SSD bisa dianggap sebagai versi canggih dari USB Flash drive dengan kapasitas yang jauh lebih besar dan berfungsi sebagai pengganti HDD yang selama ini digunakan pada perangkat komputer⁴. Manfaat dari teknologi storage memori flash ini adalah performa kecepatan dibaca (*read*) atau ditulis (*write*) lebih baik tanpa menimbulkan suara dan panas yang dihasilkan bisa direduksi (Freeman & Woodward, 2009).



Gambar 2.2 Anatomi *Solid State Drive* (SSD)

2.6 Arsitektur *Solid State Drive* (SSD)

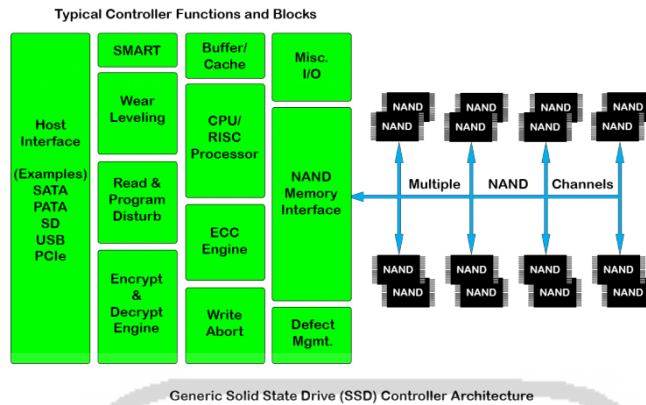
Arsitektur seperti HDD konvensional menggunakan penggerak motor listrik pada piringan disk silinder untuk dibaca (*read*) atau ditulis (*write*) pada head yang diposisikan di atas piringan disk, tetapi SSD menggunakan memori flash NAND⁵. Dampak dari teknologi

³ <https://www.gudangilmukomputer.com/2015/10/pengertian-dan-fungsi-solid-state-drive-ssd.html>

⁴ https://www.ubaya.ac.id/2018/content/articles_detail/219/Media-Penyimpanan-Data-Solid-State-Drive--SSD-.html

⁵ <https://www.anandtech.com/show/2738/5>

penyimpan tersebut tidak menghasilkan suara dan panas dari HDD konvensional. Berikut ini adalah skema arsitektur dari *Solid State Drive* (Larrivee, 2016) :



Gambar 2.3 Arsitektur *Solid State Drive*⁶

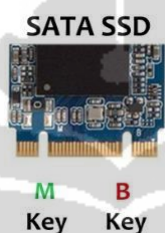
- a. Host Interface : host interface biasanya dirancang untuk interface khusus. Ada beberapa interface yang dirancang untuk mengatasi berbagai bentuk dan sistem, yang sering digunakan interface seperti SATA, SD, USB, PATA/ PCIe.
- b. SMART : berfungsi sebagai memantau dan merekam data mengenai banyaknya atribut SSD. Contohnya seperti memantau kemampuan dan mengukur daya tahan yang tersisa pada SSD.
- c. Wear Leveling : berfungsi untuk menyelaraskan jumlah cycles write di seluruh flash NAND yang tersedia. Karena setiap *block* NAND mempunyai jumlah siklus tulis/hapus yang terbatas, jika hanya satu blok fisik yang ditulis terus menerus maka akan cepat menghabiskan siklus ketahanan pada SSD tersebut.
- d. Encrypt & Decrypt Engine : berfungsi untuk keamanan aplikasi yang lebih tinggi, SSD sering menggunakan enkripsi seperti AES 256 yaitu algoritma cryptographic untuk mengamankan data.
- e. Buffer/Cache : pada umumnya buffer atau cache digunakan oleh DRAM, sebagai buffering data read dan write pada SSD, cache tersebut memiliki memory yang tidak stabil, maka data akan hilang jika daya hilang secara tak terduga.

⁶ <https://www.cactus-tech.com/resources/blog/details/solid-state-drive-primer-9-controller-architecture-controller-block-diagram/>

2.6.1 Connector Fisik M.2 SATA

Perkembangan dalam dunia komunikasi khususnya pada storage komputer lebih ditekankan ke SSD dibandingkan HDD konvensional sehingga sekarang vendor meluncurkan SSD yang berbentuk lebih kecil yang disebut M.2. Perlu diketahui bahwa interface M.2 tidak semua motherboard bisa support M.2 SSD, namun vendor komunikasi untuk sekarang sudah banyak meluncurkan *motherboard* yang lebih baru yang support SSD M.2. Untuk kompatibilitas SSD SATA (*Serial Advanced Tecnology Attachment*) umumnya menggunakan Slot B dan Slot M (Key B & Key M)⁷.

SSD M.2 dengan interface SATA menggunakan teknologi AHCI memiliki kecepatan perpindahan data kurang lebih sama dengan SSD 2.5” SATA. SATA adalah bus primer dari komputer yang di rancang untuk mentransfer data antara *motherboard* dan media penyimpanan data, mirip seperti *harddisk* dan optical drive didalam komputer (Ramadhan et al., 2016).



Gambar 2.4 Connector SSD M.2 Slot SATA

2.6.2 Connector Fisik M.2 NVMe

SSD M.2 memiliki teknologi terbaru menggunakan interface NVMe merupakan singkatan dari Non-Volatile Memory Express, NVMe bukan interface seperti SATA ataupun PCIe, tetapi NVMe telah update versi dari PCIe karena NVMe tetap menggunakan interface PCIe. Sebuah standar komunikasi yang dikembangkan khususnya pada *storage* SSD oleh vendor seperti ADATA, Samsung, Sandisk dan lainnya. Pada dasarnya, interface NVMe tersebut memiliki kemampuan serupa dengan SSD SATA, namun NVMe memiliki performa latency dan penggunaan CPU jauh lebih baik (Nikkel, 2016).

SSD M.2 NVMe hanya khusus memakai 4 jalur PCIe 3.0 dan menggunakan Slot M agar performa kecepatan transfer data, performa kecepatan protocol AHCI/SATA jauh lebih lambat dibandingkan protocol NVMe dikarenakan manajemen antriannya yang sangat baik (Xu et al., 2015).

⁷ <https://www.els.co.id/blog/mengenal-lebih-dekat-mengenai-ssd-m2/>



Gambar 2.5 Connector SSD M.2 Slot NVMe

Selanjutnya, untuk mengetahui efektivitas dari penggunaan perintah fungsi TRIM pada SSD NVMe akan dilakukan pada penelitian ini.

2.6.3 TRIM

Fitur TRIM adalah sebuah perintah yang langsung ditujukan kepada *firmware* dari SSD. Dukungan TRIM pada SSD diaktifkan secara default untuk sistem operasi Windows 10, 8 dan windows 7 tetapi di windows XP dan Vista tidak ada dukungan TRIM secara default atau tidak dapat berjalan secara optimal karna sistem operasi tersebut tidak bisa membedakan antara SSD atau HDD. TRIM adalah fitur pada SSD yang akan berhubungan dengan operating system, TRIM akan menyampaikan blok mana yang dianggap tidak digunakan dan menghapus data yang tersisa secara internal sehingga SSD dapat bekerja dengan optimal⁸.

TRIM memastikan saat sistem operasi mau menulis data baru di sektor yang sama, data yang lama akan terhapus atau akan ditimpa langsung di tempat data yang lama. Hal ini disebut dengan *overwriting*. Selain itu, fungsi TRIM juga akan membuat semua sektor yang dihapus dan diformat menjadi bersih. Kegiatan *overwriting* akan menimbulkan sampah data (*garbage collection*). *Garbage Collection* menimbulkan efek sebuah SSD akan membuat performa kecepatan SSD menurun seiring waktu berjalan, karena data lama masih ada sehingga membuat SSD harus memilah antara data lama dengan data yang baru. Hal tersebut membuat SSD melamban dalam membaca data (Chaurasia & Sharma, 2017).

Perintah TRIM sebenarnya perintah dari teknologi SSD yang dibuat oleh *host* sistem operasi yang kemudian teknologi SSD *controller* berkembang pada protocol SATA dan NVMe⁹. Oleh sebab itu ketika file dihapus dalam suatu sistem operasi, perintah TRIM dikirim ke *disk controller* dengan LBA (*Logical Block Addresses*) untuk pengapusan file. Selanjutnya SSD me-reset block-block yang menjadi ruang kosong tambahan. Sederhananya, fungsi TRIM adalah berguna untuk menghapus data secara permanen serta menambah usia penggunaan dari SSD.

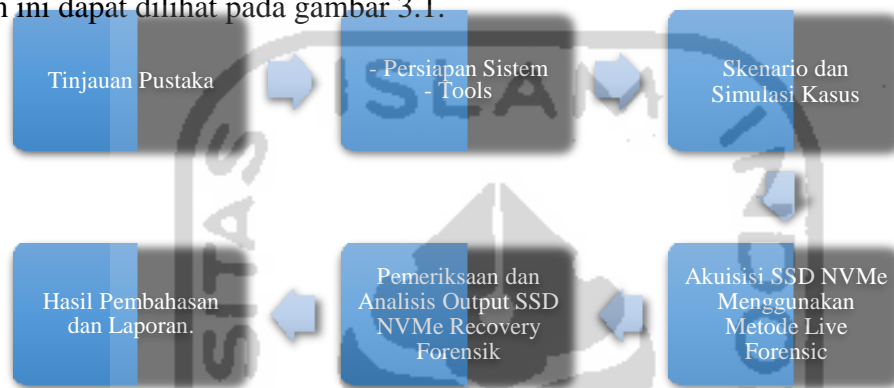
⁸ <https://www.pcplus.co.id/2014/05/tutorial/tip-agar-kinerja-ssd-optimal/>

⁹ <https://www.anandtech.com/show/2829/8>

BAB 3

Metode Penelitian

Bab ini menjelaskan bagaimana cara penelitian dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah atau tahapan-tahapan pada penelitian ini dapat dilihat pada gambar 3.1.



Gambar 3.1 Metodologi Penelitian

Pada gambar 3.1 menjelaskan bahwa metodologi penelitian ini menggunakan 6 tahapan yakni (1) Tinjauan Pustaka (2) Persiapan Sistem Mesin dan Tools (3) Skenario dan Simulasi Kasus (4) Akuisisi SSD NVMe Menggunakan Metode Live Forensic (5) Pemeriksaan dan Analisis Output SSD NVMe *Recovery* Forensik (6) Hasil Pembahasan dan Laporan.

3.1 Tinjauan Pustaka

Tinjauan pustaka dilakukan untuk mengumpulkan bahan-bahan informasi mengenai topik penelitian yang dapat bersumber dari buku, artikel, paper, jurnal, makalah, yang berupa teori, laporan penelitian, atau penemuan sebelumnya dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan teori-teori tentang digital forensik, barang bukti, *live forensic*, *Solid State Drive* (SSD) NVMe, sehingga dapat menunjang tujuan akhir dilakukannya penelitian ini.

3.2 Persiapan Sistem Mesin dan Tools

Merupakan tahapan dalam mempersiapkan spesifikasi hardware dan software yang digunakan dalam penelitian seperti melakukan perancangan dan implementasi analisis *Solid*

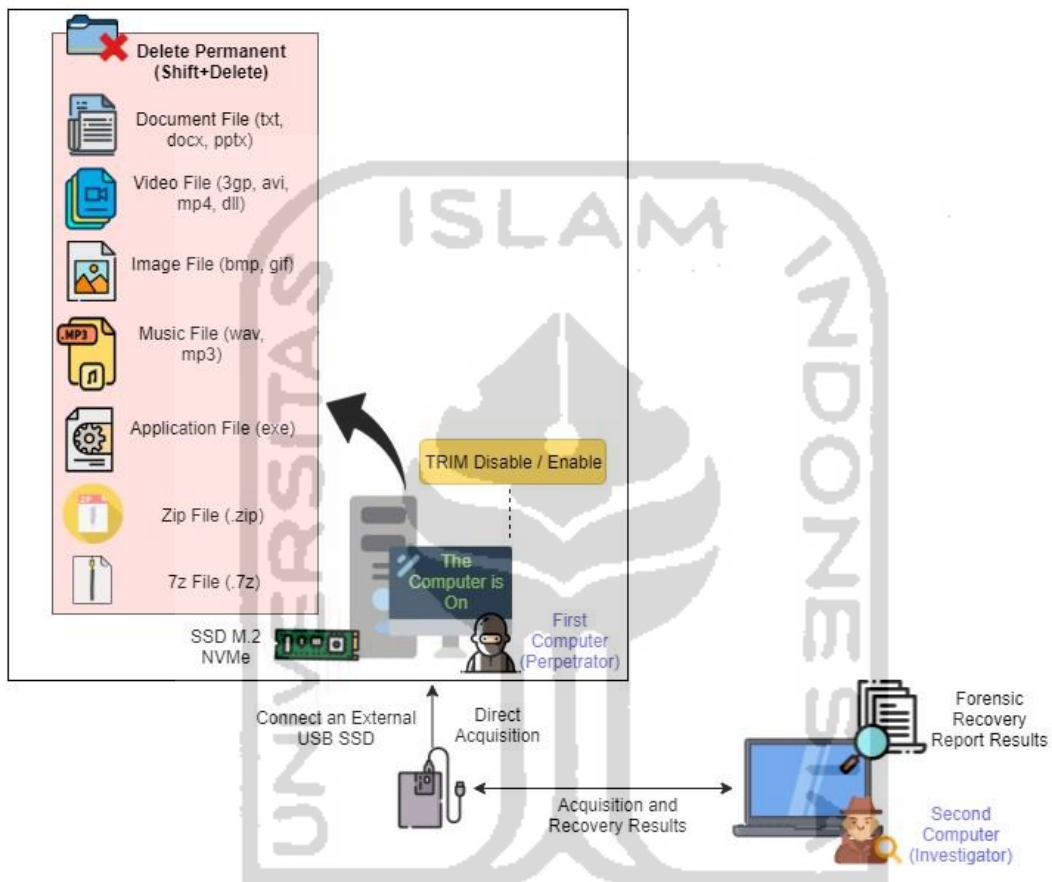
Sate Drive (SSD) Non-Volatile Memory Express (NVMe), seperti melakukan instalasi dan konfigurasi sistem, konfigurasi sistem operasi yang ada dalam komputer fisik yaitu microsoft windows 10 Pro. Agar implementasi eksperimental dapat berjalan dengan baik, maka perlu adanya *hardware* dan *software* komputer fisik sebagai alat dan bahan penelitian, berikut ini alat dan bahan yang digunakan dalam melakukan bahan penelitian eksperimen :

1. PC Pertama, Biostar seri H81MHV3 sebagai komputer simulasi dengan spesifikasi :
 - a. Processor Intel Pentium G3240 dengan kecepatan frekuensi 3.1GHz
 - b. RAM 6GB
 - c. Converter PCIe Card Support M.2 NVMe
 - d. Solid State Drive (SSD) M.2 NVMe Adata XPG SX6000 Lite dengan kapasitas 128GB
 - e. Sistem Operasi Windows 10 Professional dengan arsitektur 64bit
2. Laptop Kedua, Asus seri X455LN sebagai komputer pemeriksaan dan analisis dengan spesifikasi :
 - a. Processor Intel Core i5-4210U dengan kecepatan frekuensi 2.4GHz
 - b. RAM 8GB
 - c. HDD 1TB
 - d. Sistem Operasi Windows 10 Education dengan arsitektur 64bit
3. *Solid State Drive (SSD)* Apacer dengan kapasitas 240GB sebagai storage eksternal untuk melakukan live akuisisi dan recovery.
4. FTK Imager Porteble sebagai tool live akuisisi
5. Testdisk Recovery sebagai tools recovery
6. Sleuth Kit Autopsy Forensics sebagai tool pemeriksaan dan analisis
7. Belkasoft Evidence Center sebagai tool pemeriksaan dan analisis
8. Hashmyfile sebagai tool hashing

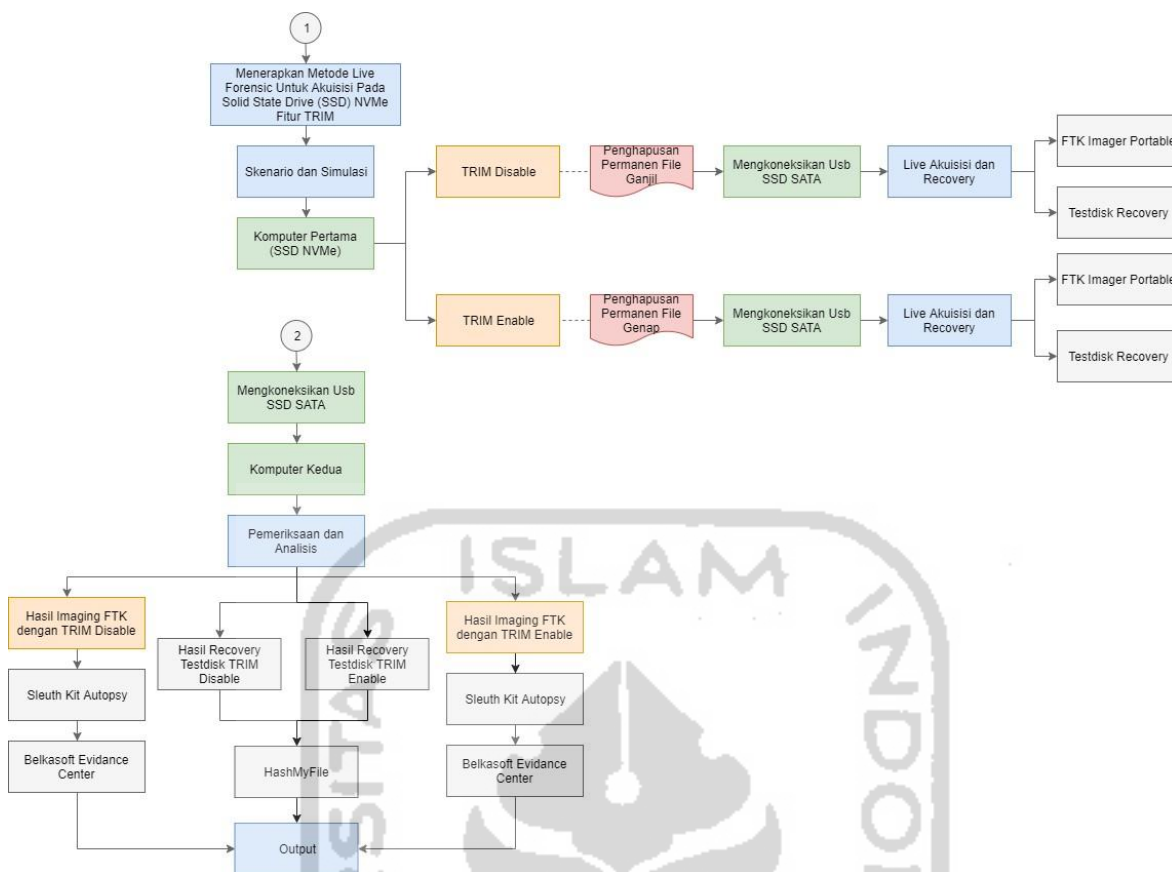
3.3 Skenario dan Simulasi Kasus

Merupakan tahapan dan membuat simulasi kasus dengan 2 komputer atau laptop yang digunakan dalam eksperimen ini. Komputer pertama akan dilakukan pemasangan SSD NVMe didalamnya menggunakan sistem operasi microsoft windows 10. Pada komputer tersebut akan dilakukan pembagian 2 partisi dimana partisi kedua digunakan untuk kebutuhan penyimpanan file yang akan dilakukan manipulasi. Kemudian pada komputer kedua sebagai laptop investigator untuk analisis hasil live akuisisi dan *recovery* SSD NVMe pada komputer pertama yang telah dilakukan skenario dan simulasi.

Untuk dilakukannya simulasi kasus pada eksperimen live akuisisi dan *recovery* SSD NVMe ini, peneliti melakukan simulasi sederhana yaitu penghapusan file dengan perintah SHIFT+DELETE dan kemudian file didalam partisi ke-dua tersebut akan dilakukan *recovery* data. Adapun alur tahapan skenario dan simulasi dapat dilihat pada gambar 3.2 dan 3.3 sebagai berikut :



Gambar 3.2 Tahapan Skenario SSD NVMe Live Forensik *Recovery*



Gambar 3.3 Tahapan Simulasi

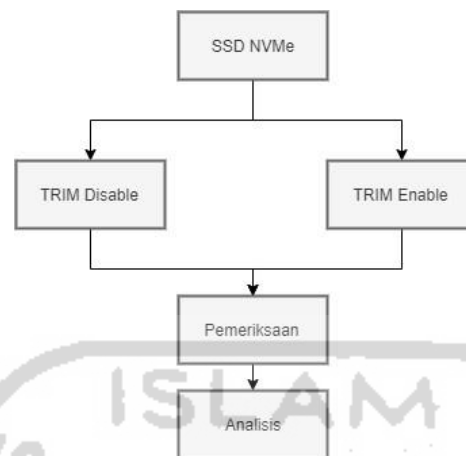
3.4 Akuisisi SSD NVMe menggunakan Metode *Live Forensic*

Pada tahapan ini dilakukan proses investigasi *live forensic* terhadap simulasi kasus komputer pertama yang menggunakan SSD NVMe dilakukan pembagian 2 partisi. Investigasi yang dilakukan diantaranya yaitu proses pencarian tempat penyimpanan pada partisi ke 2, live akuisisi *recovery*, melakukan pemeriksaan dan menganalisis data hasil akuisisi *recovery* tersebut.

Komputer pertama yang akan diakuisisi nantinya berjalan di atas sistem operasi windows 10 pro dan fungsi TRIM *disable* ataupun *enable*, kemudian file-file akan diakuisisi hanyalah file *non volatile* yang bersangkutan dengan kasus. Kemudian perlu dilakukan proses pencarian lokasi penyimpanan file dalam komputer pertama.

Selanjutnya menerapkan *live forensic* terhadap komputer pertama, karena dilakukannya dengan *live forensic* maka keadaan komputer sistem operasi windows 10 tidak dimungkinkan untuk dimatikan. Jika mematikan perangkat komputer tentu akan mematikan keseluruhan sistem yang sedang berjalan dan akan mengganggu keseluruhan sistem, maka peneliti perlu mengkoneksikan kabel usb SSD SATA (eksternal) untuk melakukan live

akuisi dan *recovery* data pada kasus tersebut. Tahapan investigasi forensik yang akan dilakukan untuk mengakuisisi SSD NVMe sebagai berikut :

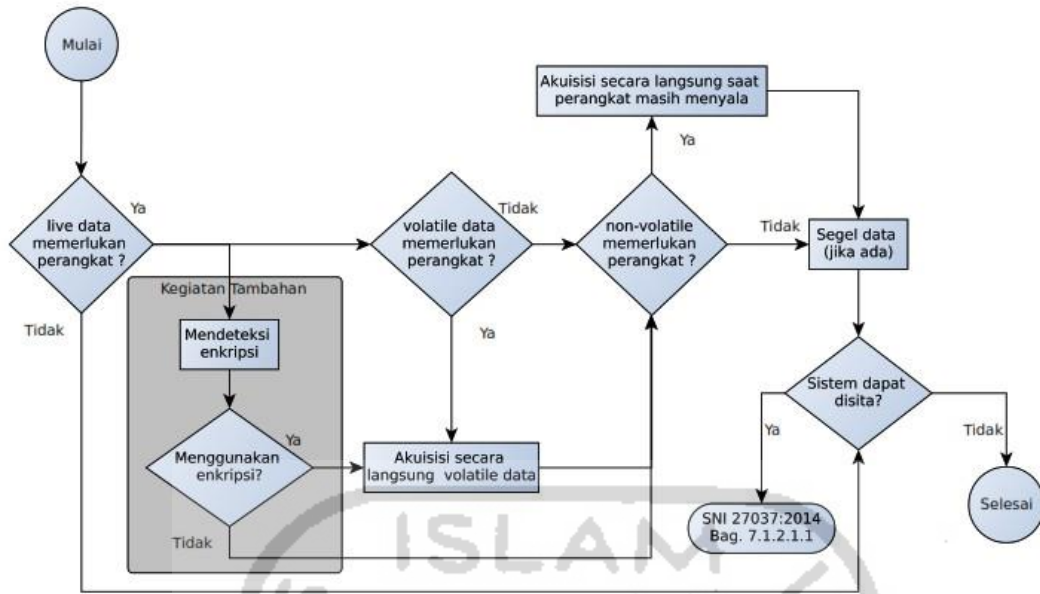


Gambar 3.4 Tahapan Investigasi SSD NVMe

Beberapa penelitian sebelumnya telah menggunakan prosedur akuisisi live forensik pada SNI 27037:2014 seperti yang dilakukan oleh (Sudyana & Lizarti, 2019). Dalam penelitian tersebut, dengan menggunakan prosedur live forensik SNI 27037:2014 dapat memberikan hasil yang optimal dalam menyelesaikan kasus yang dikerjakan. Dalam dokumen SNI tersebut sudah dijelaskan tahap-tahapan melakukan akuisisi pada perangkat digital, ada tiga kasus muncul jika akuisisi diperlukan yaitu :

1. Ketika perangkat digital masih dalam keadaan hidup/menyala.
2. Ketika perangkat digital ditemukan dalam keadaan mati.
3. Ketika perangkat digital dalam keadaan menyala tetapi tidak mungkin untuk dimatikan karena pentingnya perangkat digital.

