HASIL CEK_60020397_Point-C59-IRD-850GB-Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:50AM (UTC+0700)
Submission ID: 1471701321
File name: stem_Operasi_Proprietary_Menggunakan_Metode_Static_Forensics.pdf (1.13M)
Word count: 3326
Character count: 20675

Jurnal CoreIT, Vol.V, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics

Imam Riadi[1], Sunardi[2], Abdul Hadi[3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo, S.H, Warungboto, Yogyakarta 55164
imam.riadi@is.uad.ac.id[1], sunardi@mti.uad.ac.id[2], abdul1808048032@webmail.uad.ac.id[3]

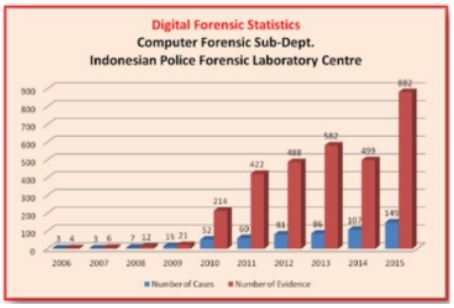
Abstrak **– Bukti digital sangat penting untuk pembuktian kasus kejahatan komputer yang melibatkan perangkat media penyimpanan. Secara *default* sistem operasi Windows 10 terapasang fitur TRIM dengan mode *enable*, fungsi TRIM otomatis menghapus data lama pada sebuah sektor sebelum ditempatkan data baru. Tujuan penelitian melakukan perbandingan kemampuan *tools forensics* untuk mengembalikan bukti digital pada SSD NVMe TRIM *enable* dan *disable*. Metode yang digunakan *static forensics* dengan *framework National Institute of Justice* (NIJ). *Tools* yang digunakan FTK Imager, Autopsy dan Recover My File. Prosentase restorasi bukti digital TRIM *enable* menggunakan Autopsy dan Recover My File 0%, sedangkan TRIM disable Autopsy 92% dan Recover My File 99%, sehinga dapat disimpulkan penghapusan bukti digital secara permanen pada SSD NVMe menggunakan fitur TRIM *enable* berdampak negatif pada analisis forensik khususnya *recovery* bukti digital.**

Kata Kunci – Digital Forensics, SSD NVMe, NIJ, Computer Forensics,TRIM

PENDAHULUAN

Kejahatan komputer merupakan kejahatan yang melibatkan teknologi, seiring perkembangan teknologi modus-modus kejahatan komputer selalu berubah sesuai perkembangan yang ada [1]. Jika diamati beberapa kasus kejahatan komputer model dan modus mengalami perubahan yan berbeda, adanya kasus kejahatan komputer terbitlah Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektornik (ITE) salah satu tujuannya adalah memberikan rasa aman, keadilan dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi. Disamping itu penanganan tindak kejahatan komputer saat ini masih minim, dari pengambilan barang bukti yang tidak cukup, kesalahan akuisisi pengambilan barang bukti, atau bahkan sampai hilang atau rusaknya barang bukti.

Model-model kejahatan terkait dengan komputer dikuatkan dengan berita dan fakta di media massa, diantaranya penyitaan barang bukti perangkat komputer dan media penyimpanan komputer sebagaimana diberitakan oleh oleh detik.com Selasa, 20 Februari 2018 dengan judul "Geledah Ruang Kerja Bupati Imas, KPK Sita Dokumen dan Komputer" berita yang dikabarkan media massa tersebut kasus suap terhadap Bupati Subang secara bersama-sama terkait pengurusan perizinan, penyidik menggeledah tiga lokasi dan menyita sejumlah dokumen dan barang bukti elektronik. Kejahatan komputer di Indonesia terjadi kenaikan kasus setiap tahunnya. Dalam 10 tahun terakhir terdapat 563 kasus kejahatan dengan total jumlah barang bukti elektronik sebanyak 3.130 unit. Statistik tersebut menunjukkan bahwa kejahatan komputer adalah permasalahan serius dalam era digital seperti Gambar 1 (Sumber: Bareskrim puslabfor polri, 2015).



Gambar 1 Statistik digital forensics 2006-2015

Kasus-kasus yang diberitakan media massa terkait tindak kejahatan elektronik dan barang bukti elektronik berupa perangkat komputer yang melibatkan media penyimpanan, menjadi pekerjaan yang harus diselesaikan dan dituntaskan oleh penyidik dan penegak hukum guna mengungkap modus, motif dan pelaku tindak kejahatan atau dengan kata lain membuktikan kejahatan terkait dengan barang bukti yang didapatkan.

