JURNAL LOCUS: Penelitian & Pengabdian
Volume 4 No. 9 September 2025
E-ISSN 2829-7334| P-ISSN 2829-5439
Hompage: https://locus.rivierapublishing.id/index.php/jl

Analisis Efektivitas File Carving dalam Forensik Digital pada Flashdisk Dengan Tools Autopsy dan FTK Imager

Leni Susanti, Akrom*
Universitas Pamulang, Indonesia
Email: dosen02617@unpam.ac.id*

ABSTRAK

Analisis efektivitas file carving dalam forensik digital pada flashdisk dengan tools autopsy dan ftk imager. Meningkatnya kejahatan siber mendorong kebutuhan akan teknik pemulihan data yang efektif, terutama dari media penyimpanan seperti flashdisk. Penelitian ini bertujuan untuk menganalisis dan membandingkan efektivitas file carving menggunakan tools Autopsy dan FTK Imager dalam memulihkan data yang telah dihapus dari flashdisk dengan tiga skenario penghapusan berbeda. Metode penelitian menggunakan pendekatan eksperimental dengan prosedur National Institute of Standards and Technology (NIST), dimana flashdisk berkapasitas 16 GB diisi dengan 35 file berbagai jenis (dokumen, gambar, video, dan aplikasi), kemudian dilakukan penghapusan data menggunakan tiga skenario: delete biasa, quick format, dan full format. Setelah penghapusan data dilakukan sesuai dengan skenario yang telah ditetapkan, flashdisk di-imaging menggunakan Autopsy dan FTK Imager. Proses imaging ini bertujuan untuk menciptakan salinan bit-by-bit dari media penyimpanan, yang kemudian dianalisis tanpa memodifikasi data asli. Selanjutnya, kedua alat forensik digunakan untuk melakukan file carving, memindai sektor-sektor memori dan memulihkan file yang telah dihapus. Hasil akuisisi menunjukan pada flashdisk yang dilakukan penghapusan pada FTK Imager memperoleh nilai 100%, sementara Autopsy memperoleh nilai 82.8%. Jika flashdisk dilakukan quick format FTK Imager memperoleh nilai 0% dibandingkan Autopsy 74,3%. Sementara itu, pada flashdisk yang dilakukan format standar FTK Imager dan Autopsy memperoleh nilai 0% karena tidak berhasil menemukan file yang terhapus. Implikasi penelitian menunjukkan bahwa FTK Imager lebih efektif untuk pemulihan data pada penghapusan sederhana, sementara Autopsy lebih unggul pada penghapusan quick format, dan kombinasi kedua tools diperlukan untuk optimalisasi pemulihan data dalam berbagai skenario investigasi forensik digital.

Kata Kunci: File Carving, Flashdik, Autopsy, FTK Imager.

ABSTRACT

Analysis of the effectiveness of file carving in digital forensics on flash drives using Autopsy and FTK Imager tools. The rise in cybercrime has driven the need for effective data recovery techniques, especially from storage media such as flash drives. This study aims to analyze and compare the effectiveness of file carving using Autopsy and FTK Imager tools in recovering deleted data from flash drives with three different deletion scenarios. The research method used an experimental approach with the National Institute of Standards and Technology (NIST) procedure, where a 16 GB flash drive was filled with 35 files of various types (documents, images, videos, and applications), then data deletion was performed using three scenarios: normal delete, quick format, and full format. After data deletion was carried out according to the predetermined scenarios, the flash drives were imaged using Autopsy and FTK Imager. The imaging process aimed to create a bit-by-bit copy of the storage media, which was then analyzed without modifying the original data. Next, both forensic tools were used to perform file carving, scanning memory sectors and recovering deleted files. The acquisition results showed that the flash drive that was deleted on FTK Imager obtained a score of 100%, while Autopsy obtained a score of 82.8%. If the flash drive was quick formatted, FTK Imager obtained a score of 0% compared to Autopsy's 74.3%. Meanwhile, on flash drives that underwent standard formatting, FTK Imager and Autopsy obtained a score of 0% because they were unable to find the deleted files. The implications of the study show that FTK Imager is more effective for data recovery in simple deletions, while Autopsy is superior in quick format deletions, and a combination of both tools is needed to optimize data recovery in various digital forensic investigation scenarios.

