Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 5 ; Nomor 2 ; Juli 2022 ; Page 185-192
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics

Nabilla Fatmah[1], Rini Indrayani[2]

[1] Program Studi Teknik Komputer, Universitas Amikom Yogyakarta
[2]Program Studi Teknik Komputer, Universitas Amikom Yogyakarta
Email: [1]nabilla.fatmah@students.amikom.ac.id, [2]rini.i@amikom.ac.id
Email Penulis Korespondensi: rini.i@amikom.ac.id

Article History:
Received Jun 12th, 2022
Revised Jul 15th, 2022
Accepted Jul 19th, 2022

Abstrak

Jumlah penggunaan *Solid State Drive* (SSD) diberbagai perusahaan semakin meningkat setiap tahunnya berbanding terbalik dengan jumlah penggunaan *Harddisk* (HDD) yang semakin menurun setiap tahunnya. Fungsi TRIM yang ada pada SSD berdampak negatif pada analisis forensik dan data yang sudah terhapus tidak dapat lagi dijamin persistensinya. Metode analisis yang digunakan pada penelitian ini adalah metode *static* dengan menerapkan standar forensik digital SNI *Acquisition* 27037:2014 sebagai panduan langkah akusisi. Proses *recovery* dilakukan dengan menggunakan tool *Autopsy* dan *OSForensics.* Hasil dari proses percobaan akuisisi dan *recovery* menunjukkan bahwa *tool OSForensics* memiliki waktu akuisisi 228 menit pada SSD TRIM *enable* dan 231 menit pada SSD TRIM *disable* sedangkan *tool Autopsy* memiliki waktu akuisisi 323 menit pada SSD TRIM *enable* dan 334 menit pada SSD TRIM *disable*. Persentase tingkat keberhasilan *recovery tool Autopsy* pada SSD TRIM *enable* sebesar 0% dan pada SSD TRIM *disable* sebesar 100%. Hasil yang sama juga didapatkan oleh *tool OSForensics* dimana persetase keberahsilan *recovery* yang dilakukan pada SSD TRIM *enable* sebesar 0% sedangkan pada SSD TRIM *disable* sebesar 100%. Dari hasil tersebut dapat disimpulkan bahwa *tool OSForensics* memiliki waktu proses akuisisi yang lebih cepat. Kemampuan *recovery* yang ditunjukkan oleh kedua *tool* serupa pada SSD TRIM *disable* maupun TRIM *enable.*

Kata Kunci : Autopsy, OSForensics, SNI Acquisition 27037:2014, SSD, TRIM

Abstract

The number of Solid State Drive (SSD) usage in various companies is increasing every year, inversely proportional to the number of Hard Drive (HDD) usage which is decreasing every year. The TRIM function present on the SSD has a negative impact on forensic analysis and data that has been erased can no longer be guaranteed for its persistence. The analytical method used in this study is the static method by applying the digital forensic standard SNI Acquisition 27037:2014 as a guide for acquisition steps. The recovery process is carried out using Autopsy and OSForensics tools. The results of the acquisition and recovery experiment show that the OSForensics tool has an acquisition time of 228 minutes on SSD TRIM enabled and 231 minutes on SSD TRIM disabled while the Autopsy tool has an acquisition time of 323 minutes on SSD TRIM enabled and 334 minutes on SSD TRIM disabled. The percentage of success rate of Autopsy recovery tool on SSD TRIM enabled is 0% and on SSD TRIM disabled is 100%. The same result was also obtained by the OSForensics tool where the percentage of successful recovery performed on SSD TRIM enabled was 0% while on SSD TRIM disabled was 100%. From these results it can be concluded that the OSForensics tool has a faster acquisition process time. The recovery capabilities shown by the two tools are similar on SSD TRIM disabled and TRIM enable

Keyword : *Autopsy, OSForensics, SNI Acquisition 27037:2014, SSD, TRIM*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 5 ; Nomor 2 ; Juli 2022 ; Page 185-192
E-ISSN : 2615-5133 ; **P-ISSN** : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

1. PENDAHULUAN

Jejak dan bukti digital yang ditemukan pada kasus kejahatan komputer harus dianalisis menggunakan ilmu dan metode forensik. Analisis forensik terhadap jejak dan bukti digital di bidang teknologi dikenal sebagai forensik digital [1]. Forensik digital pada dasarnya adalah menemukan bukti digital yang dapat disimpan dalam penyimpanan sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan dan lainnya. Kemudian, digital forensik menjadi bagian penting dalam keamanan informasi [2].