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). Teknologi media penyimpanan yang baru saat ini adalah *Solid State Drive Non-volatile Memory Express* (SSD NVMe) yang berbeda dengan SSD SATA pendahulunya dari segi kecepatan dan bentuk interfacenya

Jurnal CoreIT, Vol.V, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

[2]. Sistem operasi Windows 10 saat ini sudah terpasang secara default fasilitas TRIM dengan mode *enable* [3], fasilitias ini secara otomatis akan menghapus data lama pada sektor sebelum ditempatkan data baru [4], sehingga SSD NVMe akan membaca data secara optimal. Akan tetapi dengan adanya fungsi TRIM ini pada SSD NVMe memiliki efek negatif pada analisis forensik khususnya pada recovery data. Contoh bentuk fisik dan *interface* SSD NVMe M.2 key M seperti pada Gambar 2.

Gambar 2. Bentuk fisik dan *interface* SSD NVMe M.2 Key M.

Penelitian dengan tema sejenis pernah dilakukan Rizdqi Akbar Ramadhan judul penelitian "Implementasi dan Analisis Forensika Digital pada Fitur Trim Solid State Drive". Penelitian ini membandingkan tools forensik yang digunakan untuk analisis dan eksaminasi SSD dengan mode TRIM . Hasil penelitian menghasilkan mekanisme TRIM pada SSD saat diaktifkan menimbulkan kendala dalam penyelidikan *digital forensics*. Mekanisme TRIM memiliki pengaruh ketika diaktifkan 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 [5]. Faiz Albanna menganalisis bukti digital pada frozen *hard drive* menggunakan metode static forensic. Pada penelitian melakukan analisis digital forensics pada HDD yang terinstal aplikasi frozen seperti Deep Freeze, analisis bukti digital dilakukan setelah kondisi komputer dimatikan atau HDD dalam keadaan ter-deep freeze. Hasil dari investigasi pada beberapa file dokumen digital, gambar, *log history* internet dan *log file* terbaru dapat dikembalikan kembali, namun ditemukan tidak pada direktori aslinya atau dengan kata lain terletak pada *unlocated space drive* [6]. Binaya Raj Joshi judul penelitian "Forensic Analysis of Solid State Drive (SSD)" peneliti melakukan perbandingan fitur TRIM pada SSD 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, hasil penelitian menunjukkan hasil yang berbeda saat fitur TRIM diaktifkan dan dinon-aktifkan [7]. Imam Riadi dengan judul peneliitian "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ)" SSD SATA yang terfrozen dijadikan barang bukti digital dengan metode *static forensics*, penelitian menggunakan perangkat lunak forensik Recovery My File, Belkasoft, Forensic Toolkit (FTK) dan Encase. Untuk tool akuisisi menggunakan tableau forensic bridge dengan perangkat lunak akuisisi tableau *imager*. Metode yang digunakan adalah *static forensics* dengan menggunakan *framework* NIST, format file sistem tiap SSD adalah NTFS. Hasil eksaminasi dari SSD yang terfrozen berhasil menemukan artefak dengan *tools* forensik Recovery My File 0,9991 (100%), Autospy 100%, Belkasoft 100%, Forensic Toolkit 92%, Encase 100%. Penelitian ini juga membuat perbandingan antara SSD yang terfrozen dan yang tidak terfrozen dalam pengambilan artefak [8].

METODE PENELITIAN

Penelitian ini menggunakan metode *static forensic* dengan menggunakan *framework National Institute of Justice* (NIJ), Metode *static forensics* yaitu prosedur yang harus dipatuhi saat penanganan pertama kali mendapatkan barang bukti elektronik berupa komputer dalam keadaan mati [9]. Barang bukti digital diambil dari salinan *image* yang diambil dari salinan media penyimpanan fisik [10]. *Framework* NIJ mengarahkan langkah-langkah dan alur penelitan secara sistematis sehingga dapat menyelesaikan masalah penelitian. Menggunakan metode dan *framework* yang tepat memiliki keberhasilan hampir 100% untuk mengumpulkan barang bukti *digital forensics* [11].

