JOISIE (Journal Of Information Systems And Informatics Engineering)
Vol. 8, No.2, Desember 2024, Hlm 381- 389
Received: 26 November 2024, Revised: 30 Desember 2024, Accepted: 31 Desember 2024
p- ISSN: 2503-5304
e- ISSN: 2527-3116

ANALISIS FORENSIK TOOLWIZ TIME SOLID STATE DRIVE MENGGUNAKAN METODE NIST

Muhamad Bagas Khoirul Anam [1)], Zamah Sari [2)], Bashor Fauzan Muthohirim *[3)]
[1,2,3]Prodi Informatika, Universitas Muhammadiyah Malang, Jl. Raya Tlogomas No.246, Babatan, Tegalgondo, Kecamatan Lowokwaru, Kota Malang.
email: [1]bagaskhoirul31@webmail.umm.ac.id, [2]zamahsari@umm.ac.id, [3]**bashorfauzan@umm.ac.id**

Abstract

With the advancement of internet technology, the development of the information world has progressed rapidly. However, this progress has also brought negative impacts that could potentially threaten human life in the future. Cybercrime has now become widespread, making it a major issue that needs to be addressed. Cyber refers to illegal activities conducted using computer technology, including hacking, phishing, and identity theft. The solution proposed in this research involves the use of Autopsy software and testing with Toolwiz Time. By utilizing these software tools and incorporating forensic science, it becomes easier to identify crimes that have been concealed or deleted to eliminate evidence. The purpose of this study is to understand how the Toolwiz Time software works to freeze SSDs and how Autopsy can uncover evidence on SSDs affected by freezing. The method used in this research follows the NIST framework, which consists of four stages: collection, examination, analysis, and reporting. The results obtained from this research reveal evidence in the form of folder log changes that can be identified using Autopsy. The conclusion drawn is that the Autopsy software successfully performed an analysis of the modified time and change time as displayed by the software.

Keywords: *SSD, Digital Forensic, NIST, Digital Evidence, Toolwiz Time*

Abstract

Kini dengan berkembangnya teknologi internet, perkembangan dunia informasi sangat berkembang pesat. Tidak sedikit pengaruh negatif yang timbul dari teknologi terbaru yang kedepannya bisa mengancam kehidupan manusia. Kejahatan siber sekarang sudah marak terjadi dan menjadikan ini masalah utama yang harus diselesaikan. Siber adalah jenis aktifitas ilegal yang dilakukan menggunakan teknologi komputer. Kejahatan yang mencakup hacking, phising dan pencurian identitas dapat dilakukannya. Adapun solusi yang ditawarkan dalam penelitian ini dengan menggunakan sofware Autopsy dan sebagai uji coba menggunakan Toolwiz Time. Penggunaan dari software tersebut serta adanya ilmu forensik dapat dengan mudah mengetahui kejahatan apa saja yang sudah disembunyikan maupun dihapus untuk menghilangkan barang bukti yang dilakukan. Tujuan dari penelitian ini adalah untuk mengetahui bagaimana cara software Toolwiz Time bekerja untuk melakukan frozen pada SSD serta Autopsy dapat menemukan barang bukti pada SSD yang terkena frozen. Metode yang digunakan adalah NIST. Pada metode ini ada empat tahap yang harus dilakukan yaitu collection, examination, analisys dan reporting. Hasil yang diperoleh dari penelitian ini adalah penemuan bukti berupa perubahan log folder yang dapat diketahui dengan Autopsy. Kesimpulan yang didapat penggunaan software autopsy berhasil melakukan analisis pada modified time dan change time yang ditunjukkan pada software tersebut.

Keywords: *SSD, Digital Forensic, NIST, Bukti Digital, Toolwiz Time*

1. PENDAHULUAN

Teknologi internet semakin hari semakin berkembang. perkembangan dunia Informasi Teknologi(IT) sangat berkembang pesat terutama pada era industri 4.0 sekarang (Prasetyo et al., 2023). Penggunaan teknologi komputer baik dari sudut pandang perangkat keras maupun perangkat

lunak menjadi sangat penting mengingat hampir semua industri perorangan telah menggunakan sistem berbasis komputer (Putra et al., 2022). Sehingga semua jenis informasi dapat diakses dengan mudahnya (Jufri & Heryanto, 2021).