Static forensic merupakan salah satu metode digital forensik yang menggunakan pendekatan secara konvensional yaitu, bukti digital diproses menjadi *bit-by-bit image* untuk melakukan proses forensik. Proses forensik sendiri berjalan pada sistem yang tidak berjalan *(shutdow*n)[3].

SSD merupakan singkatan dari *Solid State Drive* dan SSD memiliki fungsi yang sama dengan HDD yang digunakan sebagai tempat penyimpanan data. SSD merupakan wadah yang digunakan untuk menyimpan segala informasi pada *chip memory flash* [4]. SSD telah memperkenalkan produk perangkat penyimpanan barunya, SSD *Non-volatile Memory Express* (SSD NVMe). SSD NVMe menggunakan *interface* PCIe (*Peripheral Component Interconnect Express*) untuk transfer data yang lebih efisien [5]. Belakangan ini banyak sekali perusahaan yang beralih ke SSD untuk mendapatkan kinerja yang lebih tinggi, ukuran fisik yang baik, dan efesiensi energi [4]. SSD saat ini memiliki fitur baru yaitu *Solid State Drive Non-Volatile Memory Express* (SSD NVMe), dan memiliki perbedaan *interface* dengan yang digunakan oleh SATA SSD yaitu *interface* PCIe (*Peripheral Component Interconnect Express*) yang dapat melakukan transfer data lebih cepat jika dibandingkan dengan *interface* yang digunakan oleh SATA SSD. SSD juga memiliki fungsi TRIM. Fungsi TRIM merupakan suatu ftur pada SSD yang berhubungan dengan sistem operasi[6]. Cara kerjanya adalah TRIM akan menghapus secara internal *block* mana yang dianggap perlu dihapus. [7].

SNI *Acquisition* 27037:2014 adalah salah satu bagian dari SNI 27037:2014 yang merupakan standar forensik digital dan seluruh isi dokumen telah di adopsi sejak ISO 27037:2012 menggunakan dua metode, yaitu *reprint* dan *reissue*. SNI 27037:2014 adalah standar yang diakui secara nasional yang menjelaskan pedoman khusus kegiatan penelitian forensik digital. SNI 27037:2014 yang mengatur tentang tata cara memperoleh barang bukti elektronik dan digital memiliki 4 bagian tahapan yaitu identifikasi, pengumpulan, akuisisi dan preservasi. Tahap akuisisi pada perangkat digital dijelaskan dalam dokumentasi SNI, terdapat 3 model akuisisi yaitu akuisisi pada perangkat digital yang ditemukan dalam keadaan hidup/*on*, akuisisi pada perangkat digital yang ditemukan dalam keadaan mati/*off* dan akuisisi *partial* pada perangkat digital yang ditemukan dalam keadaan hidup namun tidak memungkinkan untuk melakukan akuisisi terhadap keseluruhan data[8].

Berbagai penelitian telah dilakukan, salah satunya Ramadhan, Prayudi & Sugiantoro (2017), melaukan penelitian dengan me-*recovery* SSD SATA fungsi TRIM *enable* dan *disable* menggunakan metode *static*, penelitian ini memberikan hasil akhir yaitu, Sebagian besar data pada SSD SATA fungsi TRIM *disable* dapat di-*recovery*, sedangkan pada SSD SATA fungsi TRIM *enable*, sebagian besar data tidak dapat di-*recovery* kembali [4].

Penelitian lainnya yang dilakukan oleh Raidi, Umar & Nasrulloh, (2017), melakukan penelitian dengan me-*Recovery* SSD yang memiliki *software* pembeku *drive* pada sistemnya dengan menggunakan metode *National Institute of Standars and Technology* (NIST), penelitian ini memberikan hasil akhir yaitu, Bukti digital yang telah berhasil didapatkan adalah file dokumen (.doc, .xms, .pdf), file gambar (.jpg, .png) beserta *logfiles* [9]. Melanjutkan penelitiannya Riadi, Umar & Nasrulloh, (2018), melakukan *Recovery* SSD yang memiliki *software* pembeku *drive* pada sistemnya dengan jenis *shadow defender* menggunakan metode *National Institute of Justice* (NIJ), penelitian ini memberikan hasil akhir Persentase keberhasilan restorasi file yang didapatkan hanya 28,7% .[10].

