Jurnal Politeknik Caltex Riau
Terbit Online pada laman https://jurnal.pcr.ac.id/index.php/jkt/
| e- ISSN : 2460-5255 (Online) | p- ISSN : 2443-4159 (Print) |

Static Forensic Pada *USB* Mass Storage Menggunakan Forensics Toolkit *Image*r

Pradipta Mahardika Sulaksono[1], Banu Santoso[2*]
[1,2] Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
email: pradipta.s@students.amikom.ac.id, banu@amikom.ac.id
*Corresponding Author: banu@amikom.ac.id

[1] Abstrak

Peningkatan penggunaan perangkat penyimpanan USB cenderung massif & eksponensial disebabkan berbagai aspek, salah satunya ukuran dan harga perangkat penyimpanan USB yang terjangkau. Saat ini kualitas penanganan cybercrime di Indonesia masih minim, dimulai dengan masalah pengumpulan barang bukti cenderung tidak lengkap, kesalahan saat proses akuisisi barang bukti hingga yang paling parah hilang serta rusaknya barang bukti tersebut. Static Forensics merupakan salah satu jenis metode dari forensik digital yang memperoleh bukti digital dengan melakukan ekstraksi serta analisis setelah insiden terjadi, ataupun setelah sistem komputer dimatikan (post-incident). NIST Framework merupakan sebuah acuan proses pengambilan serta pengolahan bukti digital, yang dikembangkan oleh Lembaga National Institute of Standards and Technology. Hasil yang diperoleh dari analisis recovery bukti digital metode static forensics dipadu dengan framework NIST dapat diterapkan dengan baik dan optimal. Dilakukan 20 kali pengujian, dengan hasil akurasi recovery bukti digital mencapai 100% pada ketiga Devices. Oleh sebab tersebut, perpaduan antara metode, framework, serta tools yang terkait direkomendasikan untuk memproses kasus yang berkaitan dengan digital forensics khususnya proses recovery bukti digital.

Kata kunci: *Perangkat Penyimpanan USB, Static Forensics, NIST Framework*

[2] Abstract

The increase in the use of USB storage Devices tends to be massive & exponential due to various aspects, one of which is the size and affordable price of USB storage Devices. Currently, the quality of handling cybercrime in Indonesia is still minimal, starting with the problem of collecting evidence that tends to be incomplete, errors during the process of acquiring evidence to the most severe loss and damage to the evidence. Static Forensics is one type of digital forensics method that obtains digital evidence by extracting and analyzing it after an incident occurs, or after the computer system is turned off (post-incident). The NIST Framework is a reference for the digital evidence retrieval and processing process, which was developed by the National Institute of Standards and Technology. The results obtained from the analysis of digital evidence recovery using static forensics methods combined with the NIST framework can be applied properly and optimally. The test was carried out 20 times, with the results of the digital evidence recovery accuracy reaching 100% on the three Devices. Therefore, a combination of methods, frameworks and related tools is recommended to process cases related to digital forensics, especially the digital evidence recovery process.

