CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 1, Mei 2024,, hlm. 18-24

Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)

Aidil Wijaya Kusuma[1], Erick Irawadi Alwi[2], Ramdaniah Ramdaniah[3]

[1.2.3]Program Studi Teknik Informatika, Universitas Muslim Indonesia
Email: [1]aidilwijaya84@gmail.com, [2]erick.alwi@umi.ac.id, [3]ramdaniah@umi.ac.id

Abstrak

Dalam perkembangan teknologi digital yang semakin pesat, analisis bukti digital menjadi semakin penting dalam mendukung penegakan hukum dan mengamankan ranah keamanan siber. Proses analisis bukti digital melibatkan pemeriksaan terhadap berbagai informasi digital yang ditemukan dalam investigasi kejahatan atau kasus hukum. Bukti digital tersebut dapat berupa file, pesan teks, email, rekaman panggilan, atau data lainnya yang terdapat dalam perangkat digital seperti komputer, ponsel, dan tablet. Penelitian ini membahas tentang bagaimana memperoleh, mengambil, melestarikan, dan menyajikan data atau informasi tentang jejak aktivitas kasus cybercrime yang terdapat pada media penyimpanan flash disk yang telah dihapus dan bertujuan untuk mendukung penyelidikan terhadap pelaku kejahatan dengan menerapkan prinsip-prinsip forensik digital. Pada penelitian ini menggunakan metode National Institute of Standards dan Technology (NIST) dan menggunakan FTK Imager sebagai tool forensic dan Autopsy sebagai tools analisis dan juga recovery data serta HashGenerator untuk mengecek hasil hash dari tiap-tiap file. Dari hasil analisis yang telah dilakukan, didapatkan file-file yang telah dihapus oleh pelaku dengan perlakuan yang berbeda-beda pada media penyimpanan flash disk menggunakan tools forensik FTK Imager, Autopsy, dan juga HashGenerator, dimana tool Autopsy berhasil mendapatkan metadata file-file yang dihapus pada tanggal yang sama dengan tanggal pelaporan. Perbedaan dari masing-masing perlakuan penghapusan terdapat terdapat pada perlakuan ketiga yaitu dengan perintah quick format dimana nama file yang terhapus berubah menjadi nama file yang berbeda seperti nama file aslinya. Selain itu size dan nilai hash pada semua file pada tiap-tiap perlakuan tidak menunjukkan adanya perubahan pada nilai hash MD5-nya yang menandakan bahwa file-file tersebut tidak ditemukan adanya perubahan.

Kata kunci: kejahatan siber, bukti digital, NIST, digital forensik, *flash disk, forensic tools.*

Analysis Of Digital Evidence On Flash Disk Storage Media Using The National Institute Of Standards And Technology (NIST) Method

Abstract

In the rapid advancement of digital technology, the analysis of digital evidence has become increasingly vital in supporting law enforcement and securing the realm of cybersecurity. The process involves scrutinizing various digital information found in criminal investigations or legal cases. Digital evidence can encompass files, text messages, emails, call recordings, or other data within digital devices such as computers, phones, and tablets. This research delves into the acquisition, retrieval, preservation, and presentation of data or information related to traces of cybercrime activities found on deleted flash disk storage media. The aim is to support investigations into criminal perpetrators by applying principles of digital forensics. The study utilized the National Institute of Standards and Technology (NIST) methodology, employing FTK Imager as a forensic tool, Autopsy for analysis and data recovery, and HashGenerator to verify the hash results of each file. From the analysis conducted, various files deleted by the perpetrator were discovered on the flash disk storage media, subjected to different treatments using forensic tools FTK Imager, Autopsy, and HashGenerator. Autopsy successfully retrieved metadata of the deleted files on the same date as the reporting date. Notable differences were observed among the deletion methods. Particularly, in the third method involving quick format, the deleted filenames were altered to different names similar to their original names. Additionally, the size and hash values of all files for each deletion method showed no alterations in their MD5 hash values, indicating that no changes had occurred to these files.

***Keywords**: Cybercrime, Digital Evidence, NIST, Digital Forensics, Flash Disk, Forensic Tools.*

1. PENDAHULUAN

Perkembangan yang cepat dalam teknologi telah mengalami perubahan dalam ranah perangkat lunak (*software*), perangkat keras (*hardware*), dan juga perilaku pengguna (*brainware*). Penggunaan teknologi ini membawa sejumlah dampak positif dan negatif dalam rutinitas penggunaannya (Hasa, Yudhana and Fadlil, 2019). Teknologi memberikan manfaat positif dengan mempermudah individu atau kelompok dalam menjalankan aktivitasnya, namun dampak negatifnya timbul saat teknologi disalahgunakan oleh individu atau kelompok untuk melakukan kejahatan siber (*cybercrime*), yang dapat merugikan orang lain (Riskiyadi, 2020).

