

Analisis Bukti Digital *Trim Enable* SSD NVME Menggunakan Metode *Static Forensics* (*Analysis of Digital Evidence Trim Enable on SSD NVME Using Static Forensics Method*)

Imam Riadi¹, Sunardi², Abdul Hadi³

¹Program Studi Sistem Informasi, Universitas Ahmad Dahlan

²Program Studi Teknik Elektro, Universitas Ahmad Dahlan

³Program Studi Teknik Informatika, Universitas Ahmad Dahlan

¹imam.riadi@is.uad.ac.id

²sunardi@mti.uad.ac.id

³abdul1808048032@webmail.uad.ac.id

Abstrak - Bukti digital sangat penting dalam pembuktian kasus kejahatan komputer yang melibatkan perangkat penyimpanan. Salah satu media penyimpanan terkini saat ini adalah SSD NVMe, secara default sistem operasi Windows 10 terpasang TRIM dengan mode *enable*, fungsi TRIM mengoptimalkan kinerja kecepatan SSD NVMe dengan cara menghapus otomatis data lama pada sebuah sektor sebelum ditempatkan data baru sehingga menjadi tantangan investigator untuk mengembalikan bukti digital. Tujuan penelitian melakukan analisis bukti digital yang terhapus dengan metode penghapusan permanen dengan cara *shift delete* dan *delete*, *delete recycle bin* menggunakan tools *forensics* yang berbeda untuk mengembalikan bukti digital pada SSD NVMe TRIM *enable*. Metode yang digunakan *static forensics* sedangkan tools yang digunakan FTK Imager, Autopsy dan Recuva. Hasil analisis TRIM *enable* metode penghapusan *shift delete* tidak ditemukan bukti digital yang sesuai nilai *hash* dengan bukti digital asli. Sedangkan metode penghapusan *delete*, *delete recycle bin* bukti digital dapat dikembalikan dengan prosentase keberhasilan menggunakan tool Autopsy sebesar 90% dan 10% nilai *hash* bukti digital tidak valid, sedangkan tool Recuva 80% bukti digital berhasil dikembalikan dan 20% tidak berhasil dikembalikan, dapat disimpulkan hasil *recovery* penghapusan *delete*, *delete recycle bin* pada SSD NVME TRIM *enable* dapat dijadikan bukti digital yang sah menurut hukum.

Kata-kata kunci: Forensika digital, Restorasi, Hapus Permanen, NVMe, NIST

Abstract - Digital evidence is very important in proving computer crime cases involving storage devices. One of the latest storage media is the SSD NVMe, by default the Windows 10 operating system is installed TRIM with enable mode, the TRIM function optimizes the SSD NVMe speed

performance by automatically removing old data in a sector before new data is placed so that it becomes a challenge for investigators to return digital evidence. The purpose of the study is to analyze digital evidence that is erased with the method of permanent erasure by means of shift delete and delete, delete recycle bin using different forensics tools to restore digital evidence on SSD NVMe TRIM enable. The method used is static forensics while the tools used are FTK Imager, Autopsy, Recuva. The results of the TRIM enable the deletion shift delete there is not found digital evidence that matches the hash value with original digital evidence. While the method of deletion delete, delete recycle bin digital evidence can be returned with the percentage of success using the Autopsy tool of 90% and 10% hash value of invalid digital evidence, while the Recuva tool 80% of digital evidence has been returned successfully and 20% has not been returned successfully, it can be concluded that the recovery deletion delete, delete recycle bin on the SSD NVMe TRIM enable can be used as legal digital evidence according to law.

Keywords : Digital Forensics, Restoration, Delete Permanently, NVMe, NIST

I. PENDAHULUAN

Dinamika kejahatan *cyber* diberbagai negara sangat beragam yang melibatkan barang bukti elektronik maupun digital, sebagian barang bukti elektronik adalah komputer [1]. Penggunaan komputer sebagai alat kejahatan dapat berupa pengambilan data penting secara ilegal, manipulasi data, membocorkan data penting dan penyalahgunaan perangkat komputer baik *hardware* maupun *software* untuk akses tidak sah [2].

Perkembangan teknologi media penyimpanan saat ini dituntut cepat dalam membaca dan menulis data menyesuaikan perkembangan perangkat keras yang

lainnya seperti *processor* dan *Random Access Memory* (RAM). Media penyimpanan *Solid State Drive Non-volatile Memory Express* (SSD NVMe) memiliki perbedaan bentuk dan *interace* dengan SSD SATA [3], berikut perbedaan fisik SSD NVMe pada Gambar 1 (a) dan SSD SATA Gambar 1 (b).

SSD NVMe memiliki fitur TRIM secara *default* terpasang pada sistem operasi Windows dengan *mode enable* [4], fitur ini secara otomatis menghapus data lama pada sektor penyimpanan sebelum ditempatkan data baru sehingga SSD NVMe dapat membaca data secara optimal [5] [6].

Kontradiksi penggunaan fitur TRIM pada SSD NVMe dari sisi *digital forensics* adalah fungsi TRIM memiliki efek negatif pada analisis bukti *digital forensics* khususnya pada pengembalian atau restorasi bukti digital [7]. Barang bukti digital yang dihapus tidak dijamin dapat dikembalikan, karena *controller* pada SSD NVMe TRIM *enable* berfungsi untuk menghapus *garbage collection* [8] [9].

Berdasarkan studi literatur dari penelitian terdahulu sebagai pendukung penelitian ini, ditemukan penelitian dengan tema sejenis peneliti membandingkan *tools* forensik untuk analisis dan eksaminasi SSD SATA (Controller AHCI) dengan *mode* TRIM, penelitian menghasilkan mekanisme TRIM pada SSD SATA saat diaktifkan menimbulkan kendala dalam penyelidikan *digital forensics*. Ketika diaktifkan mekanisme TRIM memiliki pengaruh pada sistem operasi. Sistem operasi yang digunakan adalah windows 7 dengan file sistem NTFS, metode akuisisi yang digunakan *static forensics* dan *tool* yang digunakan adalah Forensic Toolkit (FTK) dan Sleuth Kit Autopsy [10]. Peneliti lain menganalisis perbandingan fitur TRIM *enable* dan TRIM *disable* pada SSD NVMe, metode penghapusan permanen hanya menggunakan *shift delete*, tools yang digunakan RecoverMyFile dan Autopsy. Hasil yang didapat saat TRIM *enable* aktif bukti digital tidak dapat dikembalikan sedangkan TRIM *disable* 92% dapat dikembalikan dengan baik [8]. Peneliti lain juga melakukan perbandingan fitur TRIM pada SSD SATA yang berjalan

pada sistem operasi yang berbeda, pada konektor kabel yang berbeda dan pada *file* sistem berbeda. Tools yang digunakan untuk mengembalikan artefak adalah Recuva dengan metode penghapusan *shift delete*, hasil penelitian menunjukkan hasil yang berbeda saat fitur TRIM diaktifkan dan dinon-aktifkan [11]. Peneliti lain juga melakukan analisis bukti digital pada SSD SATA dengan metode *live forensics* menggunakan perangkat lunak *Grr Rapid Response (client-server)*, metode penghapusan dengan *delete* biasa. Bukti digital yang dapat dikembalikan berupa file dokumen, hasil validitas pada bukti digital tersebut memiliki nilai *hash* yang sama dari dua algoritma validitas bukti digital yang diimplementasikan MD5 dan SHA-1 [12].

