Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 23 ; Nomor 2 ; Agustus 2024 ; Page 273-280
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

Analisis *File Carving Solid State Drive* Menggunakan Metode *National Institute of Standards and Technology*

Khoirul Anam Dahlan[1], Anton Yudhana[2], Herman Yuliansyah[3]

[123]Program Study Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia, 55191
Email : khoirulanamdhln@gmail.com, eyudhana@mti.uad.ac.id, herman.yuliansyah@tif.uad.ac.id
Email Penulis Korespondensi : khoirulanamdhln@gmail.com

Article History:
Received Jun 27th, 2024
Revised Jul 20th, 2024
Accepted Aug 08th, 2024

Abstrak

Recovery pada SSD dianggap sulit karena tingkat keberhasilan yang rendah dalam dunia teknisi, karenanya teknik *file* carving yang terbaharui menjadi salah satu solusi pengembalian *file* yang hilang, baik dengan sengaja ataupun tidak sengaja, sehingga masih ada harapan atas *file* yang telah hilang pada SSD, khususnya pada SSD Sata Geniune 120GB. Metode NIST memungkinkan untuk merangkum pelaporan yang dapat dipertanggungjawabkan dan valid, sehingga dapat digunakan dalam persidangan untuk membuktikan bahwa pelaku benar atau salah.setelah bukti fisik berupa SSD di kumpulkan, maka proses selanjutnya menggunakan laptop lenovo y520 yang dengan sistem operaasi ubuntu dan windows untuk pemeriksaan dan analisa untuk dibuatkan laporan. Dari 88 *file* yang di *recovery*, *Software* Foremost berhasil mengembalikan 46 *file* dengan tingkat keberhasilan 53% dan *Software* Autopsy berhasil mengembalikan 81 *file* dengan tingkat keberhasilan 94%, persentase keberhasilan diindikasikan dengan nilai hash yang sama menggunnakan MD5 dan *file* dapat dibuka tanpa kendala. Walaupun tidak sampai 100% yang biasa kita temukan dalam penelitian Harddisk atau Flashdisk, akan tetapi masih ada harapan kedepannya jika recovery pada SSD bisa mencapai 100%.

Kata Kunci : Ubuntu, Foremost, Autopsy, MD5, SDD Sata

Abstract

Recovery on SSDs is considered difficult due to the low success rate in the technician world. Therefore, updated file carving techniques have become one of the solutions for recovering lost files, whether intentionally or unintentionally, providing hope for files that have been lost on SSDs, especially on a Genuine 120GB SATA SSD. The NIST method allows for the summarization of accountable and valid reporting, which can be used in court to prove whether the perpetrator is guilty or not. After physical evidence in the form of an SSD is collected, the next process involves using a Lenovo Y520 laptop with Ubuntu and Windows operating systems for examination and analysis to generate a report. Out of the 88 recovered files, Foremost software successfully restored 46 files with a success rate of 53%, while Autopsy software recovered 81 files with a success rate of 94%. The success percentage is indicated by the same hash value using MD5, and the files can be opened without any issues. Although it's not the 100% success rate commonly found in HDD or Flash drive research, there is still hope for the future if SSD recovery can reach 100%.

Keyword: Ubuntu, Foremost, Autopsy, MD5, SATA SSD

1. PENDAHULUAN

Berbeda dengan *harddisk* dan *flashdisk*, setiap *Solid State Drive* (SSD) memiliki teknologi yang beragam, seperti *Triple Level Cell* (TLC) dan *Quadruple Level Cell* (QLC) [1]. Meskipun SSD yang terdiri dari NAND memory tahan terhadap guncangan dan memiliki konsumsi daya yang lebih rendah daripada harddisk, beberapa NAND memiliki kemampuan "hapus sebelum tulis", membuat sulit untuk mengembalikan data [2]. Selain itu, trim pada SSD juga memperparah kesulitan dalam proses pemulihan [3]. Forensik digital adalah penyelidikan untuk membuktikan kejahatan dengan menemukan bukti digital. Cakupannya meliputi analisis perangkat penyimpanan data digital karena data sering diblokir, dihapus, disembunyikan, atau diganti [4]. Forensik digital merupakan usaha ilmiah untuk mengembalikan dan menyelidiki materi terhadap bukti digital. Tujuannya adalah memberikan opsi dan saran kepada hakim untuk mengungkap kasus kriminal (pro-keadilan), dan proses forensik digital harus dilakukan dengan langkah-langkah yang dapat diukur dan terstruktur [5]. Berdasarkan teori yang menjelaskan model proses forensik, terdapat empat komponen tahapan, yaitu tahap