Framework NIJ terbagi menjadi 5 langkah kerja [12] yaitu *identification, collection, examination, analysis* dan *reporting* seperti Gambar 3.

Gambar 3. Metode *National Institute of Justice (NIJ)*

Identification adalah proses memilah barang bukti fisik oleh investigator dari tindak kejahatan komputer untuk dijadikan bukti otentik saat proses penyidikan. Proses *identification* berupa pelabelan dan perekaman untuk keutuhan barang bukti fisik.

Collection adalah Proses duplikasi dari barang bukti fisik yang otentik ke bukti digital untuk menjaga integritas barang bukti dari perubahan. Proses penjagaan barang bukti fisik dan membuat duplikasi menjadi *image* ini dinamakan akuisisi.

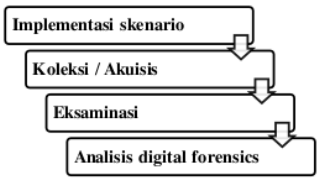
Examination atau disebut tahap pemeriksaan, hasil *image* diekstrak sehingga data digital yang ada didalamnya sama dengan barang bukti fisik. tahapan ini memastikan data yang didapat asli dan akan dicek validasinya dengan menggunakan *hashing*.

Analysis adalah proses pengecekan barang bukti digital yang telah didapat dari proses eksaminasi, barang bukti digital diproses secara detail sesuai pelaporan tindak kejahatan untuk mengungkap kasus tindak kejahatan dengan metode yang benar secara ilmiah dan dapat dipertanggungjawabkan secara sah menurut hukum.

Reporting atau proses pembuatan laporan, hasil laporan analisis menggambarkan tindakan yang dilakukan oleh pelaku kriminal, penjelasan *tools* yang dipakai dan metode yang digunakan [13].

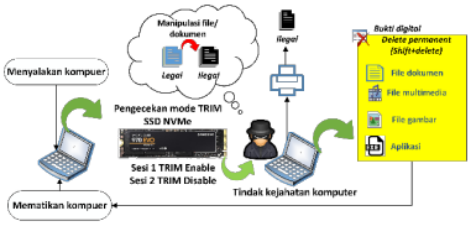
Tahapan *framework* NIJ dirangkum menjadi 4 tahapan utama seperti gambar 4.

Jurnal CoreIT, Vol.V, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)



Gambar 4. Tahapan utama penilitian

Bukti digital yang digunakan pada penelitian ini tidak didapat dari kejadian nyata, melainkan diperoleh dari hasil skenario kasus tindak kejahatan komputer melibatkan media penyimpanan SSD NVMe sesuai dengan Gambar 5.

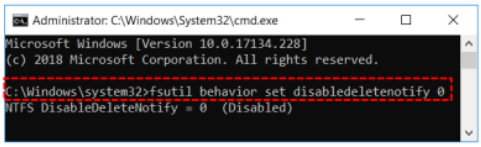


Gambar 5. Skenario kasus tindak kejahatan

Skenario ini dibagi menjadi 2 sesi, sesi yang pertama menggunakan sistem operasi Windows 10 Pro dengan file sistem NTFS dengan fitur TRIM *enable* dan sesi kedua dengan TRIM *disable*. Tahapan implementasi skenario penelitian sesuai Gambar 6.

Gambar 6. *Flowchart* implementasi skenario

Flowchart pada Gambar 6 menjelaskan persiapan awal yaitu dengan memasang SSD NVMe yang benar-benar diformat kosong dan instalasi sistem operasi Windows 10 Pro dengan file system NTFS. Sesi 1 fitur TRIM di *enable* melalui *Command Line* (CMD) pada sistem operasi Windows dengan *mode administrator*, perintah TRIM enable dapat dilihat pada Gambar 7.

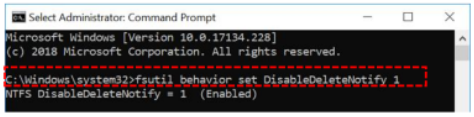


Gambar 7. Perintah TRIM *enable* di CMD

Pembuktian hasil TRIM *enable* dapat dilihat pada aplikasi Samsung Magician berbasis *General User Interface* (GUI) seperti Gambar 8.

Gambar 8. Tampilan GUI TRIM *enable*

Tahapan pada sesi 2 melakukan fitur TRIM *disable* pada sistem operasi Windows dengan perintah CMD pada Windows seperti Gambar 9.