Tujuan penelitian melakukan analisis bukti digital yang terhapus (*lost data*) dengan metode penghapusan permanen dengan cara *shift delete* dan *delete*, *delete recycle bin* menggunakan *tools forensics* yang berbeda untuk mengembalikan bukti digital pada SSD NVMe TRIM *enable*. Penelitian ini menerapkan langkah kerja (*framework*) *National Institute of Standards and Technology* (NIST) untuk mendapatkan bukti digital yang valid dan dapat dipertanggungjawabkan menurut hukum. Penulis melakukan penelitian ini menggunakan sistem operasi windows 10 *Build* 1803 dengan menerapkan metode *static forensics*.

II. METODE

Metodologi menjelaskan urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian. Adapun tahapan penelitian dimulai dari studi literatur mengumpulkan penelitian terdahulu dari berbagai sumber, menyiapkan environment berupa alat simulasi penelitian, membangun simulasi kasus yaitu membuat rancangan studi kasus yang tidak nyata, melakukan pemeriksaan dan analisis kasus yaitu melakukan implementasi simulasi kasus sesuai metode *static forensics* dan terakhir memberikan diskusi dan kesimpulan. Tahapan ini dapat dilihat pada Gambar 2.



Gambar 1. Perbedaan fisik SSD NVMe dan SSD SATA



Gambar 2. Metodologi Penelitian

Tahapan penelitian menggunakan metode *static forensics* yaitu metode konvensional penanganan barang bukti elektronik berupa komputer dalam keadaan mati [13]. Pemilihan model langkah kerja forensik harus memenuhi *individuality*, *repeatability*, *reliability*, *performance*, *testability*, *scalability*, dan *quality standards* [14]. Pada tahapan analisis peneliti menggunakan *framework National Institute of Standards and Technology (NIST)* [15]. Barang bukti digital diambil dari salinan *image* yang diambil dari salinan media penyimpanan fisik [16]. *Framework NIST* mengarahkan langkah-langkah dan alur penelitian secara sistematis sehingga dapat menyelesaikan masalah penelitian sesuai prosedur forensika digital. Menggunakan metode dan *framework* yang tepat memiliki keberhasilan hampir 100% untuk mengumpulkan barang bukti digital *forensics* [17][18]. Berikut *framework NIST* pada Gambar 3.

Penjelasan tahapan *framework NIST* sebagai berikut:

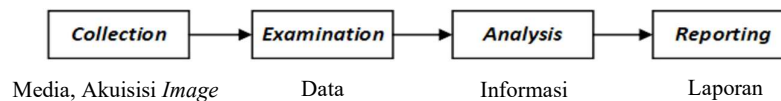
A. Collection: Melakukan identifikasi barang bukti fisik, pelabelan, *record*, *retrieve* dari sumber data yang relevan dan akuisisi *image* dengan mengaktifkan *write blocker* [19].

B. Examination: Melakukan pemilahan dan pemeriksaan bukti digital.

C. Analysis: Melakukan pemeriksaan bukti digital secara teknis dan legal untuk mendapatkan informasi berguna yang dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

D. Reporting: Pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan data analisis yang meliputi penggambaran tindakan yang dilakukan.

Alat dan bahan yang dibutuhkan pada penelitian ini adalah Desktop Mini A300, 1 pcs SSD NVMe Samsung 970 evo kapasitas 250GB, Notebook Thinkpad yoga 14 untuk analisis, Converter NVMe to USB, Windows 10 Pro Build 1803, FTK Imager, Autopsy versi 4.13 dan Recuva v.1.53 dan satu *file* bukti digital masing-masing mempunyai ekstensi .exe .pdf .docx .xlsx .ppt .jpg .bmp .png .mp3, dan .mp4 total sepuluh *file* bukti digital persesi, berikut bukti digital asli dan *hash* pada Tabel 1.