Penggunaan IT diindonesia begitu pesat, Persentase penerapan IT mengalami perlonjakan, diketahui pada tahun 2019 mencapai angka 63,53%. Pertumbuhan ini terus berlanjut seiring dengan banyaknya orang atau lembaga atau industri yang menggunakan IT untuk membantu perkerjaan mereka (Purba et al., 2021). Saat teknologi terbaru sudah berkembang, perkembangan tersebut tidak sedikit membawa dampak negatif. Sisi negatif yang ditimbulkan yaitu semakin berkembangnya teknologi kejahatan yang dilakukan oleh orang yang tidak bertanggung jawab biasa dikenal dengan *CyberCrime* (Sufi et al., 2023). Berdasarkan data dari BSSN(Badan Sandi dan Siber Negara), sepanjang bulan januari-agustus 2020, terdapat hampir 190 juta aksi penyerangan yang dilakukan oleh siber di Indonesia. Dari tahun sebelumnya aksi ini naik sampai empat kali lipat yang sebelumnya hanya tercatat 39 juta (Umbara & Setiawan, 2022).

Perkembangan yang pesat teknologi internet, ancaman kejahatan siber semakin meningkat dan menjadi isu yang mendesak untuk diatasi (Rochmadi et al., 2024). Aktivitas ilegal seperti hacking, phishing, dan pencurian identitas membawa dampak serius terhadap individu maupun organisasi, terutama dalam hal perlindungan data dan privasi (Mikayla et al., 2023). Urgensi penelitian ini juga diperkuat oleh semakin tingginya penggunaan perangkat digital, terutama SSD (Solid State Drive), sebagai media penyimpanan utama. Penelitian ini menggunakan pendekatan metode NIST, untuk menghadirkan solusi handal dalam identifikasi dan analisis bukti digital. Analisis jejak digital menggunakan ilmu forensik (Julian & Sutabri, 2023). Dikenal juga sebagai digital forensic (Marcellino et al., 2023).

Setelah seperti yang disebutkan diatas, bahwa jejak digital yang tertinggal dalam kasus kejahatan *cybercrime* didunia maya berbeda dengan bukti yang ditemukan dalam kasus pidana konvesional (Fatmah & Indrayani, 2022). oleh karena itu, penanganan dan pengungkapan barang bukti elektronik dan digital memerlukan akomodasi khusus. Hal ini disebabkan oleh sifat dan kondisi bukti digital yang tidak terlihat, rapuh, dan mudah diubah atau modifikasi. Bukti elektronik dan digital harus disimpan dengan hati – hati sebagai bagian dari proses forensik digital karena risiko gangguan atau kebocoran data (Triyanto & Fachri, 2024).

Pelaku kejahatan biasanya menggukan berbagai cara untuk menghapus bukti terkait kejahatan yang mereka lakukan. Cara yang paling umum digunakan adalah dengan menghapus atau memformat data atau informasi terkait tindakan tersebut sehingga tidak akan ditemukan bukti yang bersangkutan. Ada sebuah cara agar tindakan pelaku itu tidak diketahui oleh pihak lain yaitu dengan menggunakan *Frozen* atau pembekukan penyimpanan pada drive agar perubahan yang dilakukan tidak akan terdeteksi. Ada salah satu *software* yang bisa mendukung tindakan tersebut diantaranya adalah *Toolwiz Time*.

Toolwiz Time adalah sebuah perangkat lunak atau software yang menciptakan lingkungan virtual untuk melindungi sistem anda dari perubahan yang tidak diinginkan. Tujuan bagaimana cara Toolwiz Time berkerja dan mengidentifikasi informasi atau data pada kondisi SSD yang terkena frozen. Secara khusus, dari pemahaman forensik, seperti apa data yang dibekukan atau bukti yang ditemukan dari proses analisis menggunakan Autopsy. *Software* Toolwiz Time telah dilengkapi dengan *system restore* yang dimana itu akan membekukan aktifitas yang dilakukan pada penyimpanan SSD. Sistem ini bekerja dengan mencegah perubahan pada komputer disimpan di media penyimpanan. Saat komputer dimatikan dan dihidupkan kembali, kondisinya akan kembali seperti sebelum perubahan dilakukan.