Gambar 9. Perintah TRIM *disable* di CMD

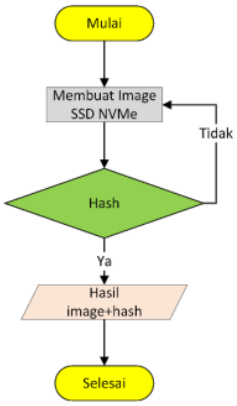
Pembuktian hasil TRIM *disable* dapat dibuktikan pada aplikasi Samsung Magician berbasis GUI seperti Gambar 10.

Gambar 10. Tampilan GUI TRIM *disable*

Selanjutnya pada sesi 1 dan 2 melakukan aktivitas kejahatan komputer sesuai Gambar 4 sekaligus menghapus barang bukti tindak kejahatan secara permanen (*shift+delete*) setelah itu mematikan komputer sesuai prosedur.

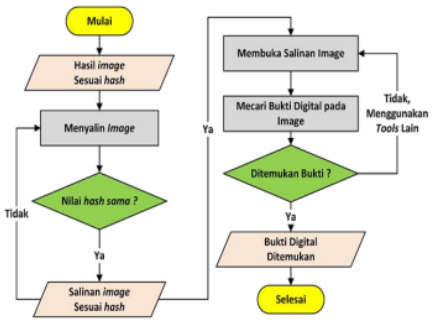
Jurnal CoreIT, Vol.V, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Akuisisi bukti digital mengacu pada metode *static forensics* yaitu menggunakan prosedur dan pendekatan konvensional dimana barang bukti dijadikan *image* secara *bit-by-bit image*, sesuai alur proses akuisisi pada Gambar 11.



Gambar 11. Proses akuisisi

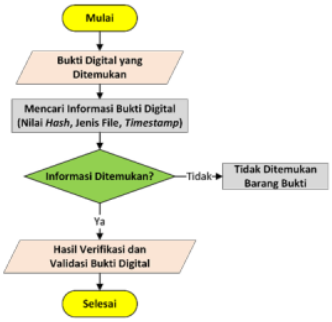
Proses eksaminasi dilakukan dari hasil salinan *image* dengan mengecek nilai *hash* yang sama, kemudian dilakukan eksaminasi menggunakan perangkat lunak yang telah disiapkan untuk menemukan bukti digital. Hasil yang diharapkan adalah menemukan bukti digital berupa file dokumen, file gambar, file multimedia file aplikasi. Alur proses eksaminasi seperti pada Gambar 12.



Gambar 12. *Flowchart* eksaminasi

Proses selanjutnya adalah analisis berdasarkan bukti digital yang ditemukan berupa jenis file, kapan file tersebut dibuat atau dimodifikasi mencari nilai *hash* pada bukti digital tersebut kemudian dilakukan verifikasi dan validasi bukti digital. Sehingga pada proses ini perlu kehati-hatian, jika salah memberikan informasi terkait barang bukti maka kesimpulan peradilan juga salah [14].

Validasi bukti digital terletak pada nilai *hash* yang memiliki kesamaan dengan file aslinya, proses ini mengatahui validitas dan integritas bukti digital dengan membandingkan nilai *hash* yang sama pada artefak digital yang ditemukan, sehingga bukti digital yang didapatkan valid dan akurat sesuai alur analisis pada Gambar 13.



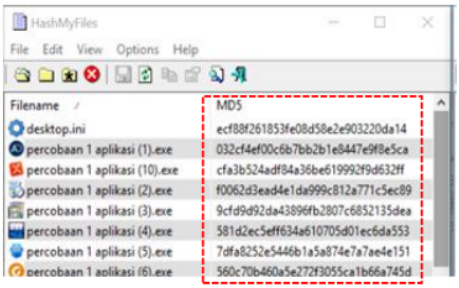
Gambar 13. Flowchart analisis

Seluruh tahapan *forensics* yang diproses menghasilkan bukti digital berupa file-file terkait tindak kejahatan komputer kemudian dibuat laporan hasil sehingga laporan analisis dapat mendukung informasi berupa siapa, kapan dan dimana kejahatan komputer tersebut dilakukan. Kemudian dilanjutkan proses hukum sesuai dengan prosedur yang ada [15].