pengoleksian (*Collection*), tahap pemeriksaan (*Examination*), tahap analisis (*Analysis)*, dan tahap pelaporan (*Reporting*) [6]. Adanya *Cybercrime* merupakan efek samping dari adanya teknologi[7], dan terdapat hubungan antara *cybercrime* dan teknologi penyimpanan data yang bersifat *volatile* dan *nonvolatile*[8]. Hasil akhirnya berupa *digital evidence* yang didefinisikan sebagai informasi apa pun yang memiliki nilai bukti yang ditarik dari data biner yang diproses secara elektronik [9].

Media penyimpanan *Solid State Drive* (SSD), baik Internal maupun Eksternal, saat ini mengalami peningkatan seiring dengan ditinggalkannya media penyimpanan *Hard Disk Drive* (HDD)[10]. Hal ini disebabkan oleh kemampuan baca dan tulis SSD yang lebih cepat, dengan rata-rata kecepatan baca HDD konvensional sekitar 200Mb/s, sedangkan rata-rata kecepatan baca SSD adalah 500Mb/s dan kecepatan tulisnya mencapai 250Mb/s [11]. SSD juga memiliki kapasitas yang lebih besar dari HDD, konsumsi daya yang lebih rendah, ukuran yang lebih kecil, dan keandalan yang lebih tinggi[10]. Hal ini menyebabkan peningkatan penjualan SSD secara signifikan sehingga muncul berbagai merek baru yang bersaing dengan harga harddisk. Metodologi yang digunakan dalam penelitian ini adalah *National Institute of Standards and Technology* (NIST). Teknik recovery konvensional relatif cepat karena melibatkan proses membaca sistem *file* saja. Pendekatan *file* carving digunakan terutama pada ruang yang tidak terisi, di mana tidak ada informasi metadata yang mengacu padanya dalam sistem *file*[12].

2. METODOLOGI PENELITIAN

Metode yang digunakan untuk menganalisis bukti digital, dengan beberapa tahapan yang mencakup pengumpulan media bukti digital, pemeriksaan, analisis informasi yang diperoleh, dan pelaporan hasil analisis, dikenal sebagai metode NIST[10]. NIST adalah sebuah lembaga di Amerika Serikat yang bertanggung jawab untuk mengembangkan dan menyebarluaskan standar dan pedoman teknis, termasuk di bidang forensik digital. Metode NIST dalam analisis forensik digital menawarkan pendekatan terstruktur untuk memeriksa dan menganalisis bukti digital dengan langkah-langkah yang terukur dan dapat direplikasi. Dengan menggunakan metodologi ini, investigator dapat memastikan bahwa analisis yang dilakukan konsisten dan hasilnya dapat diandalkan untuk keperluan hukum.

2.1. Tahapan Penelitian

Gambar 1. *National Institute of Standards Technology* (NIST) Methodology

Tahap *Collection* merupakan langkah pertama dalam proses investigasi digital yang melibatkan pengumpulan data untuk mendukung jalannya investigasi dan pencarian barang bukti kejahatan digital[13]. Setelah barang bukti terkumpul, tahap selanjutnya adalah memastikan keaslian data sambil menjaga integritasnya[14]. Tahapan berikutnya adalah menganalisis data yang terkait dengan kasus kejahatan[15], dan hasil analisis tersebut kemudian dianggap sebagai bukti digital yang dapat digunakan dan diakui secara ilmiah dan hukum[16].