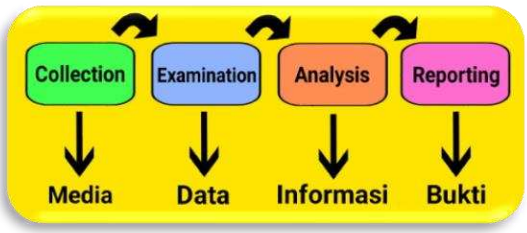
Penelitian yang dilakukan oleh (Saintikom et al., 2024), dengan tujuan memberikan opsi dan saran kepada hakim untuk mengungkap kasus kriminal (pro-keadilan), dan proses forensik digital harus dilakukan dengan langkah-langkah yang dapat diukur dan terstruktur. Hasil yang diperoleh adalah tingkat keberhasilan autopsy mencapai 94% setelah semua rangkaian dijalankan.

Penelitian yang dilakukan oleh (Kusuma et al., 2024), dengan tujuan adalah untuk mendukung upaya hukum dengan bukti yang dapat dipertanggungjawabkan secara digital. Hasil yang diperoleh dari penelitian ini adalah Bukti digital yang telah dihapus pada media penyimpanan flash disk dengan perlakuan yang berbeda berhasil ditemukan dan di recovery menggunakan tools forensic FTK Imager dan Autopsy.

Penelitian ini memperkenalkan pendekatan baru dengan menggunakan Toolwiz Time untuk membekukan SSD dan Autopsy sebagai alat analisis utama. Analisis forensik berperan penting dalam mengungkap bukti kejahatan siber, membantu mengakses informasi pribadi yang tersembunyi, dan mendukung proses hukum dengan data yang valid, terverifikasi, dan sesuai standar hukum.

2. METODE PENELITIAN

Pada penelitian ini menggunakan metode analisis forensik dari NIST(National Institute of Standart and Technology). Metode ini menjelaskan alur penelitian yang akan dilakukan, sehingga tahapan dan langkah – langkahnya dapat diidentifikasi secara sistematis dan menjadi panduan dalam menyelesaikan sebuah permasalahan yang ada (Bintang et al., 2020). Pada metode ini terdapat beberapa tahapan yang harus dilakukan yang bisa dilihat pada gambar 1.



Gambar 1. Tahapan metode NIST

tahapan metode NIST ini ada empat tahapan yang harus dilakukan yaitu collection, examination, analysis reporting (Dasmen, Rahman, et al., 2024). Untuk penjelasannya akan ditulis sebagai berikut:

1. Collection (pengumpulan)

pada tahap ini sebagai serangkaian kegiatan yang dilakukan untuk mendapatkan informasi yang mendukung proses penyelidikan dalam pencarian barang bukti (Runtuwene et al., 2024). Pada tahap ini mencangkup proses identifikasi, pelabelan, perekaman dan pengambilan informasi dari sumber yang relevan, dengan tujuan utama untuk menjaga integritas information dan mengidentifikasi alat dan teknik yang diperlukan untuk akuisisi dan analisis (Riadi et al., 2020).

2. Examination (pemeriksaan)

Pada tahap ini berisi tentang pemeriksaan informasi yang telah didapat secara forensik, baik melalui metode manual atau otomatis. Pada tahap ini bertujuan untuk memastikan bahwa informasi yang diperoleh itu asli dengan sesuai dengan yang ditemukan ditempat kejadian. Dalam hal ini sering menggunakan teknik hashing untuk identifikasi lebih lanjut (Bintang et al., 2020).

