TEKNOLOGI NUSANTARA
Jurnal Penelitian Fakultas Teknik UNINUS
http://ojs.uninus.ac.id/index.php/teknologinusantara

E-ISSN : 2964-4577

ANALISIS *LIVE FORENSICS* PADA SSD SATA FUNGSI TRIM MENGGUNAKAN METODE *NATIONAL INSTITUTE OF JUSTICE (NIJ)*

Faiz Muqorrir Kaffah[1]
Fakultas Teknik, Universitas Islam Nusantara,
faiz@uninus.ac.id
Siti Nur[2]
Fakultas Teknik, Universitas Islam Nusantara,
Sitinur.uninus@gmail.com
Adi Fitrianto[3]
Fakultas Sains, Universitas Islam Negeri SGD Bandung
adi.fitrianto@uinsgd.ac.id
Undang Syaripudin[4]
Fakultas Sains, Universitas Islam Negeri SGD Bandung
undang_if@uingd.ac.id
Darwan[5]
Fakultas FITK, IAIN Syekhnurjati Cirebon
Darwan@syekhnurjati.ac.id

ARTICLE INFO

ABSTRACT

The rapid development of technology is accompanied by an increase in computer crimes. Reporting from the Indonesian National Police, between April 2020 and July 2021, the agency received reports of 937 cases. Digital Forensics or Digital Forensics is a branch of science that investigates digital evidence and then collects, recovers, and analyzes that evidence. One of the techniques/analysis used to uncover computer crimes is Live Forensics. Performing data recovery in handling computer crime cases when the computer system is on is the application of the Live method. This research uses a method that is often used, namely the National Institute of Justice (NIJ) method. The National Institute of Justice (NIJ) is a method used to explain how the stages of research are carried out so that the research flow can be completed systematically and can be used as a guide in resolving existing problems. The purpose of this research is to find out the stages of inspection and analysis on SSDs that have the TRIM function. Apart from all the benefits and advantages contained in Solid State Drives (SSD), of course this SSD has limitations. The results of research and analysis using Autopsy and Testdisk software are all files were successfully recovered perfectly with 90% accuracy percentage.

ABSTRAK

Perkembangan teknologi yang kian pesat diiringi juga dengan kejahatan komputer yang meningkat. Dilansir dari Kepolisian Republik Indonesia, dalam rentang waktu April 2020 hingga Juli 2021 instansi tersebut mendapat laporan sebanyak 937 kasus. Digital Forensics atau Forensika Digital adalah cabang ilmu sains yang menginvestigasi barang bukti digital untuk kemudian mengumpulkan, memulihkan, dan menganalisa barang bukti tersebut . Teknik/analisis yang digunakan untuk mengungkap kejahatan komputer tersebut salah satunya adalah Live Forensics. Melakukan pemulihan data dalam penaganan kasus kejahatan komputer ketika sistem komputer dalam keadaan hidup adalah penerapan metode Live. Penelitian ini menggunakan metode yang sering digunakan yaitu metode National Institute of Justice (NIJ). National Institute of Justice (NIJ) merupakan metode yang digunakan untuk menjelaskan bagaimana tahapan penelitian yang dilakukan sehingga alur penelitian bisa selesai secara sistematis dan dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Tujuan dari penelitian ini adalah mengetahui tahapan pemeriksaan dan analisis pada SSD yang memiliki fungsi TRIM.Terlepas dari segala manfaat maupun keuntungan yang terdapat pada Solid State Drive (SSD) tentu saja SSD ini memiliki keterbatasan.Hasil penelitian dan analisis menggunakan perangkat lunak Autopsy dan Testdisk yaitu seluruh file berhasil dipulihkan secara sempurna dengan persentasi keakuratan 90 %.

Keyword:

Forensic,Solid State Drive,Kemanan Informasi

© 2022 TN. All rights reserved.

PENDAHULUAN

Teknologi semakin berkembang setiap harinya teurtama dalam kurun waktu satu dasawarsa terakhir tak terkecuali pada media penyimpanan. *Hard Disk Drive* (HDD) sebagai media penyimpanan yang sudah lama digunakan di berbagai perangkat elektronik (khususnya komputer dan laptop) perlahan-lahan mulai tergantikan oleh media penyimpanan non-mekanik yang disebut *Solid State Drive* (SSD) [1]. Dilansir dari Statista.com, sejak tahun 2016-2021, pengiriman *Hard Disk Drive* (HDD) ke seluruh dunia mengalami penurunan sedangkan *Solid State Drive* (SSD) berlaku sebaliknya.