Gambar 3. Framework NIST

TABEL I
HASH DAN LETAK ALOKASI BUKTI DIGITAL ASLI

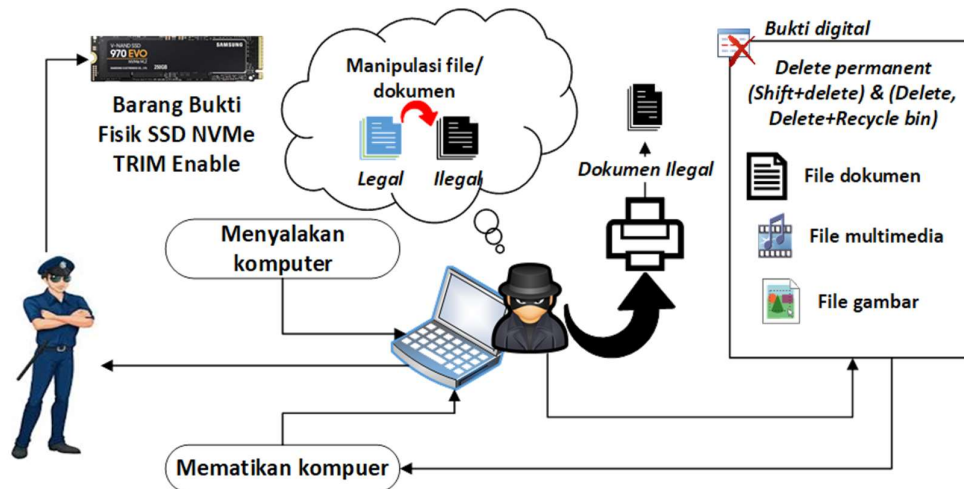
Type File	Nama File dan letak	Hash MD5
Aplikasi	D:\Sesi 1 exe	cfa3b524adf84a36be619992f9d632ff
	E:\Sesi 2 exe	1bc6927cce8627f860ae51684b32ce5d
Dokumen	D:\Sesi 1 pdf	00437830bb34f5b20c285d2f9117d4e3
	E:\Sesi 2 pdf	0a569b127c7de6bea02cf6e87e41c5f2
	D:\Sesi 1 docx	4fe577c986bcd7144c0474d75e44ed9
	E:\Sesi 2 docx	aa125f3e35214c72e3a87a11e3d4903f
	D:\Sesi 1 pptx	159f3b6c92959e4cc90242fcc4dbfe92
	E:\Sesi 2 pptx	3352425c3dd400faca160feecaf50210
Gambar	D:\Sesi 1 xlsx	53dcf316ddf8c734fccfb760fbc19d1
	E:\Sesi 2 xlsx	77ac2f423a09ef051100e4fe411f9279
	D:\Sesi 1 jpg	6288e8449d39193d9e38387d03178e5a
	E:\Sesi 2 jpg	400277f9a8290c47def497cfa8ee382c
	D:\Sesi 1 bmp	ce306ff88f3f458c2d873605e6570bc9
	E:\Sesi 2 bmp	e86e99e7b0c11c99aaa3a5f14df45ec5
Musik	D:\Sesi 1 png	c4f5d804b5d04b8bdd0935e5bb6f4a37
	E:\Sesi 2 png	90859f5a69ebca4f7d3d0ff21dd1bb97
	D:\Sesi 1 mp3	e1885b2a3bd569c94b40a1c75a0c2f91
Video	E:\Sesi 2 mp3	3c7ebc8bf7b1874f57d22a3d40ab5fe9
	E:\Sesi 1 mp4	a099b99e78725f9f21cf3e79dee3d963
	E:\Sesi 2 mp4	d1fc59d463e3e144ed43435396f5f348

Berdasar Tabel 1 untuk mempermudah eksaminasi pada penelitian, penamaan *file* barang bukti dibagi dua jenis *prefix* yang membedakan antara sesi dengan sesi yang lain yaitu “Sesi 1 jenis-ekstensi” dan “Sesi 2 jenis-ekstensi”, peletakan bukti digital sesi pertama pada drive D dan sesi kedua pada drive E. Nilai *hash* MD5 pada Tabel 1 berbeda antara bukti digital yang satu dengan yang lain karena nilai *hash* mempunyai nilai unik [20].

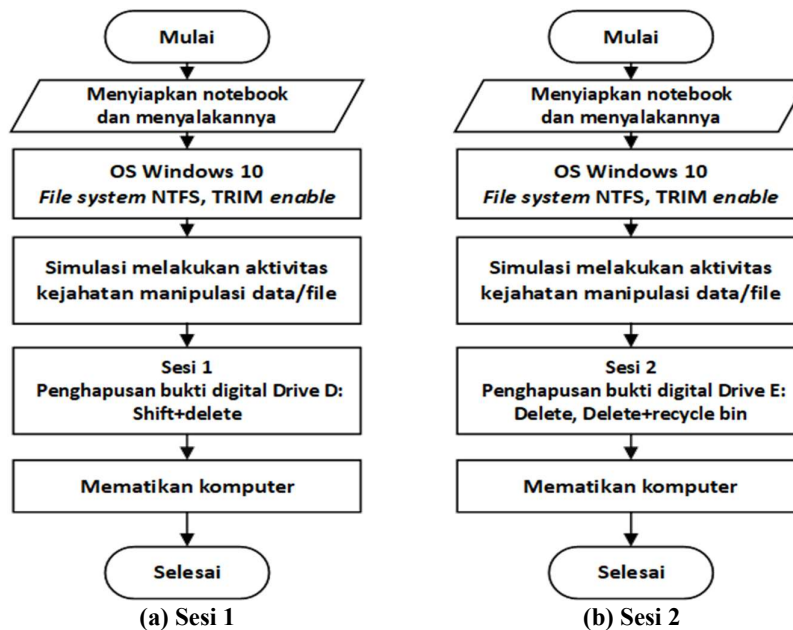
Kasus kejahatan komputer dan bukti digital yang digunakan pada penelitian ini tidak didapat dari kejadian nyata, melainkan diperoleh dari hasil skenario kasus

tindak kejahatan komputer yang melibatkan media penyimpanan SSD NVMe sesuai dengan Gambar 4.

Kasus yang diskenariokan pada penelitian ini adalah kasus *data forgery* dan *lost data*, investigator menemukan barang bukti komputer beserta media penyimpanannya. Skenario penelitian ini dibagi menjadi dua sesi, sesi yang pertama metode penghapusan *shift delete* dan sesi kedua dengan *delete*, *delete recycle bin*. Tahapan implementasi skenario penelitian sesuai Gambar 5.



Gambar 4. Skenario kejahatan komputer



Gambar 5. Implementasi metode penghapusan bukti digital

Flowchart pada Gambar 5 menjelaskan tahapan kejahatan penghapusan bukti digital terjadi. Notebook yang dipakai oleh pelaku kejahatan mempunyai sistem operasi Windows 10 dengan media penyimpanan SSD NVMe dengan fitur TRIM *enable*, Gambar 5 (a) sesi pertama pelaku kejahatan menyimpan dokumen di *drive D*, sedangkan pada Gambar 5 (b) sesi kedua disimpan di *drive E*, sesuai pada Gambar 4 pelaku melakukan manipulasi data dan menghapus data asli (*lost data*). Sesi pertama metode penghapusan menggunakan *shift delete*, sesi kedua *delete*, *delete recycle bin*. Setelah itu pelaku mematikan komputer sesuai prosedur.