Raidi, Sumardi & Hadi (2019), melakukan penelitian dengan me-*Recovery* SSD NVMe fungsi TRIM *enable* dan *disable* menggunakan metode *static*, penelitian ini memberikan hasil akhir yaitu, Persentase keberhasilan restorasi bukti digital TRIM *enable* adalah 0%, sedangkan pada TRIM *disable* 92% menggunakan *tool Autopsy* dan 99% menggunakan *tool Recover My File* [11].

Pranoto, Riadi & Prayudi (2020), melakukan penelitian perbandingan *tools* digital forensik untuk melakukan *recovery* file fungsi TRIM menggunakan metode *Live forensics*, penelitian ini memberikan hasil akhir *Recovery* TRIM *disable* menggunakan *tool Autopsy* dan *Testdisk* menunjukan persentase keberhasilan 100% sedangkan tools *Belkasoft* hanya menghasilkan persentase keberhasilan 3%. Sedangkan pada fungsi TRIM *enable* menunjukan hasil persentase keberhasilan 0% pada semua *tools* [12].

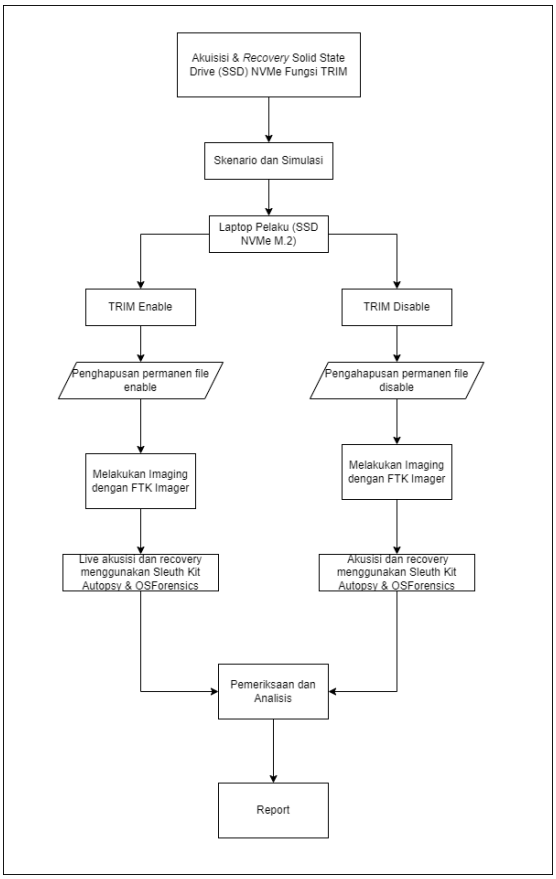
Penelitian ini dibuat dengan mengadopsi dan menerapkan kombinasi metode, *tools* yang digunakan, objek penelitian beserta teknik analisis yang ada pada penelitian terdahulu yang dijadikan acuan penelitian sehingga peneliti dapat membuat usulan penelitian baru yaitu melakukan penerapan metode *live forensic* pada SSD Fungsi TRIM Menggunakan *tool Autopsy* dan *tool OSForensics.* Metode yang digunakan yaitu metode *static* dengan menerapkan standar forensik digital SNI *Acquisition* 27037:2014 sebagai panduan langkah akusisi dengan tool *Autopsy* dan *OSForensics* sebagai tool *recovery.* Objek penelitian adalah SSD versi terbaru saat ini yaitu SSD NVme M.2. Sedangkan target data yang digunakan telah disesuaikan dengan rancangan skenario *dummy* yang telah dibuat yaitu yang berkaitan dengan kasus penggelapan dana. Fokus dari penelitian ini adalah untuk mendapatkan data perbandingan percobaan akuisisi dan *recovery* dengan *tool Autopsy* dan *tool OSForensics* pada SSD NVme M.2 fungsi TRIM *enable* dan *disable.*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 5 ; Nomor 2 ; Juli 2022 ; Page 185-192
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

2. METODOLOGI PENELITIAN

2.1 Alur Penelitian

Penelitian diawali dengan melakukan identifikasi masalah dan studi literatur terkait dengan proses akuisisi dan *recovery* SSD Fungsi TRIM *enable* dan *disable.* Langkah berikutnya yaitu membuat skenario kasus *dummy* tentang penggelapan dana yang dilakukan oleh oknum pada sebuah organisasi yang akan dijadikan sebagai acuan arah investigasi. Eksperimen dilakukan sesuai skenario yang telah dibuat dengan menerapkan standar SNI *Acquisition* 27037:2014 pada proses akuisisi dan melakukan *recovery* menggunakan *tool Autopsy* dan *OSForensics* SSD Fungsi TRIM *enable* dan *disable*. Hasil dari eksperimen kemudian diperiksa integritasnya dengan membandingkan nilai *hash* dari file *image* sebelum dan sesudah dilakukan akuisisi dan *recovery.* Kemudian dilakukan analisis dengan membandingkan file hasil *recovery* dengan barang bukti yang ditemukan di TKP. Proses alur penelitian ditunjukkan pada Gambar 1.