Dokumen diterima pada 03 April, 2022
Dipublikasikan pada 26 Juni, 2022

Keywords: *USB Mass Storage, Static Forensics, NIST Framework*

1. Pendahuluan

Penggunaan perangkat digital meningkat secara signifikan di era digital seperti saat ini. Mayoritas pengguna perangkat digital, sangat familiar dengan perangkat penyimpanan *USB* yang memiliki beragam variasi seperti *USB Flash Drive*, *Micro Memory Card*, *Hard drive*, *Solid State Drive*, dsb. Peningkatan penggunaan perangkat penyimpanan *USB* cenderung massif & eksponensial disebabkan berbagai aspek, salah satunya ukuran dan harga perangkat penyimpanan *USB* yang terjangkau [1]. Forensik digital memiliki tujuan untuk membantu menemukan dan menganalisis fakta-fakta, serta membantu menganalisa bukti digital yang berkaitan tentang suatu insiden. Timeline sebuah peristiwa di sekitar suatu insiden yang sedang diselidiki merupakan salah satu aspek paling krusial dalam penyelidikan forensic [2]. Static Forensics merupakan salah satu jenis metode dari forensik digital yang memperoleh bukti digital dengan melakukan ekstraksi serta analisis setelah insiden terjadi, ataupun setelah sistem komputer dimatikan (post incident). Berbagai implementasi teknologi pada static forensics antara lain disk *imaging*, data *recovery* serta filtering information [3]. Walaupun diklaim sebagai sebuah metode yang tradisional, namun metode ini menawarkan perbandingan yang signifikan pada aspek ekstraksi bukti digital, analisis, penilaian serta kesesuaian terhadap prosedur hukum dibandingkan metode Live Forensics. Hal ini dikarenakan live forensics melakukan analisis saat sebuah sistem masih berjalan, aspek tersebut dapat menyebabkan integritas sebuah bukti digital berubah. Tentu saja membuat bukti digital tersebut tidak valid lagi [4]. Berbagai topik yang muncul di media terkait *cybercrime*, serta proses pengambilan barang bukti elektronik meliputi perangkat komputasi yang berupa *storage Devices* oleh penegak hukum terkait kian menjadi sorotan. Saat ini kualitas penanganan *cybercrime* di Indonesia masih minim, dimulai dengan masalah pengumpulan barang bukti cenderung tidak lengkap, kesalahan saat proses akuisisi barang bukti hingga yang paling parah hilang serta rusaknya barang bukti tersebut. Telah menjadi tugas investigator serta penegak hukum terkait untuk terus memperbaiki kinerja dalam bidang keilmuan ini dan tentu saja menemukan modus, motif serta siapa pelaku kejahatan dalam kasus tersebut [5]. Penelitian ini menguji 3 buah *device* yaitu *USB Flash Drive*, *USB* Hard Disk Drive serta *Micro Memory Card* yang dihubungkan dengan *USB Card Reader* menggunakan sebuah high-level digital forensic framework hasil pengembangan dari National Institute of Standards and Technology (NIST), yang dijalankan pada sistem operasi Windows dengan dibantu oleh Forensics Toolkit *Image*r. Berbagai penelitian yang linear sebelumnya telah dilakukan, terutama dari aspek kesamaan metode, framework serta beberapa *device* yang digunakan. Seperti dibawah ini:

Penelitian pertama dilakukan oleh Faiz, A. & Imam, R. pada tahun 2017 yang memiliki judul "Forensic Analysis of Frozen *Hard drive* Using Static Forensics Method". Penelitian tersebut melakukan proses akuisisi serta analisis bukti digital dengan menggunakan metode static forensics pada Frozen *Hard drive* di sistem komputer yang telah dimatikan (shutdown) sebelumnya. Hasil penelitian tersebut menyebutkan bahwa bukti-bukti digital seperti dokumen, gambar, log files, browser history ditemukan pada *unallocated space* di *Hard drive* terkait [6].

Penelitian berikutnya dilakukan oleh Riadi, I., Sunardi serta Hadi, A. yang berjudul "Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics". Penelitian tersebut dilakukan pada tahun 2019, penelitian ini melakukan analisis bukti digital pada SSD NVMe dengan menghidupkan fitur TRIM pada SSD tersebut. Penelitian ini mengklaim bahwa fitur TRIM pada SSD memiliki efek buruk pada proses tertentu saat dilakukan proses *recovery* pada bukti digital terkait [5].

Penelitian yang dilakukan pada tahun 2019 oleh Umar Rusidy & Sahiruddin dengan judul "Metode NIST Untuk Analisis Forensik Bukti Digital Pada Perangkat Android". Penelitian ini melakukan komparasi kinerja *tools* Wondershare dengan Oxygen yang bertujuan untuk melakukan *recovery* bukti digital pada sebuah *device* Smartphone. Framework dari NIST juga digunakan pada penelitian ini [7].