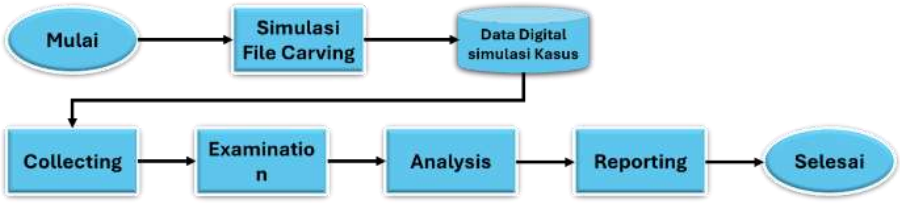
Pengembalian digital evidence melibatkan *File Carving*, sebuah teknik yang memulihkan data dengan mengidentifikasi dan merekonstruksi kumpulan *file* yang telah dihapus, disembunyikan, atau diformat menjadi seperti semula[17]. Meskipun Teknik *carving* dan *recovery* hampir mirip, namun *recovery* hanya mengembalikan data yang telah dihapus, sementara prinsip *carving* tidak memerlukan metadata *file* system, melainkan menganalisis setiap *byte* pada media penyimpanan elektronik. Namun, kekurangannya adalah tidak ada informasi seperti *filename*, *timestamp*, *status exist/deleted*, atau *fragmentas*[18].

Perangkat lunak yang digunakan dalam penelitian ini antara lain foremost, yang menggunakan perintah-perintah untuk memulihkan *file* dari berbagai sistem *file*, termasuk fat, ext3, dan lain-lain[19]. Sementara Autopsy digunakan untuk menganalisis gambar dan media lainnya, serta dapat mengekstrak data seperti *history browser* dan *cookies*[20]. Kedua perangkat lunak ini mudah dan cepat digunakan.

Untuk memvalidasi keaslian bukti digital, digunakan metode MD5 yang memeriksa kesesuaian antara hash media dengan hasil dari akuisisi gambar yang dilakukan[21]. Selain itu, *Hashing Tools* digunakan untuk mengumpulkan data, di mana seorang penyelidik harus memastikan integritas bukti dengan menghitung dan memeriksa hasil *hashing kriptografi*, yaitu jenis fungsi matematika yang menghasilkan nilai matematika unik dan tetap dari sejumlah nilai input yang acak[22].

Kerangka progres penelitian ini melibatkan beberapa tahapan. Tahap awal melibatkan simulasi sebuah kasus kejahatan dan propaganda digital pada media penyimpanan SSD. Tahap kedua melibatkan penggunaan *forensic tools* untuk menganalisis SSD dengan tujuan mendapatkan bukti digital. Kerangka kerja NIST digunakan dalam proses penelitian ini, yang dapat dilihat pada gambar 2.

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 23 ; Nomor 2 ; Agustus 2024 ; Page 273-280
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index



Gambar 2. Kerangka Simulasi Penelitian

3. HASIL DAN PEMBAHASAN

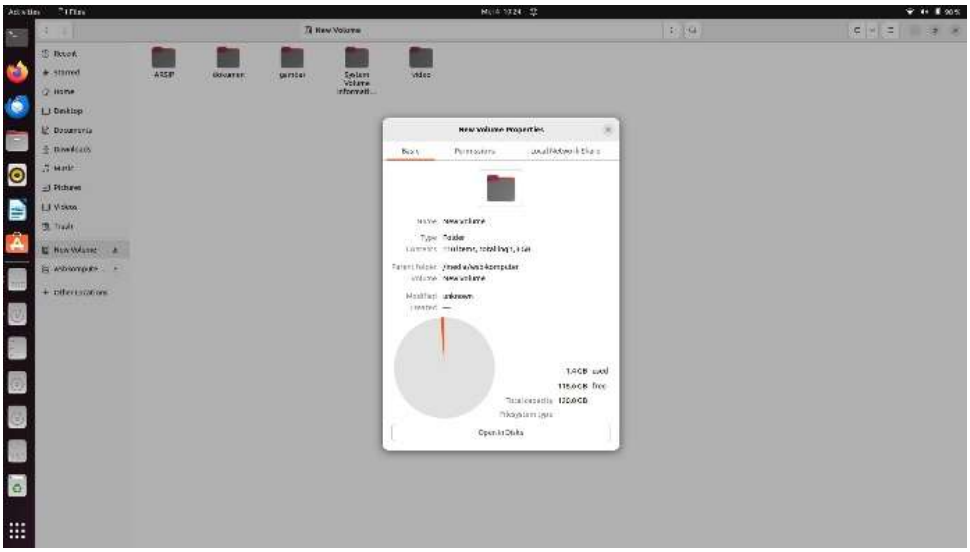
Dari penelitian yang telah dilakukan menggunakan *software* foremost dan autopsy dari data yang telah dihapus pada media penyimpanan SSD External. Berikut ini adalah informasi pada tabel 1 tentang perangkat keras, sistem operasi dan software yang digunakan dalam penelitian ini