Cybercrime merujuk pada tindakan kriminal yang dilakukan oleh individu atau sekelompok orang dengan menggunakan komputer atau internet. *Cybercrime* juga mencerminkan efek buruk dari kemajuan teknologi yang dapat menyebabkan kerugian yang signifikan di berbagai aspek kehidupan modern saat ini (Fitriana, AR and Marsya, 2020).

Berdasarkan penelitian terdahulu mengenai analisis bukti digital, *tools* yang digunakan dalam penelitian yang digunakan yaitu *tools* yang lazim dalam melakukan proses analisis dan *recovery* data dan menerapkan satu skenario proses dimana barang bukti yang dimasukkan ke dalam *flash disk* bermacam-macam oleh pelaku *cybercrime*. Pada gambaran skenario kasus dalam penelitian dilakukan tiga perlakuan dalam proses penghapusan data yaitu menggunakan perintah *delete, shift+delete, dan quick format* dan meskipun metode-metode penghapusan tersebut diterapkan, kemungkinan besar bukti digital yang relevan untuk proses investigasi dalam kasus kejahatan siber masih bisa dipulihkan.

Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi dan menganalisis metode yang efektif dalam memperoleh, mengambil, melestarikan, dan menyajikan data terkait aktivitas cybercrime yang terdapat pada media penyimpanan flash disk yang telah dihapus. Penelitian ini akan menerapkan prinsip-prinsip forensik digital dengan menggunakan metode National Institute of Standards and Technology (NIST) dan alat forensik seperti FTK Imager dan Autopsy. Dengan demikian, diharapkan hasil penelitian ini dapat memberikan kontribusi signifikan terhadap proses investigasi kejahatan siber, serta meningkatkan pemahaman tentang bagaimana bukti digital dapat dipulihkan meskipun telah dihapus oleh pelaku. Perubahan ini menekankan tujuan penelitian dan relevansinya dengan latar belakang masalah yang telah dijelaskan sebelumnya, serta menyoroti pentingnya penerapan metode NIST dalam konteks analisis bukti digital.

2. TINJAUAN PUSTAKA

Bukti terkait kejahatan siber dapat berupa perangkat elektronik sebagai benda fisik atau file digital yang memuat informasi terkait. Barang bukti elektronik mencakup perangkat keras yang terlibat dalam kejahatan seperti *Hard Disk Drive*, *Flash Disk*, *Compact Disk*, *Memori SD*, dan lainnya, sementara barang bukti digital melibatkan berkas dokumen, catatan *history*, atau *log* yang memuat informasi terkait perbuatan kriminal (Maniar and Yuniati, 2023).

Peningkatan industri *cybercrime* tidak hanya didorong oleh perkembangan teknologi informasi dan berbagai peralatan elektronik, tetapi juga oleh kegiatan *blackmarket*. *Blackmarket* merupakan lingkungan di mana berbagai pelaku dapat berinteraksi secara ekonomi untuk memperoleh layanan, alat, atau infrastruktur yang digunakan dalam tindak kejahatan siber. Keterlibatan berbagai pihak dalam *blackmarket* menyulitkan identifikasi kegiatan kejahatan dan data yang dihasilkannya, memperumit proses penanganan kejahatan siber yang membutuhkan teknik analisis yang lebih maju (Iman, Susanto and Inggi, 2020).

Forensik digital adalah disiplin ilmu yang digunakan dalam konteks hukum untuk mengumpulkan bukti digital yang sah yang dapat digunakan dalam pengungkapan dan penuntutan kejahatan komputer. Tujuannya adalah untuk mendukung upaya hukum dengan bukti yang dapat dipertanggungjawabkan secara digital (Azizah, Ramadhona and Gustitio, 2020). Forensik digital juga didefinisikan sebagai "pengetahuan ilmiah dan metode yang diterapkan untuk *identification, collection, preservation, examination*, dan *analysis* bukti digital dengan cara yang dapat diterima untuk diterapkan dalam masalah hukum" (Riadi, Fadlil and Aulia, 2021).