Dari tiga kasus dalam dokumen SNI 27037:2014, *Digital Evidence First Responder* (DEFRR) perlu membuat salinan barang bukti digital yang diduga mengandung barang bukti yang diperlukan. Adapun proses prosedur akuisisi yang tergambar pada gambar 3.5.

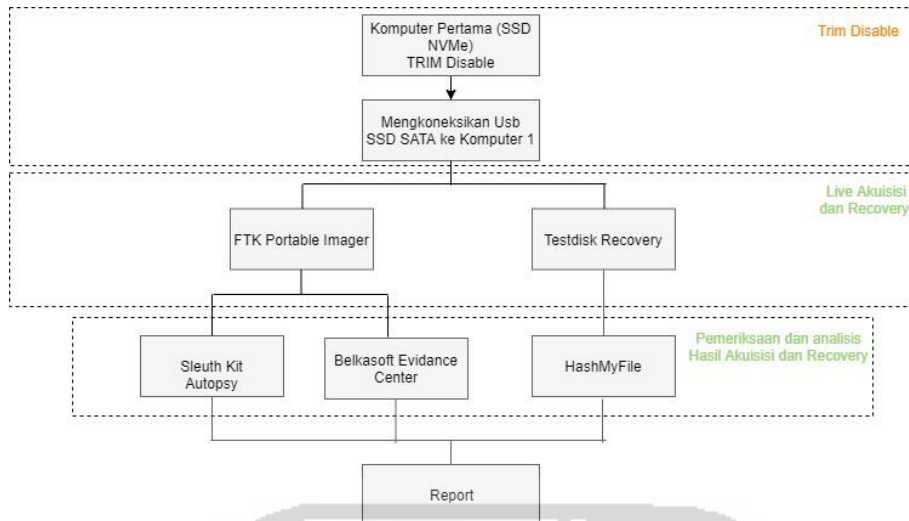


Gambar 3.5 Prosedur Akuisisi Perangkat dalam Kondisi Menyala SNI 27037:2014

Gambar 3.5 adalah proses tahapan yang akan digunakan untuk mengakuisisi SSD NVMe yaitu apakah *live data* diperlukan dalam perangkat digital, jika ya maka ketahapan selanjutnya, apakah *volatile data* diperlukan, karena yang akan diakuisisi hanya data yang *non-volatile* maka langsung ke tahapan *live* akuisisi *non-volatile* data pada perangkat digital yang sedang menyala. Setelah *live* akuisisi selesai dilakukan maka tahapan berikutnya adalah menyita hasil akuisisi.

3.4.1 Tahapan Akuisisi TRIM Disable

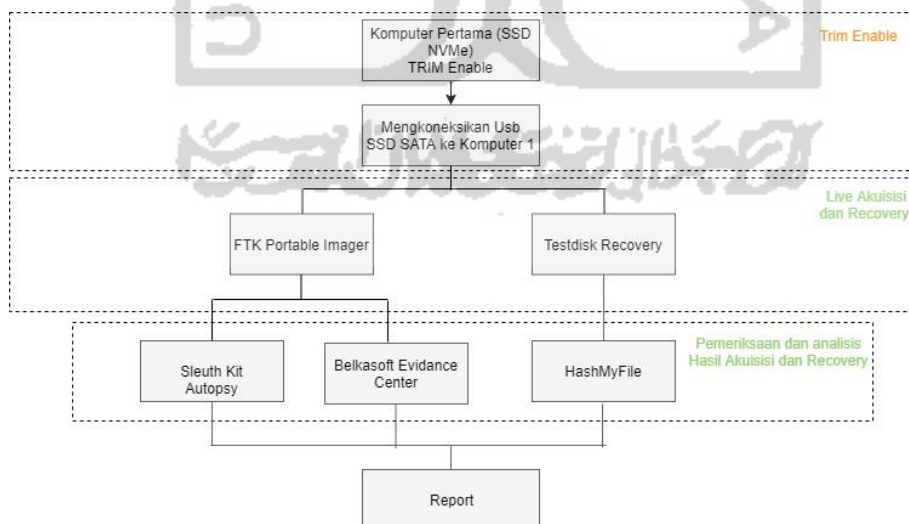
Selanjutnya, untuk melakukan eksperimen pertama adalah melakukan penulisan (write) dan penghapusan (delete) semua file dengan perintah SHIFT+DELETE, yang terdapat pada partisi ke-dua di komputer pertama kemudian akan diakuisisi dengan metode *live forensic* atau akuisisi dan *recovery* dalam keadaan komputer pertama menyala (*on*). Pada kondisi ini, TRIM *support* yang ada pada SSD NVMe dalam keadaan *disable*. Kemudian dilakukan pemeriksaan untuk melihat apakah beberapa file tersebut dapat ditemukan kembali dan selanjutnya dianalisis salinan file hasil akuisisinya didalam laptop investigator. Hasil *live* akuisisi dan *recovery* tersebut ditransfer menggunakan conector USB SSD SATA external ke komputer kedua (investigator).



Gambar 3.6 Tahapan Akuisisi TRIM *Disable*

3.4.2 Tahapan Akuisisi TRIM *Enable*

Selanjutnya untuk eksperimen kedua adalah melakukan penulisan (write) dan penghapusan (delete) semua file yang terdapat pada partisi ke-dua di komputer pertama dan akan diakuisisi dengan metode *live forensic* atau akuisisi dalam keadaan menyala (*on*). Pada kondisi ini, TRIM *support* yang ada pada SSD NVMe dalam keadaan *enabled*. Kemudian dilakukan pemeriksaan untuk melihat apakah beberapa file tersebut dapat ditemukan kembali dan selanjutnya dianalisis salinan file hasil akuisisinya didalam laptop investigator. Hasil live akuisisi dan *recovery* tersebut ditransfer menggunakan conector USB SSD SATA eksternal ke komputer kedua (investigator).

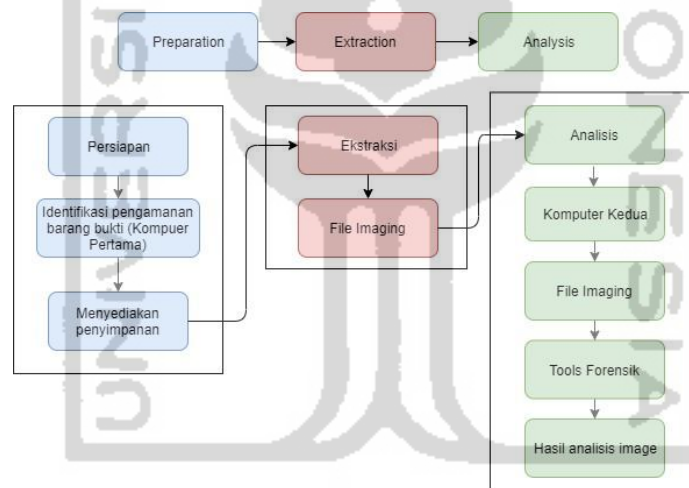


Gambar 3.7 Tahapan Akuisisi TRIM *Enable*

3.5 Pemeriksaan dan Analisis Output SSD NVMe

Merupakan tahapan pemeriksaan barang bukti digital yang telah diakuisisi, dan nantinya akan melakukan ekstraksi untuk mendapatkan petunjuk yang berkaitan dengan skenario kasus. Tahapan pemeriksaan dan hasil analisis dari proses skenario eksperimen yang akan dilakukan pada komputer pertama SSD NVMe, selanjutnya komputer kedua digunakan untuk kebutuhan analisis. Sebelum melakukan pemeriksaan terhadap hasil akuisisi tersebut, hasil akuisisi yang asli harus didublikasi dan melihat nilai *hash* antara file yang asli dengan file duplikasi, karena perlu dilakukan untuk menjaga keaslian barang bukti.

Selanjutnya untuk menjaga keaslian barang bukti maka pemeriksaan barang bukti tersebut adalah salinan file hasil akuisisi. Ada dua tools yang digunakan guna mengekstraksi dan menganalisis data hasil akuisisi yaitu *Sleuth Kit Autopsy Forensics* dan *Belkasoft Evidance Center*. Dalam melakukan pemeriksaan barang bukti terdapat 3 tahapan utama yang dapat dilihat pada gambar 3.8 sebagai berikut :



Gambar 3.8 Tahapan Pemeriksaan dan Analisis

- Tahapan Preparation : Melakukan persiapan dengan menyediakan ruang penyimpanan untuk menyimpan data yang akan *recovery* serta di ekstrak.
- Tahapan Ekstraksi : Melakukan ekstraksi file dengan mengidentifikasi dan *recovery* file yang telah terhapus. Ekstraksi file juga akan mengungkapkan karakteristik struktur file, data yang telah terhapus, nama file, time stamps, ukuran dan lokasi file.
- Tahapan Analisis : Tahapan menganalisis hasil file yang telah dilakukan pemeriksaan. Sehingga dapat mengukur tingkat efektifitas dari ekstraksi file fungsi TRIM *disable* atau *enable*, serta dapat rekomendasi tools mana yang tepat untuk *recovery* file pada penelitian ini.

Selanjutnya merupakan tahapan yang berisikan dari tahapan analisis. Dalam tahapan ini akan berisikan hasil akuisisi SSD NVMe dari dua fungsi TRIM (*disable/enable*). Dari hasil investigasi forensik nantinya akan ada beberapa tabel yang memetakan hasil dari masing-masing tahapan dalam proses investigasi forensik dapat dilihat seperti pada tabel 3.3.

Tabel 3.1 Status Storage *Disable* atau *Enable* serta Nilai Hash

SOLID STATE DRIVE (SSD) NVMe	HASH VALUE / MD5
Adata XPG SX6000 Lite	xxx

Dalam tahapan ini akan berisikan hasil dari akuisisi SSD NVMe dari eksperimen tersebut, tools yang digunakan untuk akuisisi data adalah FTK Imager Portable, *Sleuth Kit Autopsy*, *Belkasoft*, *Testdisk Recovery*. Dari hasil akuisisi SSD NVMe nantinya akan ada beberapa tabel yang menggambarkan hasil dari masing-masing tahapan proses akuisisi dan *recovery* investigasi forensik.

Tabel 3.2 Hasil Pengembalian Data Status TRIM *Disable*

TRIM STATUS	<i>Disable</i>	
TOOLS	<i>FTK Imager Portable, Sleuth Kit Autopsy Forensics, Belkasoft Evidence Center, Testdisk</i>	
JENIS FILE : File Gambar/File Musik/File Aplikasi/File Dokumen/File Multimedia		
NAMA FILE HASIL RESTORASI & NILAI HASH	STATUS RECOVERY	
	BERHASIL	TIDAK BERHASIL
Nama file : xxxxx MD5 : xxx		
Nama file : xxxxx MD5 : xxx		
Nama file : xxxxx MD5 : xxx		

Pada tabel hasil pengembalian data SSD NVMe status TRIM *Disable*, akan terlampirkan hasil akuisisi dan pengembalian file-file yang telah dilakukan penghapusan permanen dengan perintah SHIFT+DELETE, tools yang digunakan untuk akuisisi data SSD NVMe adalah *FTK Imager Portable, Sleuth Kit Autopsy Forensics, Belkasoft Evidence Center, Testdisk Recovery*.

Kemudian, pada tabel 3.5 akan terlampir hasil akuisisi dan pengembalian data SSD NVMe status TRIM *enable*, berikut ini adalah daftar tabel hasil pengembalian data atau file-file SSD NVMe status TRIM *enable* :

Tabel 3.3 Hasil Pengembalian Data Status TRIM *Enable*

TRIM STATUS	<i>Enable</i>	
TOOLS	<i>FTK Imager Portable, Sleuth Kit Autopsy Forensics, Belkasoft Evidence Center, Testdisk Recovery</i>	
JENIS FILE	File Gambar/File Musik/File Aplikasi/File Dokumen/File Multimedia	
NAMA FILE HASIL RESTORASI & NILAI HASH	STATUS RECOVERY	
	BERHASIL	TIDAK BERHASIL
Namafile : xxxxx MD5 : xxx		
Namafile : xxxxx MD5 : xxx		
Namafile : xxxxx MD5 : xxx		

Pada tabel hasil pengembalian data SSD NVMe status TRIM *enable*, akan terlampirkan hasil akuisisi dan pengembalian file-file yang telah dilakukan penghapusan permanen dengan perintah SHIFT+DELETE, tools yang digunakan untuk akuisisi data SSD NVMe adalah *FTK Imager Portable, Sleuth Kit Autopsy Forensics, Belkasoft Evidence Center, Testdisk Recovery*. Nantinya pada tabel 3.4 dan 3.5 dapat menjadi pembandingan hasil *recovery* data SSD NVMe status TRIM *disable* dan *enable*.

3.6 Hasil Pembahasan dan Laporan

Tahapan ini merupakan proses hasil dan pembahasan dari analisis yang telah dilakukan pada penelitian ini.

BAB 4

Hasil dan Pembahasan

4.1 Tinjauan Pustaka

Karakteristik storage HDD konvensional dan SSD menurut (Bednar & Katos, 2011) dalam perkembangan teknologi storage, yaitu HDD konvensional menggunakan motor listrik piringan dan head, yang dirancang dalam suatu wadah dan menyimpan data secara platter magnetis. Sedangkan SSD memiliki unsur dan karakteristik berdasarkan memori flash yang berbeda dengan hard disk konvensional, SSD dibangun dari chip semikonduktor sebagai penyimpanan data dan read file dalam memori flash, dan tidak memiliki bagian berputar yang mempunyai kelebihan yaitu interface yang baik dari segi fisik dan lebih minimalisir daya listrik, kemudian kinerja akses data yang lebih baik dan cepat menjadikan SSD relatif meninggalkan HDD jika performa menjadi tujuan utama.

Menurut (Shah et al., 2015) SSD mempunyai karakter yang tidak dimiliki di HDD konvensional, yaitu harus menghapus blok sebelum data baru dapat ditulis (write) kembali. Karna itu jelas menyebabkan masalah untuk mengambil bukti digital forensik dari SSD. Kemudian SSD meluncurkan bentuk fisik yang berbeda dari sebelumnya yaitu M.2 dengan interface SATA menggunakan protocol AHCI memiliki kecepatan perpindahan data kurang lebih sama dengan SSD 2.5" SATA.



Gambar 4.1 SSD SATA 2.5" (atas) dengan SSD SATA M.2 (bawah)¹⁰

SSD M.2 memiliki teknologi terbaru menggunakan interface NVMe, NVMe bukan interface seperti SATA atau PCIe, tetapi PCIe telah upgrade versi ke NVMe. SSD NVMe merupakan media penyimpanan komputer terbaru setelah peluncuran SSD SATA. Teknologi NVMe yang dikembangkan untuk mengatasi limitasi dari teknologi yang sudah

¹⁰ <https://mygaming.co.za/news/hardware/118533-different-types-of-ssds-explained-sata-vs-m-2-vs-pcie.html>

ada. NVMe memanfaatkan jalur PCIe (slot PCIe, M.2) SSD M.2 SATA menggunakan jalur PCIe 2.0 dengan protocol AHCI, sedangkan SSD NVMe memakai 4 jalur PCIe 3.0 secara teoritis SSD NVMe memiliki sequential mencapai 4Gbps menggunakan protocol NVMe. SSD NVMe memiliki kelebihan dari SSD SATA dari generasi sebelumnya, yaitu peningkatan kinerja, jumlah command yang tidak terbatas, manajemen antrian optimal, konsumsi daya listrik lebih kecil dari SATA (Nikkel, 2016).



Gambar 4.2 SSD M.2 NVMe Adata XPG SX6000 Lite

Terkait interface SSD protocol AHCI dan NVMe dari observasi dilapangan dan studi literature dalam berbagai sumber, SSD mempunyai interface (bus) yang bervariasi, yaitu :

- a. 2.5" SATA (1.5Gbps, 3.0Gbps, 6.0Gbps) dengan memiliki kecepatan sequential read dan write 500mbps.
- b. M.2 SATA memiliki kecepatan sequential read dan write 1000-1500mbps.
- c. M.2 NVMe memiliki kecepatan sequential read dan write 2000-2500mbps.

4.2 Persiapan Tools

Langkah pertama dalam penelitian ini adalah mempersiapkan system yang akan digunakan pada proses live akuisisi dan *recovery*. Langkah awal adalah mempersiapkan spesifikasi komputer dan pendukung-pendukung lainnya guna untuk melakukan penelitian ini. Peralatan yang perlu dipersiapkan antara lain :

Tabel 4.1 Spesifikasi penggunaan Hardware dan Software

NO	Hardware/ Software	Keterangan
1	PC Biostar seri H81MHV3 (Komputer pertama)	Hardware
2	Laptop Asus seri X455LN (Komputer kedua)	Hardware

3	<i>Solid State Drive (SSD) M.2 NVMe Adata XPG SX6000 Lite dengan kapasitas 128GB</i>	Hardware
4	<i>Solid State Drive (SSD) SATA Eksternal Apacer dengan kapasitas 240GB</i>	Hardware
5	Converter PCIe Card Support M.2 NVMe	Hardware
6	USB 3.0 SSD SATA 2.5"	Hardware
7	Sistem Operasi Windows 10 Profesional dengan arsitektur 64bit	Sistem Operasi (Komputer pertama)
8	Sistem Operasi Windows 10 Education dengan arsitektur 64-bit	Sistem Operasi (Komputer kedua)
9	FTK Imager Porteble for Windows	Forensic Tools
10	Sleuth Kit Autopsy Forensics for Windows	Forensic Tools
11	Belkasoft Evidence Center for Windows	Forensic Tools
12	Testdisk v6.14 for Windows	Recovery Tools
13	Hashmyfile	Tools Hashing

4.3 Skenario dan Simulasi

Merupakan tahapan membuat simulasi kasus pada media penyimpanan SSD NVMe dan melakukan penghapusan file. Kondisi perangkat komputer pertama pada saat ditemukan lampu indikator power dalam keadaan menyala dan terdapat kabel HDMI tertancap pada salah satu port HDMI monitor, serta terdapat perangkat converter yang membantu untuk implemementasi SSD M.2 NVMe pada motherboard yaitu Converter PCIe Card Support M.2 NVMe, dimana adapter ini memiliki slot Key M dan Key M+Key B. Berikut perangkat komputer sedang menyala serta komputer menggunakan converter untuk membantu proses device SSD NVMe itu berjalan, ditunjukan pada gambar 4.3 dan 4.4.



Gambar 4.3 Converter SSD M.2 NVMe Adata XPG SX6000 Lite



Gambar 4.4 Barang Bukti Elektronik

Secara garis besar ada 2 tahapan utama dalam penelitian ini yaitu :

1. Melakukan teknik fungsi TRIM pada SSD NVMe yaitu menonaktifkan fungsi TRIM (*TRIM disable*) dan pengaktifan fungsi TRIM (*TRIM enable*). Untuk melakukan praktek terhadap fungsi TRIM pada SSD NVMe yaitu penghapusan beragam ekstensi file secara permanen dengan perintah SHIFT+Delete.
2. Melakukan live akuisisi terhadap SSD NVMe yang telah diterapkan dengan fungsi TRIM bertujuan untuk menganalisis file-file apa saja yang dapat *recovery* setelah praktek penghapusan file pada SSD NVMe. Tools yang digunakan dalam praktek live akuisisi, *recovery* dan analisis adalah FTK Imager Portable untuk membuat image dari SSD NVMe. Kemudian Testdisk untuk melakukan *recovery* file secara langsung pada SSD NVMe. Serta tools Sleuth Kit Autopsy dan Belkasoft Evidence Center untuk melakukan pemeriksaan dan analisis hasil imaging.



Gambar 4.5 Mengkoneksikan USB Penyimpanan Eksternal

Adapun tujuan dari 2 tahapan di atas adalah untuk mengukur tingkat efektifitas akuisisi dan *recovery* dari 5 tools terkait yaitu FTK Imager Portable, Sleuth Kit Autopsy, Belkasoft Evidence Center dan Testdisk *Recovery*. Terdapat 3 perangkat yang digunakan dalam objek penelitian ini yaitu (PC Komputer pertama) dimana perangkat ini ditanamkan SSD M.2 NVMe menggunakan conector ke motherboard. Kabel usb eksternal SSD SATA 2.5” guna untuk media penyimpanan untuk melakukan live akuisisi dan *recovery* pada komputer pertama seperti pada gambar 4.6.



Gambar 4.6 Perangkat Usb Eksternal

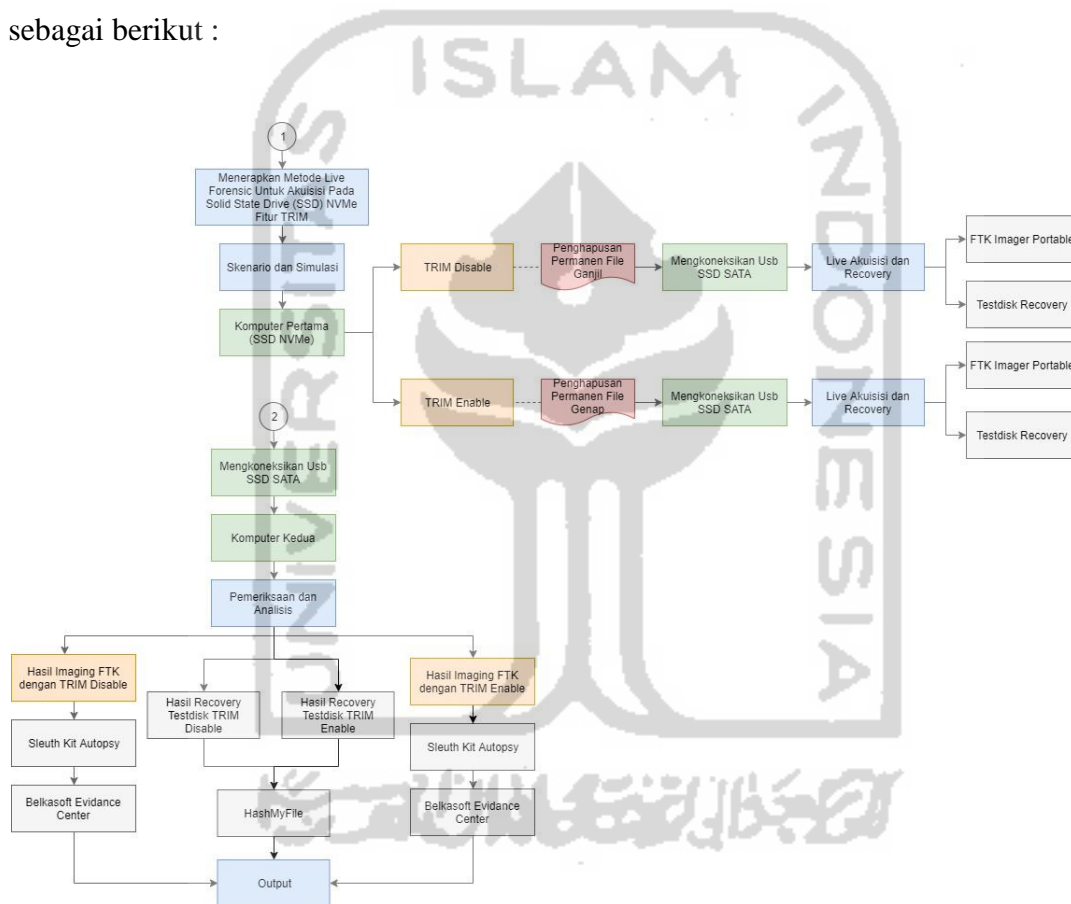
Kemudian laptop Asus seri X455LN (Komputer kedua) yang digunakan untuk kebutuhan pemeriksaan dan analisis. Berikut ini merupakan perangkat komputer yang dijadikan sebagai komputer investigator seperti pada gambar 4.6, guna untuk mengakses pemeriksaan dan analisis dari hasil image.