Fitriana Mulia, dkk, pada tahun 2020 melakukan penelitian yang berjudul "Penerapan Metode National Institute of Standards and Technology (NIST) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime". Penelitian ini berfokus pada prosedur digital forensic pada aplikasi Whatsapp yang bertujuan untuk mendapatkan bukti digital seperti daftar nomor kontak, sesi percakapan, serta foto profil yang telah dihapus dengan sengaja sebelumnya. Penelitian ini mengemukakan bahwa metode NIST yang telah diterapkan pada penelitian tersebut mempermudah dalam menemukan bukti digital pada *Devices* terkait [8].

Penelitian yang dilakukan oleh Imam Riadi dkk., pada tahun 2021. Yang berjudul "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS". Penelitian ini menjelaskan tentang proses analisis bukti digital menggunakan metode static forensics serta proses akuisisi hingga ekstraksi file yang mengandung steganografi di dalamnya. Dalam penelitian ini *Digital forensics* Research Workshop (DFRW) digunakan sebagai framework *digital forensics* [9].

2. Tinjauan Pustaka

2.1 *Digital forensics*

Merupakan disiplin ilmu ditujukan untuk melakukan identifikasi, mengumpulkan serta melakukan analisis bukti digital setelah serangan terjadi [10]. Ilmu ini memiliki tujuan untuk menentukan identitas pelaku tindak kriminal, tindakan apa yang mereka lakukan, bagaimana cara mereka melakukan serta apa motivasi mereka melakukan tindak kriminal tersebut [11]. *Digital forensics* juga bisa disebut sebuah metode yang berkaitan dengan kegiatan *recovery* serta proses penyelidikan pada sebuah bukti digital yang ditemukan [12]. Selama sebuah sistem computer menyimpan data, dan data tersebut menyimpan informasi serta dapat dijadikan barang bukti maka disitulah digital forensic diperlukan. Selama dua dekade terakhir digital forensic mulai meningkat secara signifikan popularitas di kalangan pemerintah dan lembaga penegak hukum [13].

2.2 Computer Forensic

merupakan sebuah ilmu turunan dari *digital forensics* yang bertujuan untuk mengumpulkan bukti elektronik, melakukan penyelidikan dan menyajikan bukti tersebut kepada Lembaga penegak hukum. Proses ini dilakukan secara teknis serta ilmiah untuk membuktikan kejahatan yang telah dilakukan [14]. Computer forensics juga mengacu dari sistem komputer yang disita dari Tempat Kejadian Perkara (TKP) untuk dianalisis dengan tujuan untuk menemukan bukti yang substansial oleh investigator. Tidak hanya bertujuan mengumpulkan bukti terkait tindak kriminal namun melakukan validasi terkait bukti tersebut agar bisa diterima secara legal menurut hukum di pengadilan [15] . Di dalam disiplin ini, ilmu pengetahuan dan hukum saling terintegrasi. Dengan kata lain bukti ilmiah terbaik tidak ada gunanya jika tidak valid dan dapat diterima di dalam pengadilan [16].

2.3 Static Forensics

Bisa disebut juga Dead Forensics, merupakan salah satu jenis metode dari forensik digital yang memperoleh bukti digital dengan melakukan ekstraksi serta analisis setelah insiden terjadi, ataupun setelah sistem komputer dimatikan (*post incident*) [3]. Sedangkan menurut Mamoona [4], *static forensics* merupakan pendekatan secara tradisional untuk melakukan proses forensic setelah diperolehnya *dump memory* pada sistem yang telah dimatikan sebelumnya. Metode ini digunakan

untuk menganalisa *external device* berbasis penyimpanan seperti *USB Flash Drive*, *USB Hard Disk Drive*, serta *Micro Memory Card*. Perangkat tersebut dapat dilihat pada Gambar 1, Gambar 2, serta Gambar 3 berikut :

Gambar 1. *USB Flash Drive*

Gambar 2. *USB* Hard Disk Drive

Gambar 3. *Micro Memory Card* + *Card Reader*

2.4 Digital Evidence

Merupakan sebuah istilah yang merujuk untuk sebuah data yang disimpan maupun dikirimkan melalui *Devices* tertentu, seperti personal computer (PC), laptop, smartphone dsb [17]. Bukti digital ini bersifat volatile, rapuh dan mudah terjadinya alterasi. Jika tidak diproses dengan cara yang tepat, alterasi yang terjadi pada bukti tersebut akan mengarah pada integritas bukti itu sendiri. Dan pada akhirnya bukti tersebut akan tidak berguna karena tidak valid menurut hukum [16].