Tabel 1. Alat dan Bahan

No	Bahan	Keterangan
1	Laptop	Legion Y520
2	OS	Ubuntu
		Windows 10
3	SSD Sata	Geniune 120gb
4	Foremost 1.5.7	Forensic Open source tool
5	Autopsy 4.21.0	Forensic Open source tool
6	MD5 v1.20	Checksum value

3.1 Collection

Dalam proses simulasi pengumpulan data menggunakan media SSD Sata yang menggunakan kapasitas 120GB, dengan sistem *file* NTFS



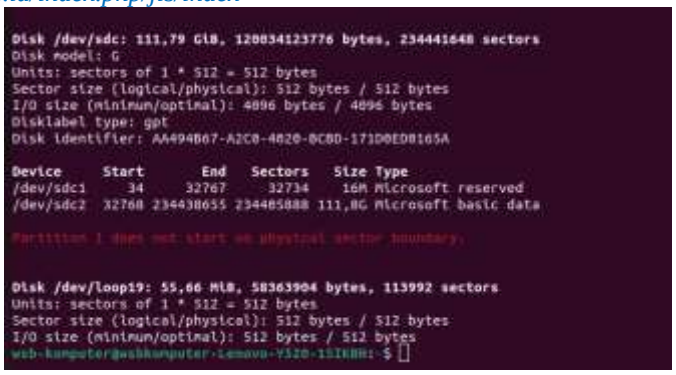
Gambar 3. media penyimpanan dengan *file* sistem NTFS

Pada gambar 3 diketahui bahwa media penyimpanan yang digunakan dalam penelitian menggunakan SSD Sata dengan kapasitas 120GB. Dalam media penyimpanan yang digunakan adalah *file* system NTFS, didalam media penyimpanan terdapat beberapa *file* yang disimpan sebelum proses penghapusan.

3.2 Examination

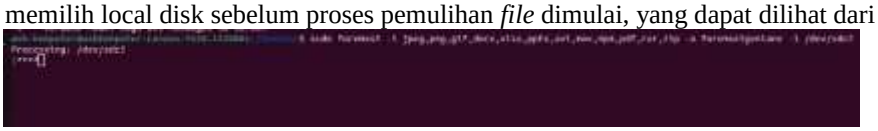
Proses pemeriksaan terhadap media penyimpanan SSD Sata dengan merk Geniune dengan kapasitas 120GB menggunakan Foremost dan Autopsy.

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 23 ; Nomor 2 ; Agustus 2024 ; Page 273-280
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

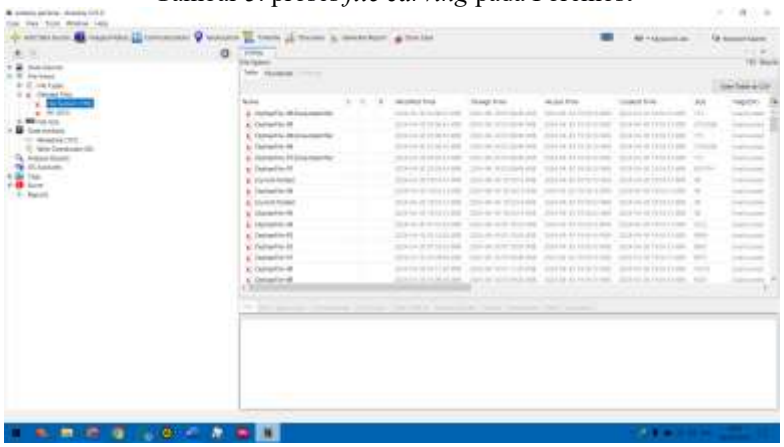


Gambar 4. memeriksa media penyimpanan SSD Sata

Pada Gambar 4, ditampilkan kode penyimpanan untuk melakukan perintah recovery. Dalam gambar tersebut, SSD memiliki volume sebesar 111,78 GiB, mendekati volume SSD pada merk yang menyatakan berkapasitas 120GB. Kode penyimpanan dalam Linux adalah /dev/sdc, dengan local disk /dev/sdc2. Pada Gambar 5, terlihat proses *file carving* menggunakan foremost dengan perintah "sudo foremost -t jpeg,png,gif,docx,xlsx,pptx,avi,mov,mp4,pdf,rar,zip -o foremostgenuine -I /dev/sdc2". Gambar 6 menampilkan proses *file carving* menggunakan aplikasi Autopsy. Dalam proses ini, pengguna harus memilih local disk sebelum proses pemulihan *file* dimulai, yang dapat dilihat dari *file explorer*.