Melihat pentingnya validitas suatu barang bukti digital, penelitian ini akan melakukan investigasi kasus forensik pada flash disk, untuk melihat valid atau tidaknya bukti digital pada flash disk. Investigasi forensik dilakukan dengan menggunakan metode Forensic Process berdasarkan standar NIST. Penelitian ini juga melibatkan pemanfaatan dan perbandingan hasil dari berbagai alat analisis, yaitu penggunaan Autopsy dan Access Data imager FTK. Penerapan metode yang akan diteliti dapat memberikan hasil yang sangat jelas dan akurat terhadap bukti digital. Penelitian ini dilakukan untuk mengetahui bahwa alat bukti digital berdasarkan temuan penyidikan dapat menjadi alat atau alat bukti yang valid dan mendukung proses persidangan. Misalnya dalam penyidikan terdapat hal-hal yang mendukung bukti digital yang dapat memberatkan hasil putusan di mata hukum(Zamsari and Wahyono, 2024).

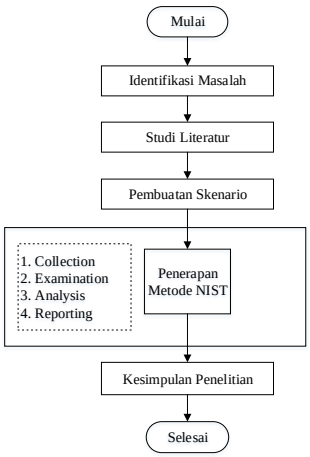
Namun demikian penelitian yang berbasis live forensic tersebut belum banyak membahas bagaimana risiko memodifikasi data selama proses pengumpulan dan kebutuhan untuk alat dan keahlian

khusus untuk(Agustiono, Suci and Prastiti, 2024)memastikan integritas dan keakuratan data yang dikumpulkan. Live forensic kurang cocok untuk analisis kejahatan carding yang biasanya melibatkan data penting seperti nomor kartu kredit, informasi identitas, dan transaksi keuangan yang sering kali disimpan di media penyimpanan permanen seperti hard drive atau flash drive. Data pada media penyimpanan ini umumnya tidak berubah meskipun sistem dimatikan, sehingga lebih efektif diakses melalui dead forensic. Teknik dead forensic ini juga memungkinkan untuk mengakses, memulihkan, dan menganalisis data yang dihapus atau disembunyikan, yang sering kali merupakan bagian penting dari bukti dalam kasus carding(Agustiono, Suci and Prastiti, 2024).

Untuk itu, penelitian ini akan melakukan analisa kinerja dari aplikasi autopsy dalam mencari dan mengembalikan data yang telah dihapus dari media penyimpanan berupa flashdisk. Instrumen penilaian akan dilakukan dengan melihat seberapa banyak file yang dapat dikembalikan dengan aplikasi tersebut dan dinyatakan identik oleh aplikasi Hash Compare. Dalam penelitian sebelumnya, seperti [9] dilakukan uji coba menggunakan file type JPG, PNG, DOCX, dan PDF, maka pada penelitian ini akan dilengkapi dengan total 70 berkas sebagai bahan uji coba, yaitu berkas dengan ekstensi DOCX, XLSX, MP3, MP4, TXT, PDF dan PNG masing-masing sebanyak 10 berkas. Penelitian juga akan dilakukan dengan menerapkan metode NIST SP 800-86(Julian and Sutabri, 2023).

Studi mengenai pemeriksaan bukti digital pada media penyimpanan telah banyak dilakukan oleh peneliti. Diantaranya adalah penelitian pada media penyimpanan *Optical Drive* menggunakan metode NIST dengan bantuan beberapa *tools* dengan hasil yang didapatkan adalah hasil akuisisi dengan FTK Imager berhasil memulihkan 10 file dengan nilai *hash* yang sesuai, sementara *Autopsy* hanya mampu mengakuisisi 7 file dan tidak menemukan 3 file dengan ekstensi *.MOV, *.exe, dan *.rar (Riadi, Fadlil and Aulia, 2021).

3. METODOLOGI



Gambar 1. Tahapan Penelitian

Pada tahapan penelitian berisi tahapan atau langkah-lagkah yang akan dilakuan yang disususn secara sistematis. Adapun tahapan penelitian sebagai berikut:

3.1. Identifikasi Masalah

Pada tahap identifikasi masalah, dilakukan identifikasi masalah sesuai dengan latar belakang dimana kasus penyalahgunaan teknologis digital telah meningkat dalam beberapa tahun terakhir seperti peretasan (*hacking*), penipuan online, pencurian data, dan lain-lain, seringkali melibatkan penggunaan *flashdisk* sebagai media penyimpanan atau alat tracnsfer data.