Gambar 4.7 Perangkat Komputer Investigator

Pada penelitian ini, metode yang digunakan adalah live forensic secara konvensional, menurut (Nuh Al-Azhar, 2012a) teknik live forensic secara konvensional dilakukan dengan mengkoneksikan usb drive ke komputer secara langsung dan mengakuisisi isi drive secara keseluruhannya. Pada metode ini, penyidik harus memastikan sistem dalam keadaan menyala (on) pada barang bukti fisik maupun digital untuk mengakuisisi secara langsung terhadap komputer, kemudian melakukan examinasi dan dianalisis pada perangkat komputer yang berbeda guna integritas barang bukti terjaga yang nantinya akan dilakukan ekstraksi untuk mendapatkan informasi dan petunjuk yang berkaitan dengan kasus sedang terjadi.

Selanjutnya tahapan dan metodologi pada penelitian ini akan dipaparkan pada gambar 4.8 sebagai berikut :



Gambar 4.8 Tahapan Simulasi

Berdasarkan gambar 4.8 menjelaskan tahapan-tahapan dari yang dilakukan terhadap komputer pertama dan komputer kedua diantaranya yaitu :

1. Menerapkan fungsi TRIM *disable/enable* pada SSD NVMe yang ditanam.
2. Menghapus beragam file ganjil dan genap pada bagian partisi kedua SSD NVMe.
3. Mengkoneksikan usb SSD SATA 2,5” ke komputer pertama yang nantinya akan digunakan untuk menyimpan hasil akuisisi dan *recovery* dari komputer pertama.

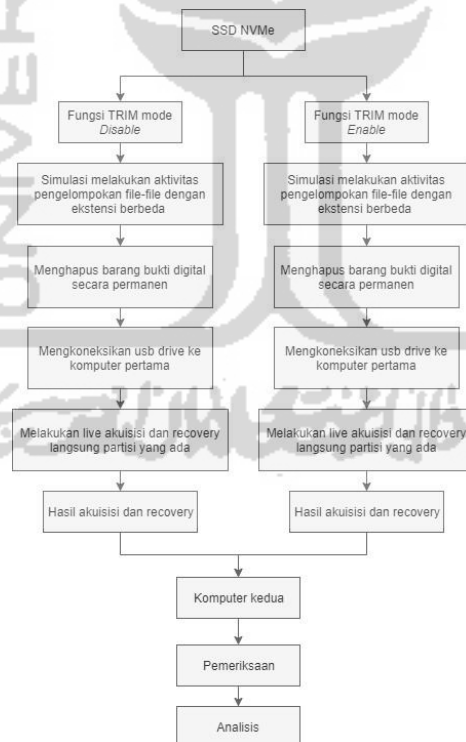
4. Melakukan akuisisi atau imaging SSD NVMe secara langsung pada komputer pertama menggunakan FTK Imager Portable.
5. Melakukan *recovery* SSD NVMe secara langsung menggunakan Testdisk *Recovery*.

Tahapan-Tahapan yang dilakukan terhadap komputer kedua antara lain :

1. Setelah mendapatkan hasil imaging dari FTK Imager Porteble kemudian melakukan pemeriksaan dan analisis menggunakan Sleuth Kit Autopsy.
2. Melakukan pemeriksaan dan analisis menggunakan Belkasoft Evidence Center.
3. Setelah melakukan *recovery* menggunakan tool Testdisk kemudian melakukan analisis keaslian data menggunakan tool Hashmyfile.
4. Melakukan pembuatan laporan.

4.4 Tahapan Akuisisi SSD NVMe

Dari hasil analisis mengenai fungsi TRIM SSD di atas, maka didapatkan dua model akuisisi dalam penelitian ini yaitu teknik akuisisi fungsi TRIM *disable* dan fungsi TRIM *enable*. Kedua model teknik akuisisi dapat dilihat pada gambar 4.9 sebagai berikut :



Gambar 4.9 Tahapan Teknik Akuisisi SSD NVMe

Gambar 4.9 adalah menjelaskan teknik yang dilakukan dalam mengakuisisi SSD NVMe. Teknik model *disable* dan *enable* merupakan teknik yang dilakukan dengan mengakuisisi secara langsung partisi yang ada, pada SSD NVMe melalui kabel usb SSD

SATA eksternal menggunakan FTK Imager Portable dan melakukan *recovery* SSD NVMe secara langsung menggunakan Testdisk *Recovery* guna untuk perbandingan. Selanjutnya hasil imaging dan *recovery* akan dipindahkan ke usb SSD SATA eksternal. Kemudian dari hasil akuisisi dua model fungsi TRIM akan dilakukan pemeriksaan dan analisis untuk mengetahui dan mengukur tingkat efektifitas akuisisi *recovery* fungsi TRIM disabel dan *enable*.

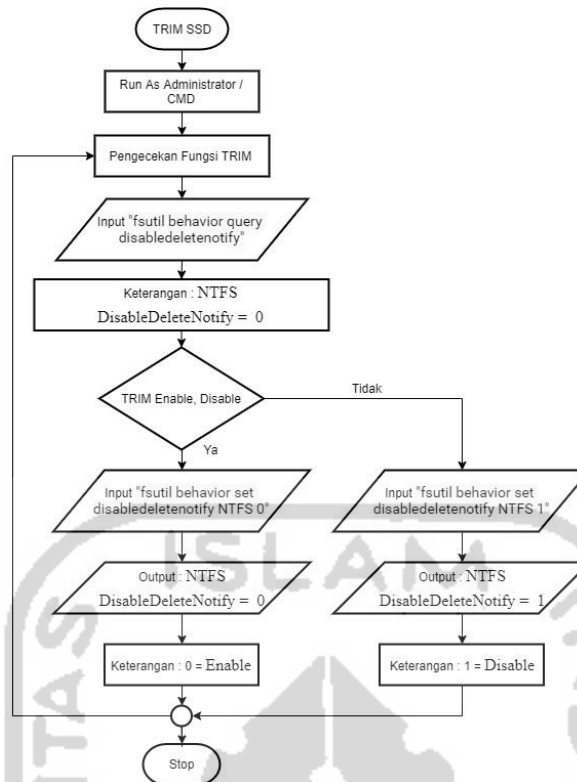
4.4.1 Tahapan Fungsi TRIM *Disable*

Proses yang digunakan controller SSD menurut pengontrol SSD membuat ulang blok mana yang lebih efisien dengan mengimpementasikan fungsi TRIM¹¹. Karna sebab itu, ketika file sudah dihapus oleh sistem operasi, perintah TRIM akan dikirim ke disk controller SSD dengan Logical block Addressing (LBA) untuk menghapus file. LBA adalah skema umum yang digunakan untuk menentukan lokasi blok data yang disimpan pada perangkat penyimpanan komputer¹². SSD kemudian mereset block-block yang menjadi ruang kosong. Kekurangan dari fungsi TRIM ini adalah akan memperpendek umur chip memory dari SSD yaitu NAND.

Selanjutnya untuk tahapan simulasi pertama penelitian ini, terdapat langkah-langkah praktek yang harus dilakukan pada SSD NVMe, kemudian fungsi TRIM pada SSD NVMe. Sebagai langkah dasar setelah melakukan pemasangan SSD NVMe menggunakan adapter PCIe di komputer pertama, kemudian melakukan instalasi operating system windows 10 profesional dengan arsitektur 64 bit. Untuk mempermudah pemahaman, peneliti membuat flowchart tahapan praktek fungsi TRIM SSD sebagai gambar 4.10 berikut :

¹¹ <https://www.anandtech.com/show/2738/5>

¹² <https://gerardnico.com/io/drive/lba>



Gambar 4.10 Flowchart Tahapan Fitur TRIM SSD

Selanjutnya akan dijelaskan pada bagian bawah ini, untuk melakukan pengecekan fungsi TRIM pada SSD NVMe secara tradisional. Dapat dilihat pada gambar 4.11 di bawah ini :

```

C:\Windows\system32>fsutil behavior query disabledeletenotify
NTFS DisableDeleteNotify = 0 (Disabled)
ReFS DisableDeleteNotify = 0 (Disabled)
  
```

Gambar 4.11 Perintah Comment Pengecekan Fungsi TRIM

Windows 10 Profesional sudah mendukung teknologi TRIM pada SSD. Berikut tahapan cara tradisional memeriksa fungsi TRIM *disable/enable* pada file sistem NTFS SSD apakah sudah aktif atau belum, perintah yang dijalankan adalah :

- a. Pada search menu windows 10, ketikkan “CMD” lalu tekan” CTRL+SHIFT+ENTER” untuk memunculkan *command prompt*.
- b. Input dengan perintah “**fsutil behavior query disabledeletenotify**” pada command prompt, tekan enter.

- c. Jikalau hasil pengecekan TRIM muncul “**NTFS DisableDeleteNotify = 0 (Disabled)**” maka dapat disimpulkan fungsi TRIM “diaktifkan/enable” untuk SSD dengan drive file system NTFS.

Selanjutnya untuk implementasi fungsi TRIM *disable* atau penonaktifan pada SSD NVMe sesuai skenario yang diterapkan dalam penelitian ini, maka perintah command prompt “CMD” yang dijalankan pada gambar 4.12 di bawah ini.

```
C:\Windows\system32>fsutil behavior set disabledeletenotify NTFS 1
NTFS DisableDeleteNotify = 1 (Enabled)
```

Gambar 4.12 Perintah Comment TRIM *Disable*/Nonaktif

Pada perintah *command prompt* seperti yang terlihat pada gambar 4.12 untuk penonaktifan/*disable* fungsi TRIM pada SSD NVMe. Perintah command tersebut adalah “**fsutil behavior set disabledeletenotify NTFS 1**”. Kemudian melakukan pengecekan apakah fungsi TRIM SSD telah dinonaktifkan/*disable*, dengan perintah “**fsutil behavior query disabledeletenotify**” dapat dilihat pada gambar 4.13.

```
C:\Windows\system32>fsutil behavior query disabledeletenotify
NTFS DisableDeleteNotify = 1 (Enabled)
ReFS DisableDeleteNotify = 0 (Disabled)
```

Gambar 4.13 Perintah Pengecekan Ulang Fungsi TRIM

Pada gambar 4.11 di atas, Apabila output perintah pengecekan fungsi TRIM muncul “**NTFS DisableDeleteNotify = 1 (Enabled)**” dapat disimpulkan fungsi TRIM “dinonaktifkan/*disable*” untuk SSD dengan drive file system NTFS¹³.

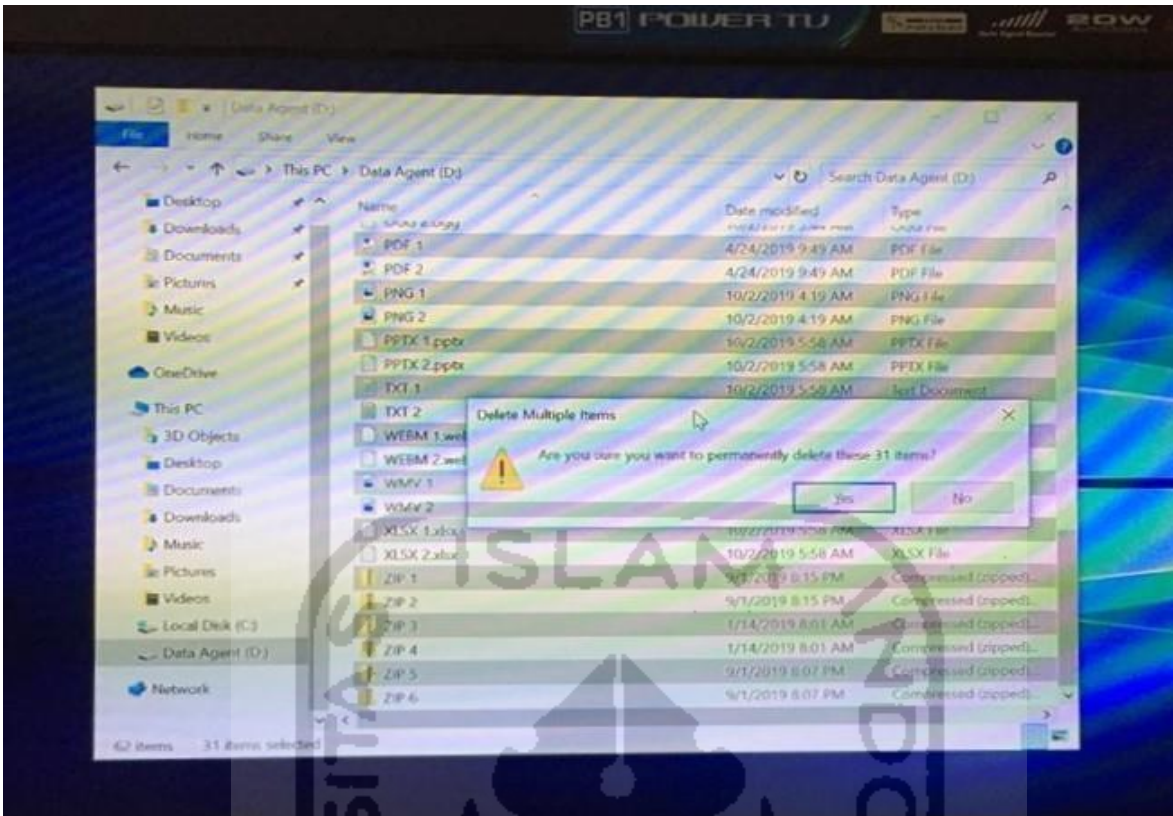
Setelah memastikan fungsi TRIM dalam keadaan *disable*/nonaktif selanjutnya adalah melakukan pemindahan file dari partisi local disk C:\ ke Data Agent D:\. Pada penelitian ini yang akan dilakukan penghapusan permanent yaitu partisi Data Agent D:\. Dalam gambar 4.14 di bawah ini terdapat bermacam ekstensi jenis file dan nilai hash yang akan dilakukan praktek penghapusan permanen dengan perintah SHIFT+DELETE, untuk mempermudah penghapusan file permanen maka perlu membedakan nama file ganjil-genap guna untuk membedakan file TRIM *disable* atau *enable*. Pengelompokan nama file pada tahapan fungsi

¹³ <https://www.thewindowsclub.com/enable-trim-in-windows-10>

TRIM *disable* penamaan ganjil (Ramadhan et al., 2016). Tabel 4.2 di bawah ini adalah pengelompokan jenis-jenis file label ganjil, nilai hashing asli dan ekstensinya :

Tabel 4.2 Keaslian Nama File Ganjil, Nilai Hashing, dan Ektensi File (TRIM *Disable*)

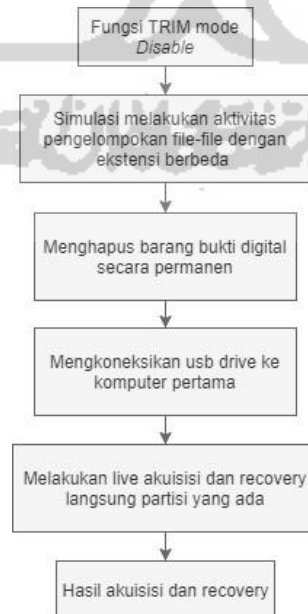
Jenis File	Nama File Asli	Nilai Hashing MD5 File Asli	Ekstensi File
File Dokumen	- DOC 1 - DOCX 1 - XLSX 1 - PPTX 1 - PDF 1 - TXT 1 - ODT 1	- 630a293939e5fc996076d2c2ec39a7c1 - 6db984ae2628503104cb46fab8b9ef8c - 56c424725531715f142e77ccc5cee774 - 1d02e044e64e79994ab5a0ca871c6fe9 - 7a3801902be546b4ee026538f246e844 - 6bb11f42a5b591be9ec1a0e95a5cd00c - d9822aa6cbe227fc935665375152bacf	.doc., docx., .xlsx, .pptx, .pdf, .txt
File Video	- 3GP 1 - FLV 1 - MPG 1 - WEBM 1 - MKV 1 - MOV 1 - OGG 1 - WMV 1 - AVI 1 - MP4 1	- cd5f422a723609bff58c699704f91d88 - 49f86ccb885b8eb2de17ece7f281434 - 293a2b5b3a18b1f283bcc2cbda358e0b - e75301e7337242951e90e6fbc598c8cb - b67c0c226b47bc77716aa30cd8d8d2c5 - 35208da889d863bc010741f9e2c7c25e - 8ca67608dcaec59718c25ed8bfa93c35 - e3935aaddb17432b48a0d45be6cfca9d - 72562d25302f0698c19040a6d50ceb0c - 0094fb55e09791154276f456d9982a0a	.flv, .mpg, .webm, .mkv, .mov, .ogg, .wmv, .avi
File Gambar	- GIF 1 - JPG 1 - PNG 1 - BMP 1	- ed28cc871584230543b5a2d8a386a2cb - d4fc57bddd2ed31d53f00002791a245d - a820b280e93967956c449b342125add8 - 8cad97ecf36337caebdd53fd81258dd	.gif, .jpg, .png .bmp
File Musik	- MP3 1 - MP3 3	- d004ad9c716fbb7262d09fcd812b7bdb - 2178cecb48c6473308487117d273eb1e	.mp3
File Aplikasi	- MASTER 1 - MASTER 3 - MASTER 5	- 562f2ea6e41020fd7bf5426bd77cd59c - 1abf96d2ddec838763cec88285a1fc6f - 076d6a1f9c0e22362ca71d0e254202b0	.exe
File Zip	- ZIP 1 - ZIP 3 - ZIP 5	- 47cf035aa29599823cce99bef2467330 - a5acca59eb9ff6017064994aa2b76db1 - 733c9420aacd6067e0d7b3050ef3b2f4	.zip
File 7Z	- 7Z 1	- e2d9c0b0a82113ce52d5334ffd24a876	.7z



Gambar 4.14 Daftar Sebelum Keseluruhan File Ganjil Dihapus Permanen

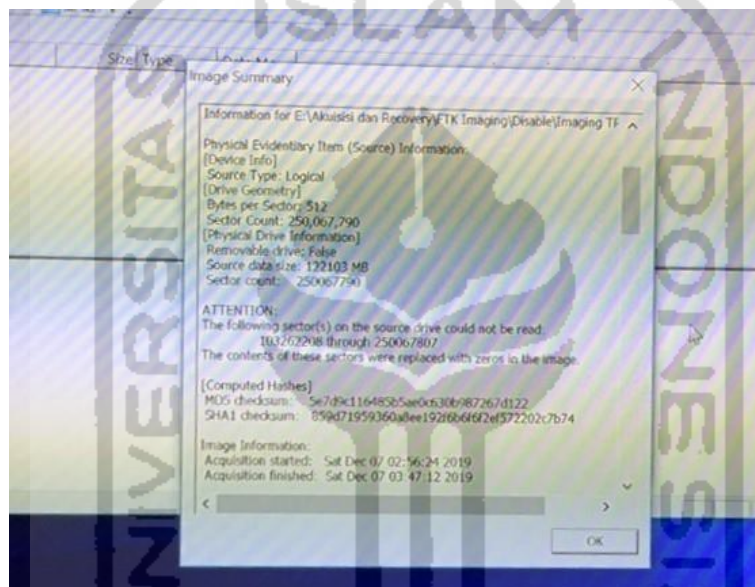
4.4.2 Teknik Akuisisi TRIM Disable

Berdasarkan penjelasan mengenai dinonaktifkan/*disable* fungsi TRIM akan ada beberapa tahapan yang digunakan dalam mengakuisisi SSD NVMe akan digambarkan dalam alur bagan sebagai berikut :



Gambar 4.15 Tahapan Teknik Akuisisi TRIM Disable

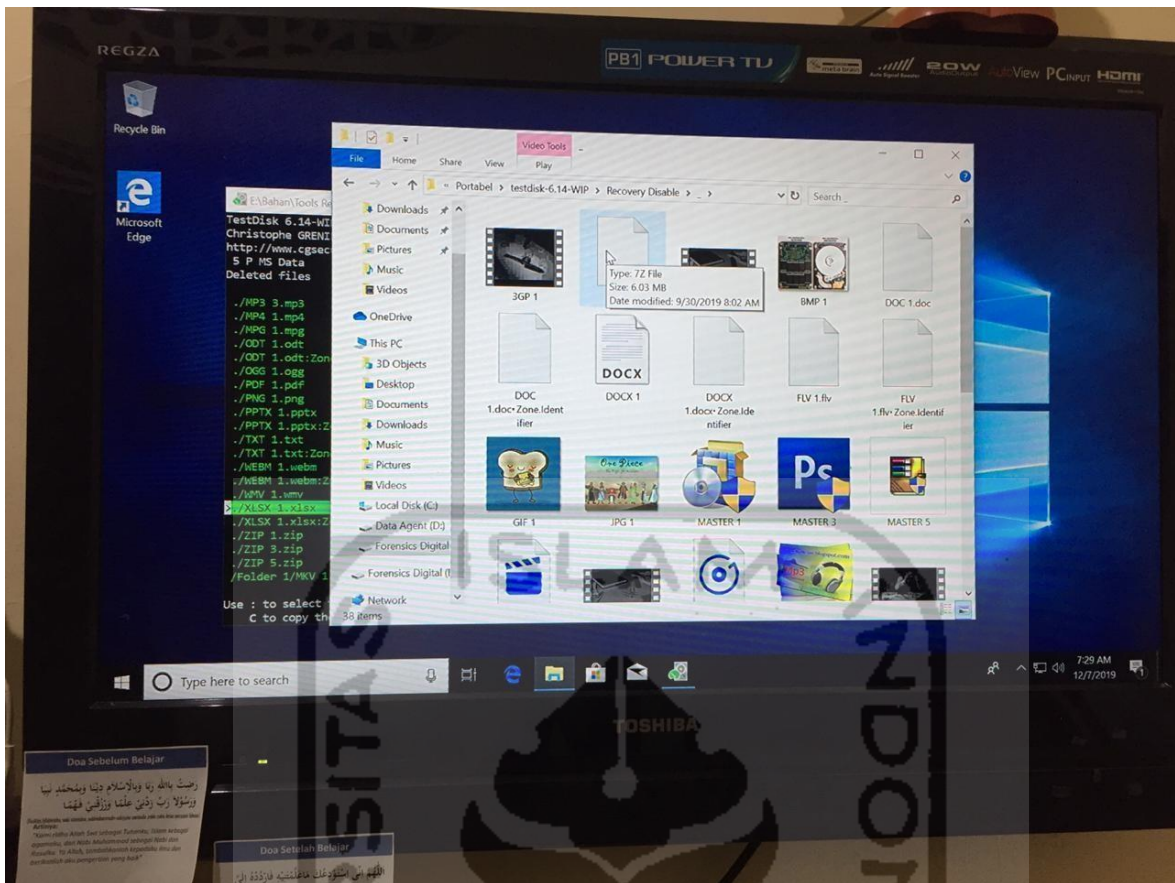
Langkah selanjutnya akuisisi fungsi TRIM *disable* yaitu menggunakan *dock* usb SSD SATA eksternal, usb diintegrasikan dengan komputer pertama agar menjaga integritas dan keaslian data, untuk melakukan praktek live akuisisi atau imaging menggunakan FTK Imager Portabel yang sudah ada di dalam usb SSD eksternal. Gambar 4.16 di bawah adalah hasil potret dokumentasi dari akuisisi SSD NVMe fungsi TRIM *disable* pada usb SSD SATA eksternal menggunakan tool forensik FTK Imager Portable. Waktu yang dibutuhkan untuk live akuisisi partisi logical SSD M.2 NVMe Adata XPG SX6000 Lite 128GB fitur TRIM *disable* menggunakan FTK Imager Portable adalah 50 menit 46 detik.