Alat yang dibutuhkan pada penelitian ini adalah Desktop Mini A300 *support* SSD NVMe, 1 pcs SSD NVMe ADATA XPG M.2 NVMe SX6000 lite, Notebook Thinkpad yoga 14, *Converter NVMe to USB*, Windows 10 Pro, FTK Imager, Autopsy versi 4.13, Recoer My File vesi 5 dan 10 file bukti digital masing-masing mempunyai format .exe, .pdf, docx, xlsx, .ppt, .jpg, .bmp, .png, .mp3, .mp4.

HASIL DAN PEMBAHASAN

Proses implementasi yang dilakukan pada penelitian ini sesuai dengan Gambar 5, SSD NVMe dijadikan barang bukti kejahatan dalam bentuk fisik. Investigator mengakuisisi barang bukti fisik ke barang bukti digital dengan cara *bit-by-bit image* dengan mencocokkan nilai *hash* pada salinan *image* dengan *image* yang asli. Salinan *image* dijadikan bahan eksperimen untuk proses ekstraksi barang bukti digital. File-file bukti digital mempunyai nilai *hash* yang berbeda, untuk klarifikasi bukti digital yang sah peneliti mencocokan sampel nilai *hash* bukti digital asli dengan temuan bukti digital dari proses restorasi seperti Gambar 14.

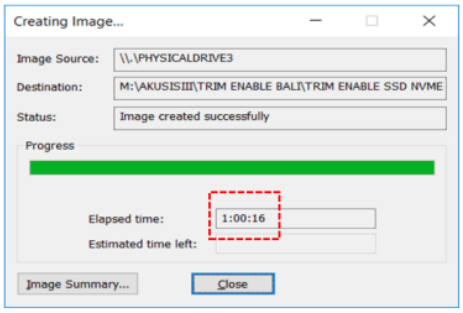


Gambar 14. Sampel nilai *hash* bukti digital asli

Jurnal CoreIT, Vol.V, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

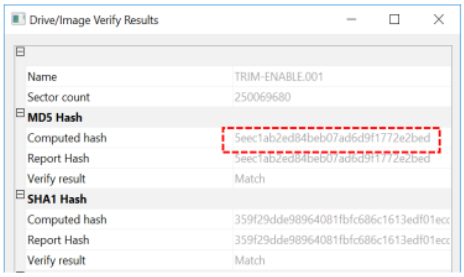
Skenario selanjutnya menghapus bukti digital secara permanen (*shift+delete*) dan mematikan komputer sesuai prosedur.

Berdasarkan metode *statics forensics*, barang bukti fisik SSD NVMe disalin dalam bentuk *image* dengan proses *bit by bit* image menggunakan *tool* FTK Imager sesuai Gambar 15.

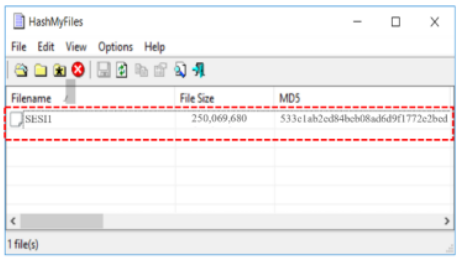


Gambar 15. Proses pembuatan *image* (akuisisi)

Gambar 15 menunjukkan proses *imaging physical drive* SSD NVMe kapasitas 128 Gb membutuhkan waktu 1 jam 16 detik. Hasil *image* yang dibuat disalin kembali untuk proses eksaminasi, untuk memastikan integritas bukti digital maka dilakukan *hashing* untuk membandingkan nilai *hash* antara file *image* asli dan salinan *image*, seperti pada Gambar 16 dan Gambar 17 validasi nilai *hash*.