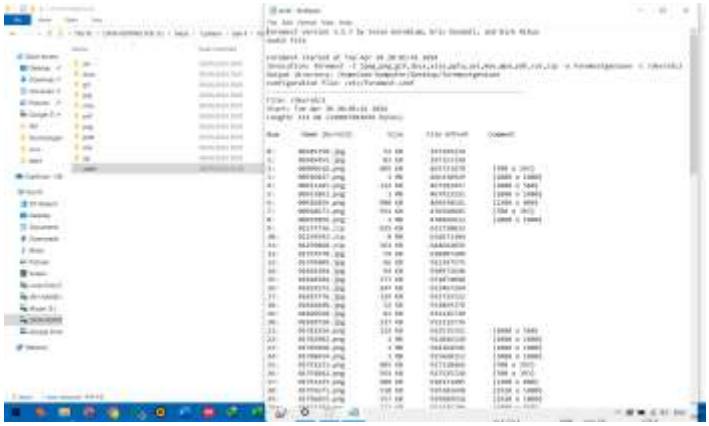
Gambar 5. proses *file carving* pada Foremost



Gambar 6. proses *file carving* pada autopsy

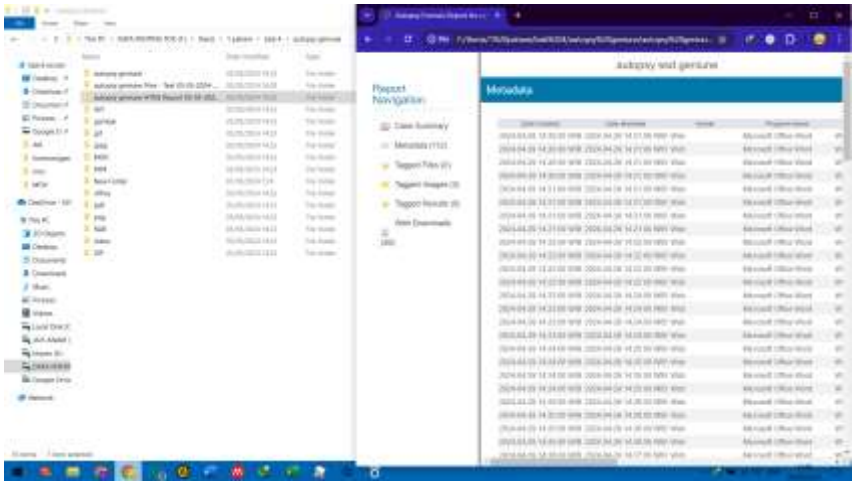
3.3 Analysis

Gambar 7 menunjukkan nama *file* yang telah dilakukan *recovery*, jenis *file*, ukuran dan lain sebagainya yang di laporkan dalam sebuah file.txt yang akan disimpan dalam sebuah folder foremostgeniune sesuai dengan perintah yang telah dijalankan pada applikasi foremost.



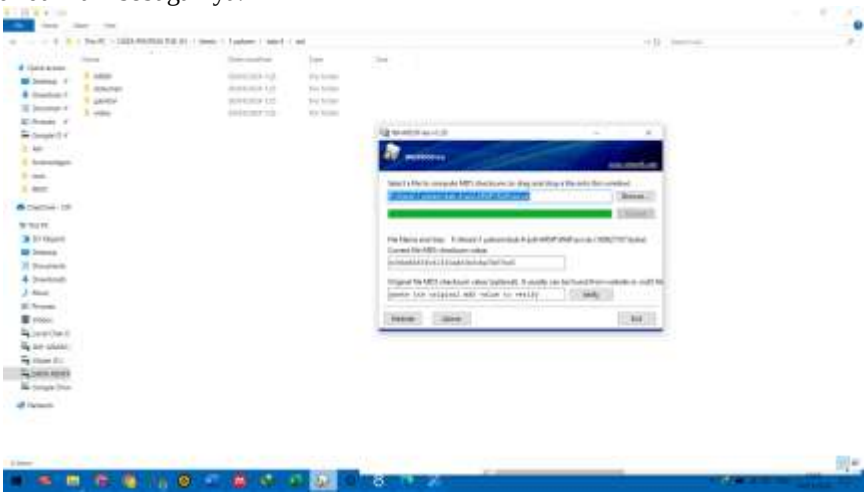
Gambar 7. Hasil analisis *File* yang telah dipulihkan Foremost