2.5 Data *Recovery*

Data *recovery* adalah kegiatan yang berkaitan dengan pengambilan informasi yang dihapus secara sengaja maupun tidak sengaja saat terjadinya crash pada sebuah system [10].

2.6 NIST Framework

Merupakan framework yang diciptakan serta dikembangkan oleh Lembaga National Institute of Standards and Technology (NIST), digunakan untuk proses pengambilan serta pengolahan bukti digital [18]. Sebagaimana terlihat pada Gambar 4, framework ini memiliki 4 tahapan umum, yaitu [19] :

Gambar 4. NIST Framework

2.6.1 Collection

Proses identifikasi, melakukan labeling, serta mengambil data dari sumber data yang relevan. Dengan mengikuti standar prosedur untuk menjaga integritas data tersebut.

2.6.2 Examination

Berkaitan dengan proses pengecekan data yang telah diperoleh dari tahap sebelumnya dengan mengikuti prosedur untuk tetap menjaga integritas data. Proses ini bisa dilakukan dengan cara otomatis maupun manual.

2.6.3 Analysis

Melakukan analisis dari hasil pemeriksaan sebelumnya. Tahap ini dilakukan menggunakan Teknik yang tepat secara legal, untuk mengetahui secara valid informasi yang terkandung di dalam bukti digital tersebut.

2.6.4 Report

Merupakan tahap terakhir yang berkaitan dengan proses pelaporan, penyajian serta rekomendasi tambahan terkait proses investigasi yang telah dilakukan. Hasil investigasi termasuk laporan tertulis untuk dokumentasi serta aspek lain terkait proses *forensic*.

2.7 *USB* Mass Storage

Merujuk kepada dua istilah yang berkesinambungan, Universal Serial Bus (*USB*) merupakan sebuah standar perangkat interface yang digunakan untuk penghubung perangkat peripheral seperti keyboard, mouse, flash drive scanner dsb. *USB* digunakan karena aspek kemudahan dalam penggunaan serta konektivitas yang tinggi [20].

3 Metode Penelitian

3.1 Alat dan Bahan

Alat serta bahan yang dibutuhkan pada penelitian ini ditampilkan pada Tabel 1 sebagai berikut :

Tabel 1. Alat dan Bahan Penelitian

Nama *Device*	Detail	Keterangan
Workstation	Lenovo IS3, 8GB RAM, 512 SSD, Windows 10 Pro.	*Hardware + Operating System*
USB Flash Drive	Sony, 16 GB	*Hardware*
USB Hard drive	Seagate, 128 GB	*Hardware*
Micro Memory Card + Card Reader	Vgen, 8GB + Roker Card Reader	*Hardware*
FTK *Image*r	Versi	*Software Tools*
HashTab	Versi	*Software Tools*
Microsoft Office	Word, Powerpoint, Excel	*Software Tools*

3.2 Alur Penelitian

Alur utama penelitian dapat dilihat pada Gambar 5 dibawah ini:

Gambar 5. Alur Utama Penelitian

Skenario dilakukan dengan menyiapkan *USB* Mass Storage yang telah diisi beberapa bukti digital berupa berbagai file yang memiliki ekstensi berbeda di dalamnya, kemudian bukti tersebut akan dihapus permanen dengan perintah (Shift + Delete) lalu dilanjutkan proses koleksi pada tahap selanjutnya.

Tahap koleksi dibantu dengan *tools* Forensics Toolkit *Image*r untuk melakukan *imaging* bukti digital, melakukan labeling pada *Devices* terkait serta proses ekstraksi sekaligus menggunakan *USB* Write Blocker untuk menjaga integritas bukti digital tetap valid dan tidak berubah ketika proses *imaging* berlangsung.