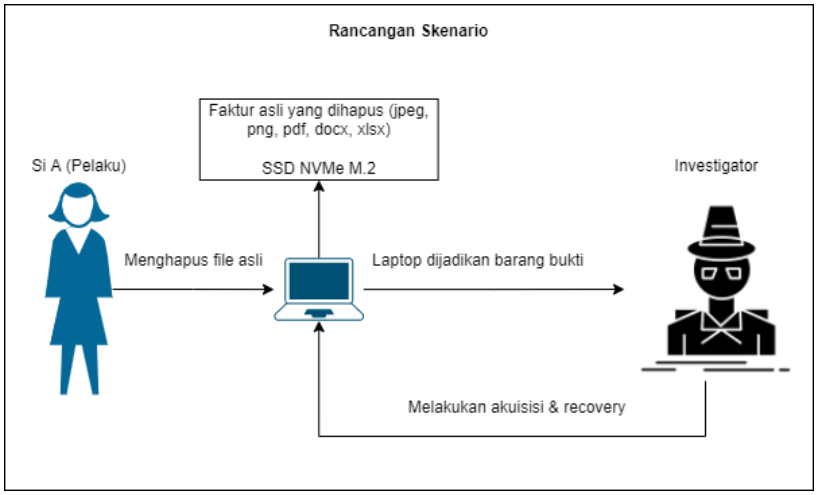
Gambar 1. Alur Penelitian

Gambar 1 menjelaskan alur penelitian yang akan dilakukan mulai dari mengaktifkan/menonaktifkan mode TRIM pada SSD kemudian dilanjutkan dengan penghapusan file secara permanen dengan perintah *SHIFT+DELETE*, selanjutnya SSD akan di-*imaging* menggunakan tool *FTK Imager*, kemudian file *image* akan diakuisisi dan selanjutnya file yang sudah terhapus akan di-*recovery* menggunakan *tool Autopsy* dan tool *OSForensics* yang selanjutnya hasil *recovery* berupa faktur akan diperiksa dengan cara membandingkannya dengan faktur dan laporan keuangan yang dibuat oleh tersangka.

2.2 Rancangan Skenario

Penelitian dilakukan dengan skenario bahwa adanya indikasi pemalsuan dokumen oleh si A dengan cara menghapus file faktur asli dan membuat file faktur palsu. Skenario dimulai dengan adanya data tidak wajar mengenai laporan keuangan organisasi, dimana biaya pengeluaran terlalu besar dan mencurigakan. Diduga adanya tindakan penggelapan dana yang terjadi. Setelah diperiksa ternyata yang bertanggung jawab membuat laporan tersebut adalah si A. Ilustrasi rancangan skenario ditampilkan pada gambar 2.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 5 ; Nomor 2 ; Juli 2022 ; Page 185-192
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index



Gambar 2. Rancangan Skenario

Sesuai dengan ilustrasi rancangan skenario pada gambar 2, kronologi dari skenario sebagai berikut :

a. Si A membuat faktur palsu dan menghapus faktur asli.
b. Si A membuat laporan keuangan dengan faktur palsu.

Semua data yang berupa faktur asli yang telah dihapus pada laptop tersangka akan diungkap atau dikembalikan menggunakan *tool Autopsy* dan tool *OSForensics.* Penyelidikan dilakukan dengan barang bukti laptop si A, laporan keuangan yang ditampilkan pada gambar 3, beserta faktur yang diduga palsu ditampilkan pada gambar 4.