Solid State Drive (SSD) merupakan media penyimpanan baru dengan ketahanan lebih kuat dan cenderung tahan terhadap guncangan serta lebih hemat daya karena tidak seperti *Hard Disk Drive* (HDD) yang memiliki komponen bergerak [2]. Salah satu fungsi yang terdapat pada SSD adalah fungsi TRIM. TRIM adalah istilah yang digunakan untuk mengidentifikasi perintah ATA *(Advanced Technology Attachment)* tertentu yang memungkinkan sistem operasi untuk memberi tahu *controller Solid State Drive* (SSD) bahwa data tersebut tidak dibutuhkan lagi. Arti kata TRIM berasal dari kenyataan bahwa area media penyimpanan dikurangi atau dipangkas (dibuat lebih kecil). Fungsi TRIM menjadi perlu untuk memungkinkan sistem operasi memberi tahu kepada SSD bahwa suatu area sudah tidak dibutuhkan lagi [3].

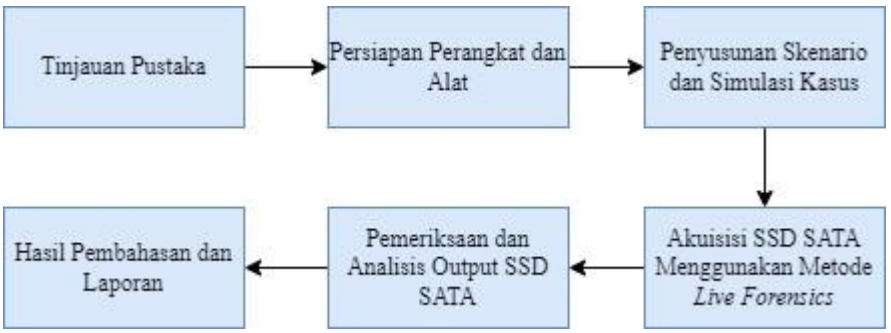
Digital Forensics atau Forensika Digital adalah cabang ilmu sains yang menginvestigasi barang bukti digital untuk kemudian mengumpulkan, memulihkan, dan menganalisa barang bukti tersebut. Barang bukti digital pada kejahatan komputer tersebut dapat diambil/dicari pada perangkat komunikasi seperti gawai, laptop, maupun komputer [4]. Teknik/analisis yang digunakan untuk mengungkap kejahatan komputer tersebut salah satunya adalah *Live Forensics.* Melakukan pemulihan data dalam penaganan kasus kejahatan komputer ketika sistem komputer dalam keadaan hidup adalah penerapan metode *Live Forensics* [5].

Penelitian ini menggunakan metode yang sering digunakan yaitu metode *National Institute of Justice* (NIJ). *National Institute of Justice (NIJ)* merupakan metode yang digunakan untuk menjelaskan bagaimana tahapan penelitian yang dilakukan sehingga alur penelitian bisa selesai secara sistematis dan dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada [6]. Tahapan metode dari *National Institute of Justice* (NIJ) terbagi menjadi lima tahapan yakni *identification, collection, examination, analysis,* dan *reporting* [7].

METODE PENELITIAN

Pada penelitian ini berfokus pada penerapan metode kualitatif.Proses yang di lakukan berupa eksperimen dan uji peneltian berdasarkan standarisasi perangkat dalam hasil bukti digital.

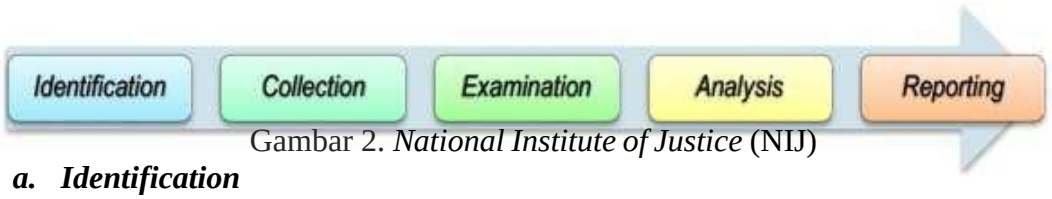
Metode penelitian ini juga menggunakan tinjauan pustaka dan studi literatur. Kedua cara ini ditempuh untuk mencari referensi dari jurnal, makalah, buku, paper, artikel, laporan penelitian, dan penemuan sebelumnya serta mengunjungi situs-situs di internet seputar forensika digital, barang bukti, *live forensic*, dan SSD demi tercapainya tujuan penelitian ini.