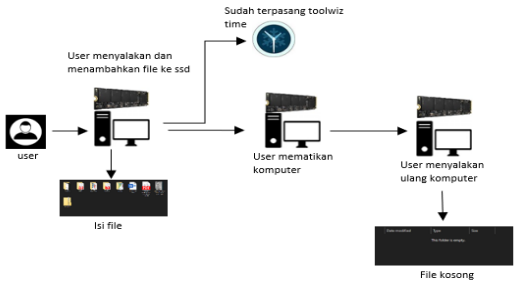
3. Analysis (penelitian)

Pada tahap analysis ini dilakukan setelah data digital yang relevan didapatkan dari proses pemeriksaan sebelumnya (Pujiyanta & Maulana, 2024). Data yang diperoleh tersebut kemudian dianalisis dengan teliti dan menyeluruh menggunakan metode yang telah diakui secara teknik dan hukum untuk membantu membuktikan keasliannya. Hasil yang diperoleh dari proses ini akan di kategorikan sebagai barang bukti digital yang nantinya dapat dipertanggung jawabkan baik secara ilmiah maupun secara hukum (Ramadhan & Mualfah, 2020).

4. Reporting (pelaporan)

Reporting dilakukan setelah semua barang bukti didapatkan melalui tiga proses sebelumnya yang sudah sesuai dengan kebutuhan penyelidikan (Achmad Iqbal Yuladi & ..., 2021). Pada tahap ini, hasil yang didapat dilaporkan dengan mendetail termasuk deskripsi tindakan apa saja yang telah diambil, penjelasan tentang alat serta metode yang digunakan, dan langkah demi langkah pendukung yang sudah dilakukan, seperti halnya pemeriksaan forensik tambahan, pengamanan celah yang ada, atau peningkatan kontrol keamanan. Selain itu, laporan ini juga mencakup rekomendasi untuk perbaikan dalam kebijakan, metode, alat, atau aspek lain yang mendukung proses digital forensik(Ali Diko Putra et al., 2024).

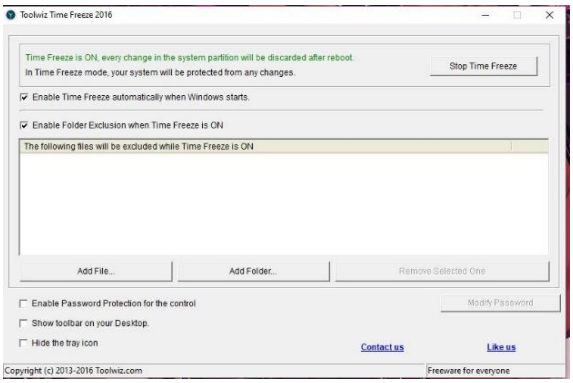
Berikut adalah cara kerja dari software toolwiz time yang dimana data yang disimpan sebelumnya tidak akan tersimpan setelah komputer itu dimatikan lalu dinyalakan kembali. Untuk contohnya pada gambar 2.



Gambar 2. Cara kerja Toolwiz time

Pada gambar 2 merupakan sebuah alur terjadinya kondisi frozen pada SSD. Hal yang dilakukan pertama oleh user tersebut adalah user menyalakan komputer dan user menambah beberapa file kedalam local disk yang ada di perangkat tersebut. Saat ini komputer tersebut sudah terpasang software toolwiz time. Setelah itu user mematikan komputer atau men shutdown. Lalu user tersebut menyalakan ulang komputer yang sebelumnya sudah ditambahkan beberapa file dan sudah terinstall software toolwiz time. Setelah mengecek isi local disk yang sebelumnya sudah terisi beberapa file, file tersebut hilang.

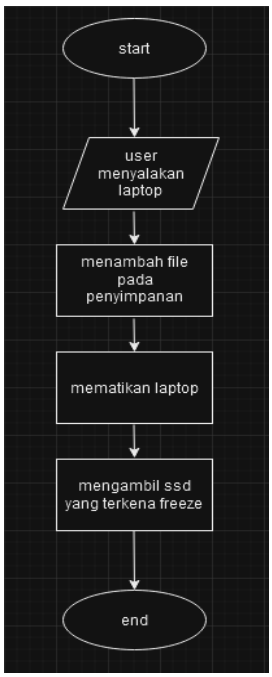
Tampilan dari software Toolwiz Time bisa dilihat pada gambar 3.



Gambar 3. Tampilan software

Pada gambar 3 diperlihatkan tampilan dalam software toolwiz time terdapat beberapa menu yang harus dijalankan. Yaitu centang kedua kolom enable yang berfungsi untuk frozen otomatis waktu windows atau komputer dinyalakan. Lalu add folder yang dimana itu adalah folder yang akan kita masukkan ke mode frozen. Bagian kanan atas terdapat start to frozen guna menjalankan software tersebut.