Studi Literatur

Pada tahapan ini, dilakukan *literatur review* dengan cara mengumpulkan informasi dari berbagai penelitian sebelumnya mengenai forensik digital sebagai acuan dari berbagai sumber. Hasil dari riset tersebut menjadi acuan dalam merencanakan atau merancang skenario pada penelitian ini.

Data yang digunakan pada penelitian ini adalah data sekunder dikarenakan pada penelitian ini menggunakan sebuah ilustrasi pada skenario yang telah dirancang sebelumnya. Data yang digunakan sebagai ilustrasi pada skenario ini adalah file dengan ekstensi docx, xlsx, pptx dan pdf yang dimasukkan ke dalam media penyimpanan *flash disk.*

3.2. Pembuatan Skenario

Pemilihan skenario kasus kejahatan siber terkait dengan salah satu jenis pelanggaran terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang melibatkan pencurian data/*cybertheft* dimana pelaku melakukan pencurian data sensitif dari perusahaan untuk keuntungan pribadi.

Penelitian ini sesuai dengan skenario simulasi penelitian dimana skenario dari seorang tersangka yang sebelumnya merupakan karyawan Perusahaan PT InginNaikKeRadiant, telah melakukan tindakan pencurian data sensitif dari sistem perusahaan untuk keuntungan pribadi. Tersangka menggunakan tiga buah *flash disk* sebagai alat untuk menyalin dan mengambil data tersebut. Berdasarkan tindakan *cybercrime* tersebut telah dilakukan penyitaan alat bukti eletronik diantaranya berupa *flash disk* dengan penyimpanan 8GB, 16GB, dan 32GB, yang selanjutanya dijadikan simulasi dalam penelitian ini. Pelaku tindakan *cybercrime* pada umumnya dalam melakukan aksinya melakukan penghapusan permanen atas file yang digunakan dalam melakukan tindakannya dengan tujuan untuk menghilangkan jejak kejahatan.

Flash disk sebagai simulasi dalam penelitian ini sebelumnya dilakukan *quick format* menggunakan *file system* NTFS, selanjutnya *flash disk* diisi dengan beberapa file berekstensi docx, xlsx, dan juga pdf. Selanjutnya ketiga *flash disk* tersebut dilakukan tiga buah perlakuan yang

berbeda. Perlakuan pertama yaitu *flash disk* menggunakan perintah *delete* biasa pada proses penghapusannya. Perlakuan kedua yaitu menggunakan perintah (*shift+delete*) dalam proses penghapusan permanen file. Dan perlakuan ketiga yaitu dengan melakukan *quick format* menggunakan *file system* NTFS, kemudian dilakukan *imaging* data secara *physical drive* dari *flash disk* yang menjadi target menggunakan FTK *Imager*. Pemilihan proses *imaging* data dalam bentuk *physical drive* dilakukan agar semua informasi yang ada dalam *flash disk* dapat diwakili dan disimpan dalam hasil *imaging*. Lalu dilakukan analisa atas hasil *imaging* data tersebut dengan menggunakan *tools Autopsy* serta mengecek dan juga melakukan *recovery* terhadap file yang sebelumnya terformat.

3.3. Penerapan Metode NIST

1. Collection

Pada tahapan ini, dilakukan duplikasi barang bukti fisik menjadi format digital untuk menjaga integritas bukti dari perubahan. Proses ini, melibatkan pemeliharaan barang bukti fisik serta pembuatan salinan dalam bentuk file *image*, atau dikenal dengan akuisisi dengan menggunakan *tool* forensik FTK *Imager*.

2. Examination

Tahap *examination* atau tahap pemeriksaan dilakukan ekstraksi data dari hasil *image* untuk memastikan data digital di dalamnya sama dengan barang bukti fisik. Proses ini bertujuan untuk memverifikasi keaslian data yang diambil dan melakukan validasi dengan melakukan *hashing* pada hasil *image* tersebut.

3. Analysis

Pada tahapan analisis, dilakukan pemeriksaan rinci terhadap barang bukti digital yang diperoleh dari proses *examination*. Bukti tersebut dianalisis sesuai dengan laporan kejahatan untuk mengungkap kasus kejahatan dengan menerapkan metode NIST (*National Institute of Standards and Technology*) yang ilmiah dan dapat diandalkan secara hukum.

4. Reporting

Tahapan terakhir yaitu pembuatan laporan dari proses pemeriksaan dan analisis barang bukti digital. Laporan ini merangkum dan menjelaskan alat yang digunakan, serta metodologi yang diterapkan dalam analisis.