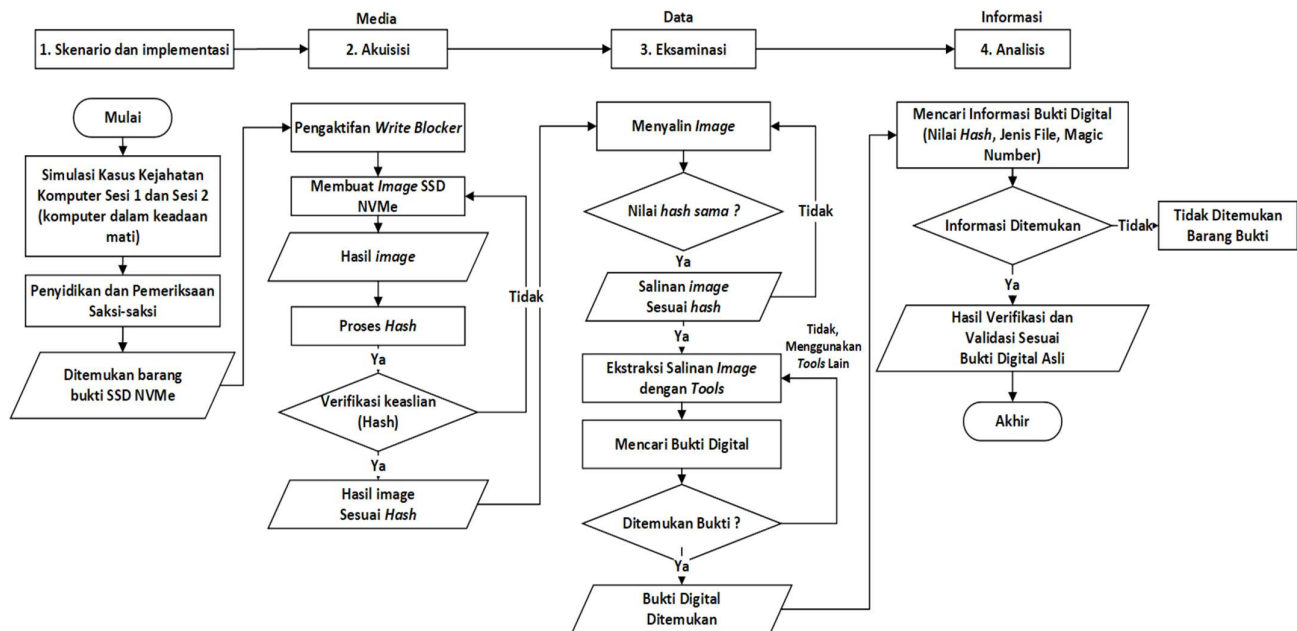
Adapun tahapan penelitian yang dilalui pada penelitian ini dirangkum menjadi pada tiga tahap dari framework NIST dan ditambah satu tahapan yaitu skenario dan implementasi sehingga menjadi empat tahapan utama seperti pada *flowchart* pada Gambar 6 [16].

III. HASIL DAN PEMBAHASAN

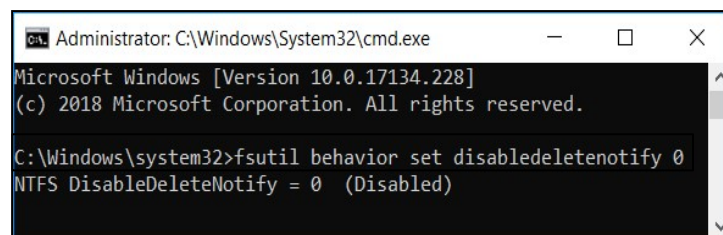
A. Skenario dan Implementasi

Kasus kejahatan pada penelitian ini berdasar pada skenario kasus pada Gambar 4. Skenario kejahatan pada penelitian ini berupa manipulasi data (*forgery data*) dan menghapus data asli (*lost data*). Pelaku kejahatan mencetak data palsu untuk dijadikan laporan fiktif, investigator menemukan barang bukti fisik berupa laptop dan mengambil media penyimpanan berupa SSD NVMe sebagai barang bukti elektronik.

Implementasi penghapusan bukti digital yang dilakukan oleh pelaku kejahatan seperti pada Gambar 6. Sistem operasi yang digunakan Windows 10 dengan TRIM *enable*, untuk pengecekan fungsi TRIM *enable* berjalan pada sistem operasi dilakukan uji coba dengan menggunakan CMD pada windows dan memasukkan perintah "*fsutil behavior set disabledeletenotify 0*" seperti pada Gambar 7 [21].

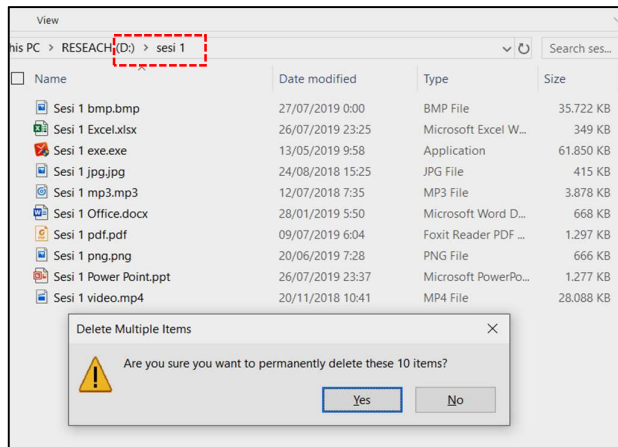


Gambar 6. Empat tahapan utama penelitian



Gambar 7. Perintah TRIM *enable* di CMD

Pelaku kejahatan melakukan aksinya dengan memanipulasi data dan menghapus barang bukti sesuai sesi pertama dengan metode penghapusan *shift delete* pada drive D untuk menghilangkan jejak bukti digital dan mematikan komputer sesuai prosedur, penghapusan *shift delete* seperti pada Gambar 8 (a). Pelaku kejahatan juga melakukan manipulasi data dan menghapus bukti digital sesuai sesi kedua dengan metode penghapusan *delete*, *delete recycle bin* pada drive E untuk menghilangkan bukti digital seperti pada Gambar 8 (b), setelah menghapus bukti digital pelaku kejahatan mematikan komputer sesuai prosedur.

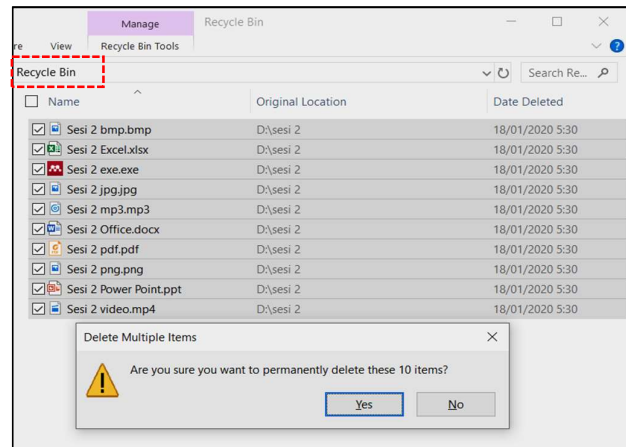


(a) Sesi 1 *shift delete* drive D:

B. Akuisisi

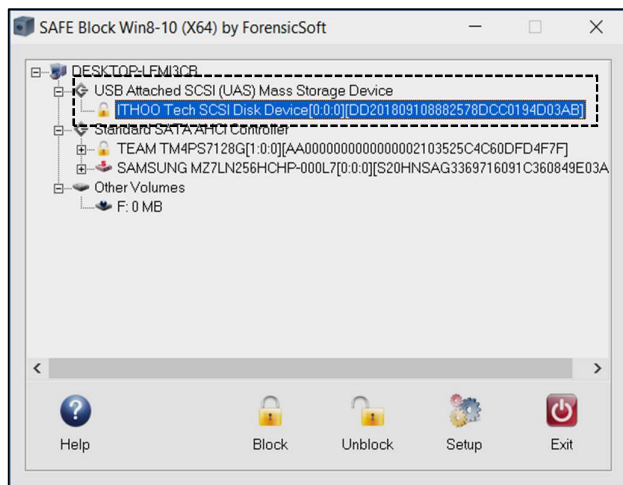
Sebelum melakukan proses akuisisi pada penelitian ini, pencegahan perubahan struktur data yang ada didalam media penyimpan dilakukan dengan pengaktifan *write blocker* menggunakan tool Safe Block, jika terjadi perubahan struktur data pada media penyimpanan akan merusak nilai *hash* pada bukti digital. Tampilan konfigurasi *write block* pada tool Safe Block seperti pada Gambar 9.

Proses ekstraksi bukti digital tidak secara langsung melalui media penyimpanan SSD NVMe namun dibuat *image* menggunakan teknik akuisisi *bit-by-bit-image* menggunakan tool FTK Imager berikut Gambar 10 hasil proses pembuatan *image*.

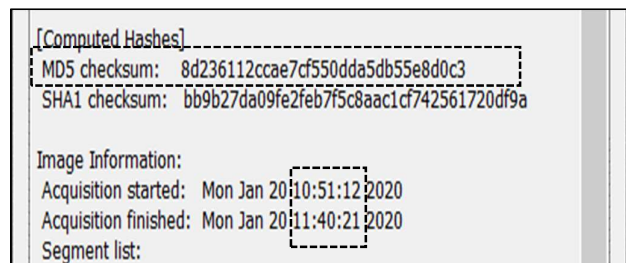


(b) Sesi 2 *delete*, *delete recycle bin* drive E:

Gambar 8. Metode penghapusan sesi 1 dan sesi 2



Gambar 9. Mengaktifkan *write blocker* pada konverter SSD NVMe to USB



Gambar 10. Hasil laporan pembuatan *image* asli

Hasil laporan pembuatan *image* pada Gambar 10 berupa nilai *hash* MD5 dengan kode yang unik yaitu 8d236112ccae7cf550dda5db55e8d0c3, waktu yang dihabiskan untuk pembuatan *image* 49:09 menit. Proses ekstraksi barang bukti menggunakan salinan dari hasil pembuatan *image* dengan proses *copy paste* dan diverifikasi kembali nilai *hash* antara *image* asli dan *image* salinan. Berikut Gambar 11 nilai *hash* salinan *image*.

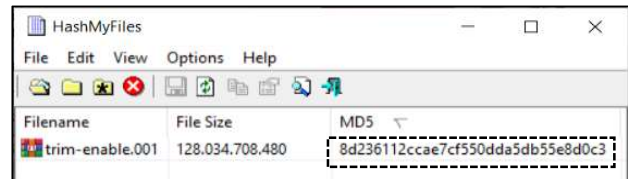
Berdasarkan Gambar 10 dan 11 proses *copy paste* *image* antara *image* asli dan *image* salinan mempunyai nilai yang sama.

C. Eksaminasi

Proses eksaminasi menggunakan salinan *image* yang sudah diverifikasi nilai *hash* dengan salinan asli. Tahapan eksaminasi berupa ekstraksi dan pemilahan berdasar verifikasi nilai *hash* bukti digital yang terhapus menggunakan *tool forensics* yang telah disiapkan yaitu Autopsy dan Recuva. Hasil eksaminasi SSD NVMe

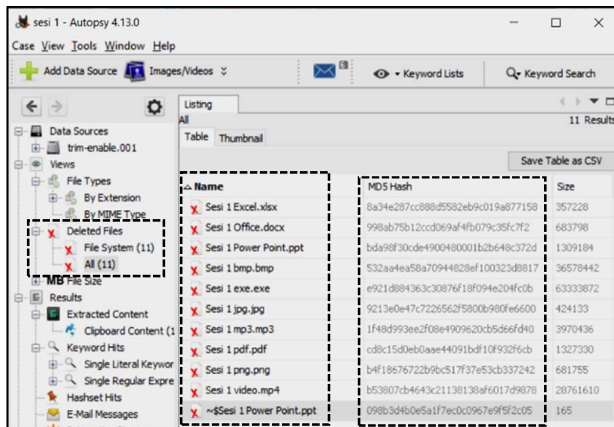
menggunakan Autopsy sesi pertama Gambar 12 (a) dan sesi kedua Gambar 12 (b).

Hasil eksaminasi menggunakan Autopsy pada sesi pertama Gambar 12 (a) ditemukan 11 bukti digital dengan karakteristik nama *file* dan *size* sama tapi nilai *hash* berbeda, lokasi file berada di /img_trim-enable.001. Sedangkan pada Gambar 12 (b) sesi kedua ditemukan 29 bukti digital dengan karakteristik nama *file* berubah, *size* dan nilai *hash* sama dengan bukti digital asli, letak file berada di img_trim-enable.001/\$RECYCLE.BIN. Proses eksaminasi menggunakan Recuva sesi pertama pada Gambar 13 (a) dan sesi kedua pada Gambar 13 (b).