Gambar 4.16 Hasil Output Akuisisi TRIM *Disable* Menggunakan FTK Imager Portable

Gambar 4.16 di atas dapat disimpulkan bahwa SSD NVMe fungsi TRIM *disable* telah berhasil di imaging menggunakan FTK Imager Portable dengan mendapatkan nilai hash MD5 “5e7d9c116485b5ae0c630b987267d122” dan nilai hash SHA1 adalah “859d71959360a8ee192f6b6f6f2ef572202c7b74”.

Khusus untuk melakukan praktek live *recovery* dalam penelitian ini menggunakan tools Testdisk guna untuk memperbandingkan hasil *recovery* data SSD NVMe fungsi TRIM *disable*. Gambar 4.17 di bawah adalah hasil potret dokumentasi dari *recovery* SSD NVMe fungsi TRIM *disable* pada usb SSD SATA eksternal menggunakan tool *recovery* Testdisk.

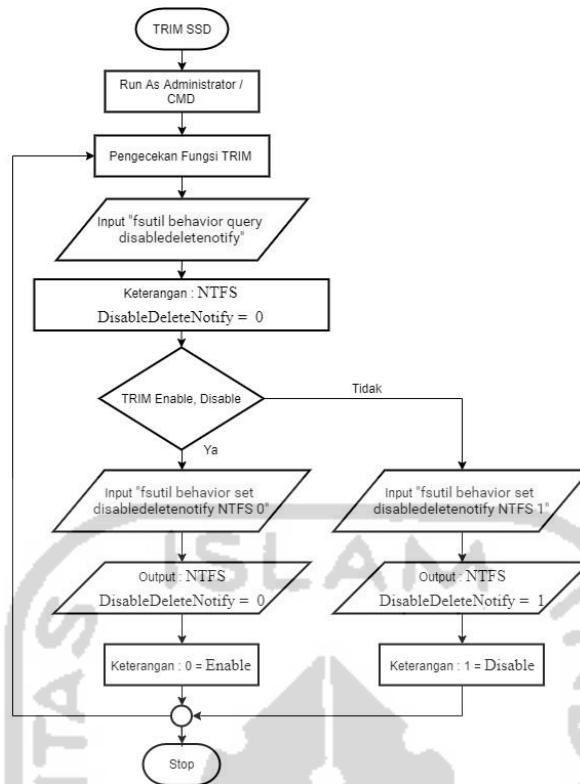


Gambar 4.17 Proses dan Hasil Output *Recovery TRIM Disable* Menggunakan Testdisk

4.4.3 Tahapan Fitur *TRIM Enable*

Fungsi dari *TRIM enable* menurut (Hubbard, 2016) yaitu perintah proses controller melakukan penghapusan data/file pada SSD dari sektor blok yang telah dihapus oleh pengguna komputer. Penghapusan data *TRIM* bisa dilakukan saat sistem operasi sedang berjalan atau ketika sistem di restart. Pada sistem operasi windows, fungsi *TRIM* tidak terlibat pada file sistem selain NTFS.

Berikut ini adalah simulasi tahapan eksperimen kedua, merupakan proses praktek fungsi *TRIM enable*/aktif terhadap SSD NVMe. Simulasi penelitian ini masih menggunakan sistem operasi Windows 10 Pro, sama halnya dengan proses pengaktifan fungsi *TRIM disable* sebelumnya. Untuk mempermudah pemahaman, peneliti membuat *flowchart* tahapan praktek fungsi *TRIM SSD* sebagai berikut :



Gambar 4.18 Flowchart Tahapan Fitur TRIM SSD

Selanjutnya pada gambar 4.19 di bawah ini adalah pengecekan fungsi TRIM pada SSD NVMe secara tradisional.

```

C:\Windows\system32>fsutil behavior query disabledeletenotify
NTFS DisableDeleteNotify = 1 (Enabled)
ReFS DisableDeleteNotify = 0 (Disabled)
  
```

Gambar 4.19 Perintah Comment Pengecekan Fungsi TRIM

Untuk melakukan pengecekan kembali fungsi TRIM pada SSD NVMe adalah dengan perintah sebagai berikut :

- a. Pada search menu windows 10, ketikkan “CMD” lalu tekan” CTRL+SHIFT+Enter” untuk memunculkan command prompt.
- b. Input dengan perintah “**fsutil behavior query disabledeletenotify**” pada command prompt, tekan enter.
- c. Jikalau hasil pengecekan TRIM muncul “**NTFS DisableDeleteNotify = 1 (Enabled)**” maka dapat disimpulkan fungsi TRIM “dinonaktifkan/disable” untuk SSD dengan drive file system NTFS.

Selanjutnya untuk implementasi fungsi TRIM *enable*/aktif pada SSD NVMe sesuai skenario yang diterapkan dalam penelitian ini, maka perintah command prompt “CMD” yang dijalankan pada gambar 4.20 di bawah ini.

```
C:\Windows\system32>fsutil behavior set disabledeletenotify NTFS 0
NTFS DisableDeleteNotify = 0 (Disabled)
```

Gambar 4.20 Perintah Comment TRIM *Enable*/Aktif

Pada perintah command prompt seperti yang terlihat pada gambar 4.20 untuk pengaktifan/*enable* fungsi TRIM pada SSD NVMe. Perintah command tersebut adalah “**fsutil behavior set disabledeletenotify NTFS 0**”. Kemudian melakukan pengecekan apakah fungsi TRIM SSD telah *enable*/aktif, dengan perintah “**fsutil behavior query disabledeletenotify**” dapat dilihat pada gambar 4.21.

```
C:\Windows\system32>fsutil behavior query disabledeletenotify
NTFS DisableDeleteNotify = 0 (Disabled)
ReFS DisableDeleteNotify = 0 (Disabled)
```

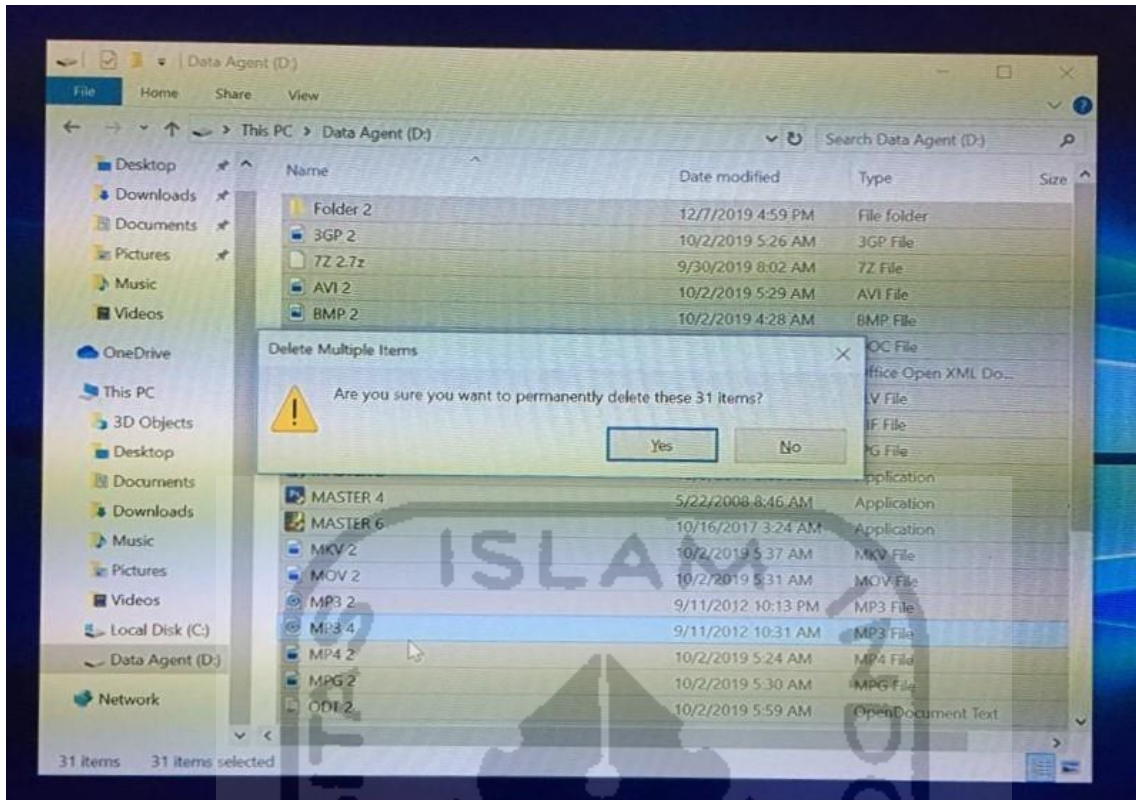
Gambar 4.21 Perintah Comment Pengecekan Ulang Fungsi TRIM *Enable*

Pada gambar 4.16 di atas, Apabila output perintah pengecekan fungsi TRIM muncul “**NTFS disableDeleteNotify = 0 (Disabled)**” dapat disimpulkan drive file sistem NTFS SSD fitur TRIM tersebut dalam keadaan “*enable*/diaktifkan”.

Setelah memastikan fungsi TRIM dalam keadaan *enable*/aktif selanjutnya adalah melakukan pemindahan file dari partisi local disk C:\ ke Data Agent D:\ pada penelitian ini yang akan dilakukan penghapusan permanen yaitu partisi Data Agent D:\. Pada gambar 4.22 di bawah ini terdapat beragam ekstensi jenis file dan nilai hash yang akan dilakukan praktek penghapusan permanen dengan perintah SHIFT+DELETE, untuk mempermudah penghapusan file permanen maka perlu membedakan nama file ganjil-genap guna untuk membedakan file TRIM *disable* atau *enable*. Pengelompokan nama file pada tahapan fungsi TRIM *enable* penamaan genap. Tabel 4.3 di bawah ini adalah pengelompokan jenis-jenis file label genap, nilai hashing asli dan ekstensinya :

Tabel 4.3 Keaslian Nama File Genap, Nilai Hashing dan Ektensi File (TRIM *Enable*)

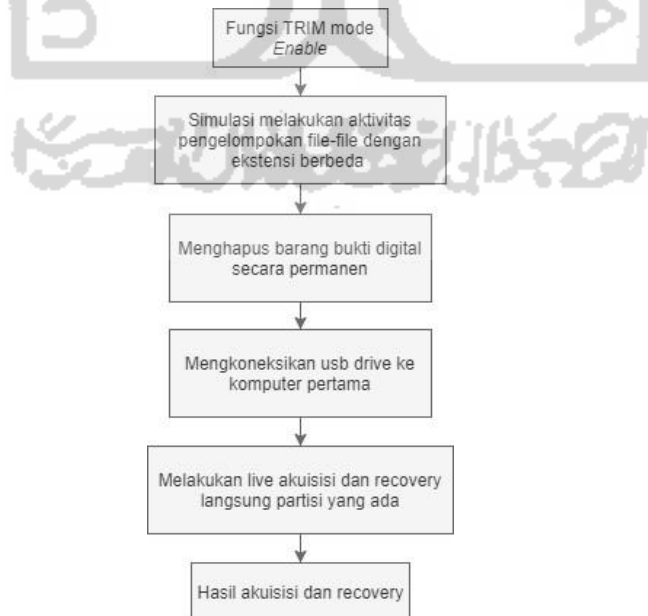
Jenis File	Nama File Asli	Nilai Hashing MD5 File Asli	Ekstensi File
File Dokumen	- DOC 2 - DOCX 2 - XLSX 2 - PPTX 2 - PDF 2 - TXT 2 - ODT 2	- 630a293939e5fc996076d2c2ec39a7c1 - 6db984ae2628503104cb46fab8b9ef8c - 56c424725531715f142e77ccc5cee774 - 1d02e044e64e79994ab5a0ca871c6fe9 - 7a3801902be546b4ee026538f246e844 - 6bb11f42a5b591be9ec1a0e95a5cd00c - d9822aa6cbe227fc935665375152bacf	.doc, .docx, .xlsx, .pptx, .pdf, .txt, .odt
File Video	- 3GP 2 - FLV 2 - MPG 2 - WEBM 2 - MKV 2 - MOV 2 - OGG 2 - WMV 2 - AVI 2 - MP4 2	- cd5f422a723609bff58c699704f91d88 - 49f86ccbba885b8eb2de17ece7f281434 - 293a2b5b3a18b1f283bcc2cbda358e0b - e75301e7337242951e90e6fbc598c8cb - b67c0c226b47bc77716aa30cd8d8d2c5 - 35208da889d863bc010741f9e2c7c25e - 8ca67608dcaec59718c25ed8bfa93c35 - e3935aaddb17432b48a0d45be6cfca9d - 72562d25302f0698c19040a6d50ceb0c - 0094fb55e09791154276f456d9982a0a	.flv, .mpg, .webm, .mkv, .mov, .ogg, .wmv, .avi, .mp4
File Gambar	- GIF 2 - JPG 2 - PNG 2 - BMP 2	- ed28cc871584230543b5a2d8a386a2cb - d4fc57bddd2ed31d53f00002791a245d - a820b280e93967956c449b342125add8 - 8cad97ecf36337caebedd53fd81258dd	.gif, .jpg, .png, .bmp
File Musik	- MP3 2 - MP3 4	- d004ad9c716fbb7262d09fcd812b7bdb - 2178cecb48c6473308487117d273eb1e	.mp3
File Aplikasi	- MASTER 2 - MASTER 4 - MASTER 6	- 562f2ea6e41020fd7bf5426bd77cd59c - 1abf96d2ddec838763cec88285a1fc6f - 076d6a1f9c0e22362ca71d0e254202b0	.exe
File Zip	- ZIP 2 - ZIP 4 - ZIP 6	- 47cf035aa29599823cce99bef2467330 - a5acca59eb9ff6017064994aa2b76db1 - 733c9420aacd6067e0d7b3050ef3b2f4	.zip
File 7Zip	- 7Z 2	- e2d9c0b0a82113ce52d5334ffd24a876	.7z



Gambar 4.22 Daftar Sebelum Keseluruhan File Genap Dihapus Permanen

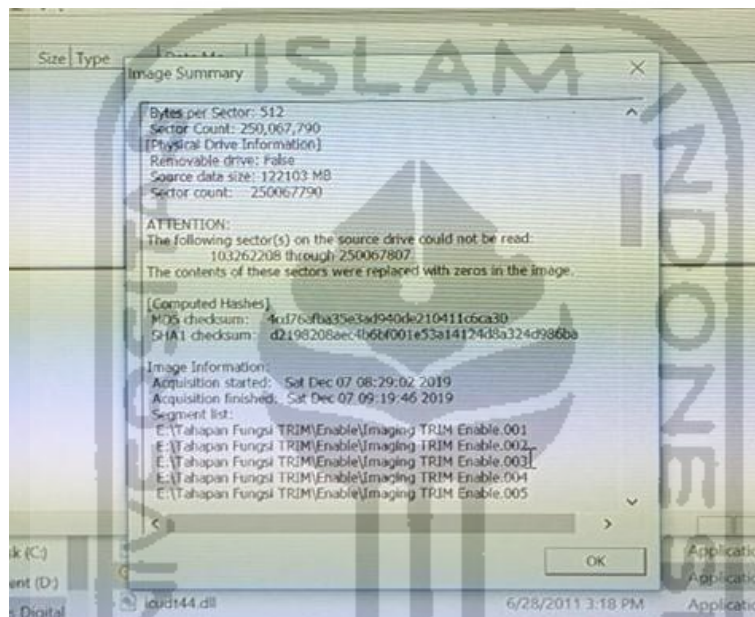
4.4.4 Teknik Akuisisi TRIM *Enable*

Berdasarkan penjelasan mengenai *enable*/aktif fungsi TRIM, akan ada beberapa tahapan yang digunakan dalam mengakuisisi SSD NVMe akan digambarkan dalam alur bagan sebagai berikut :



Gambar 4.23 Tahapan Teknik Akuisisi TRIM *Enable*

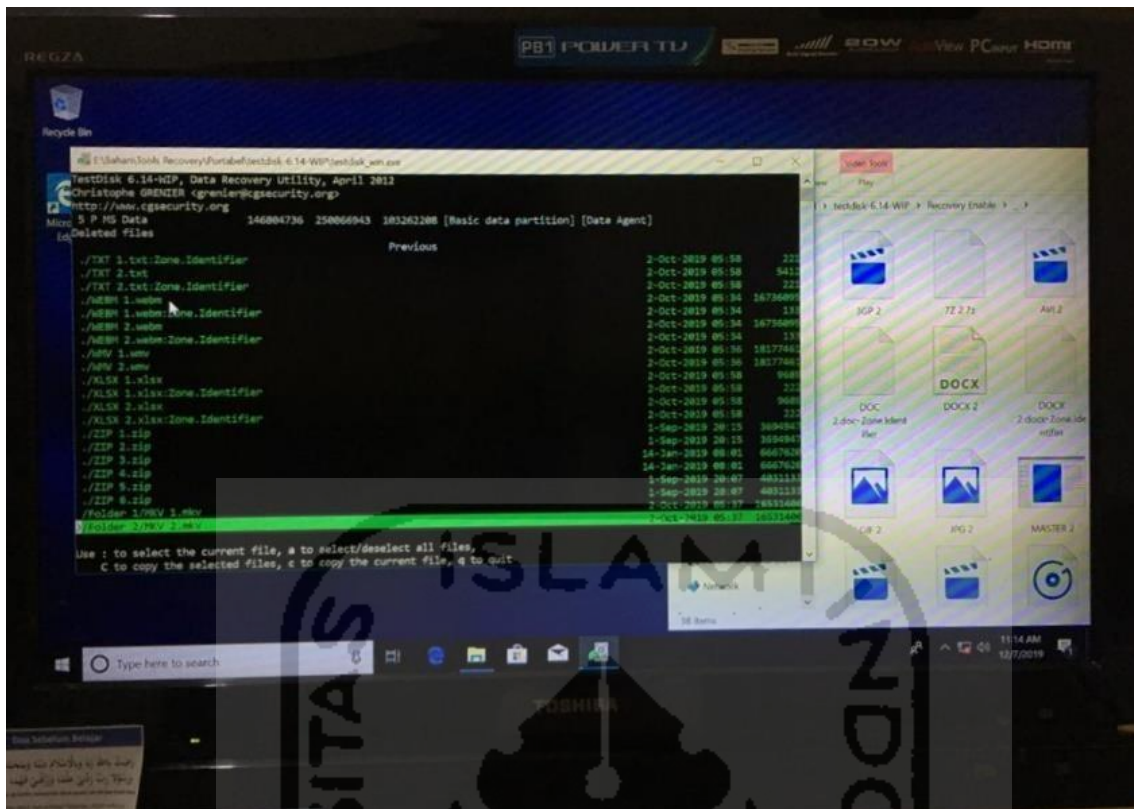
Langkah selanjutnya akuisisi fungsi TRIM *enable* yaitu menggunakan dock usb SSD SATA eksternal, usb diintegrasikan dengan komputer pertama agar menjaga integritas dan keaslian data, untuk melakukan praktek live akuisisi atau imaging menggunakan FTK Imager Portabel yang sudah ada di dalam usb SSD eksternal. Gambar 4.24 di bawah adalah hasil dari akuisisi SSD fungsi TRIM *enable* pada usb eksternal menggunakan FTK Imager Portable. Waktu yang dibutuhkan untuk live akuisisi partisi logical SSD M.2 NVMe Adata XPG SX6000 Lite 128GB fungsi TRIM *enable* menggunakan FTK Imager Portable adalah 50 menit 44 detik.



Gambar 4.24 Hasil Output Akuisisi TRIM *Enable* Menggunakan FTK Imager Portable

Gambar 4.24 di atas dapat disimpulkan bahwa SSD NVMe fungsi TRIM *enable* telah berhasil di akuisisi menggunakan FTK Imager Portable dengan mendapatkan nilai hash MD5 “4cd76afba35e3ad940de210411c6ca30” dan nilai hash SHA1 adalah “d2198208aec4b6bf001e53a14124d8a324d986ba”.

Khusus untuk melakukan praktek live *recovery* dalam penelitian ini menggunakan tools Testdisk guna untuk memperbandingkan hasil *recovery* data SSD NVMe fungsi TRIM *enable*. Gambar 4.25 di bawah adalah hasil potret dokumentasi dari *recovery* SSD NVMe fungsi TRIM *enable* pada usb SSD SATA eksternal menggunakan tool *recovery* Testdisk.



Gambar 4.25 Proses dan Hasil Output *Recovery TRIM Enable* Menggunakan Testdisk

Tahapan akuisisi TRIM *disable* dan TRIM *enable* dikatakan sebagai *partial acquisition* karena file yang diakuisisi hanya sebagian partisinya saja bukan keseluruhan isi SSD. Kedua tahapan akuisisi ini telah memenuhi persyaratan untuk dilakukannya *partial acquisition*. Hal ini berdasarkan persyaratan yang dipaparkan dalam SNI 27037:2014, adapun persyaratan dilakukannya *partial acquisition* sebagai berikut :

- a. Kapasitas penyimpanan terlalu besar untuk dilakukan akuisisi.
- b. Pentingnya sistem sehingga tidak memungkinkan untuk mematikan sistem.
- c. Ketika data yang diakuisisi hanya sebagian data atau data yang diperlukan saja.
- d. Ketika dibatasi oleh penegak hukum seperti surat perintah pencarian yang membatasi ruanglingkup akuisisi.

Ketika keputusan telah dibuat untuk melakukan *partial acquisition*. Kegiatan untuk akuisisi meliputi :

- a. Mengidentifikasi folder, file atau data apapun yang relevan sehingga memperoleh data yang diinginkan.
- b. Melakukan *partial acquisition* pada data tersebut untuk melakukan identifikasi lebih lanjut.

4.5 Pemeriksaan dan Analisis Output

Setelah melakukan imaging TRIM *disable* dan *enable*, berikut merupakan tahapan pemeriksaan untuk mendapatkan petunjuk atau informasi yang berkaitan dengan kasus. Sebelum melakukan pemeriksaan terhadap hasil akuisisi TRIM *disable* dan *enable*, hasil imaging yang asli harus di duplikasikan terlebih dahulu dan melihat kesamaan nilai hash antara file yang asli dengan salinannya guna untuk menjaga integritas dan keaslian imaging tersebut. Untuk menjaga keaslian barang bukti maka proses pemeriksaan adalah salinan file imagingnya.