LAPORAN KEUANGAN
ORGANISASI XYZ

Pemasukan

Detail	ESTIMATION		
	Qty	Price	Total
Subsidi Organisasi	1	Rp100,000,000,-	Rp100,000,000,-
TOTAL INCOME			Rp100,000,000,-

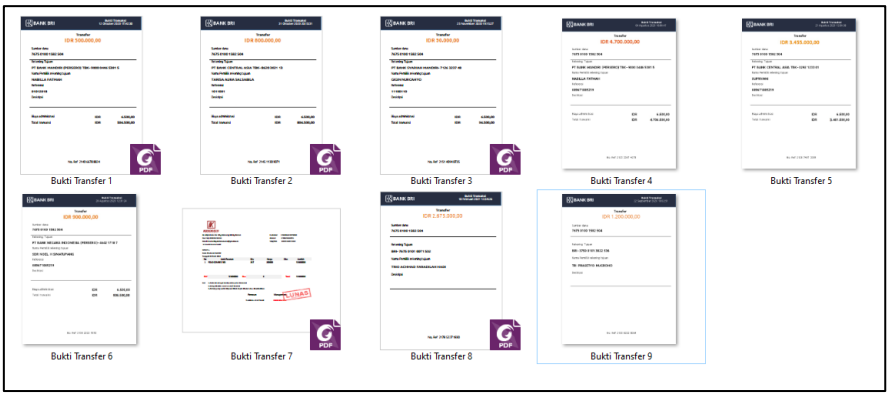
Pengeluaran

Pengeluaran	Tanggal Transaksi	Pengeluaran		
		Qty	Price	Total
Kertas HVS F4	12/10/2020	5	Rp100,000,-	Rp500,000,-
Keyboard Logitech	31/10/2020	2	Rp400,000,-	Rp800,000,-
Isolasi	25/11/2020	6	Rp15,000,-	Rp90,000,-
Baju Event Organisasi (Polo Combed 30S)	02/02/2022	267	Rp200,000,-	Rp53,400,000,-
Sewa Ruangan 1 hari	18/02/2021	1	Rp2,675,000,-	Rp2,675,000,-
Paket Alat Tulis	04/08/2020	100	Rp47,000	Rp4,700,000,-
Printer Epson K300	21/08/2020	1	Rp.455,000,-	Rp3,455,000,-
Tinta Printer	28/08/2020	10	Rp 90,000	Rp900,000,-
Router TP-LINK Archer	22/09/2020	2	Rp600,000	Rp1,200,000,-
Sub Total				Rp67,720,000,-

Gambar 3. Laporan Keuangan Sebagai Barang Bukti

Gambar 3 menunjukkan laporan keuangan yang digunakan sebagai barang bukti yang berisi tentang pengeluaran organisasi yang didalamnya ada tanggal transaksi, total pengeluaran beserta apa saja detail pengeluaran tersebut. Semua data pada laporan keuangan diatas memiliki faktur/bukti pembayaran yang sesuai dengan apa yang tertera pada laporan keuangan.

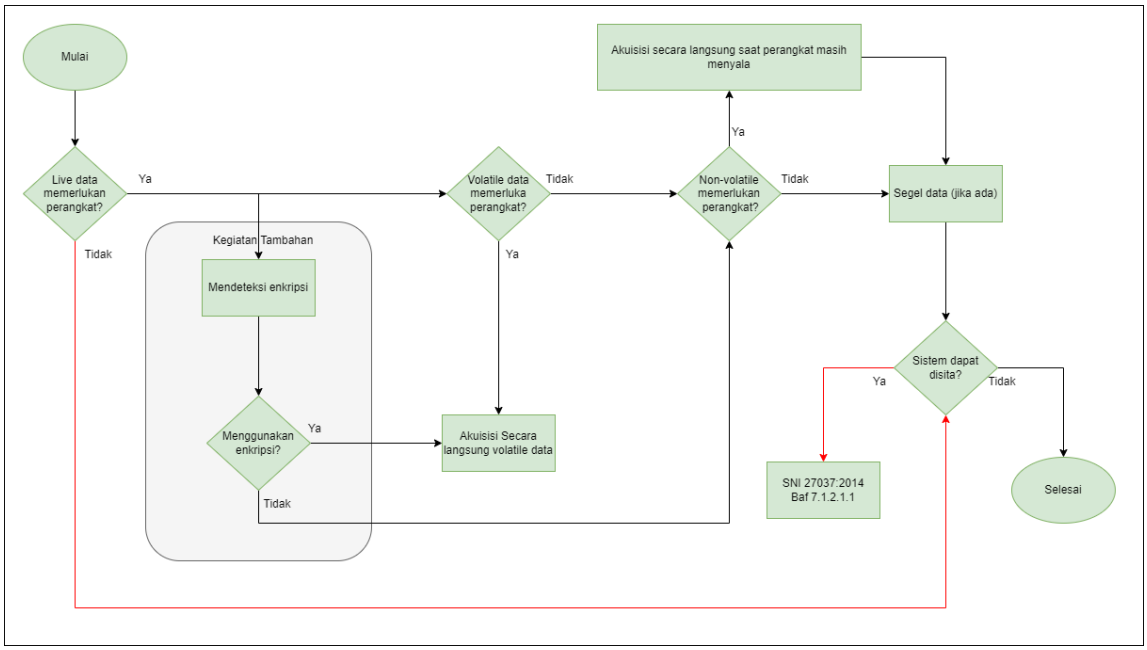
Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 5 ; Nomor 2 ; Juli 2022 ; Page 185-192
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index