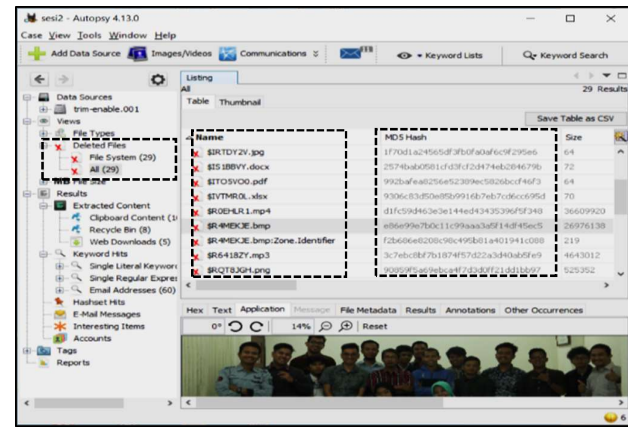
Filename	File Size	MD5
trim-enable.001	128.034.708.480	8d236112ccae7cf550dda5db55e8d0c3

Gambar 11. Nilai *hash* salinan *image*



Name	MD5 Hash	Size
Sesi 1 Excel.xlsx	8a34e287cc88d5582eb9c019a877158	357228
Sesi 1 Office.docx	998ab75b12cc0d69af4fb079c35f7f2	683798
Sesi 1 Power Point.ppt	bda9f30cde4900480001b2b648c372d	1309184
Sesi 1 mp3.mp3	532aa4ea58a70944828ef100323d817	36578442
Sesi 1 exe.exe	e921d89436c30876f18f094e204fc0b	63333872
Sesi 1 jpg.jpg	921360e47c7226562f5900b980e6600	424133
Sesi 1 mp3.mp3	1f48d993ae2f08e4909620cb5d6fd40	3970436
Sesi 1 pdf.pdf	cd8c15d0eb0aee44091bd1f09326cb	1327330
Sesi 1 png.png	b4f18676722b9c51737e53cb337242	681755
Sesi 1 video.mp4	b53807cb4643c21138138af601796878	28761610
~\$Sesi 1 Power Point.ppt	098b3d40d5a17ec0c0967e9f92c05	165

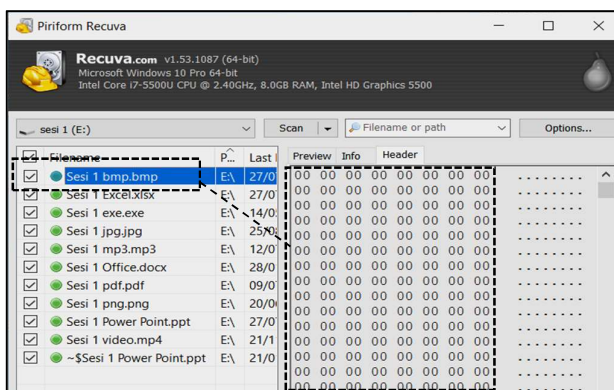
(a) Eksaminasi Sesi 1



Name	MD5 Hash	Size
\$RTDY2V.jpg	177d11a24f565df8f0abaf6c9cf295eb	14
\$S18BVV.docx	9274a4eb95c1d1d81d394744b20479b	12
\$RTOSV00.pdf	92b0f4e6276a5a23899e5020b0cf4f3	14
\$VTMR0L.xlsx	1936c63f80d8f9916b7b7c6cc95d40	70
\$R4MEKEJ.bmp	11cf59d463e3e144ed43435396f5f340	16609920
\$R4MEKEJ.bmp:Zone.Identifier	66e999e7b0c11c99a3a3af14bf45e5	26976138
\$R6418ZY.mp3	f2b666e6200c9b0c495b01a401941c08b	219
\$RQT8IGH.png	1c7ebc0bf7b1874f57d2a3d40ab9fa9	1643012
\$RQT8IGH.png	1c7ebc0bf7b1874f57d2a3d40ab9fa9	1643012

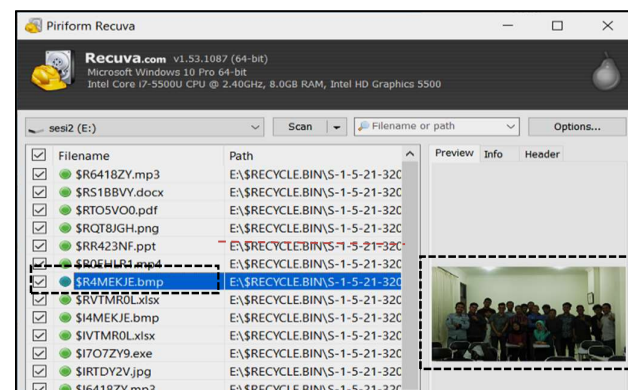
(b) Eksaminasi Sesi 2

Gambar 12. Eksaminasi menggunakan *tool* Autopsy



Filename	Path	Size
Sesi 1 bmp.bmp	E:\	27/0
Sesi 1 Excel.xlsx	E:\	27/0
Sesi 1 exe.exe	E:\	14/0
Sesi 1 jpg.jpg	E:\	25/0
Sesi 1 mp3.mp3	E:\	12/0
Sesi 1 Office.docx	E:\	28/0
Sesi 1 pdf.pdf	E:\	09/0
Sesi 1 png.png	E:\	20/0
Sesi 1 Power Point.ppt	E:\	27/0
Sesi 1 video.mp4	E:\	21/1
~\$Sesi 1 Power Point.ppt	E:\	21/0

(a) Eksaminasi Sesi 1



Filename	Path	Size
\$R6418ZY.mp3	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$R518BVV.docx	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$RTOSV00.pdf	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$RQT8IGH.png	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$R423NF.ppt	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$R4MEKEJ.bmp	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$VTMR0L.xlsx	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$I4MEKEJ.bmp	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$VTMR0L.xlsx	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$I707Z9.exe	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$RTDY2V.jpg	E:\\$RECYCLE.BIN\S-1-5-21-32C	
\$I6418ZY.mp3	E:\\$RECYCLE.BIN\S-1-5-21-32C	

(b) Eksaminasi Sesi 2

Gambar 13. Eksaminasi menggunakan *tool* Recuva

Hasil eksaminasi menggunakan Recuva pada sesi pertama Gambar 13 (b) ditemukan 11 file dengan karakteristik nama file sama, *size* sama tapi nilai *hash* berbeda, lokasi file berada di E:\. Sedangkan pada Gambar 13 (b) sesi kedua ditemukan 18 file dengan karakteristik nama file berubah, *size* dan nilai *hash* sama dengan bukti digital asli, letak file berada di E:\\$RECYCLE.BIN.

Berdasarkan hasil Gambar 12 dan Gambar 13 beberapa file dapat direstorasi menggunakan kedua tool tersebut. Rekapitulasi *recovery* file pada Tabel 2.