Untuk simulasi sistem perancangan guna memperoleh hasil bukti digital agar dapat dilakukan tahap analisis digital forensik. Skenario yang dilakukan yaitu seorang user melakukan aktifitas berupa menambah dan mendownload beberapa file dari website. Lalu user tersebut mematikan laptop untuk sementara waktu. Lalu setelah beberapa saat user menyalakan laptopnya kembali untuk melihat hasil download yang telah dilakukan sebelumnya. Waktu user membuka file, file tersebut tidak tersimpan, semua perubahan yang user lakukan juga tidak tersimpan. Dari keadaan diatas alur atau langkah - langkah guna mendapatkan kembali salinan bukti digital pada SSD yang terpasang software toolwiz time dapat dilihat pada gambar 4.



Gambar 4. Tahap implementasi

Pada gambar 4 adalah skenario yang akan digunakan dalam proses pengambilan data yang mana nantinya akan didapatkan barang bukti dari SSD atau perangkat laptop yang terpasang software Toolwiz Time.

3. HASIL DAN PEMBAHASAN

Proses yang akan digunakan guna memperoleh barang bukti digital melalui laptop atau komputer dengan menggunakan sistem operasi berbasis windows serta alat yang akan digunakan adalah Autopsy. Alat dan bahan akan disertakan pada tabel 1.

Tabel 1. Alat dan bahan

No.	Nama item	Spesifikasi
1	Laptop	DESKTOP-GH84LDA
2	SSD	SAMSUNG MZALQ256HAJD-000L2
3	Toolwiz Time	Versi 3.2.0.2000
4	Autopsy	Versi 4.21.0-64bit

1. Collection

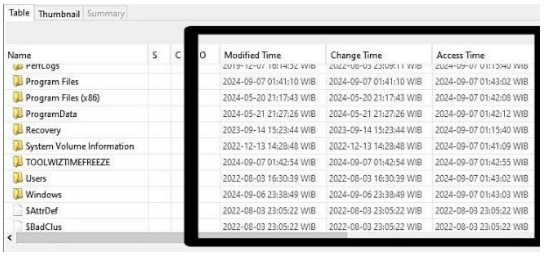
Pada tahap ini merupakan proses pengumpulan barang bukti guna menunjang penelitian ini. Disini menggunakan perangkat keras laptop sebagai bahan simulasi. Dengan sistem operasi windows 10 serta menggunakan SSD dengan spesifikasi SAMSUNG MZALQ256HAJD-000L2 sebagai media untuk uji coba (Bintang et al., 2020). Gambar akan ditampilkan pada gambar 5.

Gambar 5. SSD dan Laptop yang dipakai

Kondisi laptop pada gambar 5 dalam posisi sudah terinstal Toolwiz Time. Jadi apapun perubahan yang dilakukan tidak akan berlaku. Setelah mendapat barang bukti yang diperlukan guna menunjang proses penyelidikan dalam pencarian barang bukti, tahap selanjutnya adalah Examination.

2. Examination

Pada proses ini merupakan pengujian pada SSD dan laptop yang sebelumnya sudah terpasang software Toolwiz Time yang secara fungsi itu dapat membekukan proses yang terjadi didalam SSD. Dengan menggunakan tools yang telah disediakan ini mampu untuk mengekstrak data dan mencari data pada SSD. Pada penelitian ini menggunakan tools Autopsy guna menunjang pencarian jejek digital yang masih tertinggal pada perangkat tersebut. Proses tersebut bisa dilihat pada gambar 6.