Gambar 1. Metodologi Penelitian

Bukti digital yang digunakan tidak didapatkan pada lingkungan yang sebenarnya atau dengan kata lain barang bukti tidak didapatkan dari hasil tindak kejahatan komputer yang sebenarnya[8]. Bukti digital dibuat dan diperoleh dari hasil desain skenario dengan tujuan untuk mendapatkan bukti digital seperti pada kasus kejahatan komputer yang sebenarnya.

Penelitian ini menggunakan metode dari *National Institute of Justice* (NIJ) yang dijelaskan di bawah ini:



Gambar 2. *National Institute of Justice* (NIJ)

a. Identification

Tahap *Identification* adalah tahap pemilahan barang bukti dan data-data yang berkaitan dalam proses penyidikan dengan tujuan mencari barang bukti digital. Barang bukti yang ditemukan lalu diidentifikasi, diberi label atau didokumentasikan agar barang bukti tidak rusak.[9]

b. Collection

Tahap ini berisi kegiatan untuk mengumpulkan data-data demi kepentingan proses penyelidikan dalam pencarian barang bukti. Dalam tahap ini dilakukan pengambilan data dari sumber yang berkaitan serta menjaga keaslian barang bukti dari kontaminasi.[10]

c. Examination

Pada tahap ini data dikumpulkan lalu diperiksa secara forensik untuk memastikan data tersebut terjaga keasliannya sesuai dengan temuan yang didapat di TKP. Agar hal tersebut bisa dilaksanakan dengan baik maka data diidentifikasi dan divalidasi menggunakan teknik *hashing.[11]*

d. Analysis

Teknik Analisis dilakukan setelah data atau file digital didapatkan dari proses eksaminasi. Analisis data dilakukan secara detail dan menyeluruh menggunakan panduan yang sudah ditentukan baik dalam hal teknis maupun hukum agar data tersebut dapat dibuktikan. Kemudian hasil analisis tersebut dapat digunakan sebagai barang bukti digital dan temuan tersebut dapat dibuktikan baik secara hukum maupun ilmiah.[12]

e. Reporting

Setelah barang bukti digital diperoleh dari proses pemeriksaan lalu kemudian dianalisis, maka dibuatlah laporannya. Isi dari laporan tersebut antara lain tindakan yang dilakukan, penggunaan serta penjelasan metode dan perangkat lunak yang digunakan, tindakan penunjang lain yang diambil, serta merekomendasikan aspek-aspek lainnya dalam proses tindakan *digital forensics*.[13]

PEMBAHASAN

Tahapan ini merupakan tahapan skenario kasus pada SSD SATA dengan melakukan penghapusan file. Keadaan perangkat komputer pertama pada skenario ini adalah dalam keadaan menyala (*standby*). Terdapat dua tahapan utama dalam penelitian ini yaitu sebagai berikut:

1. Mengaktifkan fungsi TRIM (TRIM *enable)* dan menonaktifan fungsi TRIM (TRIM *disable*). Pada prakteknya fungsi ini digunakan dalam penghapusan file secara permanen dengan beragam format/ekstensi menggunakan kombinasi tombol SHIFT+DELETE.

2. Mengakuisisi langsung SSD dengan fungsi TRIM yang sudah diterapkan. Hal ini bertujuan untuk menganalisis file-file apa saja yang dapat dipulihkan setelah dilakukan penghapusan pada SSD tersebut. Dalam akuisisi langsung, pemulihan, dan analisis ini digunakan perangkat lunak FTK Imager untuk membuat *image* dari SSD tersebut. Selanjutnya digunakan perangkat lunak Testdisk untuk melakukan pemulihan file secara langsung serta Autopsy dan Belkasoft Evidence Center X untuk melakukan pemeriksaan dan analisis pada *image file* yang sudah dibuat sebelumnya.

Dua tahapan tersebut dilakukan untuk mengetahui efektivitas akuisisi dan pemulihan dari perangkat lunak tersebut. Pada penelitian ini terdapat tiga perangkat yang digunakan yaitu laptop pertama (ASUS A43E) yang sudah dipasang SSD SATA, laptop kedua (ASUS FX553VD) yang digunakan untuk keperluan analisis dan pemeriksaan, serta perangkat ketiga yaitu SSD eksternal berukuran 2,5 inch sebagai media akuisisi langsung dan pemulihan dari laptop pertama[9].