Keywords: *File Carving, Flashdisk, Autopsy, FTK Imager*

PENDAHULUAN

Seiring dengan perkembangan teknologi informasi dan komunikasi yang sangat pesat membuat dinamika kejahatan siber menjadi sangat beragam dan terus meningkat setiap tahunnya (Rosita, 2023). Berdasarkan data lembaga Southeast Asia Freedom of Expression

Network (SAFEnet), ada 61 insiden keamanan digital di Indonesia pada kuartal I 2024. Dimana dalam hal ini terjadi peningkatan jumlah kejahatan siber hampir dua kali lipat dari jumlah insiden tahun sebelumnya pada periode yang sama.

Kejahatan siber diartikan sebagai aktivitas yang menggunakan teknologi sebagai alat atau media untuk melakukan kejahatan, seperti meretas jaringan, mencuri informasi, menghapus informasi, menyembunyikan informasi, dan merusak informasi (Butarbutar, 2023; Tamhidah, 2023). Dengan adanya peningkatan kejahatan siber sering kali melibatkan teknologi komputer untuk menyimpan data-datanya, dimana hasil kejahatan siber biasanya disembunyikan di media penyimpanan untuk dipergunakan dalam pencurian, pengintaian, bullying, dan penipuan. Biasanya para pelaku kejahatan siber akan memilih untuk menghapus, menyembunyikan, dan memformat semua data yang dikumpulkan pada saat tindak kejahatannya dilakukan, sehingga bukti digital yang ditemukan perlu dilakukan proses file carving. (Yuwono, Juhairiah, & Sonedi, 2019).

Bukti digital bersifat mudah rusak, tidak stabil, dan rawan jika tidak dikelola dengan baik. Menurut UU No. 11 Tahun 2008 RI tentang Informasi dan Transaksi Elektronik, bukti digital disebut sebagai informasi elektronik dan dokumen elektronik. Maka, untuk mengungkap kasus kejahatan terkait dengan bukti elektronik atau digital, perlu mencari dan menganalisis dengan cermat jenis barang bukti serta keterkaitan setiap file. Analisis jenis dan format file menjadi penting karena digital evidence memiliki sifat rentan terhadap perubahan metadata dan autentikasi yang dapat dipertanyakan (Ilham, 2025). Keandalan bukti digital juga sangat tergantung pada sistem elektronik yang digunakan, termasuk keamanan, keutuhannya (integrity), dan prosedur tata kelola bukti seperti chain of custody (Subarzah, 2023). Apalagi, dalam praktiknya, tantangan teknis seperti kecepatan pengumpulan data, volume data besar, dan kurangnya SDM forensik dapat menghambat proses memperoleh bukti yang valid (Optimizing, 2024). Di sisi hukum, UU ITE secara eksplisit menetapkan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya dapat diakui sebagai alat bukti hukum yang sah apabila memenuhi persyaratan formil dan materil yang diatur dalam undang-undang ini (Analisis Yuridis, 2022). Dengan demikian, investigasi digital harus memperhatikan legalitas pengumpulan bukti, stabilitas format, keaslian, dan korelasi antarfail agar bukti digital bisa diterima di pengadilan.

Teknologi penyimpanan digital, termasuk flashdisk, terus berkembang dari waktu ke waktu, meningkatkan kapasitas penyimpanan dan aksesibilitas data (Wang & Yan, 2019). Di satu sisi, hal ini memberikan keuntungan dalam hal produktivitas dan mobilitas (Singh & Kapoor, 2021). Namun, di sisi lain, hal ini juga memperluas peluang bagi para pelaku kejahatan siber dan kriminal lain untuk menggunakan perangkat ini dalam kegiatan ilegal (Rahman et al., 2022). Data penting sering kali disimpan pada flashdisk karena ukurannya yang kecil dan portabilitasnya, yang membuatnya mudah untuk disembunyikan atau dipindahkan (Ramesh & Gupta, 2020). Oleh karena itu, manajemen keamanan data pada perangkat portabel seperti flashdisk menjadi tantangan serius yang harus ditangani dengan strategi forensik digital dan kebijakan perlindungan data yang tepat (Kumar & Kumar, 2023).