Berikutnya tahap eksaminasi, hasil *imaging* akan diperiksa secara menyeluruh dengan menggunakan bantuan *tools* FTK *Image*r, proses pencarian bukti digital ini dilakukan pada masing-masing *USB* mass *storage Devices* tersebut hingga ditemukan bukti digital.

Tahap analisis ini merupakan tahap validasi bukti digital dari proses sebelumnya. Setelah bukti digital ditemukan, perlu adanya pengecekan pada nilai hash, ekstensi file, serta kapan file tersebut terakhir dimodifikasi (timestamp).

Tahap terakhir menjabarkan tentang proses pembuatan report dari hasil analisis yang telah dilakukan beberapa tahap sebelumnya. Dalam konteks penelitian ini, report akan berupa laporan tertulis serta tabel persentase akurasi dengan menggunakan persamaan matematika (1) sebagai berikut:

$$P = \frac{\sum dr}{\sum dv} \times 100\% \quad (1)$$

P : Persentase (%)
∑dr : Jumlah data *recovery*
∑dv : Jumlah data asli yang valid

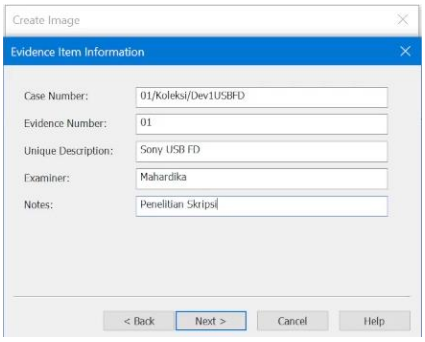
4 Hasil dan Pembahasan

4.1 Skenario

Proses pelaksanaan skenario penelitian dilakukan dengan menggunakan 3 *Devices* yaitu *USB Flash Drive*, *USB* Hard Disk Drive, serta *Micro Memory Card*. *Devices* tersebut memiliki spesifikasi seperti pada Tabel 3.1. Sebelum melakukan penghapusan file secara permanen dengan perintah Shift + Delete, dilakukan pengecekan hash MD5 pada setiap file yang akan dihapus sebagai bukti validasi file. Total file eksperimen berjumlah 35 files dengan 7 ekstensi berbeda.

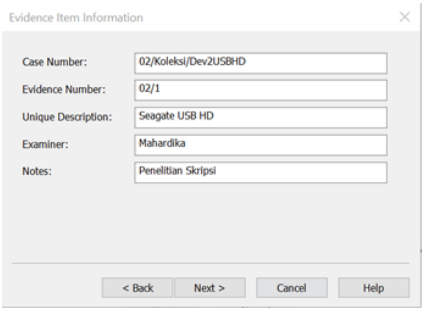
4.2 Koleksi

Pada tahap ini diperlukan waktu 13 menit 11 detik untuk melakukan *imaging* terhadap *USB Flash Drive*. Salah satu proses *imaging* tersebut berkaitan dengan melakukan labeling pada *device* yang digambarkan pada Gambar 6 dibawah ini :



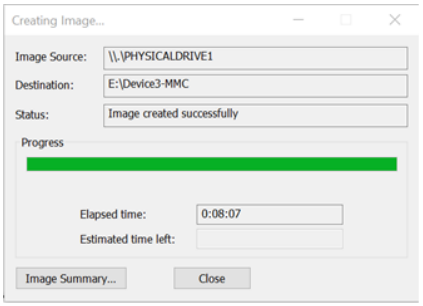
Gambar 6. Labelling *USB Flash Drive*

Pada pengujian tahap ini diperlukan waktu 1 jam 6 menit 7 detik untuk melakukan *imaging* terhadap *USB* Hard Disk Drive. Berikutnya proses labeling pada *device* ini dilakukan, berikut Gambar 7 merupakan tampilan label pada *device* tersebut.