Pada tahapan ini terdapat langkah-langkah yang harus dilakukan untuk mengatur fungsi TRIM menjadi *disable* pada SSD SATA yang berada di laptop pertama. Laptop pertama sendiri sudah terinstall sistem operasi Windows 11 Professional dengan arsitektur 64-bit yang sudah mendukung fungsi TRIM. Pengecekan fungsi TRIM ini dilakukan melalui *command prompt* yang dijalankan dengan otoritas *run as administrator*.

Setelah melakukan pengecekan tersebut dan diketahui bahwasanya fungsi TRIM sudah aktif (*enabled*), maka langkah selanjutnya yaitu adalah mengatur fungsi TRIM agar menjadi nonaktif (*disable*). Untuk melakukan hal tersebut maka ada perintah yang harus diketik pada *command prompt* yaitu **“fsutil behavior set disabledeletenotify NTFS 1”** untuk kemudian dieksekusi.

Setelah dipastikan bahwa fungsi TRIM dalam keadaan nonaktif, langkah selanjutnya yaitu mengunduh file yang sudah disiapkan sesuai skenario penelitian untuk kemudian disimpan pada partisi Local . File yang sudah disimpan pada partisi tersebut kemudian dihapus secara permanen .

Table 1 Pemulihan File TRIM

Status TRIM	*Disable*				
Software	Autopsy				
Jenis File	**Nama File**	***File Signature***	***MD5 Hash Value***	**Status Pemulihan**	
				Berhasil	**Gagal**
Dokumen	CSV 1.csv	22 43 61 70	e06ed8e9c9f1235af7e435431ded1b27	✓	
	DOC 1.doc	do cf 11 e0	4d827afc80998f284d1211782a0ea115	✓	
	PDF 1.pdf	25 50 44 46	6df360b4ff260d641cab4b0f0dd68d24	✓	
	PPT 1.ppt	do cf 11 eo	96ab0617153ae9349df2f150ba72c60a	✓	
	PPTX 1.pptx	50 4b 03 04	f861609c896dfd39667faaf7358ab7ed	✓	
	TXT 1.txt	55 73 65 72	d14d4dee25676462c2c08985816abcce	✓	
	XLSX 1.xlsx	50 4b 03 04	5071f7789b86f4234d70f933b854a2f4	✓	
Gambar	DDS 1.dds	44 44 53 20	850e5d424018619db0158f3ac5ec6c9a	✓	
	GIF 1.gif	47 49 46 38	850e5d424018619db0158f3ac5ec6c9a	✓	
	JPG 1.jpg	Ff d8 ff e0	dd5c1d7ff70b1b9c4731b32ed1aef059	✓	
	PNG 1.png	89 50 4e 47	dd9fc2f19c878cdffa40d55bb219a86e	✓	
	PSD 1.psd	38 42 50 53	869f7838b2ef0403db75c304d8dca0d8	✓	
	TGA 1.tga	00 00 02 00	fc75c9f2b1cf2b1d5473a46a7ff5b6b9	✓	

Status TRIM	*Disable*				
Software	Autopsy				
Jenis File	**Nama File**	***File Signature***	***MD5 Hash Value***	**Status Pemulihan**	
				Berhasil	**Gagal**
Video	MKV 1.mkv	1a 45 df a3	26a3107f2d164774860b2cf7d53b5e56	✓	
	MP4 1.mp4	00 00 00 20	a8b907061f77f587886c076bb9bb13c3	✓	
Audio	MP3 1.mp3	ff fb 90 6c	e1a514a4dadae9175e4201690f533b1f	✓	
	WAV 1.wav	52 49 46 46	3406668652a31819f53e246b4194bc53	✓	
Aplikasi	APK 1.apk	50 4b 03 04	6bf9aa32f9c5a0272fc09e9cfdf75f4f	✓	
	MASTER 1.exe	4d 5a 90 00	3ef1cc1779d2461cb70e9a1c32801588	✓	
	MASTER 3.exe	4d 5a 90 00	2e989b16100ee9f8193a86ff9c8a3998	✓	
	MASTER 5.msi	do cf 11 eo	2e7e27587d3b3cbea705cd5a0a5b2d2b	✓	
	MASTER 7.exe	4d 5a 90 00	b685f77ace37783d5a8c3568e96c68c8	✓	
7Z	7Z 1.7z	37 7a bc af	ba7ebb8a9a6caad81b3d6f44d7ba57a3	✓	
RAR	RAR 1.rar	52 61 72 21	c7870a4b8df98e9b1372f5ef93446687	✓	
ZIP	ZIP 1.zip	50 4b 03 04	0638ace7af99167f1dba9e0d64a7718f	✓	