Ada tiga tools yang digunakan untuk melakukan ekstraksi dan analisis yaitu Sleuth Kit Autopsy, Belkasoft Evidence Center, Teskdisk. Untuk melakukan pemeriksaan barang bukti tersebut memiliki beberapa tahapan pada umumnya yaitu preparation, ekstration dan analisis.

a. Preparation

Tahapan persiapan ini adalah mempersiapkan media penyimpanan untuk menyimpan salinan barang bukti digital atau hasil imaging untuk melakukan ekstraksi data. Proses tersebut guna untuk memastikan bahwa file yang akan dilakukan pemeriksaan dan analisis file/data yang telah terjaga keasliannya.

b. Extraction

Tahapan extraction ini adalah melakukan proses ekstraksi data hasil akuisisi/imaging. Selanjutnya hasil imaging yang akan dilakukan ekstraksi adalah salinan dari hasil imaging tersebut guna untuk menjaga integritas dan keaslian barang bukti tersebut. Tools untuk membantu proses ekstration imaging tersebut menggunakan Sleuth Kit Autopsy dan Belkasoft Evidence Center merupakan tools analisis dari investigasi digital forensik, kemudian melakukan pengembalian data.

c. Analisis

Merupakan tahapan untuk melakukan analisis terhadap hasil ekstration imaging. Dalam melakukan analisis, yang akan dianalisis adalah salinan dari file imaging bertujuan untuk mencari informasi yang tersimpan pada kasus.

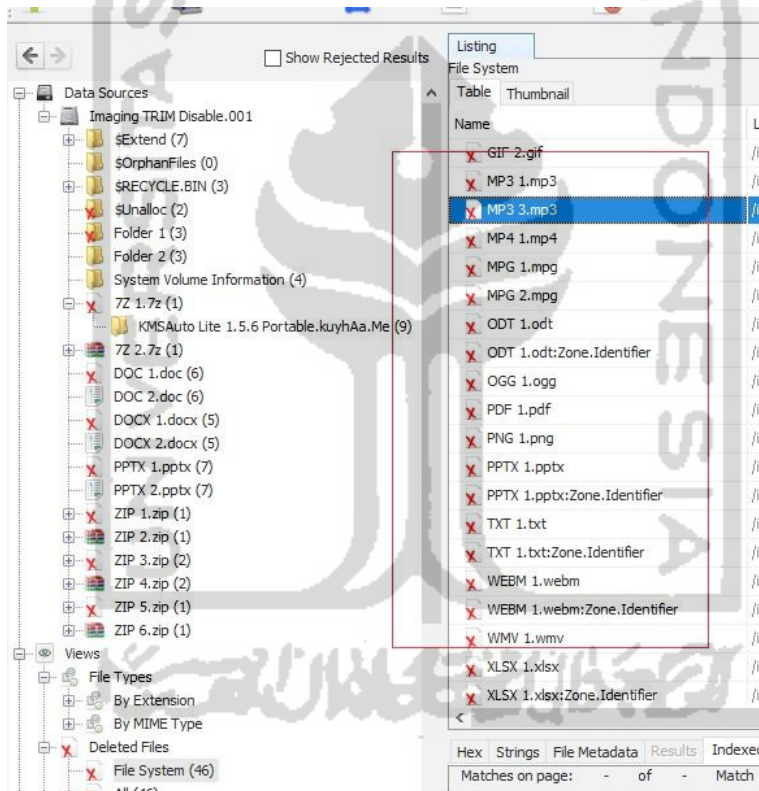
4.5.1 Pemeriksaan dan Analisis TRIM *Disable* Menggunakan Autopsy

Setelah berhasil melakukan live akuisisi/imaging dua fungsi TRIM *disable* dan *enable* dengan FTK Imager Portable. Selanjutnya melakukan tahapan pemeriksaan dan menganalisis. Pemeriksaan dan analisis yang dilakukan pada tahapan ini menggunakan tool forensik Sleuth Kit Autopsy.



Gambar 4.26 Pemeriksaan TRIM *Disable* dengan Sleuth Kit Autopsy













Gambar 4.26 adalah hasil akuisisi dari SSD M.2 NVMe Adata XPG SX6000 Lite dengan kapasitas 128034708480 bytes dengan *file system* NTFS (*New Technology File System*).



Gambar 4.27 Daftar File *Recovery Ganjil* TRIM *Disable* dengan Sleuth Kit Autopsy

Dapat disimpulkan pada gambar 4.27 ini dapat melakukan recovery semua file yang dihapus permanen dengan perintah SHIFT+DELETE pada SSD NVMe dengan fungsi TRIM *disable* bisa direcovery dengan tools forensik Sleuth Kit Autopsy. Tabel 4.4 di bawah ini adalah tabel ringkasan hasil *recovery* Autopsy *Forensics*.





Tabel 4.4 Daftar File Ganjil Hasil Analisis TRIM *Disable* dengan Sleuth Kit Autopsy

Trim Status		Disable		
Tools		Sleuth Kit Autopsy		
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature		Status Recovery		
File Dokumen	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : DOC 1.doc MD5 : 630a293939e5fc996076d2c2ec39a7c1 SHA1 : c7a12c327089fbe3de6917f01c07a3cb8b5a646e		d0 cf 11 e0	✓	
Nama file : DOCX 1.docx MD5 : 6db984ae2628503104cb46fab8b9ef8c SHA1 : 811767706c6dedb07721e2334183cffd93908abb		d0 cf 11 e0	✓	
Nama file : XLSX 1.xlsx MD5 : 56c424725531715f142e77ccc5cee774 SHA1 : 0e8ad73a6cb2573086d17b79a03ab5cbe77c3e5e		50 4b 03 04	✓	
Nama file : PPTX 1.pptx MD5 : 1d02e044e64e79994ab5a0ca871c6fe9 SHA1 : c45f505b05ae9d8a171065bdf109b140c038598e		50 4b 03 04	✓	
Nama file : PDF 1.pdf MD5 : 7a3801902be546b4ee026538f246e844 SHA1 : 83de136e1fc13b4e74158d9c8d27169295ce5753		25 50 44 46	✓	
Nama file : TXT 1.txt MD5 : 6bb11f42a5b591be9ec1a0e95a5cd00c SHA1 : b52cdb3aada6a51ecb52ffd6ef8c0b7dfbed778e		20 20 20 20	✓	
Nama file : ODT 1.odt MD5 : d9822aa6cbe227fc935665375152bacf SHA1 : 4d5dcf9a29d1d92d77dc4d8215ee76b717577500		50 4b 03 04	✓	
FILE Video				
Nama file : 3GP 1.3gp MD5 : cd5f422a723609bff58c699704f91d88 SHA1 : 5d7c170d622cdba4de7c97403ef70af36f1a8f77		66 74 79 70	✓	
Nama file : FLV 1.flv MD5 : 49f86ccba885b8eb2de17ece7f281434 SHA1 : f8f6e752108f5b5e2d1db7ff6a57a1d9b6016ca4		46 4c 56 01	✓	
Nama file : MPG 1.mpg MD5 : 293a2b5b3a18b1f283bcc2cbda358e0b SHA1 : 77af46417570aa78962d6db4deb16d341e7bac51		00 00 01 ba	✓	
Nama file : WEBM 1.webm MD5 : e75301e7337242951e90e6fbc598c8cb SHA1 : c2861b40f5a5f6334045c6bf96230f6778474b7f		1a 45 df a3	✓	
Nama file : MKV 1.mkv MD5 : b67c0c226b47bc77716aa30cd8d8d2c5 SHA1 : 75e6c0d69c3cb4f93b88e05765acab67c572a353		1a 45 df a3	✓	

Tabel 4.5 Daftar File Ganjil Hasil Analisis TRIM *Disable* dengan Autopsy (Lanjutan)

Trim Status			Disable	
Tools			Sleuth Kit Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : MOV 1.mov MD5 : 35208da889d863bc010741f9e2c7c25e SHA1 : 79a798afbba8e1a7bfe8d6be46fb7dfa6d130019		66 74 79 70 71 74 20 20	√	
Nama file : OGG 1.ogg MD5 : 8ca67608dcaec59718c25ed8bfa93c35 SHA1 : dd9cf50928d3a30323c2f805d5cd0153a68ef3fc		4f 67 67 53 00 02	√	
Nama file : WMV 1.wmv MD5 : e3935aaddb17432b48a0d45be6cfca9d SHA1 : 677083c5bc1de4a8c1830e0361fd334a1140051b		30 26 b2 75 8e 66 cf 11	√	
Nama file : AVI 1.avi MD5 : 72562d25302f0698c19040a6d50ceb0c SHA1 : ab7007f37ad838976b8e9d4d4c755fa355deab90		41 56 49 20 4c 49 53	√	
Nama file : MP4 1.mp4 MD5 : 0094fb55e09791154276f456d9982a0a SHA1 : 5780166537985e77d0ea3a601adb6e707d574ef3		66 74 79 70 6d 70 34 32	√	
File Gambar				
Nama file : GIF 1.gif MD5 : ed28cc871584230543b5a2d8a386a2cb SHA1 : b981419393314ea3d20d80c41715a2eb1e039b2b		47 49 46 38 39 61	√	
Nama file : JPG 1.jpg MD5 : d4fc57bddd2ed31d53f00002791a245d SHA1 : 77af0aebff4bf31b1dc54f0a15c133fa140c0c81		ff d8 ff e0	√	
Nama file : PNG 1.png MD5 : a820b280e93967956c449b342125add8 SHA1 : f5c0b6a7946dccc88904ca32944c4b8f5c52aa29		89 50 4e 47	√	
Nama file : BMP 1.bmp MD5 : 8cad97ecf36337caebdd53fd81258dd SHA1 : 37fb769bbdf892335dc21bd6b527eca381043102		42 4d	√	
File Musik				
Nama file : MP3 1.mp3 MD5 : d004ad9c716fbb7262d09fcd812b7bdb SHA1 : c8532124d281a38687cde4ae15389a927934dd31		49 44 33 03	√	
Nama file : MP3 3.mp3 MD5 : 2178cecb48c6473308487117d273eb1e SHA1 : 7b5d4cae778f07c92ba0246323fb582865422e82		49 44 33 03	√	
File Aplikasi				
Nama file : MASTER 1.exe MD5 : 562f2ea6e41020fd7bf5426bd77cd59c SHA1 : 7f9eaa9aa18ff1dfd77cb367ae868b761a4c5204		4d 5a 90 00 03 00 00 00	√	
Nama file : MASTER 3.exe MD5 : 1abf96d2ddec838763cec88285a1fc6f SHA1 : c60146bc8744d55f9753fce5b32881fa355db683		4d 5a 50 00 02 00 00 00	√	
Nama file : MASTER 5.exe MD5 : 076d6a1f9c0e22362ca71d0e254202b0 SHA1 : 1f1a1a8cfa672ed49119e8fe424bc6491771000		4d 5a 90 00 03 00 00 00	√	

Tabel 4.6 Daftar File Ganji Hasil Analisis TRIM *Disable* dengan Autopsy (Lanjutan)

Trim Status			Disable	
Tools			Sleuth Kit Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Zip	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : ZIP 1.zip MD5 : 47cf035aa29599823cce99bef2467330 SHA1 : 69de9b3f3479c0da03ac463dcfd5db5ca2c9784a		50 4b 03 04	✓	
Nama file : ZIP 3.zip MD5 : a5acca59eb9ff6017064994aa2b76db1 SHA1 : 29e8553a3c0aba7775b574a6f9af551fa816ffa9		50 4b 03 04	✓	
Nama file : ZIP 5.zip MD5 : 733c9420aacd6067e0d7b3050ef3b2f4 SHA1 : 125045d49c926b645e0433c6011e46ed7e7c870e		50 4b 03 04	✓	
File 7z				
Nama file : 7Z 1.7z MD5 : e2d9c0b0a82113ce52d5334ffd24a876 SHA1 : 0e181cbe6a879275437db7eb928279cc8bbc8c1a		37 7a bc af 27 1c	✓	

Dari hasil pemeriksaan dan analisa tabel 4.4 di atas, secara keseluruhan file dapat *direcovery* dengan baik menggunakan tool forensik yaitu Sleuth Kit Autopsy dengan skenario penghapusan permanen perintah SHIFT+DELETE implementasi fungsi TRIM *disable*. Kemudian melihat keaslian barang bukti dari file tersebut, dapat diasumsikan bahwa keseluruhan file mempunyai nilai MD5/SHA1 yang idientik dan juga dengan melihat file signature pada file sesuai dengan setiap format filenya, kemudian metode live akuisisi pada SSD NVMe dapat digunakan untuk fungsi TRIM *disable*.

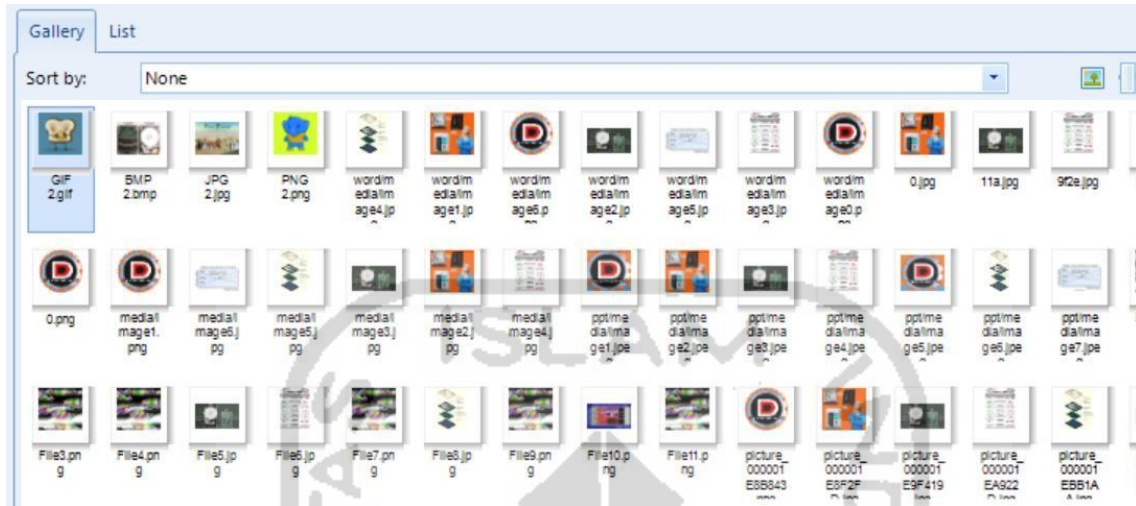
4.5.2 Pemeriksaan dan Analisis TRIM *Disable* Menggunakan Belkasoft

Tahapan berikutnya setelah dilakukannya pemeriksaan dan analisis pada *Sleuth Kit Autopsy* adalah mencoba melakukan pemeriksaan dan analisis lainnya dengan menggunakan tools forensik Belkasoft Evidence Center. Berikut ini adalah gambar 4.28 hasil ekstraksi imaging FTK Imager Portable dari SSD M.2 NVMe Adata XPG SX6000 Lite dengan kapasitas 52870250496 byte dengan *file system* NTFS, jika dibandingkan ukuran file pemeriksaan tools autopsy sebelumnya berada di angka kapasistas 128034708480 bytes.

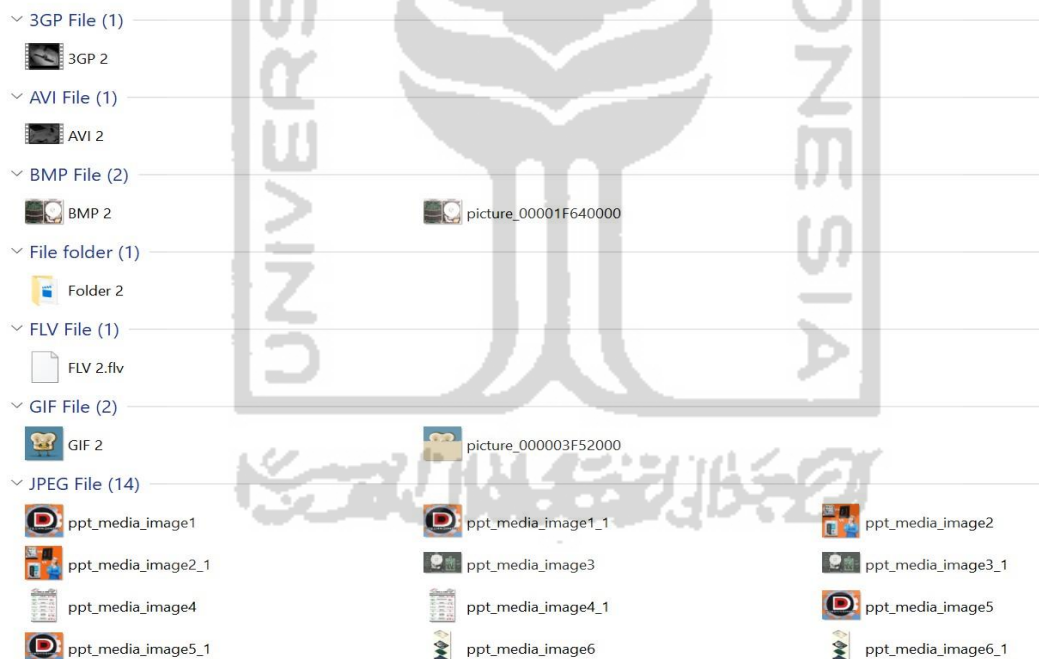
Offset (bytes)	Label	File System	Size	Drive Letter	Sector size (bytes)
0	Partition	NTFS	50421 Gb	image:\vol_0	512

Gambar 4.28 Pemeriksaan TRIM *Disable* dengan Belkasoft Evidence Center

Berdasarkan pengamatan pada pemeriksaan ini, waktu yang dibutuhkan untuk pemeriksaan dan verifikasi imaging SSD NVMe Adata XPG SX6000 Lite dengan kapasitas 52870250496 byte dengan tool forensik Belkasoft Evidence Center adalah 56 menit lebih 58 detik.



Gambar 4.29 Daftar File Setelah Pemeriksaan TRIM *Disable* dengan Belkasoft



Gambar 4.30 Daftar File *Recovery* TRIM *Disable* dengan Belkasoft Evidence Center

Gambar 4.29 dan 4.30 adalah daftar file setelah melakukan pemeriksaan dan recovery, hanya file jenis file gambar yang dapat ditampilkan dan dapat disimpulkan hampir semua file yang dihapus permanen dengan perintah keyboard SHIFT+DELETE pada SSD NVMe dengan fungsi TRIM *disable* tidak bisa direcovery sepenuhnya oleh tool forensik Belkasoft Evidence Center. Hasil *recovery* tool Belkasoft akan dirangkum pada tabel 4.7 berikut ini :

Tabel 4.7 Daftar File Ganjil Hasil Analisis TRIM *Disable* dengan Belkasoft Evidence

Trim Status			Disable	
Tools			Belkasoft Evidence	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Dokumen	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : DOC 1.doc MD5 : - SHA1 : -	-	-		√
Nama file : DOCX 1.docx MD5 : - SHA1 : -	-	-		√
Nama file : XLSX 1.xlsx MD5 : - SHA1 : -	-	-		√
Nama file : PPTX 1.pptx MD5 : - SHA1 : -	-	-		√
Nama file : PDF 1.pdf MD5 : - SHA1 : -	-	-		√
Nama file : TXT 1.txt MD5 : - SHA1 : -	-	-		√
Nama file : ODT 1.odt MD5 : - SHA1 : -	-	-		√
File Video				
Nama file : 3GP 1.3gp MD5 : - SHA1 : -	-	-		√
Nama file : FLV 1.flv MD5 : - SHA1 : -	-	-		√
Nama file : MPG 1.mpg MD5 : - SHA1 : -	-	-		√
Nama file : WEBM 1.webm MD5 : - SHA1 : -	-	-		√
Nama file : MKV 1.mkv MD5 : - SHA1 : -	-	-		√
Nama file : MOV 1.mov MD5 : - SHA1 : -	-	-		√
Nama file : OGG 1.ogg MD5 : - SHA1 : -	-	-		√
Nama file : WMV 1.wmv MD5 : - SHA1 : -	-	-		√

Tabel 4.8 Daftar File Ganjil Hasil Analisis TRIM *Disable* dengan Belkasoft (Lanjutan)

Trim Status			Disable	
Tools			Belkasoft Evidence	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : AVI 1.avi MD5 : - SHA1 : -	-	-		√
Nama file : MP4 1.mp4 MD5 : - SHA1 : -	-	-		√
File Gambar				
Nama file : picture_000003F52000.gif MD5 : 7ac62754ea19fc0fede4f2f902a9be94 SHA1 : d8d96864fb8e777648e4fbb077eb76bc0b782e7c		47 49 46 38 39 61		√
Nama file : picture_00000414A000.jpg MD5 : d4fc57bddd2ed31d53f00002791a245d SHA1 : 77af0aebff4bf31b1dc54f0a15c133fa140c0c81		ff d8 ff e0	√	
Nama file : picture_000014A33000.png MD5 : ecec4d4b31f17d5123552f4e4cb25edd SHA1 : 61085f448c9abb4607e632a0793c52272d414571		89 50 4e 47	√	
Nama file : picture_00001F640000.bmp MD5 : 8cad97ecf36337caebdd53fd81258dd SHA1 : 37fb769bbdf892335dc21bd6b527eca381043102		42 4d	√	
File Musik				
Nama file : MP3 1.mp3 MD5 : - SHA1 : -	-	-		√
Nama file : MP3 3.mp3 MD5 : - SHA1 : -	-	-		√
File Aplikasi				
Nama file : MASTER 1.exe MD5 : - SHA1 : -	-	-		√
Nama file : MASTER 3.exe MD5 : - SHA1 : -	-	-		√
Nama file : MASTER 5.exe MD5 : - SHA1 : -	-	-		√
File Zip				
Nama file : ZIP 1.zip MD5 : - SHA1 : -	-	-		√
Nama file : ZIP 3.zip MD5 : - SHA1 : -	-	-		√
Nama file : ZIP 5.zip MD5 : - SHA1 : -	-	-		√

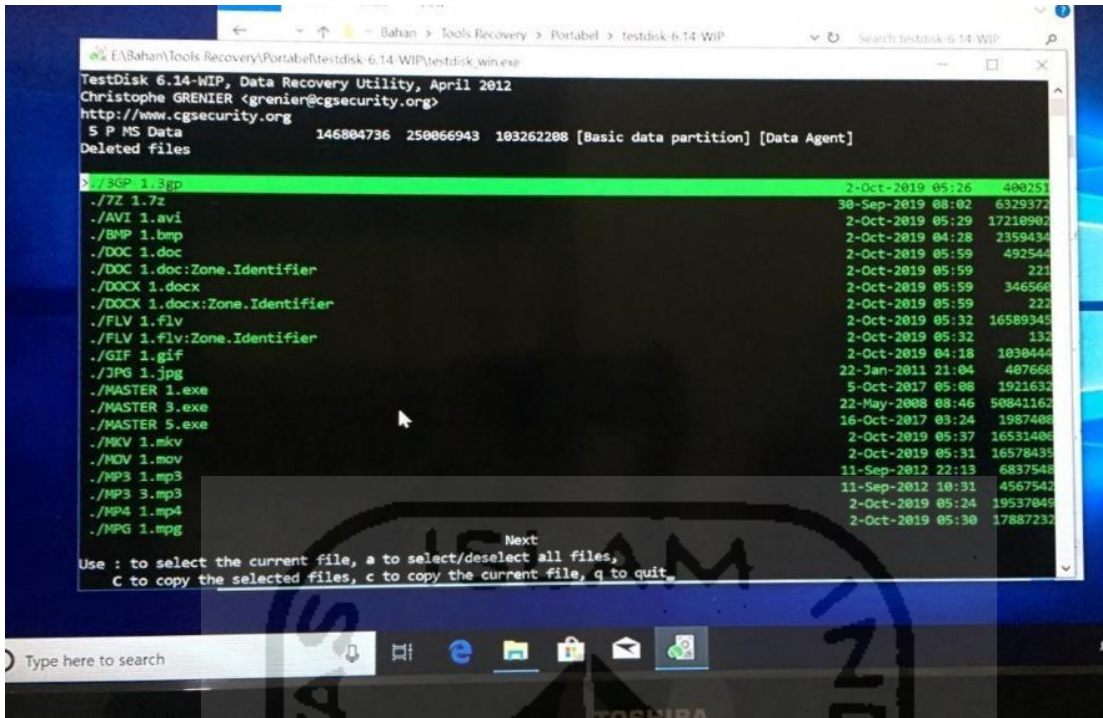
Tabel 4.9 Daftar File Ganjil Hasil Analisis TRIM *Disable* dengan Belkasoft (Lanjutan)

Trim Status			Disable	
Tools			Belkasoft Evidence	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File 7z	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : 7Z 1.7z MD5 : - SHA1 : -	-	-		√

Pada pemeriksaan TRIM disable menggunakan tools Belkasoft Evidence Center, file yang sudah terhapus permanen fungsi TRIM disable dapat melakukan recovery terhadap file jenis ekstensi .jpg, .gif, .png, dan .bmp. Tetapi label nama berubah seperti picture_00000414A000.jpg, picture_000014A33000.png, dan picture_00001F640000.bmp, sedangkan file ekstensi .gif mengalami kerusakan. Dapat disimpulkan bahwa Belkasoft saat ini tidak bisa mendukung analisis digital forensik dengan permasalahan *recovery* sepenuhnya.