Gambar 7. Labelling *USB* Hard Disk Drive

Selanjutnya, dibutuhkan waktu 8 menit 7 detik untuk melakukan *imaging* terhadap *Micro Memory Card* pada pengujian pertama. Dapat dilihat pada Gambar 8 berikut:

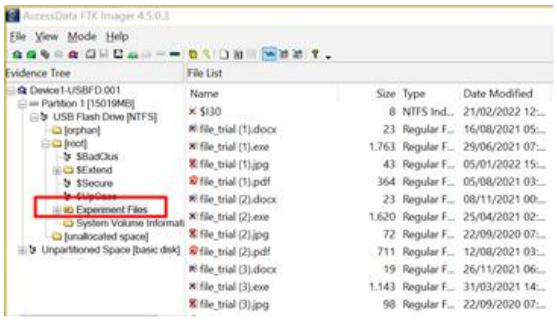


Gambar 8. *Imaging Micro Memory Card*

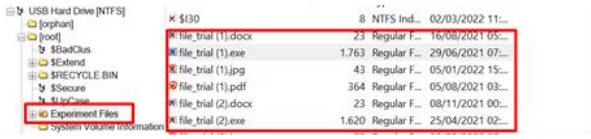
Setelah proses *imaging* selesai, ditampilkan hasil verifikasi *image* pada *device* tersebut. Pada hasil tersebut nilai hash harus *match*, agar terciptanya bukti digital yang valid.

4.3 Eksaminasi

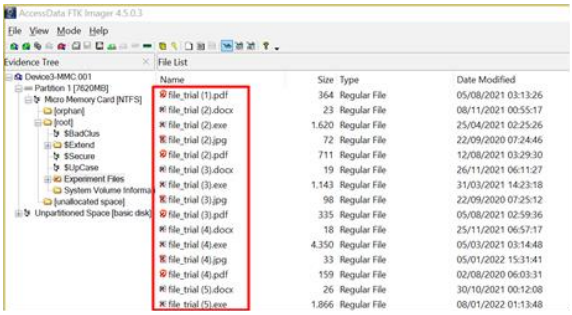
Dengan bantuan *tools* FTK *Image*r, *evidence image* diakses pada setiap *Devices* yang telah di proses pada tahap sebelumnya untuk mencari bukti digital. Pada *evidence image* tersebut ditemukan sebuah *folder* yang telah terhapus, berisikan files eksperimen yang berkaitan dengan skenario. Tampilan *evidence image* pada 3 *Devices* yang diuji dapat dilihat pada, Gambar 9, Gambar 10, dan Gambar 11 dibawah ini :



Gambar 9. *Evidence image USB Flash Drive*



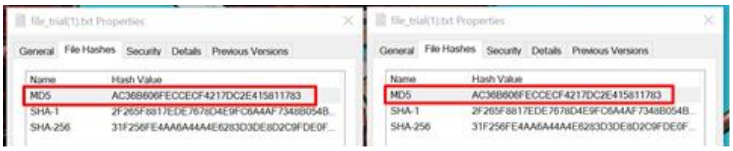
Gambar 10. *Evidence image USB* Hard Disk Drive



Gambar 11. *Evidence image Micro Memory Card*

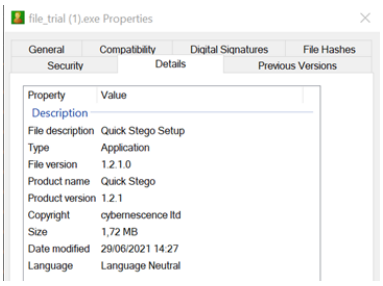
4.4 Analisa

Setelah melakukan pemeriksaan serta kalkulasi dengan seksama pada 3 *evidence image* sebelumnya, ditemukan bahwa *folder* yang terindikasi terhapus tersebut berisi 35 file dengan 7 ekstensi yang berbeda. Pada Gambar 12 diperlihatkan komparasi hash pada *USB Flash Drive*, sisi kiri merupakan properties file hasil ekstraksi sedangkan sisi kanan merupakan properties file asli sebelum dihapus saat eksperimen. Karena tidak adanya proses alterasi ketika skenario dibuat, kedua hash pada file tersebut *match* dan tidak ada indikasi rusaknya integritas file tersebut.