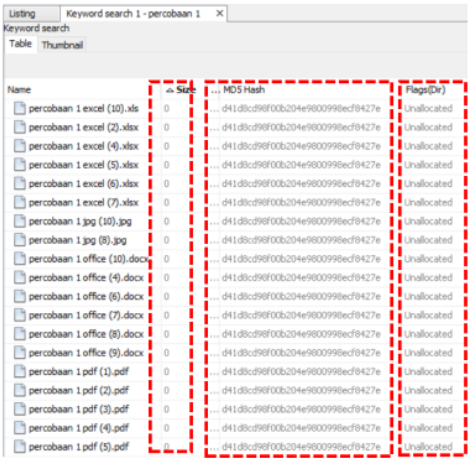
Gambar 16. Nilai hash pada *image*



Gambar 17. Validasi nilai *hash* pada salinan *image*

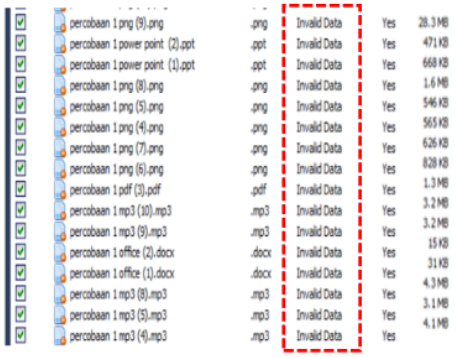
Tahapan selanjutnya melakukan eksaminasi dan analisis bukti digital pada salinan *image* menggunakan *tool* Autopsy dan Recover my file.

Eksperimen sesi pertama eksaminasi SSD NVMe TRIM *enable* menggunakan tool Autopsy, barang bukti yang ditemukan 87 dari 100 file berada pada lokasi terkahir diakses dan tidak ada perubahan nama *file* dan extensi, catatan terakhir pengguna (*recent activity*) dapat ditampilkan, kondisi kapasistas *file* bertatus *zero size*, adanya perubahan nilai *hash* pada file, *flag directory* dan metadata berstatus *unallocated* seperti Gambar 18.



Gambar 18. Hasil Eksaminasi Autopsy TRIM enable

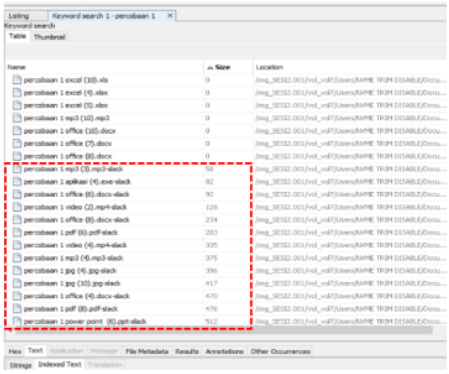
Selanjutnya menggunakan *tool* Recover My File, barang bukti yang ditemukan sebanyak 100 dari 100 file. Kondisi nama *file* dan ekstensi tidak berubah, tetapi keseluruhan struktur data pada *file* rusak dengan status "*invalid data*" dan nilai *hash* tidak sama dengan nilai *hash* bukti digital asli seperti Gambar 19.



Gambar 19. Hasil Eksaminasi Recover My File TRIM *enable*

Jurnal CoreIT, Vol.V, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

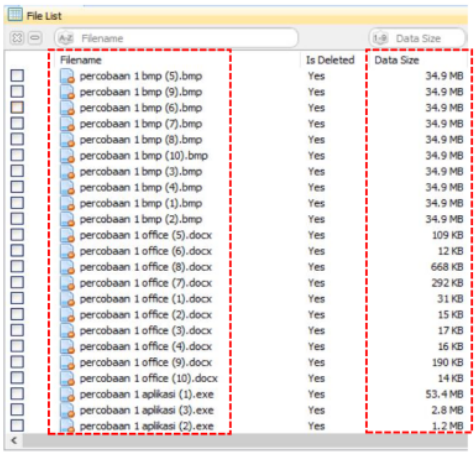
Eksperimen sesi kedua eksaminasi SSD NVMe TRIM *disable* menggunakan *tool* Autopsy, barang bukti yang ditemukan sebanyak 92 dari 100 file. Kondisi nama file dan ekstensi tidak berubah, struktur data ketika direstorasi terbaca dengan baik, nilai *hash* sama dengan bukti digital yang asli, status *flags directory* dan metadata *unallocated* seperti Gambar 20.



Gambar 20. Hasil Eksaminasi Autopsy TRIM *disable*

Hasil eksaminasi pada Gambar 20 ditemukan barang bukti 7 dari 100 file yang mempunyai struktur data yang rusak dengan nilai *size* 0, mempunyai nilai *hash* yang berbeda dengan nilai *hash* bukti digital asli.

Selanjutnya menggunakan *tool* Recover My bukti digital yang ditemukan 99 dari 100 *file*. Kondisi nama, *size* dan ekstensi *file* tidak berubah, setelah direstorasi nilai *hash* sama dengan nilai *hash* bukti digital asli, hasil eksmanisi *tool* Recover My File seperti pada Gambar 21.