3.4. Kesimpulan

Penarikan kesimpulan mengenai penelitian, yaitu analisis bukti digital yang didapatkan melalui barang bukti digital pada skenario yang telah dibuat Dengan memanfaatkan *tools* forensik dan menerapkan metode *National Institute of Standards and Technology*.

4. HASIL DAN PEMBAHASAN

4.1. Deskripsi Data

Dalam kasus ini bukti digital yang didapatkan bukti elektronik yang digunakan pelaku untuk melakukan kejahatannya yaitu berupa tiga buah *flash disk* dengan kapasitas penyimpanan 8GB, 16GB, dan 32GB. Untuk keterangan spesifikasi dari *flash disk* dapat dilihat pada gambar 2.

Gambar 2. Barang Bukti Elektronik yang Ditemukan

Tabel 1. Spesifikasi Barang Bukti

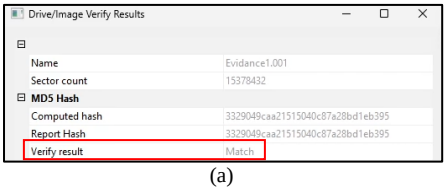
Bukti Digital	Merk	Spesifikasi	Keterangan
Flash Disk	Adata	8 Gb Storage	Barang Bukti Elektronik
Flash Disk	Kingston	16 Gb Storage	Barang Bukti Elektronik
Flash Disk	Sandisk	32 Gb Storage	Barang Bukti Elektronik

4.2. Collection

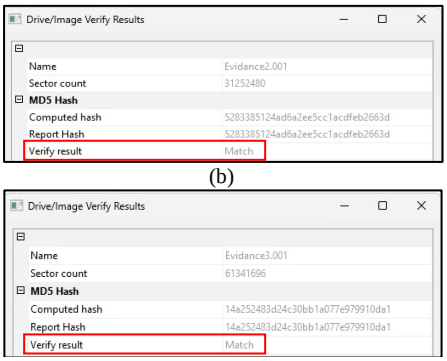
Pada tahap ini dilakukan duplikasi barang bukti fisik menjadi format digital untuk menjaga integritas bukti dari perubahan. Proses ini, melibatkan pemeliharaan barang bukti fisik serta pembuatan salinan dalam bentuk file *image*, atau dikenal dengan akuisisi dengan menggunakan tool forensik FTK *Imager*.

4.3. Examination

Tahap *examination* dilakukan untuk mengekstrak hasil dari *image* agar data digital yang terdapat di dalamnya identik dengan barang bukti fisik. Proses ini bertujuan untuk memeriksa integritas sumber data untuk mempertahankan integritas sumbernya agar tidak terjadi perubahan baik secara fisik maupun digital. Pada hasil akhir *imaging* dari *flash disk* dengan tool FTK *Imager* akan muncul *Drive/Image Verify Result* yang menampilkan nilai *hash* dari *flash disk* dan juga *verify result* yang akan menampilkan hasil pencocokan nilai *hash* dari *flash disk* yang telah selesai dilakukan proses *imaging*.



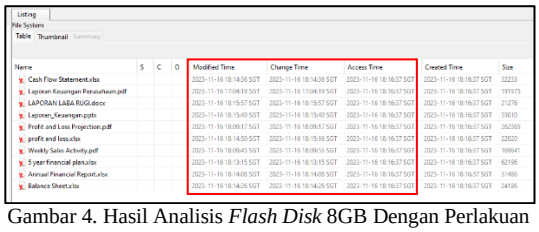
(a)



Gambar 3. Hasil *Hash* File *Imaging Flash Disk* (a) 8GB, (b) 16GB, (c) 32GB

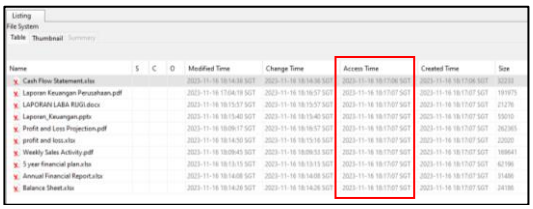
4.4. Analisis

Dalam tahap analisis, dilakukan pemeriksaan menyeluruh terhadap bukti digital yang diperoleh dari proses *examination*. Analisis bukti digital ini dilakukan dengan mempertimbangkan laporan kejahatan yang ada, dengan tujuan mengungkap kasus tindak kejahatan melalui pendekatan ilmiah yang sesuai dan dapat diandalkan dari segi hukum. Dalam proses ini hasil *imaging* dari ketiga *flash disk* akan dianalisis menggunakan *tool Autopsy*.