Hasil pemeriksaan dan analisis yang terdapat pada tabel di atas menunjukkan bahwa keseluruhan file dapat dipulihkan menggunakan *software* Autopsy dengan skenario semua file dihapus secara permanen menggunakan kombinasi tombol dalam keadaan TRIM *disable*. File-file tersebut diasumsikan keasliannya sebagai barang bukti dengan nilai *hash* yang identik dan *file signature* yang sesuai dengan masing-masing ekstensi file. Dengan ini dapat disimpulkan bahwaa metode akuisisi langsung pada SSD SATA dengan fungsi TRIM *disable* dapat digunakan.

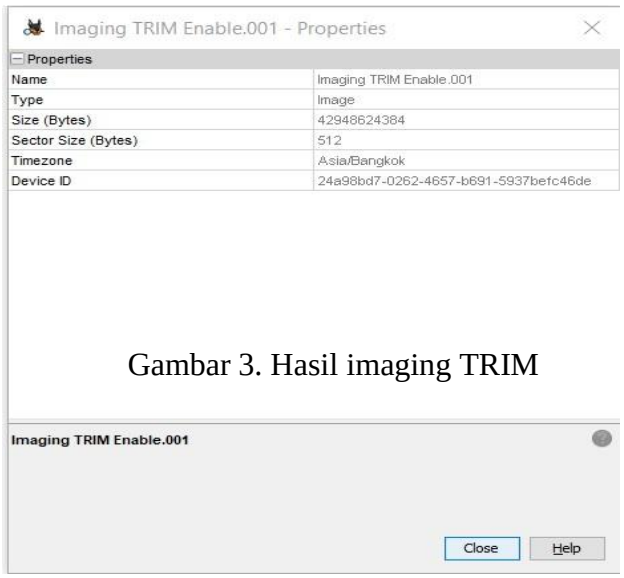
Pada tahapan selanjutnya berisi langkah-langkah yang dilakukan untuk mengaktifkan fungsi TRIM (*enable*) pada SSD SATA yang ada di komputer pertama. Tahapan ini tidak jauh berbeda dengan tahap menonaktifkan fungsi TRIM (*disable*). Setelah dipastikan bahwa fungsi TRIM dalam keadaan aktif kembali, langkah selanjutnya yaitu mengunduh file yang sudah disiapkan sesuai skenario penelitian untuk kemudian disimpan pada partisi *Local*. File yang sudah disimpan pada partisi tersebut kemudian dihapus secara permanen menggunakan perintah shortcut-key. Untuk memudahkan penelitian ini maka perlu dilakukan pengelompokan file berdasarkan penghapusan file pada masing-masing fungsi TRIM. Untuk TRIM *enable* diberi nomor genap. Tabel berikut menunjukkan daftar file nomor genap, nilai *hashing*, serta ekstensi/formatnya.

Table 2. Daftar file objek

Jenis File	**Nama File**	**MD5 *Hash***	**Ekstensi File**
Dokumen	DOC 2	feb475a3b4370a46827b219376667892	.doc
	PDF 2	ae3492816c772a3b9064eaa5448b64fd	.pdf
	PPT 2	6113717e4c0d922c5d5e21b144d326ec	.ppt
	PPTX 2	404cf486b0abe9b6e7eb6bb8e4ab8973	.pptx
	TXT 2	eb218faed4c9e906486ae03dc0d5c326	.txt
	XLSX 2	55c85f3579e1065dd6e7ff724f83b19c	.xlsx
Gambar	DDS 2	29441460157856c7c70a2bc31c5f9679	.dds
	GIF 2	4b090ef1cd04d08de2e8d3edf7da2134	.gif
	JPG 2	9971cff4d4e82a945f62a249812cbe22	.jpg
	PNG 2	25bd56d1801cca2f97bc9e68902bf976	.png