Gambar 21. Hasil Eksaminasi Recover My File TRIM *disable*

Hasil eksaminasi menggunakan kedua *tools* pada sesi 1 dan sesi 2 mempunyai hasil yang berbeda, proses eksaminasi pada SSD NVME fitur TRIM *enable* bisa direstorasi tetapi tidak bisa dijadikan barang bukti yang sah menurut hukum karena nilai *hash* tidak sama dengan barang bukti asli. Sedangkan pada fitur TRIM *disable* hampir keseluruhan file dapat direstorasi dengan nilai *hash* yang sama. Berikut rangkuman hasil restorasi file SSD NVMe berdasar nilai *hash* yang sama pada Tabel 1.

Tabel 1. Hasil rangkuman restorasi bukti digital SSD NVMe berdasar nilai *hash* yang sama

Kategori File	**Jumlah File**	**Hasil Restorasi Tools Forensics**			
		Autopsy		Recover My File	
		TRIM Enable	TRIM Disable	TRIM Enable	TRIM Disable
File Office					
.docx	10	0	7	0	10
.xlsx	10	0	7	0	10
.pptx	10	0	10	0	10
.pdf	10	0	10	0	10
File Gambar					
.jpg	10	0	10	0	10
.png	10	0	10	0	10
.bmp	10	0	10	0	10
File Multimedia					
.mp3	10	0	9	0	10
.mp4	10	0	10	0	10
File Aplikasi					
.exe	10	0	9	0	9

Hasil prosentase restorasi bukti digital pada Tabel 1 fitur TRIM *enable* nilai *hash* yang sama dengan bukti digital yang asli sebanyak 0%. Sedangkan prosentase keberhasilan restorasi bukti digital TRIM *disable* menggunakan *tool* Autopsy sebanyak 92% dan Recovery My File 99%.

Kedua sesi dianalisis dengan membandingkan nilai *hash*. Sesi pertama semua bukti digital yang ditemukan tidak sama nilai *hash* dengan bukti digital yang asli. Sedangkan analisis sesi kedua beberapa bukti digital mempunyai nilai *hash* yang berbeda seperti Tabel 2.

Jurnal CoreIT, Vol.V, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Tabel 2. Sampel beberapa hasil bukti digital yang ditemukan berdasarkan nilai *hash* yang berbeda

Nama File	Nilai Hash MD5 Asli	Nilai Hash MD5 TRIM enable	Nilai Hash MD5 Trim disable
File Office			
Percobaan excel (10).xls	5dafdaea21ccae084a441540bd3f2647	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e
Percobaan excel (4).xlsx	a090ae66c8227ceadc522254ed4d6387	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e
Percobaan excel (5).xlsx	10108084d8d48ec61449af4a6aa3f816	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e
Percobaan office (10).docx	d4008f5625deb252f951e08415184c7a	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e
Percobaan office (7).docx	aa125f3e35214c72e3a87a11e3d4903f	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e
Percobaan office (8).docx	4fe577c986bcdb7144c0474d75e44ed9	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e
File Aplikasi			
Percobaan Aplikasi (10).exe	cfa3b524adf84a36be619992f9d632ff	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e
File Audio			
Percobaan mp3 (10).mp3	37b01c0d896741ea8fb0abc9b68cc49f	d41d8c98f00b204e9800998ecf8427e	d418cd98f00b204e9800998ecf8427e

Meskipun nama file identik dengan bukti digital asli tetapi tidak bisa dijadikan barang bukti digital yang sah dan valid menurut hukum karena bukti digital yang ditemukan berdasar Tabel 2 mempunyai nilai *hash* yang berbeda dengan bukti digital yang asli.

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan dengan menganalisis bukti digital pada fitur TRIM SSD NVMe pada sistem operasi *proprietary* menggunakan *static forensics*, maka didapatkan kesimpulan sebagai berikut :

1. Analisis bukti digital pada fitur TRIM SSD NVMe berhasil diterapkan dengan baik menggunakan metode *static forensics* dengan *framework National Institute of Justice* (NIJ).
2. Fitur TRIM *enable* terbukti berdampak negatif pada proses eksaminasi dan analisis yang dilakukan investigator untuk mengembalikan barang bukti digital. Nilai hash yang didapat dari barang bukti TRIM *enable* tidak identik dengan nilai hash bukti digital asli.
3. Prosentase bukti digital yang dapat dikembalikan saat fitur TRIM *disable* pada SSD NVMe menggunakan *tool* Autopsy 92% dan Recover My File 99%, sebagian data dapat dikembalikan seperti proses *recovery* pada media penyimpanan *hardisk* (HDD).