Gambar 4. File Bukti Transaksi diduga Palsu

2.3 Metode Akuisisi

Tahapan penelitian dalam melakukan akuisisi dan *recovery* SSD Fungsi TRIM *enable* dan *disable* dengan menggunakan *tool Autopsy* dan *OSForensics* berdasarkan metode *static forensic* dengan menerapkan standar forensik digital SNI *Acquisition* 27037:2014 sebagai panduan langkah akusisi. *Static forensic* menggunakan pendekatan secara konvensional yaitu, bukti digital diproses menjadi *bit-by-bit image* untuk melakukan proses forensik yang berjalan pada sistem yang sedang tidak berjalan *(shutdow*n).[3] SNI *Acquisition* 27037:2014 adalah salah satu bagian dari SNI 27037:2014 yang merupakan standar yang diakui secara nasional yang menjelaskan pedoman khusus kegiatan penelitian forensik digital. Model akuisisi yang digunakan adalah akuisisi pada perangkat digital yang ditemukan dalam keadaan mati/*off*. *Flowchart* akuisisi ditunjukkan pada Gambar 5 [8].



Gambar 5. *Flowchart* Akuisisi Perangkat dalam Keadaan Mati

Gambar 5 menunjukan alur ilustrasi proses yang digunakan untuk mengakuisisi SSD NVMe pada perangkat digital yang sudah mati/*off*. Alur yang digunakan bisa ditelusuri pada garis panah merah pada gambar, dimulai dari apakah *live* data memerlukan perangkat? Karena perangkat sudah ditemukan dalam keadaan mati/*off* dan proses forensik yang akan dilakukan adalah akuisisi dan *recovery* terhadap data *non-volatile* maka proses akan langsung menuju ke tahap penyitaan sistem.

3. HASIL DAN PEMBAHASAN

Pemeriksaan dilakukan dengan membandingkan nilai *hash* SHA-1 dan MD5 dari file *image* sebelum dan sesudah dilakukan akuisisi dan *recovery* oleh *tool Autopsy* dan *tool OSForensics* untuk memastikan bahwa file *image* tersebut identik. Berikut tabel perbandingan nilai *hash:*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 5 ; Nomor 2 ; Juli 2022 ; Page 185-192
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Tabel 1. Perbandingan Nilai *Hash* File *Image*

Tools	***Hash***	**TRIM *enable***	**TRIM *disable***
AccessData FTK Imager	MD5	1acbaa94536d37328b3066a2ed666cf0	7947603e7aa7f3612e690fa4b5b6b0bb
	SHA-1	96878d733ea07b2327dc9e8f308b1f23c8620b7	2315dcb894bb6e86593bce60b70e299f4a230dbb
Sleuthkit Autopsy	MD5	1acbaa94536d37328b3066a2ed666cf0	7947603e7aa7f3612e690fa4b5b6b0bb
	SHA-1	96878d733ea07b2327dc9e8f308b1f23c8620b7	2315dcb894bb6e86593bce60b70e299f4a230dbb
OSForensics	MD5	1acbaa94536d37328b3066a2ed666cf0	7947603e7aa7f3612e690fa4b5b6b0bb
	SHA-1	96878d733ea07b2327dc9e8f308b1f23c8620b7	2315dcb894bb6e86593bce60b70e299f4a230dbb
Identik (Ya/Tidak)		Ya	Ya

Tabel 1 menampilkan nilai *hash* MD5 dan SHA-1 dari file *image* SSD TRIM *enable* dan TRIM *disable* sebelum dilakukan akuisisi (*AccessData FTK Imager*) dan setelah dilakukan akuisisi dan *recovery* oleh *tool Sleuthkit Autopsy* dan *tool OSForensics.* Perbandingan menunjukkan nilai *hash* yang identik baik MD5 maupun SHA-1.