	TGA 2	c28d7320d5353665949dc0005d44cafd	.tga
Video	AVI 2	837962fe0a60b10478af5c3a77776b30	.avi
	MKV 2	79fa6bf237b805bd85379c5dcc63ec8f	.mkv
	MP4 2	83a270704b0300b52a753754d3c7c7ea	.mp4
Audio	MP3 2	760043d3459f0c21bed506528d04041b	.mp3
	WAV 2	5449a2a9883487265acb2b1d8bb75206	.wav
Aplikasi	APK 2	2a286861e593b988b1d22847804b5809	.apk
	MASTER 2	14a7e49abb000a937e90808211b8927f	.msi
	MASTER 4	c7e39fd9dfdb7cb58f34bde530a1310e	.exe
	MASTER 6	4e387e33458164690f22b4d51cf2abaf	.exe
	MASTER 8	f9b4b42870d9291ad55d03590fb411de	.exe
7Z	7Z 2	b9fe073b846f21f63a5a37e42610f494	.7z
RAR	RAR 2	27094bc8283b84c15b4a1e31c304d6a8	.rar
ZIP	ZIP 2	5d4151ef24fe97e9380ee6a2a1fe9cca	.zip
Lainnya	CDP 2	12dd1cab08d876e9da44c07fb06810be	.cdp
	IM 2	3ce0caf6a38b918cf6a7a24e3f7e78bb	.im
	SCS 2	bc9b33a0fe988749b4ed95b07ece980a	.scs
	SQL 2	4d0ff20b987b9ee5a87b1edfe64ce397	.sql
	SRT 2	4f178436d3c49549df6412e30c4a9879	.srt
	TTF 2	50145685042b4df07a1fd19957275b81	.ttf

Setelah melakukan *imaging* atau akuisisi menggunakan *software* FTK Imager Portable, langkah selanjutnya adalah melakukan analisa dan pemeriksaan *image* menggunakan *software* Autopsy.



Gambar 3. Hasil imaging TRIM

Tampilan di atas merupakan deskripsi dari hasil akuisisi SSD SATA PNY CS900 dengan kapasitas 42948624384 bytes (40 GB pada partisi Local Disk D) yang menggunakan file sistem NTFS.

SSD sebagai media penyimpanan terbaru yang umumnya digunakan pada perangkat komputer ternyata berdampak negatif terutama dalam analisis forensik yang dibutuhkan untuk mempelajari data dan memahami informasi yang ada pada SSD tersebut. Hal ini tentunya menjadi hambatan dan juga tantangan bagi para penyidik dalam melakukan analisis forensik [14].

Berdasarkan hasil di atas dapat disimpulkan bahwa *software* Belkasoft Evidence Center X saat ini belum mendukung untuk analisis forensika digital baik dengan keadaan TRIM *disable* maupun *enable* termasuk untuk pemulihan file secara keseluruhan dengan mencapai akurasi 90 %.

KESIMPULAN

1. Metode *live forensics* yang diterapkan pada laptop pertama yang dipasang SSD dengan *interface* SATA merk PNY seri CS900 dengan Windows 11 Professional sebagai sistem operasinya untuk kemudian dilakukan akuisisi pada partisi kedua (Local Disk D) dalam keadaan menyala. Untuk keperluan akuisisi secara langsung maka dibuat *image file* dengan masing-masing fungsi TRIM menggunakan perangkat lunak FTK Imager untuk selanjutnya *image file* tersebut diperiksa dan dianalisis dengan tujuan memulihkan file.
2. Pemeriksaan forensik digital yang dilakukan pada penelitian ini dengan masing-masing fungsi TRIM baik secara *disable* maupun *enable* meliputi beberapa tahapan yaitu membuat *image file/imaging*, pemeriksaan, analisa, dan pemulihan file menggunakan perangkat lunak Autopsy, Testdisk, dan Belkasoft, kemudian untuk keperluan *hashing* menggunakan perangkat lunak HashMyFiles. Hasil yang didapatkan adalah ketika fungsi TRIM dalam keadaan *disable*, pemulihan file berhasil dilakukan dan file dapat dibuka secara sempurna serta keaslian file tetap terjaga yang dibuktikan dengan MD5 *hash value* yang tetap sama sebelum dan sesudah skenario dijalankan. Di lain sisi penerapan fungsi TRIM dalam keadaan *enable* tidak membuahkan hasil seperti dalam keadaan TRIM *disable*. Seluruh file yang dipulihkan dalam keadaan TRIM *enable* sama sekali tidak dapat terbaca atau rusak kecuali satu file dengan ekstensi .txt. Hal ini disebabkan karena ukuran file dengan ekstensi .txt tersebut lebih kecil dari 512 KB atau 2 MB tergantung model SSD, kemungkinan besar tidak terpengaruh oleh masing- masing fungsi TRIM, yang dengan hal itu masih memungkinkan untuk dipulihkan secara forensik. Dengan hasil tersebut file

yang dipulihkan memiliki nilai yang berbeda sebelum dan sesudah skenario dijalankan sehingga keaslian barang bukti diragukan.