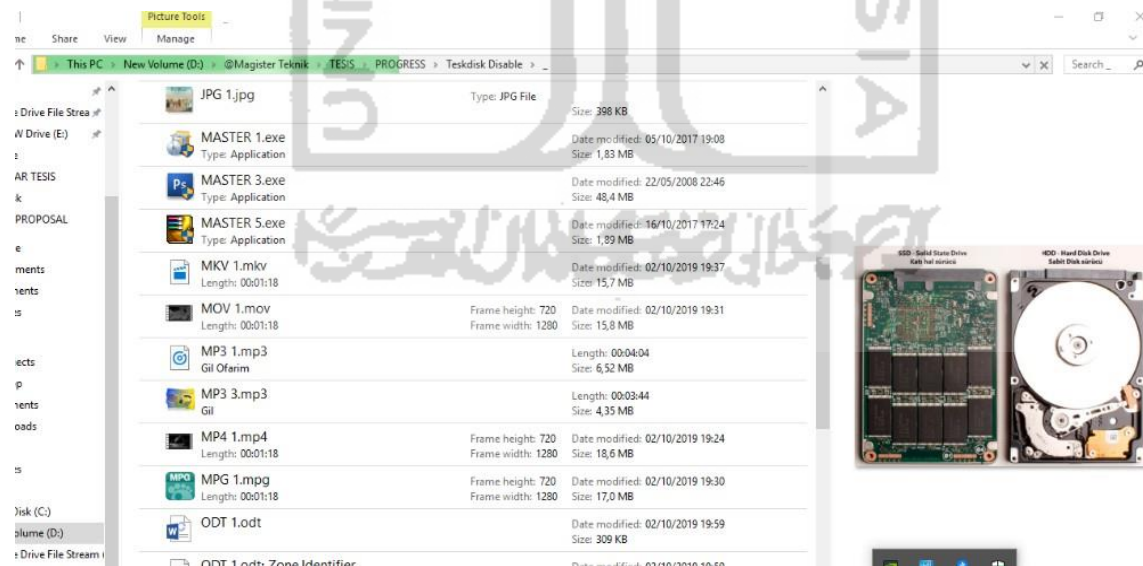
4.5.3 Pemeriksaan dan Analisis TRIM *Disable* Menggunakan Testdisk

Tahapan berikutnya setelah dilakukannya pemeriksaan dan analisis hasil imaging pada *Sleuth Kit Autopsy* dan Belkasoft Evidence Center, kemudian melakukan praktek pemeriksaan dan analisis yang telah *direcovery* menggunakan tool khusus *recovery* yaitu Testdisk guna untuk memperbandingkan hasil *recovery* data SSD NVMe fungsi TRIM *disable*/nonaktif dari tools forensik seperti *Sleuth Kit Autopsy* dan Belkasoft Evidence Center.



Gambar 4.31 Proses *Recovery TRIM Disable* Menggunakan Testdisk

Berdasarkan pengamatan pada pemeriksaan ini, waktu yang dibutuhkan untuk mengembalikan data pada partisi SSD NVMe Adata XPG SX6000 Lite dengan tool *recovery* testdisk tidak membutuhkan waktu recovery, karna testdisk membangun file kembali pada partisi cache/buffer yg ada pada controller arsitektur SSD (Grenier, 2019).














Gambar 4.32 Daftar File *Recovery TRIM Disable* dengan Testdisk

Gambar 4.31 dan 4.32 adalah daftar file setelah melakukan pemeriksaan dan recovery, semua file dengan label ganjil dapat direcovery atau tampil dengan baik tanpa ada kerusakan file dan dapat disimpulkan hampir semua file yang dihapus permanen dengan

perintah keyboard SHIFT+DELETE pada SSD NVMe dengan fungsi TRIM *disable* bisa *direcovery* oleh tool *recovery* Testdisk. Khusus pada tahapan analisis, tool *recovery* testdisk tidak memiliki kelebihan untuk pengecekan nilai keaslian barang bukti atau hash dan MD5 pada file, dikarenakan Testdisk hanya untuk melakukan *recovery* pada partisi, maka perlu menggunakan tool analisis tambahan yaitu Hashmyfile. Hasil *recovery* tool Testdisk akan dirangkum pada tabel 4.10 berikut ini :








Tabel 4.10 Daftar File Ganjil Hasil Analisis TRIM *Disable* dengan Testdisk

Trim Status			Disable	
Tools			Testdisk	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Dokumen	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : DOC 1.doc MD5 : 630a293939e5fc996076d2c2ec39a7c1 SHA1 : c7a12c327089fbc3de6917f01c07a3cb8b5a646e		d0 cf 11 e0	√	
Nama file : DOCX 1.docx MD5 : 6db984ae2628503104cb46fab8b9ef8c SHA1 : 811767706c6dedb07721e2334183cffd93908abb		d0 cf 11 e0	√	
Nama file : XLSX 1.xlsx MD5 : 56c424725531715f142e77ccc5cee774 SHA1 : 0e8ad73a6cb2573086d17b79a03ab5cbe77c3e5e		50 4b 03 04	√	
Nama file : PPTX 1.pptx MD5 : 1d02e044e64e79994ab5a0ca871c6fe9 SHA1 : c45f505b05ae9d8a171065bdf109b140c038598e		50 4b 03 04	√	
Nama file : PDF 1.pdf MD5 : 7a3801902be546b4ee026538f246e844 SHA1 : 83de136e1fc13b4e74158d9c8d27169295ce5753		25 50 44 46	√	
Nama file : TXT 1.txt MD5 : 6bb11f42a5b591be9ec1a0e95a5cd00c SHA1 : b52cdb3aada6a51ecb52ffd6ef8c0b7dfbed778e		20 20 20 20	√	
Nama file : ODT 1.odt MD5 : d9822aa6cbe227fc935665375152bacf SHA1 : 4d5dcf9a29d1d92d77dc4d8215ee76b717577500		50 4b 03 04	√	
FILE Video				
Nama file : 3GP 1.3gp MD5 : cd5f422a723609bff58c699704f91d88 SHA1 : 5d7c170d622cdba4de7c97403ef70af36f1a8f77		66 74 79 70	√	
Nama file : FLV 1.flv MD5 : 49f86ccb885b8eb2de17ece7f281434 SHA1 : f8f6e752108f5b5e2d1db7ff6a57a1d9b6016ca4		46 4c 56 01	√	
Nama file : MPG 1.mpg MD5 : 293a2b5b3a18b1f283bcc2cbda358e0b SHA1 : 77af46417570aa78962d6db4deb16d341e7bac51		00 00 01 ba	√	
Nama file : WEBM 1.webm MD5 : e75301e7337242951e90e6fbc598c8cb SHA1 : c2861b40f5a5f6334045c6bf96230f6778474b7f		1a 45 df a3	√	

Tabel 4.11 Daftar File Ganjil Hasil Analisis TRIM *Disable* dengan Testdisk (Lanjutan)

Trim Status			Disable	
Tools			Testdisk	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : MKV 1.mkv MD5 : b67c0c226b47bc77716aa30cd8d8d2c5 SHA1 : 75e6c0d69c3cb4f93b88e05765acab67c572a353		1a 45 df a3	√	
Nama file : MOV 1.mov MD5 : 35208da889d863bc010741f9e2c7c25e SHA1 : 79a798afbba8e1a7bfe8d6be46fb7dfa6d130019		66 74 79 70 71 74 20 20	√	
Nama file : OGG 1.ogg MD5 : 8ca67608dcaec59718c25ed8bfa93c35 SHA1 : dd9cf50928d3a30323c2f805d5cd0153a68ef3fc		4f 67 67 53 00 02	√	
Nama file : WMV 1.wmv MD5 : e3935aaddb17432b48a0d45be6cfca9d SHA1 : 677083c5bc1de4a8c1830e0361fd334a1140051b		30 26 b2 75 8e 66 cf 11	√	
Nama file : AVI 1.avi MD5 : 72562d25302f0698c19040a6d50ceb0c SHA1 : ab7007f37ad838976b8e9d4d4c755fa355deab90		41 56 49 20 4c 49 53	√	
Nama file : MP4 1.mp4 MD5 : 0094fb55e09791154276f456d9982a0a SHA1 : 5780166537985e77d0ea3a601adb6e707d574ef3		66 74 79 70 6d 70 34 32	√	
File Gambar				
Nama file : GIF 1.gif MD5 : ed28cc871584230543b5a2d8a386a2cb SHA1 : b981419393314ea3d20d80c41715a2eb1e039b2b		47 49 46 38 39 61	√	
Nama file : JPG 1.jpg MD5 : d4fc57bddd2ed31d53f00002791a245d SHA1 : 77af0aebff4bf31b1dc54f0a15c133fa140c0c81		ff d8 ff e0	√	
Nama file : PNG 1.png MD5 : a820b280e93967956c449b342125add8 SHA1 : f5c0b6a7946dccc88904ca32944c4b8f5c52aa29		89 50 4e 47	√	
Nama file : BMP 1.bmp MD5 : 8cad97ecf36337caebdd53fd81258dd SHA1 : 37fb769bbdf892335dc21bd6b527eca381043102		42 4d	√	
File Musik				
Nama file : MP3 1.mp3 MD5 : d004ad9c716fbb7262d09fcd812b7bdb SHA1 : c8532124d281a38687cde4ae15389a927934dd31		49 44 33 03	√	
Nama file : MP3 3.mp3 MD5 : 2178cecb48c6473308487117d273eb1e SHA1 : 7b5d4cae778f07c92ba0246323fb582865422e82		49 44 33 03	√	

Tabel 4.12 Daftar File Ganji Hasil Analisis TRIM *Disable* dengan Autopsy (Lanjutan)

Trim Status			Disable	
Tools			Testdisk	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Aplikasi	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : MASTER 1.exe MD5 : 562f2ea6e41020fd7bf5426bd77cd59c SHA1 : 7f9eaa9aa18ff1dfd77cb367ae868b761a4c5204		4d 5a 90 00 03 00 00 00	√	
Nama file : MASTER 3.exe MD5 : 1abf96d2ddec838763cec88285a1fc6f SHA1 : c60146bc8744d55f9753fce5b32881fa355db683		4d 5a 50 00 02 00 00 00	√	
Nama file : MASTER 5.exe MD5 : 076d6a1f9c0e22362ca71d0e254202b0 SHA1 : 1f1a1a8cfca672ed49119e8fe424bc6491771000		4d 5a 90 00 03 00 00 00	√	
File Zip				
Nama file : ZIP 1.zip MD5 : 47cf035aa29599823cce99bef2467330 SHA1 : 69de9b3f3479c0da03ac463dcfd5db5ca2c9784a		50 4b 03 04	√	
Nama file : ZIP 3.zip MD5 : a5acca59eb9ff6017064994aa2b76db1 SHA1 : 29e8553a3c0aba7775b574a6f9af551fa816ffa9		50 4b 03 04	√	
Nama file : ZIP 5.zip MD5 : 733c9420aacd6067e0d7b3050ef3b2f4 SHA1 : 125045d49c926b645e0433c6011e46ed7e7c870e		50 4b 03 04	√	
File 7z				
Nama file : 7Z 1.7z MD5 : e2d9c0b0a82113ce52d5334ffd24a876 SHA1 : 0e181cbe6a879275437db7eb928279cc8bbc8c1a		37 7a bc af 27 1c	√	

Berdasarkan tabel 4.10 di atas, pemeriksaan *recovery tools* Testdisk dan analisis menggunakan Hashmyfile, secara keseluruhan file dapat *direcovery* dengan baik menggunakan tool *recovery* yaitu Testdisk dengan skenario penghapusan permanen implementasi fungsi TRIM *disable*. Kemudian untuk melihat keaslian/analisis dari file tersebut melakukan teknik hashing dengan tool Hashmyfile, jika diasumsikan bahwa keseluruhan hasil *recovery* memiliki nilai MD5/SHA1 sama, dapat dikatakan file identik atau integritas barang bukti terjaga. Dapat disimpulkan bahwa Testdisk saat ini bisa memulihkan dan menjaga integritas dan keaslian file dalam analisis digital forensik.

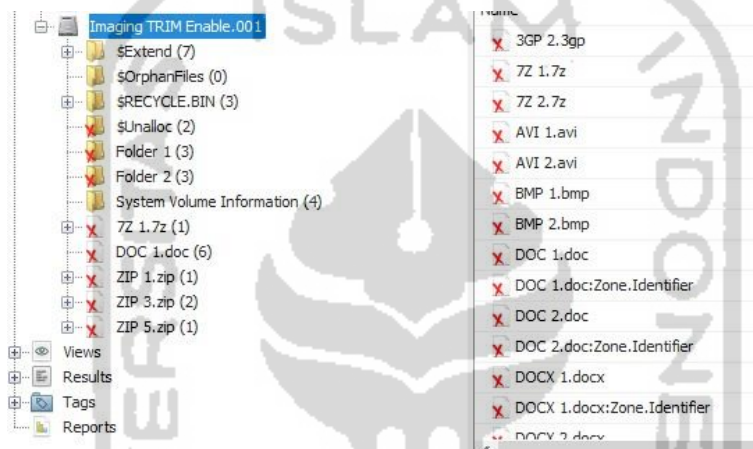
4.5.4 Pemeriksaan dan Analisis TRIM *Enable* Menggunakan Autopsy

Setelah berhasil melakukan akuisisi/imaging fungsi TRIM *enable*, selanjutnya melakukan tahapan pemeriksaan dan analisis. Pemeriksaan dan analisis yang dilakukan pada tahapan ini menggunakan tool forensik Sleuth Kit Autopsy.

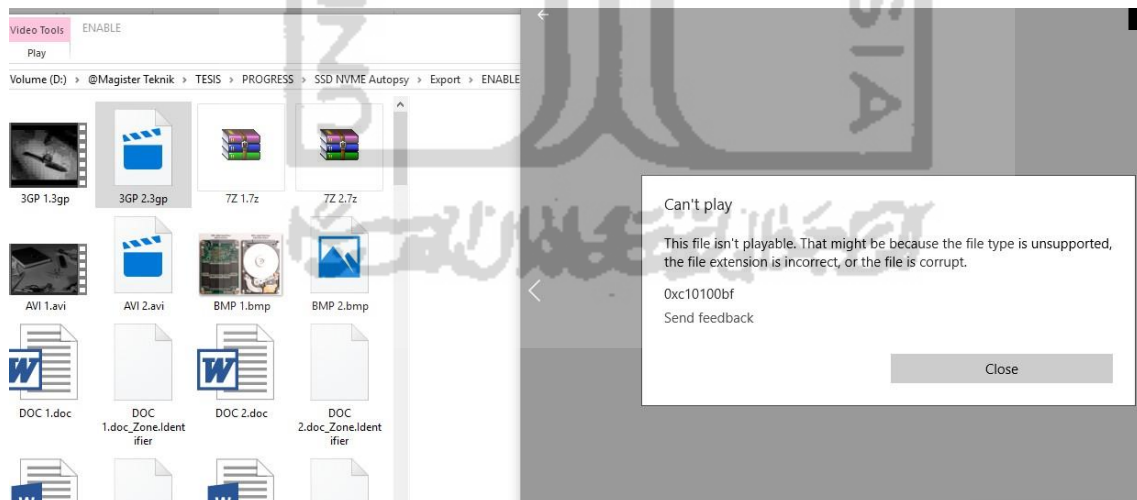


Gambar 4.32 Pemeriksaan dengan Sleuth Kit Autopsy TRIM *Enable*

Gambar 4.32 adalah hasil imaging dari SSD M.2 NVMe Adata XPG SX6000 Lite dengan kapasitas 128034708480 bytes dengan file system NTFS (New Technology File System).



Gambar 4.33 Daftar File Genap Setelah Pemeriksaan TRIM *Enable* dengan Autopsy









Gambar 4.34 Daftar File *Recovery* TRIM *Enable* dengan Sleuth Kit Autopsy




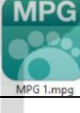

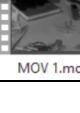
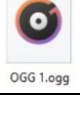
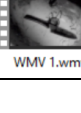
Dapat disimpulkan pada gambar 4.34 dan 4.35 ini tidak semua file yang sudah dihapus permanen dengan perintah SHIFT+DELETE pada SSD NVMe dengan fungsi TRIM *enable* dengan tools forensik Sleuth Kit Autopsy. Ada satu file label ganjil yang tidak dapat

direcovery, yaitu .mpg bahwa file tersebut terindikasi kerusakan. Sedangkan file label genap saat penghapusan TRIM enable tidak ada satupun yang dapat dibaca. File-file yang bisa *direcovery* sempurna dengan tool Sleuth Kit Autopsy pada penghapusan fungsi TRIM *enable* adalah file label ganjil, karena file label ganjil tersebut sudah terhapus sebelumnya saat status TRIM disable. Secara ringkas dapat dilihat pada tabel 4.13 di bawah ini :

Tabel 4.9 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Autopsy

Trim Status			Enable	
Tools			Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Dokumen	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : DOC 1.doc MD5 : 630a293939e5fc996076d2c2ec39a7c1 SHA1 : c7a12c327089fbc3de6917f01c07a3cb8b5a646e		d0 cf 11 e0	√	
Nama file : DOC 2.doc MD5 : 00f8e30447dbfb9e5e5e3d820826c52f SHA1 : 8fd2a48cece30294c52ccedc986a6b8c65896760				√
Nama file : DOCX 1.docx MD5 : 6db984ae2628503104cb46fab8b9ef8c SHA1 : 811767706c6dedb07721e2334183cfd93908abb		d0 cf 11 e0	√	
Nama file : DOCX 2.docx MD5 : 821d1ae6d9543f57e95a82c26fcbcb6 SHA1 : e64a608643b8acfc03a3f1fbd86801587d1ecba9				√
Nama file : XLSX 1.xlsx MD5 : 56c424725531715f142e77ccc5cee774 SHA1 : 0e8ad73a6cb2573086d17b79a03ab5cbe77c3e5e		50 4b 03 04	√	
Nama file : XLSX 2.xlsx MD5 : c4e4f86f732fd5873e050500e18bb414 SHA1 : 3b14143368bc900dbce275abd9025c81fcd1ca0a				√
Nama file : PPTX 1.pptx MD5 : 1d02e044e64e79994ab5a0ca871c6fe9 SHA1 : c45f505b05ae9d8a171065bdf109b140c038598e		50 4b 03 04	√	
Nama file : PPTX 2.pptx MD5 : 0b080dffa116ee20924fe1bc5817bf3e SHA1 : c9e9efe4fe768e067262e44d42560346f3d8ea42				√
Nama file : PDF 1.pdf MD5 : 7a3801902be546b4ee026538f246e844 SHA1 : 83de136e1fc13b4e74158d9c8d27169295ce5753		25 50 44 46	√	
Nama file : PDF 2.pdf MD5 : c44b1979483b451f9b1e91b4abba44c3 SHA1 : 5c8c29f3cad44631c6e5dbf47f8ead47b4fcc15				√
Nama file : TXT 1.txt MD5 : 6bb11f42a5b591be9ec1a0e95a5cd00c SHA1 : b52cdb3aada6a51ecb52ffd6ef8c0b7dfbed778e		20 20 20 20	√	
Nama file : TXT 2.txt MD5 : 9ba601b1c111c9ebc50b523d09ea5f21 SHA1 : 7dbe175eed4b81be86e43129893b8ec8b5062da8				√

Tabel 4.10 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Autopsy (Lanjutan)

Trim Status			Enable	
Tools			Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Dokumen	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : ODT 1.odt MD5 : d9822aa6cbe227fc935665375152bacf SHA1 : 4d5dcf9a29d1d92d77dc4d8215ee76b717577500		50 4b 03 04	√	
Nama file : ODT 2.odt MD5 : 7d559ed79eca8de750e63f822ab17ee1 SHA1 : 1cf841fb7d0acd8cb89c1df02cd609143a0fbfb4				√
FILE Video				
Nama file : 3GP 1.3gp MD5 : cd5f422a723609bff58c699704f91d88 SHA1 : 5d7c170d622cdba4de7c97403ef70af36f1a8f77		66 74 79 70	√	
Nama file : 3GP 2.3gp MD5 : 299e23fd97392eae859b7117dfb91634 SHA1 : 68ac1fe0cd4f0e6ab76e7fbd33ad8e8941b3cc7				√
Nama file : FLV 1.flv MD5 : 49f86ccba885b8eb2de17ece7f281434 SHA1 : f8f6e752108f5b5e2d1db7ff6a57a1d9b6016ca4		46 4c 56 01	√	
Nama file : FLV 2.flv MD5 : - SHA1 : -				√
Nama file : MPG 1.mpg MD5 : - SHA1 : -		00 00 01 ba		√
Nama file : MPG 2.mpg MD5 : - SHA1 : -				√
Nama file : WEBM 1.webm MD5 : e75301e7337242951e90e6fbc598c8cb SHA1 : c2861b40f5a5f6334045c6bf96230f6778474b7f		1a 45 df a3	√	
Nama file : WEBM 2.webm MD5 : 7d57e1bbbf413f91ccbf55a0f8df9fd SHA1 : 2ba1191f295a3680e1780e023d6a5ed5dc1cdf43				√
Nama file : MOV 1.mov MD5 : 35208da889d863bc010741f9e2c7c25e SHA1 : 79a798afbba8e1a7bfe8d6be46fb7dfa6d130019		66 74 79 70 71 74 20 20	√	
Nama file : MOV 2.mov MD5 : 4e0514db784fa7ce788c39dcf70e6343 SHA1 : c0d38b0a3cc12b60f52dcb402ada86b88550924e				√
Nama file : OGG 1.ogg MD5 : 8ca67608dcaec59718c25ed8bfa93c35 SHA1 : dd9cf50928d3a30323c2f805d5cd0153a68ef3fc		4f 67 67 53 00 02	√	
Nama file : OGG 2.ogg MD5 : 3ae510eb17e1ece3125ee603b4904b2d SHA1 : 9b40fac4ed0994827fc48fbb932cd5577a99b641				√
Nama file : WMV 1.wmv MD5 : e3935aaddb17432b48a0d45be6cfca9d SHA1 : 677083c5bc1de4a8c1830e0361fd334a1140051b		30 26 b2 75 8e 66 cf 11	√	

Tabel 4.11 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Autopsy (Lanjutan)