Analisis hasil *recovery* dilakukan dengan membandingkan file yang telah berhasil di-*recovery* dengan barang bukti yang ada berupa laporan keuangan dan bukti transaksi yang diduga palsu. Dari 25 file yang berhasil di-*recovery*, ada 7 file mencurigakan yang diduga adalah file bukti transaksi asli sebelum dimanipulasi. File bukti transaksi tersebut tidak konsisten dimana semua informasi didalamnya termasuk tanggal transaksi, sumber dana, rekening tujuan, nama pemilik rekening tujuan dan nomor referensi memiliki info yang sama kecuali nominal transfer/transaksi memiliki nominal yang berbeda yang berarti ada tindakan manipulasi pada bukti transaksi tersebut menggunakan laptop si A, berikut adalah gambar daftar dari data pengeluaran pada laporan keuangan yang sudah terbukti dimanipulasi ditampilkan pada gambar 6:

Pengeluaran

Pengeluaran	Tanggal Transaksi	Pengeluaran		
		Qty	Price	Total
Kertas HVS F4	12/10/2020	5	Rp100,000,-	Rp500,000,-
Keyboard Logitech	31/10/2020	2	Rp400,000,-	Rp800,000,-
Isolasi	25/11/2020	6	Rp15,000,-	Rp90,000,-
Baju Event Organisasi (Polo Combed 30S)	02/02/2022	267	Rp200,000,-	Rp53,400,000,-
Sewa Ruangan 1 hari	18/02/2021	1	Rp2,675,000,-	Rp2,675,000,-
Paket Alat Tulis	04/08/2020	100	Rp47,000	Rp4,700,000,-
Printer Epson K300	21/08/2020	1	Rp.455,000,-	Rp3,455,000,-
Tinta Printer	28/08/2020	10	Rp 90,000	Rp900,000,-
Router TP-LINK Archer	22/09/2020	2	Rp600,000	Rp1,200,000,-
		Sub Total		Rp67,720,000,-

Gambar 6. Laporan Keuangan yang Sudah dimanipulasi

Gambar 6 menunjukkan 7 transaksi keuangan pada laporan keuangan yang memiliki perbedaan nominal dengan file bukti transaksi hasil *recovery* dan terbukti sudah dimanipulasi, diantaranya adalah pengeluaran Kertas HVS F4, Keyboard Logitech, Isolasi, Baju Event Organisasi (Polo Combed 30S), Paket Alat Tulis, Printer Epson K300 dan Tinta Printer.

3.1 Hasil Recovery

Setelah hasil dari percobaan akuisisi dan *recovery* diperiksa dan dinyatakan identik, maka langkah selanjutnya adalah perhitungan persentase tingkat keberhasilan *recovery* pada *Solid State Drive* (SSD) NVMe M.2 fungsi TRIM *enable* dan *disable* dan perbandingan durasi waktu proses percobaan akuisisi menggunakan *tool Autopsy* dan *tool OSForensics.* Untuk mendapatkan data dalam bentuk persentase akan dilakukan perhitungan dengan menggunakan persamaan indeks tidak tertimbang yang ditunjukkan pada persamaan (1).

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 5 ; Nomor 2 ; Juli 2022 ; Page 185-192
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

$$Pon = \frac{\sum Pn}{\sum Po} x100\% \quad (1)$$

Pon menunjukkan hasil persentase tingkat keberhasilan berdasarkan data hasil penelitian, *ΣPn* adalah jumlah data yang berhasil ditemukan pada percobaan yang dilakukan, *ΣPo* adalah jumlah data target yang ingin dicari[13].

Perbandingan tingkat keberhasilan *recovery* berdasarkan fungsi TRIM ditampilkan pada tabel 2.