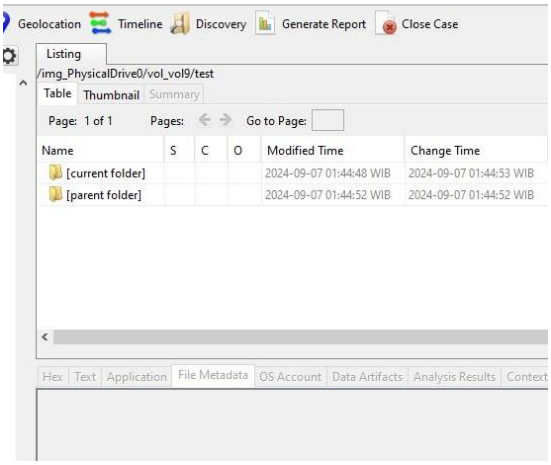


Gambar 6. Proses yang dilakukan

Pada gambar 6 ditampilkan setelah proses running pada autopsy. Terdapat beberapa folder dan file yang terlihat pada local disk. Beberapa folder diantaranya sudah pernah dibuka sebelumnya dan disini terdapat bukti bahwa folder yang ada pada local disk sudah pernah diakses walaupun sebelumnya komputer tersebut sudah dimatikan.

3. Analysis

Pada tahap ini, lanjutan dari proses Examination yang dimana aktifitas yang dilakukan pada waktu itu masih bisa dideteksi atau dilihat menggunakan tools autopsy (Santoso & Sulaksono, 2022). meski tidak semua bisa terlihat tapi dengan beberapa bukti yang telah ditemukan maka bisa dipastikan bahwa local disk sudah pernah diakses oleh seseorang. Hal itu bisa terlihat melalui log modified atau modified time yang ada pada tools tersebut. Gambar bisa dilihat pada gambar 7.



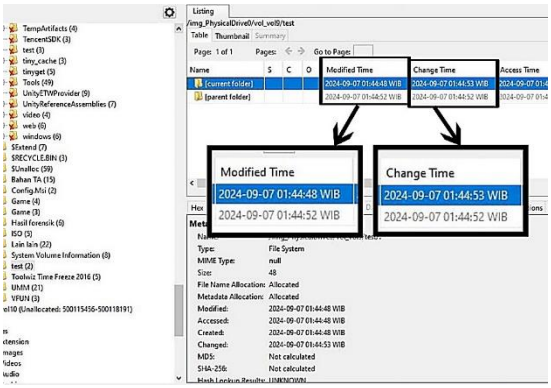
Gambar 7. Modified time

Pada gambar 7 ditunjukkan ada 2 folder salah satu folder itu bernama current folder yang artinya folder tersebut sedang bekerja atau aktif sebelum terjadi nya shutdown pada laptop. Dan pada gambar tersebut dibagian modified time tertera tanggal 07-09-2024 yang artinya pada tanggal tersebut folder telah mengalami modifikasi beberapa waktu yang lalu.

4. Reporting

Pada tahap akhir pada metode ini adalah reporting. Pada digital forensik, laporan adalah pembuatan dokumen yang sudah merangkum hasil dari penyelidikan yang sudah dilakukan

sebelumnya. Pada proses yang sudah dilakukan di SSD dengan spesifikasi SAMSUNG MZALQ256HAJD-000L2 yang dimana kondisi dari SSD tersebut terkena frozen menggunakan software Toolwiz Time. Untuk hasilnya setelah melakukan kegiatan analysis terhadap SSD tersebut didapatkan bukti berupa teraksesnya beberapa folder yang ada pada local disk. Gambar dapat dilihat pada gambar 8.



Gambar 8. Bukti folder yang diakses

Hasil dari data yang didapat setelah proses analisis menggunakan software Autopsy adalah tidak semua dapat menampilkan bukti bahwa file yang ada didalam SSD diakses oleh seseorang. Adapun terdapat beberapa file yang rusak sehingga file tersebut memang tidak bisa diakses sama sekali. Hanya file yang berupa folder yang menunjukkan log yang berbeda meskipun SSD tersebut dalam kondisi frozen atau frozen (Sontani et al., 2024). Lebih lengkapnya data yang diperoleh akan disajikan dalam bentuk tabel. Dapat dilihat pada tabel 2.

Tabel 2. Hasil yang diperoleh

Nama Software	Nama File	Jumlah file	File yang diakses
Autopsy	Folder	12	4
	Gambar	3	0
	Video	0	0

Laporan ini merinci penemuan, bukti yang dikumpulkan, dan metode yang digunakan. Tahap ini sangat penting karena itu berfungsi sebagai dokumen atau barang bukti yang dapat digunakan untuk keperluan hukum maupun internal.