Trim Status			Enable	
Tools			Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : WMV 2.wmv MD5 : c9607cc9e10e03659810d4735ee5570e SHA1 : c020b670420026822cb92148b7b93faadf736942				√
Nama file : AVI 1.avi MD5 : 72562d25302f0698c19040a6d50ceb0c SHA1 : ab7007f37ad838976b8e9d4d4c755fa355deab90		41 56 49 20 4c 49 53	√	
Nama file : AVI 2.avi MD5 : a13a97acca90cce38197742e79ebd152 SHA1 : 54af4c0c0af5fe7171820d13813c28d4ae786948				√
Nama file : MP4 1.mp4 MD5 : 0094fb55e09791154276f456d9982a0a SHA1 : 5780166537985e77d0ea3a601adb6e707d574ef3		66 74 79 70 6d 70 34 32	√	
Nama file : MP4 2.mp4 MD5 : - SHA1 : -				√
File Gambar				
Nama file : GIF 1.gif MD5 : ed28cc871584230543b5a2d8a386a2cb SHA1 : b981419393314ea3d20d80c41715a2eb1e039b2b		47 49 46 38 39 61	√	
Nama file : GIF 2.gif MD5 : - SHA1 : -				√
Nama file : JPG 1.jpg MD5 : d4fc57bddd2ed31d53f00002791a245d SHA1 : 77af0aebff4bf31b1dc54f0a15c133fa140c0c81		ff d8 ff e0	√	
Nama file : JPG 2.jpg MD5 : 756a62e9962edb459bd97b326c59747d SHA1 : fa5a986f53012328281407e069f30e1ebf2b7452				√
Nama file : PNG 1.png MD5 : a820b280e93967956c449b342125add8 SHA1 : f5c0b6a7946dccc88904ca32944c4b8f5c52aa29		89 50 4e 47	√	
Nama file : PNG 2.png MD5 : 36d9545775536fd74bcffae544d86fb9 SHA1 : 7f34b112a5657ba8b878b099698897e901735304				√
Nama file : BMP 1.bmp MD5 : 8cad97ecf36337caebdd53fd81258dd SHA1 : 37fb769bbdf892335dc21bd6b527eca381043102		42 4d	√	
Nama file : BMP 2.bmp MD5 : 4dcf21702d5967541fc68d1b136904a5 SHA1 : dfedf90ae0a367bd61b62eb757b9a89b778d6ef1				√
File Musik				
Nama file : MP3 1.mp3 MD5 : d004ad9c716fbb7262d09fcd812b7bdb SHA1 : c8532124d281a38687cde4ae15389a927934dd31		49 44 33 03	√	
Nama file : MP3 2.mp3 MD5 : 255f0e8c535c187b3e13adb241eae315 SHA1 : fa98410a0c41c85e4b72f3fc3d4d8eb1ff950982				√

Tabel 4.12 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Autopsy (Lanjutan)

Trim Status			Enable	
Tools			Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Musik	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : MP3 3.mp3 MD5 : 2178cecb48c6473308487117d273eb1e SHA1 : 7b5d4cae778f07c92ba0246323fb582865422e82		49 44 33 03	√	
Nama file : MP3 4.mp3 MD5 : e52801cb33b2c76086dd44a370aba407 SHA1 : 42c4f31cef8b4cb39a82265b3b31bc57a151e401				√
File Aplikasi				
Nama file : MASTER 1.exe MD5 : 562f2ea6e41020fd7bf5426bd77cd59c SHA1 : 7f9eaa9aa18ff1dfd77cb367ae868b761a4c5204		4d 5a 90 00 03 00 00 00	√	
Nama file : MASTER 2.exe MD5 : a6e1964dd6a7e6d0498522db4c157335 SHA1 : f3bd0efa71334c5e640866457df9d6566abdde6f				√
Nama file : MASTER 3.exe MD5 : 1abf96d2ddec838763cec88285a1fc6f SHA1 : c60146bc8744d55f9753fce5b32881fa355db683		4d 5a 50 00 02 00 00 00	√	
Nama file : MASTER 4.exe MD5 : c4219977f6880f21c370c08632412078 SHA1 : ca467df8ccc76e4c203b177d3711f66e401df47d				√
Nama file : MASTER 5.exe MD5 : 076d6a1f9c0e22362ca71d0e254202b0 SHA1 : 1f1a1a8cfa672ed49119e8fe424bc6491771000		4d 5a 90 00 03 00 00 00	√	
Nama file : MASTER 6.exe MD5 : - SHA1 : -				√
File Zip				
Nama file : ZIP 1.zip MD5 : 47cf035aa29599823cce99bef2467330 SHA1 : 69de9b3f3479c0da03ac463dcfd5db5ca2c9784a		50 4b 03 04	√	
Nama file : ZIP 2.zip MD5 : 9ba7bb2ab23acedeedb3b9207f51d2c0 SHA1 : 53366cc4c97c7e21debbab65ff1fdde186dbec24				√
Nama file : ZIP 3.zip MD5 : a5acca59eb9ff6017064994aa2b76db1 SHA1 : 29e8553a3c0aba7775b574a6f9af551fa816ffa9		50 4b 03 04	√	
Nama file : ZIP 4.zip MD5 : 626432da22a8c2d01ba8e6f0bdc7863d SHA1 : d59056c16d0b6ca95d436fb4929a013c0f248365				√
Nama file : ZIP 5.zip MD5 : 733c9420aacd6067e0d7b3050ef3b2f4 SHA1 : 125045d49c926b645e0433c6011e46ed7e7c870e		50 4b 03 04	√	
Nama file : ZIP 6.zip MD5 : - SHA1 : -				√

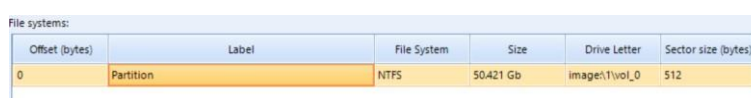
Tabel 4.13 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Autopsy (Lanjutan)

Trim Status			Enable	
Tools			Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File 7z	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : 7Z 1.7z MD5 : e2d9c0b0a82113ce52d5334ffd24a876 SHA1 : 0e181cbe6a879275437db7eb928279cc8bbc8c1a		37 7a bc af 27 1c	√	
Nama file : 7Z 2.7z MD5 : d184ed7759220cb6d86fae5cb6965174 SHA1: 01c06216786995d07a21c6b7996e5492cc726e3d				√

Berdasarkan tabel 4.13 di atas adalah daftar file setelah melakukan pemeriksaan, semua file dengan label ganjil dapat direcovery dan tampil dengan baik tanpa ada kerusakan, tetapi hanya file video ekstensi (.mpg) yang tidak dapat direcovery. Sedangkan label genap dapat direcovery tetapi semua ekstensi file tersebut tidak dapat satupun dibaca dan keseluruhan file label genap ada kerusakan, kemudian nilai hash file tersebut berubah. karena penghapusan file tersebut TRIM dalam keadaan enable. Tool forensik Autopsy tidak dapat melakukan recovery file genap secara sempurna saat penghapusan file dalam keadaan enable, tetapi file ganjil yang sudah terhapus sebelumnya pada status TRIM disable dapat dilakukan recovery dengan sempurna walaupun ada kerusakan pada file ekstensi (.mpg). Dapat disimpulkan, bahwa ketika penghapusan file label ganjil sebelumnya dalam keadaan disable dapat dikembalikan sempurna, tetapi file label genap yang sudah dihapus permanen saat TRIM enable/aktif, file label genap tidak dapat direcovery seluruhnya.

4.5.5 Pemeriksaan dan Analisis TRIM *Enable* Menggunakan Belkasoft

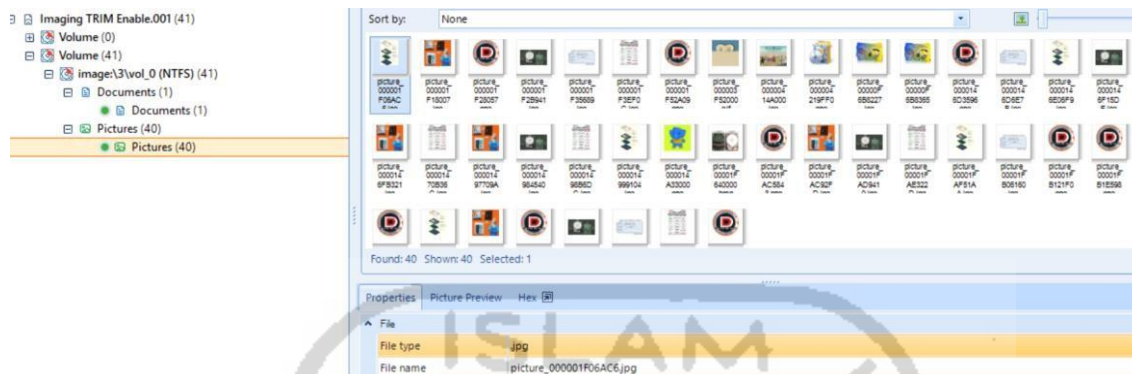
Tahapan berikutnya setelah dilakukannya pemeriksaan dan analisis pada *Sleuth Kit Autopsy* adalah mencoba melakukan pemeriksaan dan analisis dengan mengekstraksikan hasil file imange SSD NVMe fungsi TRIM *enable* menggunakan tools forensik Belkasoft Evidence Center. Berikut ini adalah gambar 4.36 hasil ekstraksi imaging logical partisi menggunakan FTK Imager dari SSD M.2 NVMe Adata XPG SX6000 Lite dengan kapasitas 52870250496 byte dengan *file system* NTFS, jika dibandingkan ukuran file pemeriksaan tools autopsy sebelumnya berada di angka kapasistas 128034708480 byte.



Offset (bytes)	Label	File System	Size	Drive Letter	Sector size (bytes)
0	Partition	NTFS	50421 Gb	image:\vol_0	512

Gambar 4.35 Pemeriksaan TRIM *Enable* dengan Belkasoft Evidence Center

Berdasarkan pengamatan pada pemeriksaan ini, waktu yang dibutuhkan pemeriksaan imaging SSD NVMe Adata XPG SX6000 Lite dengan kapasitas 52870250496 byte dengan tool forensik Belkasoft Evidence Center adalah 1 jam lebih 11 menit 19 detik.



Gambar 4.36 Daftar File Setelah Pemeriksaan TRIM *Enable* dengan Belkasoft Evidence



Gambar 4.37 Daftar File *Recovery* TRIM *Enable* dengan Belkasoft Evidence Center

Gambar 4.37 dan 4.38 adalah daftar file setelah melakukan pemeriksaan dan recovery, tidak satupun file dengan label genap yang ditemukan/tidak tampil dan yang dihapus permanen dengan perintah keyboard SHIFT+DELETE pada SSD NVMe dengan fungsi TRIM *enable* tidak bisa direcovery oleh tool forensik Belkasoft Evidence Center. Tercatat hanya ada dua file yang dapat direcovery dengan sempurna meskipun nama file tidak sama dengan aslinya, yaitu document_000001F02000.docx dan picture_00001F640000.bmp. Hasil *recovery* tool Belkasoft akan dirangkum pada tabel 4.19 berikut ini :

Tabel 4.14 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Belkasoft

Trim Status			Enable	
Tools			Belkasoft Evidence	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Dokumen	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : DOC 1.doc MD5 : - SHA1 : -	-	-		√
Nama file : DOC 2.doc MD5 : - SHA1 : -	-	-		√
Nama file : document_000001F02000.docx MD5 : 6db984ae2628503104cb46fab8b9ef8c SHA1 : 811767706c6dedb07721e2334183cffd93908abb	-	-		√
Nama file : DOCX 2.docx MD5 : - SHA1 : -	-	-		√
Nama file : XLSX 1.xlsx MD5 : - SHA1 : -	-	-		√
Nama file : XLSX 2.xlsx MD5 : - SHA1 : -	-	-		√
Nama file : PPTX 1.pptx MD5 : - SHA1 : -	-	-		√
Nama file : PPTX 2.pptx MD5 : - SHA1 : -	-	-		√
Nama file : PDF 1.pdf MD5 : - SHA1 : -	-	-		√
Nama file : PDF 2.pdf MD5 : - SHA1 : -	-	-		√
Nama file : TXT 1.txt MD5 : - SHA1 : -	-	-		√
Nama file : TXT 2.txt MD5 : - SHA1 : -	-	-		√
Nama file : ODT 1.odt MD5 : - SHA1 : -	-	-		√
Nama file : ODT 2.odt MD5 : - SHA1 : -	-	-		√

Tabel 4.15 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Belkasoft (Lanjutan)

Trim Status			Enable	
Tools			Belkasoft Evidence	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : 3GP 1.3gp MD5 : - SHA1 : -	-	-		√
Nama file : 3GP 2.3gp MD5 : - SHA1 : -	-	-		√
Nama file : FLV 1.flv MD5 : - SHA1 : -	-	-		√
Nama file : FLV 2.flv MD5 : - SHA1 : -	-	-		√
Nama file : MPG 1.mpg MD5 : - SHA1 : -	-	-		√
Nama file : MPG 2.mpg MD5 : - SHA1 : -	-	-		√
Nama file : WEBM 1.webm MD5 : - SHA1 : -	-	-		√
Nama file : WEBM 2.webm MD5 : - SHA1 : -	-	-		√
Nama file : MKV 1.mkv MD5 : 081988e8c44e575b84cda8934058e9b2 SHA1 : 0d0c86be290d9b0a2fa8b8d833f4f73f9a845e98	-	-		√
Nama file : MKV 2.mkv MD5 : SHA1 :	-	-		√
Nama file : MOV 1.mov MD5 : - SHA1 : -	-	-		√
Nama file : MOV 2.mov MD5 : - SHA1 : -	-	-		√
Nama file : OGG 1.ogg MD5 : - SHA1 : -	-	-		√
Nama file : OGG 2.ogg MD5 : - SHA1 : -	-	-		√
Nama file : WMV 1.wmv MD5 : - SHA1 : -	-	-		√
Nama file : WMV 2.wmv MD5 : - SHA1 : -	-	-		√
Nama file : AVI 1.avi MD5 : - SHA1 : -	-	-		√

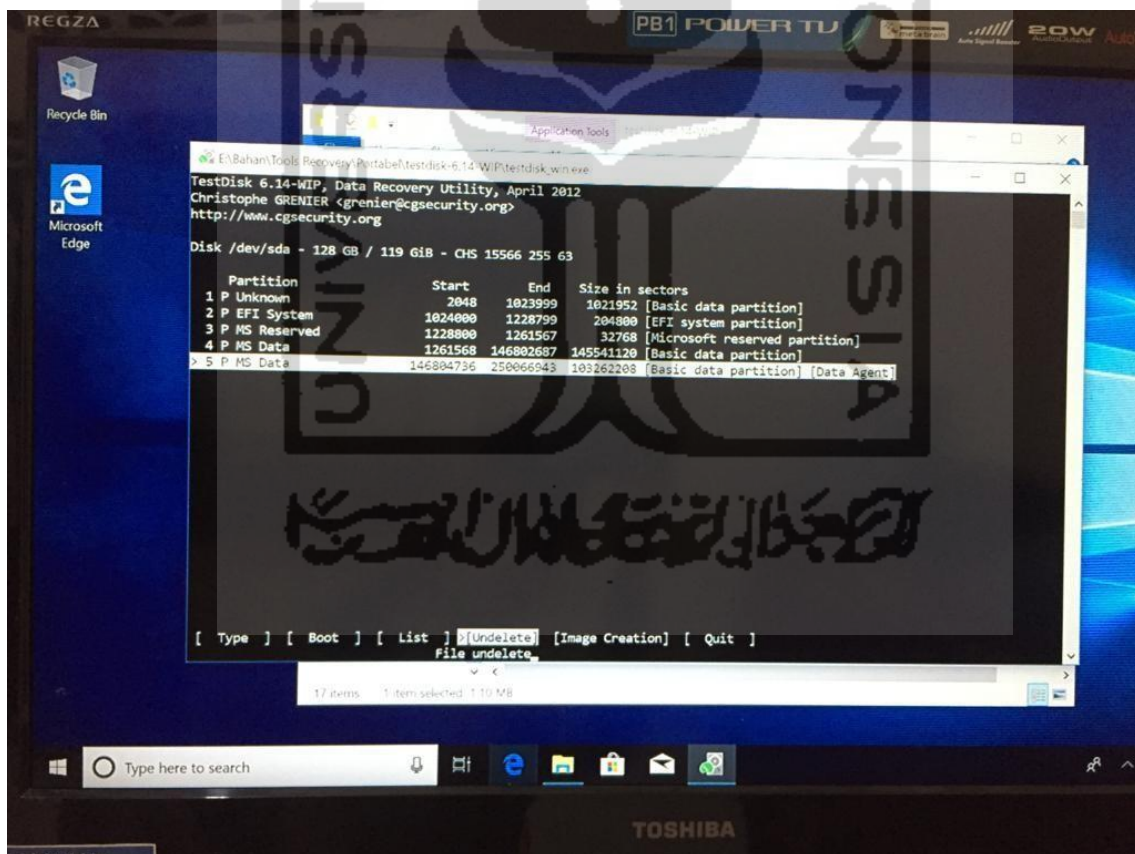
Tabel 4.16 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Belkasoft (Lanjutan)

Trim Status			Disable	
Tools			Belkasoft Evidence	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : AVI 2.avi MD5 : - SHA1 : -	-	-		√
Nama file : MP4 1.mp4 MD5 : - SHA1 : -	-	-		√
Nama file : MP4 2.mp4 MD5 : - SHA1 : -	-	-		√
File Gambar				
Nama file : picture_000003F52000.gif MD5 : 7ac62754ea19fc0fede4f2f902a9be94 SHA1 : d8d96864fb8e777648e4fbb077eb76bc0b782e7c		47 49 46 38 39 61		√
Nama file : JPG 1.jpg MD5 : - SHA1 : -	-	-		√
Nama file : PNG 1.png MD5 : - SHA1 : -	-	-		√
Nama file : picture_00001F640000.bmp MD5 : 8cad97ecf36337caebdd53fd81258dd SHA1 : 37fb769bbdf892335dc21bd6b527eca381043102		42 4d	√	
File Musik				
Nama file : MP3 1.mp3 MD5 : - SHA1 : -	-	-		√
Nama file : MP3 3.mp3 MD5 : - SHA1 : -	-	-		√
File Aplikasi				
Nama file : MASTER 1.exe MD5 : - SHA1 : -	-	-		√
Nama file : MASTER 3.exe MD5 : - SHA1 : -	-	-		√
Nama file : MASTER 5.exe MD5 : - SHA1 : -	-	-		√
File Zip				
Nama file : ZIP 1.zip MD5 : - SHA1 : -	-	-		√
Nama file : ZIP 3.zip MD5 : - SHA1 : -	-	-		√
Nama file : ZIP 5.zip MD5 : - SHA1 : -	-	-		√

Pada Tabel 4.19 pemeriksaan *recovery* tools Belkasoft Evidence Center, tool forensik Belkasoft dengan skenario penghapusan permanen perintah SHIFT+DELETE tidak dapat melakukan *recovery* terhadap file-file selain jenis ekstensi .docx dan .bmp, Belkasoft hanya dapat melakukan *recovery* terhadap file-file ekstensi .docx dan .bmp dengan sempurna walaupun nilai hash berubah. Dapat disimpulkan bahwa Belkasoft saat ini belum bisa maksimal untuk mendukung permasalahan *recovery* pada *Solid State Drive* NVMe.

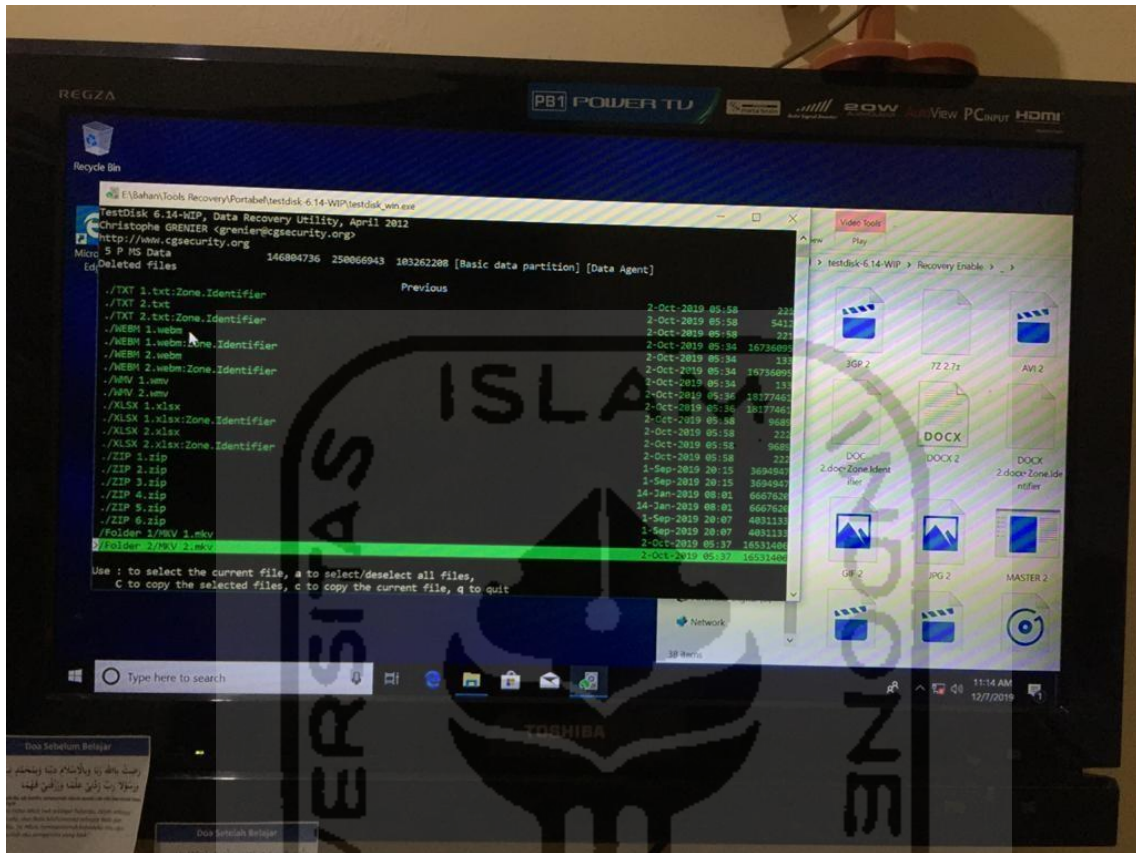
4.5.6 Pemeriksaan dan Analisis TRIM Enable Menggunakan Testdisk

Selanjutnya tahapan berikutnya setelah dilakukannya pemeriksaan dan analisis hasil imaging pada *Sleuth Kit Autopsy* dan Belkasoft Evidence Center. Kemudian melakukan praktek pemeriksaan dan analisis yang telah *recovery* menggunakan tool khusus *recovery* yaitu Testdisk guna untuk membandingkan hasil *recovery* data SSD NVMe fungsi TRIM *enable*/aktif dari tools forensik seperti *Sleuth Kit Autopsy* dan Belkasoft Evidence Center.



Gambar 4.38 Proses *Recovery* TRIM Enable Menggunakan Testdisk















Berdasarkan pengamatan pada pemeriksaan ini, waktu yang dibutuhkan untuk mengembalikan data pada partisi SSD NVMe Adata XPG SX6000 Lite dengan tool *recovery* testdisk tidak membutuhkan waktu recovery.