D. Analisis

Hasil *recovery* bukti digital dianalisis menggunakan tool *forensics* untuk pengecekan *magic number* pada header file disesuaikan dengan file signature berupa nilai hexadesimal dan validasi nilai *hash* [22], berikut Gambar 14 contoh analisis bukti digital menggunakan tool

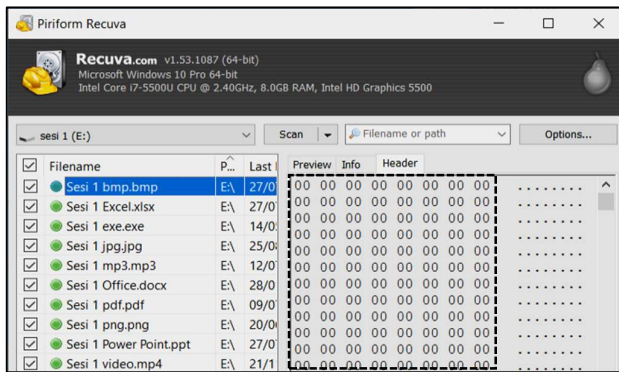
Recuva dengan pengecekan *magic number* pada sesi pertama dan sesi kedua.

Header pada Gambar 14 (a) tidak mempunyai nilai (*zero*) meskipun memiliki nilai *size* yang sama. Sedangkan pada header Gambar 14 (b) mempunyai nilai yang unik, 4 digit diawal header 42 4D menunjukkan *magic number* dengan ekstensi .bmp.

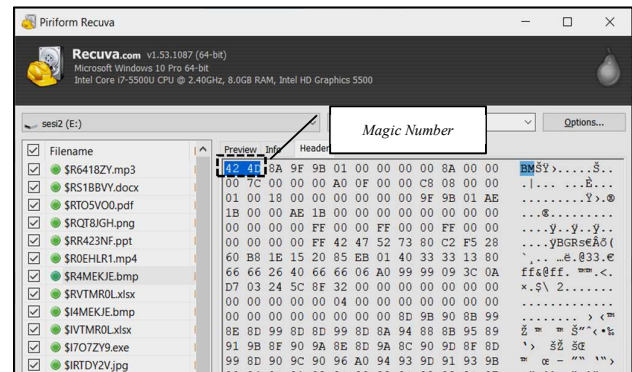
Selanjutnya tahapan analisis *recovery* bukti digital dengan validasi nilai *hash* dirangkum pada Tabel 3 untuk sesi pertama dan sesi kedua dengan menggunakan tool Autopsy.

TABEL II
HASIL REKAPITULASI RECOVERY AUTOPSY DAN RECUVA

Sesi	Autopsy	Recuva
Sesi 1	11	11
Sesi 2	29	18



(a) Analisis Sesi 1



(b) Analisis Sesi 2

Gambar 14. Contoh analisis *magic number* pada header menggunakan tool Autopsy

TABEL III
VALIDASI NILAI HASH SESI 1 MENGGUNAKAN TOOL AUTOPSY

Nama File	Hash MD5	Validasi hash
Sesi 1 bmp	532aa4ea58a70944828ef100323d8817	Tidak valid
Sesi 1 xlsx	8a34e287cc888d5582eb9c019a877158	Tidak valid
Sesi 1 exe	e921d884363c30876f18f094e204fc0b	Tidak valid
Sesi 1 jpg	9213e0e47c7226562f5800b980fe6600	Tidak valid
Sesi 1 mp3	1f48d993ee2f08e4909620cb5d66fd40	Tidak valid
Sesi 1 docx	998ab75b12ccd069af4fb079c35fc7f2	Tidak valid
Sesi 1 pdf	cd8c15d0eb0aae44091bdf10f932f6cb	Tidak valid
Sesi 1 png	b4f18676722b9bc517f37e53cb337242	Tidak valid
Sesi 1 ppt	bda98f30cde4900480001b2b648c372d	Tidak valid
Sesi 1 mp4	b53807cb4643c21138138af6017d9878	Tidak valid
Sesi 2 bmp	e86e99e7b0c11c99aaa3a5f14df45ec5	Valid
Sesi 2 xlsx	77ac2f423a09ef051100e4fe411f9279	Valid
Sesi 2 exe	e502f644456067d08942faecf5d4169a	Tidak valid
Sesi 2 jpg	400277f9a8290c47def497cfa8ee382c	Valid
Sesi 2 mp3	3c7ebc8bf7b1874f57d22a3d40ab5fe9	Valid
Sesi 2 docx	aa125f3e35214c72e3a87a11e3d4903f	Valid
Sesi 2 pdf	0a569b127c7de6bea02cf6e87e41c5f2	Valid
Sesi 2 png	90859f5a69ebca4f7d3d0ff21dd1bb97	Valid
Sesi 2 ppt	3352425c3dd400faca160feceaf50210	Valid
Sesi 2 mp4	d1fc59d463e3e144ed43435396f5f348	Valid

Hasil analisis *tool* Autopsy sesi pertama dengan mencocokkan nilai *hash* Tabel 1 dan Tabel 3 tidak ditemukan bukti digital yang cocok dengan bukti digital asli. Sedangkan pada Sesi kedua ditemukan 9 dari 10 bukti digital dinyatakan sama nilai *hash* dengan bukti digital asli dan 1 bukti digital yang tidak sama nilai *hash* dengan ekstensi .exe.

Tahapan selanjutnya analisis *recovery* bukti digital yang ditemukan dengan mencocokkan nilai *hash* Tabel 1 dengan Tabel 4 untuk sesi pertama dan sesi kedua dengan menggunakan *tool* Recuva.

Hasil analisis *tool* Recuva sesi pertama pada Tabel 4 tidak ditemukan bukti digital yang cocok dengan bukti digital asli. Sedangkan sesi kedua ditemukan 8 dari 10 bukti digital mempunyai nilai *hash* yang sama dengan bukti digital asli, bukti digital tidak dapat ditemukan berupa satu *file* dengan ekstensi exe dan satu *file* ekstensi jpg.

Peneliti merangkum seluruh hasil penelitian pada Tabel 5 sebagai perbandingan *tools forensics* untuk *recovery* bukti digital pada SSD NVMe dengan metode penghapusan *shift delete* dan *delete, delete recycle bin*.

IV. PENUTUP

Berdasarkan hasil analisis *recovery* bukti digital pada SSD NVMe menggunakan metode *static forensics* yang telah peneliti lakukan, fitur TRIM *enable* dengan metode penghapusan *shift delete* tidak dapat mengembalikan bukti digital yang sesuai nilai *hash* dengan bukti digital yang asli sedangkan metode penghapusan *delete, delete recycle bin* bukti digital dapat dikembalikan identik dengan nilai *hash* bukti digital yang asli. Prosentase dari 10 sampel bukti digital yang dapat dikembalikan dengan metode penghapusan *delete, delete recycle bin* menggunakan *tool* Autopsy sebesar 90% dan 10% nilai *hash* bukti digital tidak valid, sedangkan *tool* Recuva 80% bukti digital berhasil dikembalikan dan 20% tidak berhasil dikembalikan. Dapat disimpulkan hasil *recovery* penghapusan *delete, delete recycle bin* pada SSD NVMe TRIM *enable* dapat dijadikan bukti digital yang sah menurut hukum. Pada penelitian berikutnya dapat dilanjutkan dengan menggunakan metode yang berbeda yaitu *live forensics* dan penggunaan *tools forensics* yang berbeda.