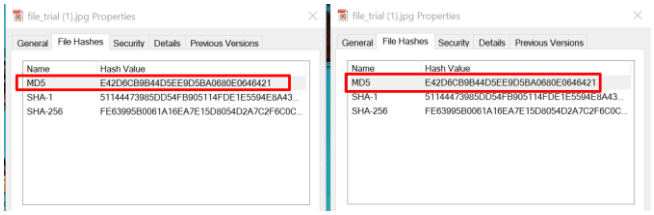
Gambar 12. Komparasi Hash File Pada *USB Flash Drive*

Pada Gambar 13 terlihat bahwa file_trial(1) yang memiliki ekstensi .exe, berukuran 1,72 MB dengan software version 1.2.1.0. Hal tersebut merupakan metadata dari file_trial(1) yang ada pada *evidence image USB* Hard Disk Drive.



Gambar 13. Metadata File pada *USB* Hard Disk Drive

Pada Gambar 14 terlihat komparasi hash file yang ditemukan pada *device Micro Memory Card*. Pada komparasi tersebut, terlihat bahwa hash file sama persis dan tidak ada indikasi adanya alterasi.



Gambar 14. Komparasi Hash File Pada *Micro Memory Card*

4.5 Pelaporan

Berdasarkan dari hasil bukti digital yang telah di *recovery* menggunakan bantuan *tools* FTK *Image*r di 3 *device* yang berbeda, didapatkan rerata hasil waktu *imaging* pada *device* 1 sebesar 816 detik, dengan file bukti *recovery* 35 files. Untuk *device* 2 didapatkan rerata hasil waktu *imaging* 3991 detik dengan file bukti *recovery* 35 files. Sedangkan pada *device* 3 didapatkan rerata hasil waktu *imaging* 472 detik, dengan file bukti *recovery* yang sama dengan kedua *device* sebelumnya. Hasil rangkuman *recovery* dapat dilihat pada Tabel 2 dan Tabel 3 dibawah ini:

Tabel 2. Rangkuman *Recovery* File

Device	**Ekstensi File**	**Jumlah Pengujian**	**File Bukti *Recovery* (File)**	**File Bukti Asli (File)**
USB Flash Drive (16 GB)	docx, pdf, txt, xlsx, exe, jpg, mp3	20	35	35
USB Hard drive (128 GB)	docx, pdf, txt, xlsx, exe, jpg, mp3	20	35	35
Micro Memory Card (8 GB)	docx, pdf, txt, xlsx, exe, jpg, mp3	20	35	35

Tabel 3. Waktu *Imaging Devices*

Keterangan	***Device* 1 (16 GB)**	***Device* 2 (128 GB)**	***Device* 3 (8 GB)**
Rerata Waktu *Imaging* (Detik)	816	3991	472
Maksimum Waktu *Imaging* (Detik)	840	4022	491
Minimum Waktu *Imaging* (Detik)	791	3886	450
Total Waktu *Imaging* (Detik)	16318	79825	9438

Pada Gambar 15, Gambar 16, serta Gambar 17 dibawah ini menunjukkan perhitungan akurasi *recovery* files bukti digital pada masing – masing *device* terkait:

- *Device* 1 – *USB Flash Drive*

$$P = \frac{35}{35} \times 100\% = 100\%$$

Gambar 15. Perhitungan Akurasi *Device* 1

- *Device* 2 – *USB Hard drive*

$$P = \frac{35}{35} \times 100\% = 100\%$$

Gambar 16. Perhitungan Akurasi *Device* 2

- *Device* 3 – *Micro Memory Card*

$$P = \frac{35}{35} \times 100\% = 100\%$$

Gambar 17. Perhitungan Akurasi *Device* 3

5 Kesimpulan

Dari hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa *recovery* bukti digital metode static forensics dipadu dengan framework NIST dapat diterapkan dengan baik dan optimal. Dilakukan 20 kali pengujian pada setiap *device* dengan dibantu oleh *tools* FTK *Image*r, akurasi *recovery* bukti digital mencapai nilai 100% pada ketiga *device* yang diuji. Hal tersebut ditampilkan pada Gambar 15 hingga Gambar 17. Perpaduan metode, framework, serta *tools* yang terkait direkomendasikan untuk pemeriksaan kasus yang berkaitan dengan *digital forensics* khususnya proses *recovery* bukti digital.