Gambar 4.39 Daftar File *Recovery* TRIM Enable dengan Testdisk

Gambar 4.39 dan 4.40 adalah daftar file setelah melakukan pemeriksaan dan recovery, hampir semua file yang dihapus permanen dengan perintah keyboard SHIFT+DELETE pada SSD NVMe dengan fungsi TRIM *Enable* dapat direcovery oleh tool recovery Testdisk tetapi tidak dapat dibaca atau rusak. Khusus pada tahapan analisis, tool *recovery* testdisk tidak memiliki kelebihan untuk pengecekan nilai keaslian barang bukti atau MD5 dan SHA1 pada file *recovery*, dikarenakan Testdisk hanya untuk melakukan *recovery* pada partisi, maka perlu menggunakan tool analisis tambahan yaitu Hashmyfile untuk melakukan pemeriksaan keaslian nilai hashing. Hasil *recovery* tool Testdisk akan dirangkum pada tabel 4.23 berikut ini :

Tabel 4.17 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Testdisk

Trim Status			Enable	
Tools			Testdisk	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Dokumen	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : DOC 1.doc MD5 : 630a293939e5fc996076d2c2ec39a7c1 SHA1 : c7a12c327089fbe3de6917f01c07a3cb8b5a646e		d0 cf 11 e0	√	
Nama file : DOC 2.doc MD5 : 00f8e30447dbfb9e5e5e3d820826c52f SHA1 : 8fd2a48cece30294c52ccedc986a6b8c65896760		00 00 00 00 00		√
Nama file : DOCX 1.docx MD5 : 6db984ae2628503104cb46fab8b9ef8c SHA1 : 811767706c6dedb07721e2334183cffd93908abb		d0 cf 11 e0	√	
Nama file : DOCX 2.docx MD5 : 821d1ae6d9543f57e95a82c26fcbcb6 SHA1 : e64a608643b8acfc03a3f1fbd86801587d1ecba9		00 00 00 00 00		√
Nama file : XLSX 1.xlsx MD5 : 56c424725531715f142e77ccc5cee774 SHA1 : 0e8ad73a6cb2573086d17b79a03ab5cbe77c3e5e		50 4b 03 04	√	
Nama file : XLSX 2.xlsx MD5 : c4e4f86f732fd5873e050500e18bb414 SHA1 : 3b14143368bc900dbce275abd9025c81fcd1ca0a		00 00 00 00 00		√
Nama file : PPTX 1.pptx MD5 : 1d02e044e64e79994ab5a0ca871c6fe9 SHA1 : c45f505b05ae9d8a171065bdf109b140c038598e		50 4b 03 04	√	
Nama file : PPTX 2.pptx MD5 : 0b080dffa116ee20924fe1bc5817bf3e SHA1 : c9e9efe4fe768e067262e44d42560346f3d8ea42		00 00 00 00 00		√
Nama file : PDF 1.pdf MD5 : 7a3801902be546b4ee026538f246e844 SHA1 : 83de136e1fc13b4e74158d9c8d27169295ce5753		25 50 44 46	√	
Nama file : PDF 2.pdf MD5 : c44b1979483b451f9b1e91b4abba44c3 SHA1 : 5c8c29f3cad44631c6e5dbf47f88ead47b4fcc15		00 00 00 00 00		√
Nama file : TXT 1.txt MD5 : 6bb11f42a5b591be9ec1a0e95a5cd00c SHA1 : b52cdb3aada6a51ecb52ffd6ef8c0b7dfbed778e		20 20 20 20	√	
Nama file : TXT 2.txt MD5 : 9ba601b1c111c9ebc50b523d09ea5f21 SHA1 : 7dbe175eed4b81be86e43129893b8ec8b5062da8		00 00 00 00 00		√
Nama file : ODT 1.odt MD5 : d9822aa6cbe227fc935665375152bacf SHA1 : 4d5dcf9a29d1d92d77dc4d8215ee76b717577500		50 4b 03 04	√	
Nama file : ODT 2.odt MD5 : 7d559ed79eca8de750e63f822ab17ee1 SHA1 : 1cf841fb7d0acd8cb89c1df02cd609143a0fbfb4		00 00 00 00 00		√








Tabel 4.18 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Testdisk

Trim Status			Enable	
Tools			Autopsy	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : 3GP 1.3gp MD5 : cd5f422a723609bff58c699704f91d88 SHA1 : 5d7c170d622cdba4de7c97403ef70af36f1a8f77		66 74 79 70	√	
Nama file : 3GP 2.3gp MD5 : 299e23fd97392eae859b7117dfb91634 SHA1 : 68ac1fe0cd4f0e6ab76e7fbd33ad8e8941b3cc7		00 00 00 00 00		√
Nama file : FLV 1.flv MD5 : 49f86ccb885b8eb2de17ece7f281434 SHA1 : f8f6e752108f5b5e2d1db7ff6a57a1d9b6016ca4		46 4c 56 01	√	
Nama file : FLV 2.flv MD5 : - SHA1 : -		00 00 00 00 00		√
Nama file : MPG 1.mpg MD5 : - SHA1 : -		00 00 01 ba		√
Nama file : MPG 2.mpg MD5 : - SHA1 : -		00 00 00 00 00		√
Nama file : WEBM 1.webm MD5 : e75301e7337242951e90e6fbc598c8cb SHA1 : c2861b40f5a5f6334045c6bf96230f6778474b7f		1a 45 df a3	√	
Nama file : WEBM 2.webm MD5 : 7d57e1bbb413f91ccbf55a0f8df9fd SHA1 : 2ba1191f295a3680e1780e023d6a5ed5dc1cdf43		00 00 00 00 00		√
Nama file : MOV 1.mov MD5 : 35208da889d863bc010741f9e2c7c25e SHA1 : 79a798afbba8e1a7bfe8d6be46fb7dfa6d130019		66 74 79 70 71 74 20 20	√	
Nama file : MOV 2.mov MD5 : 4e0514db784fa7ce788c39dcf70e6343 SHA1 : c0d38b0a3cc12b60f52dcb402ada86b88550924e		00 00 00 00 00		√
Nama file : OGG 1.ogg MD5 : 8ca67608dcaec59718c25ed8bfa93c35 SHA1 : dd9cf50928d3a30323c2f805d5cd0153a68ef3fc		4f 67 67 53 00 02	√	
Nama file : OGG 2.ogg MD5 : 3ae510eb17e1ece3125ee603b4904b2d SHA1 : 9b40fac4ed0994827fc48fbb932cd5577a99b641		00 00 00 00 00		√
Nama file : WMV 1.wmv MD5 : e3935aadb17432b48a0d45be6cfca9d SHA1 : 677083c5bc1de4a8c1830e0361fd334a1140051b		30 26 b2 75 8e 66 cf 11	√	
Nama file : WMV 2.wmv MD5 : c9607cc9e10e03659810d4735ee5570e SHA1 : c020b670420026822cb92148b7b93faadf736942		00 00 00 00 00		√
Nama file : AVI 1.avi MD5 : 72562d25302f0698c19040a6d50ceb0c SHA1 : ab7007f37ad838976b8e9d4d4c755fa355deab90		41 56 49 20 4c 49 53	√	

Tabel 4.19 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Testdisk

Trim Status			Enable	
Tools			Testdisk	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Video	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : AVI 2.avi MD5 : a13a97acca90cce38197742e79ebd152 SHA1 : 54af4c0c0af5fe7171820d13813c28d4ae786948	-	00 00 00 00 00		√
Nama file : MP4 1.mp4 MD5 : 0094fb55e09791154276f456d9982a0a SHA1 : 5780166537985e77d0ea3a601adb6e707d574ef3		66 74 79 70 6d 70 34 32	√	
Nama file : MP4 2.mp4 MD5 : - SHA1 : -		00 00 00 00 00		√
File Gambar				
Nama file : GIF 1.gif MD5 : ed28cc871584230543b5a2d8a386a2cb SHA1 : b981419393314ea3d20d80c41715a2eb1e039b2b		47 49 46 38 39 61	√	
Nama file : GIF 2.gif MD5 : - SHA1 : -		00 00 00 00 00		√
Nama file : JPG 1.jpg MD5 : d4fc57bddd2ed31d53f00002791a245d SHA1 : 77af0aebff4bf31b1dc54f0a15c133fa140c0c81		ff d8 ff e0	√	
Nama file : JPG 2.jpg MD5 : 756a62e9962edb459bd97b326c59747d SHA1 : fa5a986f53012328281407e069f30e1ebf2b7452		00 00 00 00 00		√
Nama file : PNG 1.png MD5 : a820b280e93967956c449b342125add8 SHA1 : f5c0b6a7946dccc88904ca32944c4b8f5c52aa29		89 50 4e 47	√	
Nama file : PNG 2.png MD5 : 36d9545775536fd74bcffae544d86fb9 SHA1 : 7f34b112a5657ba8b878b099698897e901735304	-	00 00 00 00 00		√
Nama file : BMP 1.bmp MD5 : 8cad97ecf36337caebdd53fd81258dd SHA1 : 37fb769bbdf892335dc21bd6b527eca381043102		42 4d	√	
Nama file : BMP 2.bmp MD5 : 4dcf21702d5967541fc68d1b136904a5 SHA1 : dfedf90ae0a367bd61b62eb757b9a89b778d6ef1		00 00 00 00 00		√
File Musik				
Nama file : MP3 1.mp3 MD5 : d004ad9c716fbb7262d09fcd812b7bdb SHA1 : c8532124d281a38687cde4ae15389a927934dd31		49 44 33 03	√	
Nama file : MP3 2.mp3 MD5 : 255f0e8c535c187b3e13adb241eae315 SHA1 : fa98410a0c41c85e4b72f3fc3d4d8eb1ff950982		00 00 00 00 00		√
Nama file : MP3 3.mp3 MD5 : 2178cecb48c6473308487117d273eb1e SHA1 : 7b5d4cae778f07c92ba0246323fb582865422e82		49 44 33 03	√	
Nama file : MP3 4.mp3 MD5 : e52801cb33b2c76086dd44a370aba407 SHA1 : 42c4f31cef8b4cb39a82265b3b31bc57a151e401		00 00 00 00 00		√

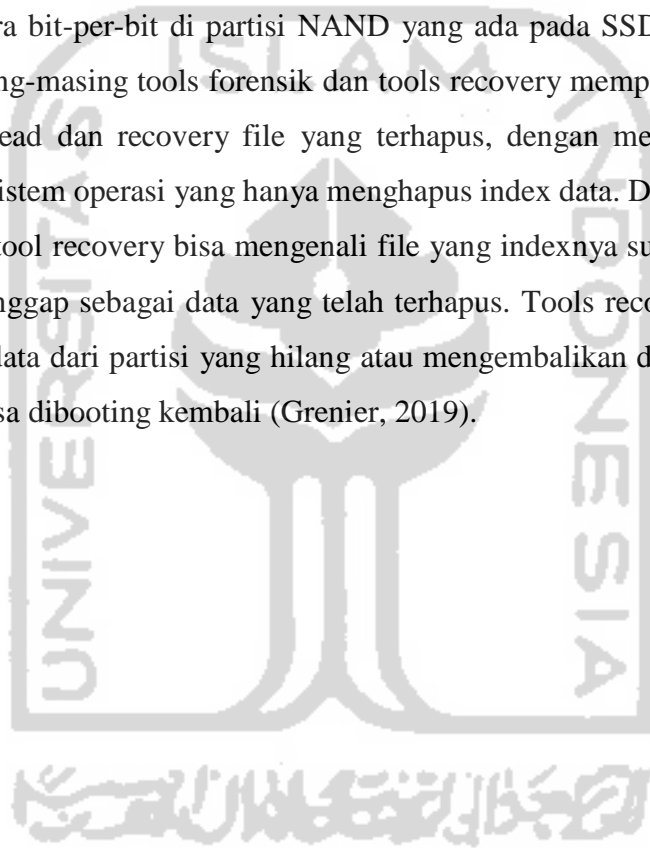
Tabel 4.20 Daftar File Genap Hasil Analisis TRIM *Enable* dengan Testdisk

Trim Status			Enable	
Tools			Testdisk	
Nama File Hasil Restorasi, Nilai Hash, Picture, dan File Signature			Status Recovery	
File Musik	Picture	File Signature	Berhasil	Tidak Berhasil
Nama file : MASTER 1.exe MD5 : 562f2ea6e41020fd7bf5426bd77cd59c SHA1 : 7f9eaa9aa18ff1dfd77cb367ae868b761a4c5204		4d 5a 90 00 03 00 00 00	√	
Nama file : MASTER 2.exe MD5 : a6e1964dd6a7e6d0498522db4c157335 SHA1 : f3bd0efa71334c5e640866457df9d6566abdde6f		00 00 00 00 00		√
Nama file : MASTER 3.exe MD5 : 1abf96d2ddec838763cec88285a1fc6f SHA1 : c60146bc8744d55f9753fce5b32881fa355db683		4d 5a 50 00 02 00 00 00	√	
Nama file : MASTER 4.exe MD5 : c4219977f6880f21c370c08632412078 SHA1 : ca467df8ccc76e4c203b177d3711f66e401df47d		00 00 00 00 00		√
Nama file : MASTER 5.exe MD5 : 076d6a1f9c0e22362ca71d0e254202b0 SHA1 : 1f1a1a8cfa672ed49119e8fe424bc6491771000		4d 5a 90 00 03 00 00 00	√	
Nama file : MASTER 6.exe MD5 : - SHA1 : -	-			√
File 7z				
Nama file : 7Z 1.7z MD5 : e2d9c0b0a82113ce52d5334ffd24a876 SHA1 : 0e181cbe6a879275437db7eb928279cc8bbc8c1a		37 7a bc af 27 1c	√	
Nama file : 7Z 2.7z MD5 : d184ed7759220cb6d86fae5cb6965174 SHA1: 01c06216786995d07a21c6b7996e5492cc726e3d		00 00 00 00 00		√

Berdasarkan tabel 4.23 di atas, selanjutnya pada file yang sudah ditemukan untuk mengecek keaslian dari file tersebut melakukan teknik hashing dengan tool *Hashmyfile*, jika diasumsikan bahwa keseluruhan hasil *recovery* file label genap memiliki nilai MD5/SHA1 tidak sesuai dengan file asli dan tidak dapat dibaca atau rusak, dapat dikatakan file berlainan atau integritas barang bukti tidak valid, karena penghapusan file tersebut TRIM dalam keadaan enable. Namun semua file dengan label ganjil dapat direcovery/tampil dengan sempurna tanpa ada kerusakan. Maka dapat disimpulkan bahwa testdisk tidak dapat melakukan pemulihan file TRIM fungsi enable dan tidak bisa menjaga integritas atau keaslian file dalam analisis digital forensik.

Berdasarkan informasi yang dikumpulkan yang sudah dijabarkan dari literatur-literatur, metode dan eksperimen yang diimplementasikan pada penelitian ini, membuktikan bahwa fungsi TRIM menyebabkan masalah dan tantangan bagi penyidik digital forensik, dikarenakan fungsi TRIM memiliki pengaruh negatif untuk *recovery* data ketika fungsi TRIM *enable* pada sistem operasi.

Teknologi pada media penyimpanan *Solid State Drive* memiliki nilai negatif, khususnya pada analisis forensik untuk menemukan informasi dan memahami data yang tersimpan pada media penyimpanan SSD, faktanya bahwa SSD menjadi tantangan untuk analisis forensik (Gubanov & Afonin, 2014). Tools forensik FTK imager melakukan imaging/cloning secara bit-per-bit di partisi NAND yang ada pada SSD untuk melakukan proses forensik. Masing-masing tools forensik dan tools recovery mempunyai metode yang hampir sama untuk read dan recovery file yang terhapus, dengan mengandalkan proses penghapusan data di sistem operasi yang hanya menghapus index data. Dengan men-scan isi media penyimpanan, tool recovery bisa mengenali file yang indexnya sudah tidak ada. File itulah yang mereka anggap sebagai data yang telah terhapus. Tools recovery data teskdisk melakukan recovery data dari partisi yang hilang atau mengembalikan disk yang tidak bisa di-booting menjadi bisa di-booting kembali (Grenier, 2019).



BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Adapun kesimpulan yang dapat ditarik dari penelitian ini adalah sebagai berikut:

1. Berdasarkan penerapan metode live forensik dilakukan dengan mengakuisisi partisi komputer pertama yang menggunakan sistem operasi windows 10 profesional dalam keadaan menyala atau sedang hidup. Untuk melakukan imaging menggunakan *live acquisition* atau *logical acquisition* dengan kedua fungsi TRIM disable dan enable yang telah diimplementasikan berhasil melakukan imaging dengan tool FTK Imager Portable dan tools Testdisk dapat melakukan recovery secara langsung terhadap fungsi TRIM disable.
2. Berdasarkan proses pemeriksaan dan analisis pada SSD NVMe fungsi TRIM. Pada tahapan pemeriksaan sama halnya dengan tahapan pemeriksaan forensik digital pada media penyimpanan lainnya, yaitu dengan tahapan imaging, recovery, hashing, dan lain-lainnya. SSD NVMe memiliki dua fitur yaitu TRIM disable dan enable. Proses pemeriksaan dan analisis pada SSD dengan kedua fungsi TRIM disable dan enable, bahwa proses recovery TRIM disable dapat menjaga integritas barang bukti. Hal ini dibuktikan dengan nilai hash MD5 pada file asli dan file hasil recovery memiliki nilai hash yang sama. Sedangkan TRIM enable hasil file recovery tersebut mengalami kerusakan dan tidak identik dengan file aslinya sehingga integritas barang bukti tidak terjamin.
3. Bukti digital file imaging dapat diperoleh dari kedua fungsi TRIM yaitu *disable* dan *enable*. Pada fungsi TRIM *disable*, keseluruhan jenis file yang ada maupun yang telah terhapus permanen dapat *direcovery* dengan sempurna oleh tool forensik Autopsy serta tools recovery Testdisk. Sedangkan pada fitur TRIM *enable*, data yang telah terhapus permanen sesuai dengan skenario, tidak satupun file dapat dikembalikan dengan tools forensik ataupun tools recovery.

5.2 Saran

Adapun saran untuk penelitian selanjutnya adalah sebagai berikut :

1. Penelitian ini berfokus pada *recovery* data pada SSD NVMe dengan kedua fungsi TRIM. Untuk penelitian selanjutnya dapat melakukan pengujian implementasi fungsi TRIM dalam sistem operasi lainnya, *file system* yang berbeda (FAT16, FAT32, ExFaT, dan ReFS), eksplorasi metode penghapusan, metode penanganan SSD NVMe, dan tools yang digunakan untuk melakukan eksplorasi SSD NVMe dalam bidang forensik digital.



Daftar Pustaka

- ACPO. (2012). ACPO Good Practice Guide. *Acpo*, (March), 43. Retrieved from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
- Adelstein, F. (2006). Live Forensics: Diagnosing Your System Without Killing it First. *Communication of The ACM*, 49(2), 63–66.
- Bednar, P., & Katos, V. (2011). SSD: New Challenges for Digital Forensics. *ItAIS 2011, Proceedings of the 8th Conference of the Italian Chapter of the Association for Information Systems*, (October 2011), 1–8.
- Chaurasia, R. K., & Sharma, P. (2017). Solid State Drive (SSD) Forensics Analysis : A New Challenge. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* © 2017 IJSRCSEIT, 6(2), 1081–1085. Retrieved from www.ijsrcseit.com
- Dwi. (2018). Laporan Dwi Bulan I 2014. *Incident Monitoring Report*, 1–9.
- Faiz, A., & Imam, R. (2017). *Forensic Analysis of “Frozen” Hard Drive Using Deep Freeze Method*. (March). Retrieved from <http://www.forensickb.com/2010/10/forensic-analysis-of-frozen-hard-drive.html>
- Faiz, M. N., Umar, R., & Yudhana, A. (2017). Live Forensics Implementation for Browser Comparison on Email Security. *JISKa*, 1(3), 108–114.
- Freeman, M., & Woodward, A. (2009). Secure State Deletion: Testing the efficacy and integrity of secure deletion tools on Solid State Drives. *Proceedings of the 7th Australian Digital Forensics Conference*, (January 2009), 32–40.
- Geier, F. (2015). *The differences between SSD and HDD technology regarding forensic investigations*. 67. Retrieved from <http://lnu.diva-portal.org/smash/get/diva2:824922/FULLTEXT01.pdf>
- Grenier, C. (2019). *TestDisk Documentation*.
- Gubanov, Y., & Afonin, O. (2014). *Recovering Evidence from SSD Drives: Understanding TRIM, Garbage Collection, and Exclusions*. Retrieved from <http://www.dfinews.com/articles/2014/09/recovering-evidence-ssd-drives-understanding-trim-garbage-collection-and-exclusions>
- Hadi, A., & Riadi, Imam, S. (2019). *Forensik Bukti Digital Pada Solid State Drive (SSD) NVMe Menggunakan Metode National Institute Standards and Technology (NIST)*.

551–558.

- Horsman, D. G. (2019). Formalising Investigative Decision Making in Digital Forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. *Digital Investigation*, 28, 146–151. <https://doi.org/10.1016/j.diin.2019.01.007>
- Hubbard, R. (2016). *Forensics Analysis of Solid State Drive (SSD)*. 1–11.
- Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers and Security*, 38, 103–115. <https://doi.org/10.1016/j.cose.2013.05.001>
- Larrivee, S. (2016). *Solid State Drive 101*.
- Nasional, B. S. (2014). Teknologi Informasi – Teknik Keamanan – Pedoman Identifikasi, Pengumpulan Akuisisi, dan Preservasi Bukti Digital. In *SNI 27037:2014*. Jakarta.
- Nikkel, B. (2016). NVM express drives and digital forensics. *Digital Investigation*, 16, 38–45. <https://doi.org/10.1016/j.diin.2016.01.001>
- Nisbet, A., Lawrence, S., & Ruff, M. (2013). A Forensic Analysis and Comparison of Solid State Drive Data Retention With Trim Enabled File Systems. *Australian Digital Forensics Conference*, 10. <https://doi.org/10.4225/75/57b3d766fb873>
- Nuh Al-Azhar, M. (2012a). *Digital Forensic Practical Guildelines for Computer Investigation*.
- Nuh Al-Azhar, M. (2012b). *digital forensics*. 302.
- Prayudi, Y. (2014). Problema dan Solusi Digital Chain of Custody. *Senasti - Seminar Nasional Sains Dan Teknologi Informasi*, (2011).
- Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, 4(10), 1048–1056. Retrieved from <http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf>
- Rahman, S., & Khan, M. N. A. (2015). Review of Live Forensic Analysis Techniques. *International Journal of Hybrid Information Technology*, 8(2), 379–388. <https://doi.org/10.14257/ijhit.2015.8.2.35>
- Ramadhan, R. A., Prayudi, Y., & Sugiantoro, B. (2016). Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD) (Vol. 9). Retrieved from <http://teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf>
- Riadi, I., & Rauli, M. E. (2019). Live forensics analysis of line app on proprietary operating system. *Kinetik: Game Technology, Information System, Computer Network*,

- Computing, Electronics, and Control*, 4(4), 305–314.
<https://doi.org/10.22219/kinetik.v4i4.850>
- Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ). *Elinvo (Electronics, Informatics, and Vocational Education)*, 3(1), 70–82.
<https://doi.org/10.21831/elinvo.v3i1.19308>
- Sant, P. (2014). *Digital Forensics : the need for Integration Digital Forensics : the need for Integration Keywords*. (June).
- Shah, Z., Mahmood, A. N., & Slay, J. (2015). Forensic Potentials of Solid State Drives. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 153(September), 113–126.
https://doi.org/10.1007/978-3-319-23802-9_11
- Sivashankar, Scholar, P. ., & S, R. (2015). *Design and Implementation of Non-Volatile Memory Express*. (February), 363–367. <https://doi.org/10.13140/RG.2.1.2035.1204>
- Soni, Sudyana, D., Prayudi, Y., Mukhtar, H., & Sugiantoro, B. (2019). Server Virtualization Acquisition Using Live Forensics Method. *Advances in Engineering Research*, 190, 18–23.
- Sudyana, D., & Lizarti, N. (2019). Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method. *Scientific Journal of Informatics*, 6(1), 125–137.
- Xu, Q., Siyamwala, H., Ghosh, M., Suri, T., Awasthi, M., Guz, Z., ... Balakrishnan, V. (2015). Performance Analysis of NVMe SSDs and their Implication on Real World Databases. *SYSTOR 2015 - Proceedings of the 8th ACM International Systems and Storage Conference*. <https://doi.org/10.1145/2757667.2757684>
- Yudhistira, D. S. (2018). *Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop*.