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 23 ; Nomor 2 ; Agustus 2024 ; Page 273-280
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index



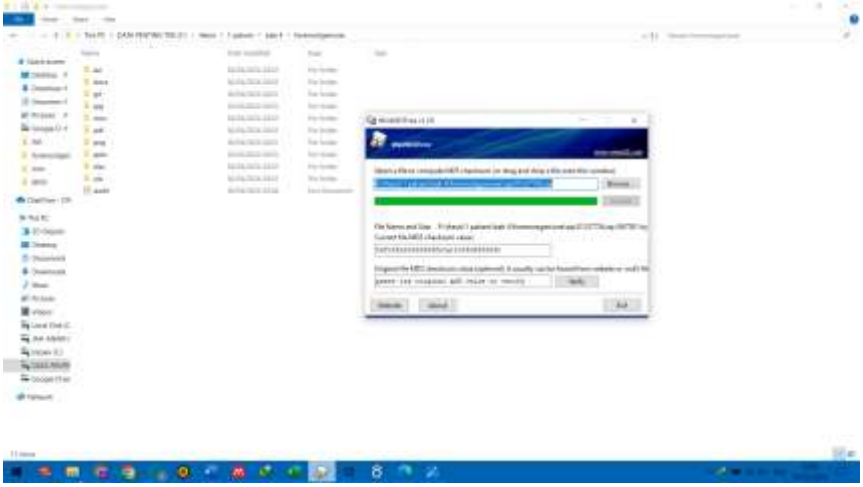
Gambar 8. hasil analisis *File* yang telah dipulihkan Autopsy

Pada Gambar 8 menunjukkan hasil pelaporan aplikasi Autopsy berupa *file* .html yang berisi keterangan waktu *recovery*, lokasi, *user* dan lain sebagainya.



Gambar 9. proses pengecekan nilai MD5 pada *file* asli

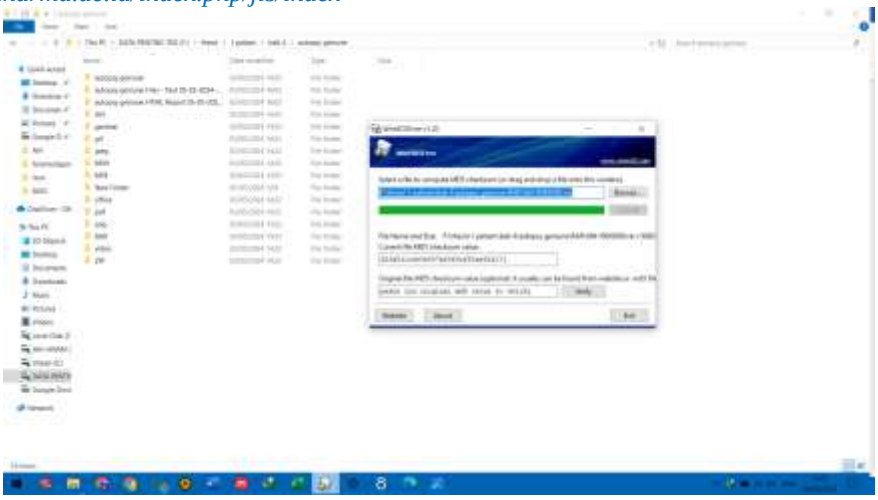
Setelah *file* berhasil dilakukan *recovery*, Gambar 9 menunjukkan pencarian nilai checksum/ hash yang unik disetiap *file* yang tak mungkin sama pada *file* yang berbeda / telah dirubah.



Gambar 10. proses pengecekan nilai MD5 pada *file* recovery foremost

Gambar 10 menunjukkan pencarian nilai checksum menggunakan MD5 pada *file* hasil recovery aplikasi foremost.

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 23 ; Nomor 2 ; Agustus 2024 ; Page 273-280
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index



Gambar 11. proses pengecekan nilai MD5 pada *file* recovery Autopsy

Gambar 11 menunjukkan pencarian nilai checksum menggunakan MD5 pada *file* hasil recovery aplikasi Autopsy.