Flashdisk, yang juga dikenal sebagai USB flash drive, merupakan sebuah perangkat penyimpanan data portabel yang memiliki tipe NAND yang dilengkapi dengan port USB internal serta dapat terhubung ke Flashdisk adalah media penyimpanan data yang paling sering digunakan saat ini dan dapat dibawa ke mana-mana. Flashdisk bisa dimanfaatkan untuk beberapa keperluan, seperti sebagai pengganti CD/DVDROM dan sebagai tempat penyimpanan sistem operasi yang diperlukan untuk melawan kejahatan digital steganografi, memerlukan panduan tentang metode dan teknik investigasi untuk mengumpulkan bukti ilmiah. (Mubarok, dkk. 2024).

Flashdisk bisa menjadi salah satu barang bukti digital yang dapat mendukung investigasi dan membuktikan keterlibatan pelaku dalam kejahatan. Dalam investigasi digital forensik, salah satu tantangan terbesar adalah memulihkan data yang telah dihapus dari perangkat penyimpanan seperti flashdisk. Data yang dihapus melalui berbagai metode penghapusan, seperti delete, quick format, dan full format, meninggalkan jejak yang berbeda pada media penyimpanan. Banyak kasus kriminal, pelaku kejahatan sering menghapus data dengan tujuan untuk menyembunyikan bukti. Namun, meskipun file telah dihapus, data yang mendasarinya tetap ada pada media penyimpanan hingga ditimpa oleh data baru. Teknik file carving memungkinkan penyidik forensik untuk mengekstraksi data tersebut dan menggunakannya sebagai bukti dalam pengadilan. File carving adalah teknik dalam forensik digital yang digunakan untuk mengekstraksi data dari media penyimpanan digital tanpa bergantung pada informasi file sistem. Teknik ini bermanfaat saat sistem file mengalami kerusakan atau data dihapus oleh pelaku kejahatan. (Riadi, Fadlil, & Aulia, Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST), 2020). Pada prinsipnya, file carving beroperasi dengan mencari motif header dan footer yang khas dari berbagai jenis file, seperti gambar, dokumen, dan file multimedia. Saat pola ini terdeteksi, konten antara bagian awal dan akhir dianggap sebagai satu file utuh.

Terdapat berbagai alat yang dapat digunakan untuk melakukan file carving, dua diantaranya yang sering digunakan dalam forensik digital adalah Autopsy dan FTK Imager. Keduanya adalah perangkat lunak forensik digital yang dirancang untuk memfasilitasi analisis data dari berbagai jenis media penyimpanan. Meskipun kedua tools ini memiliki kemampuan untuk melakukan file carving, ada perbedaan signifikan dalam hal metode, kecepatan, akurasi, dan fitur yang disediakan.

Berdasarkan penjelasan yang telah dijelaskan di atas, penelitian ini akan menganalisis secara komparatif kinerja Autopsy dan FTK Imager dalam melakukan file carving pada flashdisk dengan menggunakan metode penghapusan delete, quick format, dan format untuk mengevaluasi kemampuan kedua tools tersebut dalam proses memulihkan data. Sedangkan dalam proses pengumpulan data, penelitian ini menggunakan prosedur National Institute of Standards and Technology (NIST) untuk memperoleh bukti digital yang valid dan efektif.

Dalam konteks investigasi forensik digital, pemulihan data yang telah dihapus dari media penyimpanan flashdisk menghadapi beberapa tantangan utama. Pertama, berbagai metode penghapusan data (delete, quick format, full format) menghasilkan tingkat kesulitan pemulihan yang berbeda, dimana tidak semua tools forensik memiliki kemampuan yang sama dalam menangani setiap skenario penghapusan. Kedua, kurangnya penelitian komparatif yang komprehensif mengenai efektivitas tools forensik populer seperti Autopsy dan FTK Imager dalam melakukan file carving pada flashdisk. Ketiga, ketidakpastian mengenai tingkat akurasi dan kecepatan pemulihan data antara kedua tools tersebut pada berbagai skenario penghapusan. Keempat, belum adanya panduan yang jelas mengenai tools mana yang paling efektif untuk setiap jenis skenario penghapusan data dalam investigasi forensik digital.