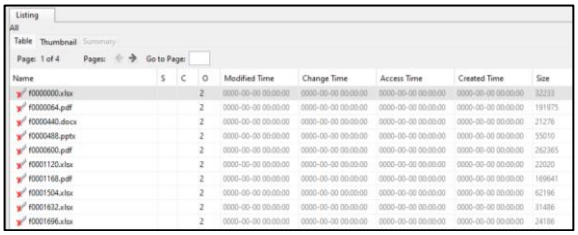
Gambar 4. Hasil Analisis *Flash Disk* 8GB Dengan Perlakuan Pertama

Pada gambar 4 didapatkan hasil analisis dari *flash disk* dengan perlakukan pertama yaitu penghapusan dengan perintah *delete* yang memiliki *size* 8GB dimana hasil *deleted file* pada *file system* ditemukan beberapa file dengan *modified time*, *change time*, *access time* serta nama file yang sesuai dengan tanggal pelaporan pada *tool Autopsy*.



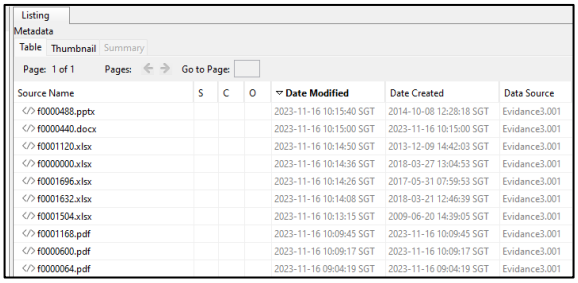
Gambar 5. Hasil Analisis Flash Disk 8GB Dengan Perlakuan Kedua

Pada Gambar 5, hasil analisis pada *flash disk* dengan perlakuan kudua yaitu dengan perintah *shift+delete* yang memiliki kapasitas 16GB menunjukkan adanya file yang ditemukan di *deleted file* pada *file system* yang memiliki kesamaan dengan kondisi pada perlakuan pertama. Meskipun *modified time*, *change time* dan juga nama file serupa dengan yang terlihat pada Gambar 4, namun terdapat perbedaan pada *access time*-nya yang menandakan file-file tersebut terakhir diakses pada waktu tersebut.



Gambar 6. Hasil Analisis Flash Disk 8GB Dengan Perlakuan Ketiga

Pada analisis *flash disk* yang berukuran 32GB dengan perlakuan ketiga menggunakan *quick format* terdapat perbedaan pada *deleted file*-nya dimana nama-nama dari file yang terhapus berubah serta *modified time*, *change time*, dan *access time* pada file yang terhapus juga tidak ditampilkan. Namun *date modified* serta *date created* file-file yang terhapus tersebut ditemukan pada analisis *metadata* yang dilakukan seperti yang terlihat pada gambar 7.



Gambar 7. Hasil Analisis Metadata *Flash Disk* 16GB

Setelah mendapatkan file-file yang telah terhapus, kemudian proses selanjutnya yaitu proses *recovery* dari file yang ditemukan dengan menggunakan *tool* yang sama yaitu *Autopsy*. Kemudian file yang telah di-*recovery* dari tiap *flash disk* akan dilakukan pengecekan nilai *hash* atau validasi keaslian menggunakan *tool Autopsy* dan *Hash Generator* serta nilai *hash* dari masing-masing file akan dibandingkan dengan file aslinya.

Tabel 2. Hasil Validasi Nilai *Hash* Pada Perlakuan Pertama

Nama File	Autopsy	Validasi
66-Case Flow Statement.xls	b6c734284977ba55e7736e107f669bbe	Cocok
68-Laporan Keuangan Perusahaan.pdf	6d0c27c32ff116a486c7fdddcb93a29c	Cocok
70-LAPORAN LABA RUGI.docx	a041f036c2f81f0c74e6b469afc76868	Cocok
72-Laporan Keuangan.pptx	9d2f5e092f5b089690f9c560eda451ed	Cocok
74-Profit and Loss Projection.pdf	ae5e93796d0c620006189 8bcf040247f	Cocok
76-profit and loss.xlsx	40527bdf6eaa09b8977bb206b7fdf28f	Cocok
78-Weekly Sales Activity.pdf	aff94403f8ad53f197d8c75c3248906a	Cocok
80-5 year financial plan.xlsx	2c50778309b52119a5411438eda17b9f	Cocok
82-Annual Financial	8a7e94314e33d2e462461	Cocok

Report.xlsx	94442668054	
84-Balance Sheet.xlsx	a292a3a4aa8ae258b444f6 354381ce70	Cocok

Tabel 2 menunjukkan semua nilai *hash* pada file yang telah di-*recovery* pada *flash disk* dengan perlakuan pertama yang memiliki nilai validasi setelah dicocokkan dengan nilai *hash Autopsy* dan *Hash Generator*.