3.3 Reporting

Setelah mendapatkan nilai checksum, nilai tersebut dimasukkan ke dalam aplikasi Excel untuk membandingkan nilai hash *file* asli dengan *file* yang dihasilkan dari proses pemulihan menggunakan foremost dan Autopsy. Dalam aplikasi Excel, nilai hash *file* asli akan dibandingkan dengan nilai hash dari *file* hasil recovery. Jika hash kedua *file* sama, maka nilai dalam sel akan menjadi 1, mengindikasikan kesamaan hash. Namun, jika *file* tidak berhasil dipulihkan atau nilai hash tidak cocok, maka nilai dalam sel akan menjadi 0, menunjukkan bahwa *file* telah mengalami perubahan, seperti yang terlihat pada Gambar 12.

Gambar 12. perbandingan nilai checksum

Pada tahapan pelaporan hasil analisis yang telah dilakukan, hasil yang didapatkan dari proses *file carving* tercantum pada Tabel 2.

Tabel 2. hasil persentase keberhasilan Foremost dan Autopsy

No	Jenis *File*	Persentase nilai Hash		
		File Asli	Foremost	Autopsy
1	zip	100%	50%	100%
2	rar	100%	0%	30%
3	docx	100%	100%	100%
4	pdf	100%	86%	100%
5	pptx	100%	100%	100%
6	xls	100%	100%	100%
7	gif	100%	0%	100%
8	jpg	100%	100%	100%
9	png	100%	100%	100%
10	avi	100%	0%	100%

11	mov	100%	0%	100%
12	mp4	100%	0%	100%
Nilai Rata-rata		100%	53%	94%

Foremost dan Autopsy dapat mengembalikan 7 *file* pada setiap format dari 7 *file* dengan format docx, pptx, xls, jpg, dan png dengan persentase 100%, akan tetapi foremost gagal mengembalikan *file* zip dan rar sebanyak 10 *file* pdf, avi, mov, dan mp4 sebanyak 7 *file* setiap format dan *file* gif sebanyak 5 *file* yang gagal dilakukan *recovery* sedangkan Autopsy dapat mengembalikan semua format kecuali format .rar yang hanya berhasil mengembalikan 3 *file* yang masih utuh dari 10 *file* sehingga menghasilkan persantase 30%, sehingga tingkat keberhasilan Autopsy mencapai 94%, sedangkan Foremost hanya 53%

4. KESIMPULAN

Kesimpulan dari penelitian ini adalah bahwa tiap SSD memiliki karakteristik unik dalam hal teknologi, tingkat sel, dan sistem keamanan. Oleh karena itu, generalisasi hasil penelitian ini terhadap merek dan seri SSD lainnya harus dilakukan dengan hati-hati. Perkembangan terus-menerus dalam teknologi *file* carving dan keamanan SSD mengakibatkan hasil penelitian ini mungkin tidak dapat diterapkan secara langsung pada SSD yang berbeda atau pada waktu yang berbeda di masa depan. Dalam penelitian selanjutnya, penting untuk memperhitungkan variasi antara model SSD serta untuk mengikuti perkembangan teknologi dan keamanan yang terus berubah.

UCAPAN TERIMA KASIH

Terimakasih kepada bapak Anton Yudhana sebagai dosen pembimbing 1 yang telah membantu dalam menyelesaikan jurnal ini, dan terimakasih juga kepada bapak Herman Yuliansyah sebagai dosen pembimbing 2 yang telah membantu menata bahasa dalam penulisan jurnal ini.

DAFTAR PUSTAKA

[1] M. Fukuchi, S. Suzuki, K. Maeda, C. Matsui, and K. Takeuchi, "BER evaluation system considering device characteristics of TLC and QLC NAND flash memories in hybrid SSDs with real storage workloads," *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2021-May, 2021, doi: 10.1109/ISCAS51556.2021.9401203.

[2] A. Alahmadi and T. S. Chung, "Crash Recovery Techniques for Flash Storage Devices Leveraging Flash Translation Layer: A Review," *Electron.*, vol. 12, no. 6, pp. 1–21, 2023, doi: 10.3390/electronics12061422.

[3] W. Pranoto, I. RIadi, and Y. Prayudi, "Live Forensics Method for Acquisition on the Solid State Drive (SSD) NVMe TRIM Function," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, pp. 129–138, 2020, doi: 10.22219/kinetik.v5i2.1032.