TABEL IV
VALIDASI NILAI HASH SESI 1 MENGGUNAKAN TOOL RECUVA

Nama File	Hash MD5	Validasi hash
Sesi 1 bmp	532aa4ea58a70944828ef100323d8817	Tidak valid
Sesi 1 xlsx	8a34e287cc888d5582eb9c019a877158	Tidak valid
Sesi 1 exe	e921d884363c30876f18f094e204fc0b	Tidak valid
Sesi 1 jpg	9213e0e47c7226562f5800b980fe6600	Tidak valid
Sesi 1 mp3	1f48d993ee2f08e4909620cb5d66fd40	Tidak valid
Sesi 1 docx	998ab75b12ccd069af4fb079c35fc7f2	Tidak valid
Sesi 1 pdf	cd8c15d0eb0aae44091bdf10f932f6cb	Tidak valid
Sesi 1 png	b4f18676722b9bc517f37e53cb337242	Tidak valid
Sesi 1 ppt	bda98f30cde4900480001b2b648c372d	Tidak valid
Sesi 1 mp4	b53807cb4643c21138138af6017d9878	Tidak valid
\$R4MEKJE.bmp	e86e99e7b0c11c99aaa3a5f14df45ec5	Valid
\$RVTMR0L.xlsx	77ac2f423a09ef051100e4fe411f9279	Valid
(extensi exe)	-	Tidak ditemukan
(extensi jpg)	-	Tidak ditemukan
\$R6418ZY.mp3	3c7ebc8bf7b1874f57d22a3d40ab5fe9	Valid
\$RS1BBVY.docx	aa125f3e35214c72e3a87a11e3d4903f	Valid
\$RTO5VO0.pdf	0a569b127c7de6bea02cf6e87e41c5f2	Valid
\$RQT8JGH.png	90859f5a69ebca4f7d3d0ff21dd1bb97	Valid
\$RR423NF.ppt	3352425c3dd400faca160feecaf50210	Valid
\$R0EHLR1.mp4	d1fc59d463e3e144ed43435396f5f348	Valid

TABEL V
PERBANDINGAN RECOVERY TOOL FORENSICS

Nama File	Autopsy		Recuva	
	Sesi 1	Sesi 2	Sesi 1	Sesi 2
Valid	0	9	0	8
Tidak valid	10	1	10	0
Tidak ditemukan	0	0	0	2

DAFTAR PUSTAKA

- [1] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Analisis Kelayakan Integrated Digital Forensics Investigation Framework Untuk Investigasi Smartphone," *J. Buana Inform.*, vol. 7, no. 4, pp. 265–274, 2016.
- [2] Eliasta Ketaren, "Cybercrime, Cyber Space, dan Cyber Law," *Times*, vol. 5, no. 2, pp. 35–42, 2016.
- [3] B. J. Nikkel, "NVM Express Drives and Digital Forensics Introduction to NVM Express," *No Starch Press*, pp. 1–16, 2016.
- [4] R. K. Chaurasia and P. Sharma, "Solid State Drive (SSD) Forensics Analysis : A New Challenge," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* © 2017 IJSRCSEIT, vol. 6, no. 2, pp. 1081–1085, 2017.
- [5] M. Lawson, "Solid State Forensics," *BSc Comput. Sci. with Secur. Forensics*, p. 69, 2018.
- [6] S. S. R. Marupudi, "Solid State Drive : New Challenge for Forensic Investigation," p. 100, 2017.
- [7] Z. Shah, A. N. Mahmood, and J. Slay, "Forensic potentials of solid state drives," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 153, no. September, pp. 113–126, 2015.
- [8] I. Riadi and A. Hadi, "Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics," *CoreIt*, vol. 3321, no. 2, pp. 1–8, 2019.
- [9] A. Aldaej, M. G. Ahamad, and M. Y. Uddin, "Solid state drive data recovery in open source environment," in *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017*, 2017.
- [10] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD)," *Teknomatika*, vol. 9, no. 2, pp. 1–13, 2017.
- [11] B. J. Raj and R. Hubbard, "Forensics Analysis of Solid State Drive (SSD)," *Proc. 2016 Univers. Technol. Manag. Conf.*, pp. 1–11, 2016.
- [12] S. Sunardi, I. Riadi, and I. M. Nasrulloh, "Analisis Forensik Solid State Drive (SSD) Menggunakan Framework Rapid Response," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 5, p. 509, 2019.
- [13] I. Riadi, R. Umar, and W. Sukarno, "Analisis Forensik Serangan Sql Injection Menggunakan Metode Statis Forensik," *Pros. Interdiscip. Postgrad. Student Conf. Ist.*, vol. I, no. I, pp. 102–103, 2016.
- [14] I. Riadi, "Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 6, no. 4, pp. 198–205, 2017.
- [15] A. R. Caesarano and I. Riadi, "Network Forensics for Detecting SQL Injection Attacks using NIST Method," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 436–443, 2018.
- [16] A. Hadi and S. Riadi, Imam, "Forensik Bukti Digital Pada Solid State Drive (SSD) NVMe Menggunakan Metode National Institute of Standards and Technology (NIST)," *SEMNASSTEK 2019*, pp. 551–558, 2019.
- [17] Sunardi, I. Riadi, and A. Sugandi, "Forensic analysis of Docker Swarm cluster using GRR Rapid Response framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 2, pp. 459–466, 2019.
- [18] I. Riadi, R. Umar, and A. Sugandi, "Web Forensic On Kubernetes Cluster Services Using Grr Rapid Response Framework," vol. 9, no. 01, pp. 3484–3488, 2020.
- [19] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, p. 13, 2018.
- [20] L. S. Negara, J. Harsono, R. M. No, and J. Selatan, "Elektronik Pemerintahan Guna Mendukung E-Government," 2016.
- [21] S. Kandala, "Analyzing the Trimming Activity of Solid-State Drives in Digital Forensics," 2019.
- [22] R. Kadam, A. Saraf, D. Dave, and S. Faculty, "A Comprehensive Study On Linux Forensics," vol. 21, no. 14, pp. 12–21, 2019.