Tabel 3. Hasil Validasi Nilai *Hash* Pada Perlakuan Kedua

Nama File	Autopsy	Validasi
75-Case Flow Statement.xls	b6c734284977ba55e7736 e107f669bbe	Cocok
77-Laporan Keuangan Perusahaan.pdf	6d0c27c32ff116a486c7fd ddcb93a29c	Cocok
79-LAPORAN LABA RUGI.docx	a041f036c2f81f0c74e6b4 69afc76868	Cocok
81-Laporan Keuangan.pptx	9d2f5e092f5b089690f9c5 60eda451ed	Cocok
83-Profit and Loss Projection.pdf	ae5e93796d0c620006189 8bcf040247f	Cocok
85-profit and loss.xlsx	40527bdf6eaa09b8977bb 206b7fdf28f	Cocok
87-Weekly Sales Activity.pdf	aff94403f8ad53f197d8c7 5c3248906a	Cocok
89-5 year financial plan.xlsx	2c50778309b52119a5411 438eda17b9f	Cocok
91-Annual Financial Report.xlsx	8a7e94314e33d2e462461 94442668054	Cocok
93-Balance Sheet.xlsx	a292a3a4aa8ae258b444f6 354381ce70	Cocok

Tabel 3 menunjukkan hal yang sama pada validasi nilai *hash flash disk* dengan perlakuan kedua dimana semua nilai *hash* pada file memiliki kecocokan dengan file aslinya.

Tabel 4. Hasil Validasi Nilai *Hash* Pada Perlakuan Ketiga

Nama File	Autopsy	Validasi
89-f0000000.xlsx	b6c734284977ba55e7736e1 07f669bbe	Cocok
90-f0000064.pdf	6d0c27c32ff116a486c7fddd cb93a29c	Cocok
91-f0000440.docx	a041f036c2f81f0c74e6b469 afc76868	Cocok
92-f0000488.pptx	9d2f5e092f5b089690f9c560 eda451ed	Cocok
93-f0000600.pdf	ae5e93796d0c6200061898b cf040247f	Cocok
94-f0001120.xlsx	40527bdf6eaa09b8977bb20 6b7fdf28f	Cocok
95-f0001168.pdf	aff94403f8ad53f197d8c75c 3248906a	Cocok
96-f0001504.xlsx	2c50778309b52119a541143 8eda17b9f	Cocok
97-f0001632.xlsx	8a7e94314e33d2e46246194 442668054	Cocok
98-f0001696.xlsx	a292a3a4aa8ae258b444f635 4381ce70	Cocok

Sama seperti hasil validasi pada *flash disk* dengan perlakuan pertama dan kedua. Pada tabel 4, meskipun nama file pada hasil analisis dan ekstraksi berubah tetapi nilai validasi *hash flash disk* dengan perlakuan ketiga tidak menunjukkan adanya perubahan pada nilai *hash*-nya.

4.5. Reporting

Dari hasil analisis yang telah dilakukan, didapatkan file-file yang telah dihapus oleh pelaku dengan perlakuan yang berbeda-beda pada media penyimpanan flash disk menggunakan *tools* forensik FTK *Imager*, *Autopsy*, dan juga *HashGenerator*, dimana *tool Autopsy* berhasil mendapatkan *metadata* file-file yang dihapus pada tanggal yang sama dengan tanggal pelaporan. Perbedaan dari masing-masing perlakuan penghapusan terdapat terdapat pada perlakuan ketiga yaitu dengan perintah *quick format* dimana nama file yang terhapus berubah menjadi nama file yang berbeda tidak seperti pada penghapusan file dengan perlakuan pertama dan kedua yang nama filenya tidak berubah seperti nama file aslinya. Selain itu *size* dan nilai *hash* pada semua file pada tiap-tiap perlakuan juga tidak terlihat adanya perubahan nilai *hash* MD5-nya yang menandakan bahwa file-file tersebut tidak ditemukan adanya perubahan.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Hasil akhir dari penelitian terkait "Analisis Bukti Digital pada Media Penyimpanan Flash Disk dengan Penerapan Metode National Institute of Standards and Technology" dapat disimpulkan sebagai berikut:

1. 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. Dimana seluruh bukti digital yang telah tersebut cocok dengan bukti digital yang telah dimasukkan ke dalam flash disk sesuai dengan skenario kasus kejadian.
2. Pada perlakuan ketiga yaitu quick format nama file yang terhapus berubah menjadi format yang berbeda tidak seperti pada perlakuan pertama dan kedua tetapi untuk ekstensi pada filenya tetap sama.
3. Semua size dan nilai hash pada hasil ekstrasi tiap-tiap file dengan perlakuan pertama, kedua, dan ketiga tidak ditemukana adanya perubahan dalam nilai hash MD5-nya dengan file aslinya yang menandakan file tersebut tidak terdapat modifikasi di dalamnya.
4. Penerapan metode NIST (National Institute of Standards and Technology) dapat diterapkan sebagai salah satu acuan dalam proses analisis bukti digital pada media penyimpanan flash disk. Dimana dapat dilihat pada tahapan metode NIST (National Institute of Standards and Technology) terutama pada tahap examination dan analysis.

5.2. Saran

Adapun saran untuk pengembangan penelitian mendatang disarankan guna meningkatkan kualitas, mengingat masih terdapat kekurangan dan Batasan

dalam penelitian ini. Berikut adalah saran untuk penelitian selanjutnya:

1. Menggunakan tools forensic lain dalam melakukan imaging file ataupun analisis file serta menggunakan metode yang berbeda seperti metode static forensic dalam menganalisis bukti digital pada media penyimpanan flash disk
2. Melakukan penelitian menggunakan objek lainnya seperti Hard Disk, Micro SD, Solid State Drive (SSD), dan lainnya.

DAFTAR PUSTAKA

Agustiono, W., Suci, D.W. and Prastiti, N. (2024) 'Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus', Jurnal Teknologi dan Informasi, 14(2), pp. 174–185. Available at: https://doi.org/10.34010/jati.v14i2.12952.

Azizah, S., Ramadhona, S.A. and Gustitio, K.W. (2020) 'Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST', Jurnal Repositor, 2(10), pp. 1400–1405. Available at: https://doi.org/10.22219/repositor.v2i10.1066.

Fitriana, M., AR, K.A. and Marsya, J.M. (2020) 'Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime', Cyberspace: Jurnal Pendidikan Teknologi Informasi, 4(1), p. 29. Available at: https://doi.org/10.22373/cj.v4i1.7241.

Hasa, M.F., Yudhana, A. and Fadlil, A. (2019) 'Analisis Bukti Digital pada Storage Secure Digital Card Menggunakan Metode Static Forensic', Mobile and Forensics, 1(2), pp. 76–84. Available at: https://doi.org/10.12928/mf.v1i2.1217.

Iman, N., Susanto, A. and Inggi, R. (2020) 'Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)', Jurnal Telekomunikasi dan Komputer, 9(3), p. 186. Available at: https://doi.org/10.22441/incomtech.v9i3.7210.

Julian, D. and Sutabri, T. (2023) 'Analisa Kinerja Aplikasi Digital Forensik Autopsy untuk Pengembalian Data menggunakan Metode NIST SP 800-86', Jurnal Informatika Terpadu, 9(2), pp. 136–142. Available at: https://doi.org/10.54914/jit.v9i2.984.

Maniar, N.A.I. and Yuniati, T. (2023) 'Implementasi Mobile Forensic Pada Aplikasi Michat Dan Telegram Dengan Framework Nist 800-101', Cyber Security dan Forensik Digital, 5(2), pp. 60–65. Available at: https://doi.org/10.14421/csecurity.2022.5.2.3764.

Riadi, I., Fadlil, A. and Aulia, M.I. (2021) 'Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)', Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 1(10), pp. 820–828.

Riskiyadi, M. (2020) 'Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime', Cyber Security dan Forensik Digital, 3(2), pp. 12–21. Available at: https://doi.org/10.14421/csecurity.2020.3.2.2144.

Zamsari, F.G.P. and Wahyono, T. (2024) 'Forensic Investigation of Digital Evidence on Flash Disk with Forensic Process Method Based on NIST', Jurnal Ecotipe (Electronic, Control, Telecommunication, Information, and Power Engineering), 11(1), pp. 88–96. Available at: https://doi.org/10.33019/jurnalecotipe.v11i1.4489.