[4] S. Marcellino, H. B. Seta, and W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada KasusPenghapusan Berkas Menggunakan Metode National Institute Of Justice(NIJ)," 2023.

[5] A. Yudhana, Imam Riadi, and Budi Putra, "Digital Forensic on Secure Digital High Capacity using DFRWS Method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 6, pp. 1021–1027, Dec. 2022, doi: 10.29207/resti.v6i6.4615.

[6] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," *J. Telekomun. dan Komput.*, vol. 9, no. 3, p. 186, Jan. 2020, doi: 10.22441/incomtech.v9i3.7210.

[7] M. Riskiyadi, "INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME," 2020.

[8] L. F. Sikos, " AI in digital forensics: Ontology engineering for cybercrime investigations ," *WIREs Forensic Sci.*, vol. 3, no. 3, May 2021, doi: 10.1002/wfs2.1394.

[9] P. Lewulis, "Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law," *Crim. Law Forum*, vol. 33, no. 1, pp. 39–62, Mar. 2022, doi: 10.1007/s10609-021-09430-4.

[10] R. Kurinjimalar, S. Manjula, M. Ramachandran, and R. Sangeetha, "A Review on Solid state Drives transformer concept A new era in power supply," *Electr. Autom. Eng.*, vol. 2, no. 1, pp. 104–110, Mar. 2023, doi: 10.46632/eae/2/1/15.

[11] Haswendra AR, "AN OVERVIEW OF LAN/WLAN IN CAD/CAM/CAE APPLICATIONS," *J. Mech. Sci. Eng.*, vol. 7, no. 1, pp. 7–11, 2020.

[12] S. A. Sari and K. M. Mohamad, "A Review of Graph Theoretic and Weightage Techniques in *File* Carving," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Jun. 2020. doi: 10.1088/1742-6596/1529/5/052011.

[13] G. Ngurah, G. Wicaksana, I. Ketut, and G. Suhartana, "Forensic Analysis of Telegram Desktop-based

Applications using the National Institute of Justice (NIJ) Method," vol. 8, no. 4, pp. 2654–5101, 2020.
[14] S. K. Dirjen *et al.*, "Terakreditasi SINTA Peringkat 2," *masa berlaku mulai*, vol. 1, no. 3, pp. 820–828, 2017.
[15] R. A. Ramadhan, P. Rachmat Setiawan, and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," *IT J. Res. Dev.*, vol. 6, no. 2, pp. 162–168, 2022, doi: 10.25299/itjrd.2022.8968.
[16] P. Sukamto, Ispandi, Arman Syah Putra, Nurul Aisyah, and Rohmat Toufiq, "Forensic Digital Analysis for CCTV Video Recording," *Int. J. Sci. Technol. Manag.*, vol. 3, no. 1, pp. 284–291, 2022, doi: 10.46729/ijstm.v3i1.460.
[17] D. Teguh Yuwono, J. Raya Olat Maras, B. Alang, M. Hulu, and K. Sumbawa, "ANALISIS PERBANDINGAN *FILE* CARVING DENGAN METODE NIST."
[18] A. Ardiansyah, N. Hardi, and W. Gata, "Identifikasi dan Recovery *File* JPEG dengan Metode Signature-Based Carving dalam Model Automata," *Komputika J. Sist. Komput.*, vol. 9, no. 1, pp. 75–83, Apr. 2020, doi: 10.34010/komputika.v9i1.2733.
[19] R. Aleyamma, T. P. Scholar, and M. Mathai, "A Survey on *File* Carving Process Using Foremost and Scalpel," vol. 3, no. 1, doi: 10.5281/zenodo.5091663.
[20] H. Adamu, A. Adamu Ahmad, A. Hassan, and ad Barau Gambasha, "IJRSI) |Volume VIII, Issue V," 2021. [Online]. Available: www.rsisinternational.org
[21] A. Mohammed Ali and A. Kadhim Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-Document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020, doi: 10.1109/ACCESS.2020.2989050.
[22] Z. Moric, J. Redzepagic, and F. Gatti, "ENTERPRISE TOOLS FOR DATA FORENSICS," in *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, DAAAM International Vienna, 2021, pp. 98–105. doi: 10.2507/32nd.daaam.proceedings.014.