Tabel 2. Perbandingan Tingkat Keberhasilan *Recovery*

Jenis File	***Jumlah Target Data***	***Enable***		***Disable***	
		Autopsy	***OSForensics***	***Autopsy***	***OSForensics***
.pdf	*5*	*0*	*0*	*5*	*5*
.jpg	*5*	*0*	*0*	*5*	*5*
.png	*5*	*0*	*0*	*5*	*5*
.docx	*5*	*0*	*0*	*5*	*5*
.xlsx	*5*	*0*	*0*	*5*	*5*
Persentase		***0%***	***0%***	***100%***	***100%***

Tabel 2 menunjukkan hasil perhitungan menunjukkan bahwa persentase tingkat keberhasilan *tool Autopsy* dalam melakukan *recovery* pada *Solid State Drive* (SSD) NVMe M.2 dengan fungsi TRIM *enable* sebesar 0% sedangkan dengan fungsi TRIM *disable* 100%. Hasil yang sama juga didapatkan oleh *tool OSForensics* dimana *recovery* yang dilakukan pada *Solid State Drive* (SSD) NVMe M.2 dengan fungsi TRIM *enable* sebesar 0% sedangkan dengan fungsi TRIM *disable* 100%. Kedua *tools* menunjukkan tingkat keberhasilan yang sama dalam melakukan *recovery* data pada SSD NVMe M.2 fungsi TRIM *enable* dan TRIM *disable.* Durasi waktu proses percobaan akuisisi menggunakan *tool Autopsy* dan *tool OSForensics* ditampilkan pada tabel 3.

Tabel 3. Perbandingan Durasi Waktu Percobaan Akuisisi

Tools	*TRIM enable*	*TRIM disable*
Sleuthkit Autopsy (Analyzing)	*323 menit*	*334 menit*
OSForensics (Calculating)	*228 menit*	*231 menit*

Tabel 3 menunjukkan durasi waktu proses akuisisi dari masing-masing *tools*, jika dilihat dari tabel di atas menunjukkan bahwa *tool OSForensics* memiliki durasi waktu proses akuisisi yang lebih cepat, yaitu 228 menit dengan TRIM *enable* dan 231 menit pada TRIM *disable* sedangkan pada *tool Autopsy* 323 menit pada TRIM *enable* dan 334 menit pada TRIM *disable*.

4. KESIMPULAN

Berdasarkan hasil dari proses percobaan akuisisi dan *recovery* menunjukkan bahwa *tool OSForensics* memiliki waktu akuisisi 228 menit pada SSD TRIM *enable* dan 231 menit pada SSD TRIM *disable* sedangkan *tool Autopsy* memiliki waktu akuisisi 323 menit pada SSD TRIM *enable* dan 334 menit pada SSD TRIM *disable*. Persentase tingkat keberhasilan *recovery tool Autopsy* pada SSD TRIM *enable* sebesar 0% dan pada SSD TRIM *disable* sebesar 100%. Hasil yang sama juga didapatkan oleh *tool OSForensics* dimana persetase keberahsilan *recovery* yang dilakukan pada SSD TRIM *enable* sebesar 0% sedangkan pada SSD TRIM *disable* sebesar 100%. Dari hasil tersebut dapat disimpulkan bahwa *tool OSForensics* memiliki waktu proses akuisisi yang lebih cepat. Kemampuan *recovery* yang ditunjukkan oleh kedua *tool* serupa pada SSD TRIM *disable* maupun TRIM *enable.*

DAFTAR PUSTAKA

1] F. Ridho, A. Yudhana, and I. Riadi, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," vol. 2, no. 1, pp. 111–116, 2016.

[2] R. A. K. N. Bintang, R. Umar, and U. Yudhana, "Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128, 2018.

[3] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," *Int. J. Sci. Eng. Res.*, vol. 4, no. 10, pp. 1048–1056, 2013, [Online]. Available: http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-

Tools.pdf.
[4] 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.
[5] B. J. Nikkel, "NVM Express Drives and Digital Forensics Introduction to NVM Express," *(Mbuh)*, pp. 1–16, 2016.
[6] N. Walker, *Conference Title 2016 Universal Technology Management Conference (UTMC) Conference Dates Conference Venue Published by The Society of Digital Information and Wireless Communications (SDIWC) Wilmington , New Castle , DE 19801 , USA*, no. May 2016. 2018.
[7] F. Geier, "The differences between SSD and HDD technology regarding forensic investigations," p. 67, 2015.
[8] B. S. Nasional, *SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Jakarta, 2014.
[9] I. M. N. Imam Riadi , Rusydi Umar, "Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Standards and Technology (NIST)," *J. Insa. Comtech*, vol. 2, no. 2, pp. 33–40, 2017.
[10] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.
[11] I. Riadi, Sunardi, 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.
[12] W. Pranoto, I. Riadi, and Y. Prayudi, "Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics," *It J. Res. Dev.*, vol. 4, no. 2, pp. 135–148, 2020, doi: 10.25299/itjrd.2020.vol4(2).4615.
[13] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/ijacsa.2017.081210.