3. Dari skenario yang dijalankan, hasil pemeriksaan dan analisis dalam keadaan TRIM *disable* menggunakan perangkat lunak Autopsy dan Testdisk yaitu seluruh file berhasil dipulihkan secara sempurna. Di lain sisi dalam keadaan TRIM *enable* hanya satu file yang dapat dipulihkan secara sempurna yaitu file dengan ekstensi .txt. Hal ini disebabkan karena ukuran file dengan ekstensi .txt tersebut lebih kecil dari 512 KB atau 2 MB tergantung model SSD, kemungkinan besar tidak terpengaruh oleh masing- masing fungsi TRIM, yang dengan hal itu masih memungkinkan untuk dipulihkan secara forensik. Sementara itu perangkat lunak Belkasoft tidak berhasil memulihkan satu file pun baik ketika TRIM dalam keadaan *disable* maupun *enable.*

DAFTAR PUSTAKA

[1] A. Neyaz, B. Zhou, and N. Karpoor, "Comparative Study of Wear-leveling in Solid-State Drive with NTFS File System," *Proc. - 2019 IEEE Int. Conf. Big Data, Big Data 2019*, pp. 4294–4298, 2019, doi: 10.1109/BigData47090.2019.9006067.

[2] A. Nisbet and R. Jacob, "TRIM, wear levelling and garbage collection on solid state drives: A prediction model for forensic investigators," *Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019*, pp. 419–426, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00063.

[3] J. Vieyra and M. Scanlon, "Solid State Drive Forensics : Where Do We Stand?," *Conf. Pap.*, no. March, 2019.

[4] M. N. Al-Azhar, *The Essential of Digital Forensic*. Denpasar: Code Bali International Cyber Security Conference 2016, 2016.

[5] Soni, Y. Prayudi, B. Sugiantoro, D. Sudyana, and H. Mukhtar, "Server Virtualization Acquisition Using Live Forensics Method," *Adv. Eng. Res.*, vol. 190, no. December, 2019, doi: 10.2991/iccelst-st-19.2019.4.

[6] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," *Digit. Investig.*, vol. 9, no. 2, pp. 81–95, 2012, doi: 10.1016/j.diin.2012.05.015.

[7] D. M. Rathod, "Google Drive Forensics Notes," *Int. J. Comput. Sci. Commun.*, vol. 8, no. March, pp. 5–10, 2017, [Online]. Available: http://sysforensics.org/2012/05/google-drive-forensics-notes.html.

[8] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic Digital Forensic Investigation Model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–131, 2011, [Online]. Available:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.8647&rep=r

ep1&type=pdf.

[9] F. Ridho, A. Yudhana, and I. Riadi, "Analisis Forensik Router Terhadap Serangan Distributed Denial of Service (DDoS)," in *Annual Research Seminar 2016*, 2018, no. December 2016, pp. 22–23, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[10] M. Nuh Al-Azhar, *Digital Forensic: Practical Guidelines for Computer Investigation*. 2012.

[11] J. Williams, *ACPO Good Practice Guide for Digital Evidence*, vol. 5, no. 10. Association of Chief Police Officers, 2012.

[12] B. S. Nasional, *Teknologi Informasi - Teknik keamanan - Pedoman identifikasi, pengumpulan, akuisisi dan preservasi bukti digital (ISO/IEC 27037:2012, IDT)*, SNI 27037: Jakarta: Badan Standarisasi Nasional, 2014. [13] C. Grenier, "TestDisk Documentation," 2019.

[14] Y. Gubanov and O. Afonin, "Recovering Evidence from SSD Drives in 2014: Understanding TRIM, Garbage Collection and Exclusions | Forensic Focus - Articles," *Forensic Focus*, pp. 1–8, 2014, [Online]. Available: https://articles.forensicfocus.com/2014/09/23/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/.