Daftar Pustaka

[1] W. D. A. Chirath and L. Rupasinghe, "Comprehensive Forensic Data Extraction and Representation System for Windows Registry," *2019 Int. Conf. Adv. Comput. ICAC 2019*, pp. 346–350, 2019, doi: 10.1109/ICAC49085.2019.9103417.

[2] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4I - *Digital forensics* framework for reviewing and investigating cyber attacks," *Array*, vol. 5, no. December 2019, p. 100015, Mar. 2020, doi: 10.1016/j.array.2019.100015.

[3] Y. M. Song and K. S. Kwak, *Electronics, Information Technology and Intellectualization*. CRC Press, 2015.

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

[5] I. Riadi, Sunardi, and A. Hadi, "Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics," *CoreIT*, vol. 3321, no. 2, pp. 1–8, 2019.

[6] A. Faiz and R. Imam, "Forensic Analysis of Frozen *Hard drive* Using Static Forensics Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 1, 2017.

[7] R. Umar and Sahiruddin, "Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android," *Pros. SENDU_U_2019*, pp. 978–979, 2019.

[8] M. Fitriana, K. A. AR, and J. M. Marsya, "PENERAPANA METODE NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PENANGANAN CYBER CRIME," *Cybersp. J. Pendidik. Teknol. Inf.*, vol.

4, no. 1, p. 29, Jul. 2020, doi: 10.22373/cj.v4i1.7241.

[9] R. Sistem *et al.*, "JURNAL RESTI Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi," vol. 1, no. 10, pp. 2–6, 2021.

[10] J. Kizza and F. Migga Kizza, "Digital Evidence and Computer Crime," in *Securing the Information Infrastructure*, IGI Global, 2008, pp. 298–317.

[11] J.-P. Van Belle, "Anti-Forensics: A Practitioner Perspective," *Int. J. Cyber-Security Digit. Forensics*, vol. 4, no. 2, pp. 390–403, 2015, doi: 10.17781/P001593.

[12] M. Abdulhamid, S. E. E. Profile, V. O. Waziri, S. E. E. Profile, S. E. E. Profile, and S. E. E. Profile, "Cyber Crimes Analysis Based-On Open Source *Digital forensics Tools* Some of the authors of this publication are also working on these related projects : Nature Inspired Meta-heuristic Algorithms for Deep Learning : Recent Progress and Novel Perspective Vie," no. July 2016, 2013.

[13] N. Kishore, C. Gupta, and D. Dawar, "An Insight View of *Digital forensics*," *Int. J. Comput. Sci. Appl.*, vol. 4, no. 6, pp. 89–96, Dec. 2014, doi: 10.5121/ijcsa.2014.4608.

[14] M. Gül and E. Kugu, "A survey on anti-forensics techniques," *IDAP 2017 - Int. Artif. Intell. Data Process. Symp.*, 2017, doi: 10.1109/IDAP.2017.8090341.

[15] A. Jain and G. S. Chhabra, "Anti-forensics techniques: An analytical review," in *2014 Seventh International Conference on Contemporary Computing (IC3)*, Aug. 2014, pp. 412–418, doi: 10.1109/IC3.2014.6897209.

[16] J. Sammons, *The Basics of Digital forensics - Second Edition [2015][UnitedVRG]*. .

[17] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017.

[18] R. Umar, I. Riadi, and B. F. Muthohirin, "Live forensics of *tools* on android *Devices* for email forensics," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 17, no. 4, p. 1803, Aug. 2019, doi: 10.12928/telkomnika.v17i4.11748.

[19] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.

[20] D. He, N. Kumar, J. H. Lee, and R. Sherratt, "Enhanced three-factor security protocol for consumer *USB* mass *storage Devices*," *IEEE Trans. Consum. Electron.*, vol. 60, no. 1, pp. 30–37, 2014, doi: 10.1109/TCE.2014.6780922.