4. SIMPULAN

Melalui serangkaian tahapan penelitian, telah terbukti bahwa perangkat lunak Autopsy mampu mengidentifikasi SSD yang telah dibekukan menggunakan Toolwiz Time, sesuai dengan tujuan penelitian ini. Hasil menunjukkan bahwa dari total 12 folder, 3 foto, dan 0 video yang terdapat pada SSD, hanya 4 folder yang diakses oleh pelaku. Tingkat keberhasilan dari penelitian ini sebesar 33% dengan kondisi hanya folder yang dapat terdeteksi. Analisis lebih lanjut mengungkap bahwa perubahan waktu log file yang terdeteksi oleh Autopsy dapat digunakan sebagai bukti digital yang valid untuk kebutuhan investigasi atau proses hukum. Penelitian ini menawarkan pendekatan baru dalam mendeteksi data tersembunyi pada SSD yang dibekukan, yang berpotensi membantu dalam pengumpulan bukti digital yang relevan. Namun, terdapat keterbatasan pada cakupan penelitian ini, yakni hanya menggunakan satu jenis perangkat lunak dan SSD, sehingga hasilnya belum dapat digeneralisasi untuk semua situasi. Oleh karena itu, penelitian lanjutan disarankan untuk menguji metode ini pada berbagai jenis perangkat keras dan perangkat lunak forensik guna meningkatkan efektivitasnya (Dasmen, Pratama, et al., 2024). Temuan dari penelitian ini diharapkan dapat membantu penyidik forensik dalam mengungkap kejahatan siber dengan lebih efisien.

5. DAFTAR PUSTAKA

Achmad Iqbal Yuladi, R. I., & ... (2021). Analisis dan Perbandingan Tools Forensik Menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber. *Jurnal Teknologi Terpadu …*, *8*(2), 86–93. https://www.academia.edu/download/92883068/233.pdf

Ali Diko Putra, M., Wirawan Muhammad, A., Parga Zen, B., Yunita Kisworini, R., & Rohayati, T. (2024). Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86. *Jurnal Sistem Informasi Galuh*, *2*(1), 44–54. https://doi.org/10.25157/jsig.v2i1.3695

Bintang, R. A., Umar, R., & Yudhana, A. (2020). Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST. *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, *21*(2), 125. https://doi.org/10.30595/techno.v21i2.8494

Dasmen, R. N., Pratama, M. R., Yasir, H., & Budiman, A. (2024). Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute of Standard and Technology Sp 800-86. *Jurnal Ilmiah Informatika*, *12*(01), 68–73. https://doi.org/10.33884/jif.v12i01.8344

Dasmen, R. N., Rahman, A., Dwi, A., & Saputra, M. (2024). Analisis Digital Forensik Recovery File yang Terhapus Menggunakan Tools Autopsy Dengan Metode National Institute Of Justice. *Jurnal Ilmiah Komputasi*, *23*(2), 213–218. https://doi.org/10.32409/jikstik.23.2.3553

Fatmah, N., & Indrayani, R. (2022). Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics. *J-SISKO TECH (Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD)*, *5*(2), 185. https://doi.org/10.53513/jsk.v5i2.5755

Jufri, M., & Heryanto, H. (2021). Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *5*(2), 98–108. https://doi.org/10.35145/joisie.v5i2.1759

Julian, D., & Sutabri, T. (2023). Analisa Kinerja Aplikasi Digital Forensik Autopsy untuk Pengembalian Data menggunakan Metode NIST SP 800-86. *Jurnal Informatika Terpadu*, *9*(2), 136–142. https://doi.org/10.54914/jit.v9i2.984

Kusuma, A. W., Alwi, E. I., & Ramdaniah, R. (2024). *Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST) Analysis Of Digital Evidence On Flash Disk Storage Media Using The National Institute Of Standards And Technology (NIST) Method*. *7*(1), 18–24.