B. Saran

Berikut saran peneliti terkait analisis barang bukti digital pada fitur TRIM SSD NVMe :

1. Membandingkan metode penghapusan yang berbeda antara shift+delete dan delete, delete+recycle bin .
2. Penggunaan *tool* forensik yang berbeda diharapakan memberikan banyak informasi dari data hasil akuisisi, karena *tool* forensik memiliki kekurangan dan keunggulan masing-masing.

REFERENSI

[1] Al-Azhar, Muhammad Nuh (2012). Digital Forensic: Panduan Praktis Investigasi Komputer, Jakarta: Salemba Infotek

[2] Nikeel, Bruce (2016). Practical Forensic Imaging: Securing Digital Evidence with Linux Tools, Switzerland: Starch Press

[3] Singh, P., & Singh, A. "Computer Forensics : An Analysis on Windows and Unix from data recovery perspective", pp. 586–591, 2016.

[4] Michael, L. (2018). Solid State Forensics : Investigating the Effects of Garbage Collection on Potentially Volatile Data During the Process of Forensic Extraction of SSDs Table of Contents. (M. Daley, Ed.). United Kingdom: Cardiff University, Computer Science.

[5] Ramadhan, R. A., Prayudi, Y., & Sugiantoro, B. "Implementasi dan Analisis Forensika Digital pada Fitur Trim Solid State Drive (SSD)". Teknomatika, Vol. 9 No.2, pp 1–13, 2017.

[6] Albanna, F., & Riadi, I, "Forensic Analysis Of Frozen Hard Drive Using Static Forensic Method". International Journal Of Computer Science and Information Security (IJCSIS), Vol. 15 No. 1, pp. 173-178, 2017.

[7] Raj, B., & Hubbard, R."Forensic Analysis of Solid State Drive (SSD)". Proceedings of 2016 Universal Technology Management Conference (UMTC), Minnesota, United States of America, pp. 1-11, 2016.

[8] Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ).

[9] Riadi, I., Umar, R., & Nasrulloh, I. M., "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ)". ELINVO, Vol 3, No. 1, pp 70–82, 2018.

[10] Riadi, I., Umar, R., & Nasrulloh, I. M. "Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods". Jurnal Ilmiah Teknologi Informasi Lontar Komputer, Univesitas Udayana. Vol 9 No. 3, pp. 169-181, 2018.

[11] Sunardi, S., Riadi, I., & Nasrulloh, I. M., (2019). "Analisis Forensik Solid State Drive (SSD) Menggunakan Framework Rapid Response". Jurnal Teknologi Informasi Dan Ilmu Komputer, Vol 6, No. 5 pp. 509-518, 2019.

[12] Riadi, I., Sunardi, S., & Sahiruddin. "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)". Vol 3 No. 1, pp. 87–95, 2019.

[13] Riadi, I., Sunardi, S., & Rauli, E, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics". Jurnal Teknik Elektro, Vol 10, No. 1, pp. 18–22, 2018.

[14] Sulianta, Feri. (2016). Komputer Forensik Melacak Kejahatan Digital. Yogyakarta: Andi.

[15] Hadi, A., Riadi, Imam, & Sunardi, ., "Forensik Bukti Digital Pada Solid State Drive (SSD) NVMe Menggunakan Metode National Institute of Standards and Technology (NIST)", SEMNASTEK, pp. 551–58, 2019.

HASIL CEK_60020397_Point-C59-IRD-850GB-Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics

ORIGINALITY REPORT

7%	7%	4%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ejournal.uin-suska.ac.id Internet Source	3%
2	ojs.stmik-banjarbaru.ac.id Internet Source	1%
3	jtsiskom.undip.ac.id Internet Source	1%
4	jurnal.iaii.or.id Internet Source	1%
5	core.ac.uk Internet Source	1%
6	ejurnal.tunasbangsa.ac.id Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		