Marcellino, S., Seta, H. B., & Widi, I. W. (2023). Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute of Justice (NIJ). *Informatik : Jurnal Ilmu Komputer*, *19*(2), 141–156. https://doi.org/10.52958/iftk.v19i2.4676

Mikayla, H. S., Kusyanti, A., & Trisnawan, P. H. (2023). Analisis Forensik Digital untuk Investigasi Kasus Cyberbullying pada Media Sosial Tiktok. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(7), 1571–1582. https://doi.org/10.25126/jtiik.1078017

Prasetyo, A. D., Seta, H. B., & Pradnyana, I. W. W. (2023). Analisis Digital Forensik Spear Phishing Menggunakan Metode National Institute of Justice (Studi Kasus: Instagram Verified Account). *Informatik : Jurnal Ilmu Komputer*, *19*(1), 58–67. https://doi.org/10.52958/iftk.v19i1.4675

Pujiyanta, A., & Maulana, I. (2024). Analisis Forensik Aplikasi Penipuan Berbasis Android Menggunakan Metode Nist. *JIKA (Jurnal Informatika)*, *8*(2), 187. https://doi.org/10.31000/jika.v8i2.10575

Purba, N., Yahya, M., & Nurbaiti. (2021). Revolusi Industri 4.0 : Peran Teknologi Dalam Eksistensi Penguasaan Bisnis Dan Implementasinya. *Jurnal Perilaku Dan Strategi Bisnis*, *9*(2), 91–98.

Putra, A. S., Aisyah, N., & Safrizal, S. (2022). Analisis Pengolahan Data Forensik Pada Solid State Drive (Ssd) Menggunakan Framework Grr Rapid Response. *Tekinfo: Jurnal Bidang Teknik Industri Dan Teknik Informatika*, *23*(1), 1–12. https://doi.org/10.37817/tekinfo.v23i1.1872

Ramadhan, R. A., & Mualfah, D. (2020). Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh. *IT Journal Research and Development*, *5*(2), 183–192. https://doi.org/10.25299/itjrd.2021.vol5(2).5750

Riadi, I., Sunardi, S., & Hadi, A. (2020). Analisis Bukti Digital TRIM Enable SSD NVMe Menggunakan Metode Static Forensics. *JUITA: Jurnal Informatika*, *8*(1), 65.

https://doi.org/10.30595/juita.v8i1.6584

Rochmadi, T., Fadlil, A., Riadi, I., Informatika, P. S., Dahlan, U. A., Studi, P., Informasi, S., & Ata, U. A. (2024). *Tinjauan Pustaka Sistematis : Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital Systematic Literature Review : Challenges And Factors For Developing Digital Forensic Readiness*. *7*(2), 81–89.

Runtuwene, E. R., Kumajas, S. C., & Kainde, Q. C. (2024). *Face Identification Using Image Procesing With The National Institute Of Standards And Technology (Nist) Method Identifikasi Wajah Menggunakan Image Processing Dengan Metode National Institute Of Sandards And Technology (NIST)*. *5*(4), 375–384.

Saintikom, J., Sains, J., Informatika, M., Dahlan, K. A., Yudhana, A., & Yuliansyah, H. (2024). *Analisis File Carving Solid State Drive Menggunakan Metode National Institute of Standards and Technology*. *23*, 273–280.

Santoso, B. S., & Sulaksono, P. M. (2022). Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager. *Jurnal Komputer Terapan*, *8*(1), 132–142. https://doi.org/10.35143/jkt.v8i1.5334

Sontani, L. T., Budiono, A., Widjajarto, A., & Negara, S. (2024). *Implementasi dan Analisis Sistem Forensik Digital pada Linux Vulnerable Machine Menggunakan Framework Forensics Zachman*. *2*(2), 1–6.

Sufi, F. Y. N., Putri, D. K., & Suhartini, D. (2023). Analisis Ancaman Cybercrime dan Peran Sistem Biometrik : Systematic Literature Review. *Prosiding Senapan*, *3*(1), 19–29.

Triyanto, A. R., & Fachri, F. (2024). Analisis Forensik Bukti Digital Pada Kejahatan Pembunuhan Berencana Menggunakan Metode National Institute of Justice. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(2), 1031–1042. https://doi.org/10.29100/jipi.v9i2.5558

Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*, 81–88. https://doi.org/10.29313/jrih.v2i2.1324