Urgensi penelitian ini didorong oleh beberapa faktor kritis. Pertama, meningkatnya kejahatan siber yang melibatkan penghapusan bukti digital secara sengaja memerlukan teknik pemulihan data yang efektif dan reliable. Kedua, penyidik forensik digital membutuhkan panduan yang akurat dalam memilih tools yang tepat untuk setiap skenario investigasi agar dapat memaksimalkan tingkat keberhasilan pemulihan bukti. Ketiga, perkembangan teknologi penyimpanan yang semakin canggih menuntut evaluasi berkelanjutan terhadap efektivitas tools forensik yang tersedia. Keempat, keterbatasan waktu dalam investigasi kriminal mengharuskan penggunaan tools yang paling efisien dan akurat untuk mempercepat proses pemulihan bukti digital.

Beberapa penelitian sebelumnya telah mengkaji aspek file carving dalam forensik digital. Yuwono, Juhairiah, & Sonedi (2019) melakukan analisis file carving pada file system menggunakan metode NIST, namun fokus pada aspek metodologi tanpa perbandingan tools spesifik. Riadi, Fadlil, & Aulia (2020) meneliti investigasi bukti digital optical drive menggunakan metode NIST, tetapi terbatas pada media CD/DVD. Matondang, Maulana, & Carudin (2023) melakukan analisis perbandingan perangkat lunak forensik digital file carving menggunakan NIST, namun belum secara spesifik membandingkan efektivitas Autopsy dan FTK Imager pada flashdisk. Dasmen et al. (2024) menganalisis digital forensik recovery file menggunakan tools Autopsy dengan metode NIJ, tetapi hanya fokus pada satu tools tanpa perbandingan.

Terdapat beberapa kesenjangan dalam penelitian-penelitian sebelumnya. Pertama, belum ada penelitian yang secara komprehensif membandingkan efektivitas Autopsy dan FTK Imager khusus untuk file carving pada flashdisk dengan berbagai skenario penghapusan. Kedua, kurangnya analisis mendalam mengenai tingkat akurasi pemulihan data berdasarkan validasi hash MD5 pada kedua tools tersebut. Ketiga, belum adanya evaluasi performa yang mencakup aspek kecepatan pemrosesan dan tingkat keberhasilan pemulihan data secara bersamaan. Keempat, minimnya panduan praktis bagi penyidik forensik dalam memilih tools yang tepat untuk setiap skenario investigasi.

Penelitian ini menawarkan kebaruan dalam beberapa aspek. Pertama, melakukan perbandingan komprehensif antara Autopsy dan FTK Imager khusus untuk file carving pada flashdisk dengan tiga skenario penghapusan yang berbeda. Kedua, menggunakan validasi hash MD5 untuk memastikan integritas dan akurasi data yang dipulihkan. Ketiga, menganalisis aspek performa yang mencakup tingkat keberhasilan pemulihan dan kecepatan pemrosesan secara bersamaan. Keempat, menggunakan prosedur standar NIST untuk memastikan validitas dan reliabilitas hasil penelitian. Kelima, memberikan rekomendasi praktis bagi penyidik forensik digital dalam memilih tools yang optimal untuk setiap skenario investigasi.

Tujuan utama penelitian ini adalah menganalisis dan membandingkan efektivitas file carving menggunakan tools Autopsy dan FTK Imager dalam memulihkan data yang telah dihapus dari flashdisk dengan tiga skenario penghapusan yang berbeda (delete, quick format, full format). Tujuan khusus meliputi mengevaluasi tingkat keberhasilan pemulihan data, menganalisis kecepatan pemrosesan, dan memvalidasi integritas data yang dipulihkan menggunakan hash MD5. Manfaat penelitian ini bagi akademisi adalah memberikan kontribusi literature mengenai perbandingan tools forensik digital dan memperkaya pemahaman tentang teknik file carving. Bagi praktisi forensik digital, penelitian ini memberikan panduan praktis dalam memilih tools yang tepat untuk setiap skenario investigasi dan meningkatkan efektivitas pemulihan bukti digital. Bagi penegak hukum, penelitian ini dapat meningkatkan kualitas investigasi kriminal yang melibatkan bukti digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental kuantitatif dengan metode perbandingan (comparative method) untuk menganalisis efektivitas file carving pada flashdisk. Dimana skenario yang akan dilakukan adalah dengan menganalisis tiga skenario penghapusan data pada flashdisk, di mana setiap skenario akan dianalisis menggunakan file carving. Adapun prosedur yang akan dilakukan dalam penelitian ini adalah sebagai berikut:

a. Langkah Pertama:

Flashdisk akan diisi dengan berbagai file, termasuk 16 file dokumen (Excel, Word, PDF, PPT dan TXT), 9 file gambar (JPEG), 5 file video (MP3, MP4, AVI), 5 file aplikasi (ZIP).

Setiap file akan disimpan dalam folder yang terorganisir, dan total data yang disimpan adalah 16 GB. Sebelum dilakukan penghapusan untuk proses validasi maka perlu dicatat terlebih dahulu Hash pada masing-masing dokumen yang ada di flashdisk. Berikut merupakan file asli sebagai acuan bukti digital pada penelitian ini.

b. Langkah Kedua

Penghapusan Data Flashdisk akan menjalani tiga metode penghapusan data yang berbeda:

1) Skenario 1: Delete: Semua file di flashdisk akan dihapus menggunakan fitur delete biasa pada Windows, yang hanya menghilangkan pointer file tetapi tidak menimpa data secara fisik.
2) Skenario 2: Quick Format: Flashdisk akan diformat menggunakan fitur quick format, yang menghapus tabel alokasi file tanpa menimpa data di sektor-sektor penyimpanan.
3) Skenario 3: Full Format: Flashdisk akan diformat menggunakan full format, yang menimpa seluruh sektor penyimpanan, sehingga data dihapus secara permanen.

c. Langkah Ketiga

Setelah penghapusan data di setiap skenario, flashdisk akan di akuisisi menggunakan Autopsy versi 4.21.0 dan FTK Imager versi 4.7.1. Proses imaging menciptakan salinan bit-by-bit dari flashdisk yang akan digunakan untuk analisis lebih lanjut tanpa memodifikasi data asli.

d. Langkah Keempat

1) Autopsy: Alat ini akan digunakan untuk melakukan file carving dari image yang diambil. Autopsy akan memindai sektor-sektor memori untuk menemukan jejak file yang telah dihapus.
2) FTK Imager: Alat ini juga akan melakukan file carving pada disk image yang sama, menggunakan teknik yang berbeda untuk merekonstruksi file dari data mentah.

Dalam memudahkan tahapan prosedur penelitian ditampilkan dapat dibuat pada table berikut:

Tabel 1. Tahapan Prosedur Penelitian

Tahap	Uraian Kegiatan	Output
1. Persiapan Data Uji	Menyalin 35 file uji ke flashdisk.	Flashdisk berisi file uji lengkap.
2. Skenario Penghapusan	Melakukan penghapusan data sesuai 3 skenario: Delete Quick Format Full Format	Flashdisk dalam kondisi sesuai skenario penghapusan.
3. Akuisisi Data	Membuat forensic image (.E01) dari flashdisk menggunakan FTK Imager.	Image file yang siap dianalisis.
4. Pemulihan Data (File Carving)	Mengimpor image file ke Autopsy dan FTK Imager untuk proses file carving.	Data hasil pemulihan.

HASIL DAN PEMBAHASAN

A. Collection

Pengumpulan barang bukti merupakan langkah awal yang dilakukan sebelum melakukan file carving. Mengumpulkan barang bukti digital yang tersimpan atau pernah tersimpan pada bukti elektronik melalui akuisisi data dikenal sebagai collection. Dengan metode imaging atau pencitraan, seluruh file di flashdisk secara fisik (sektor per sektor) di akuisisi, sehingga dokumen di disk akan sama dengan bukti secara fisik. Imaging dilakukan untuk memastikan

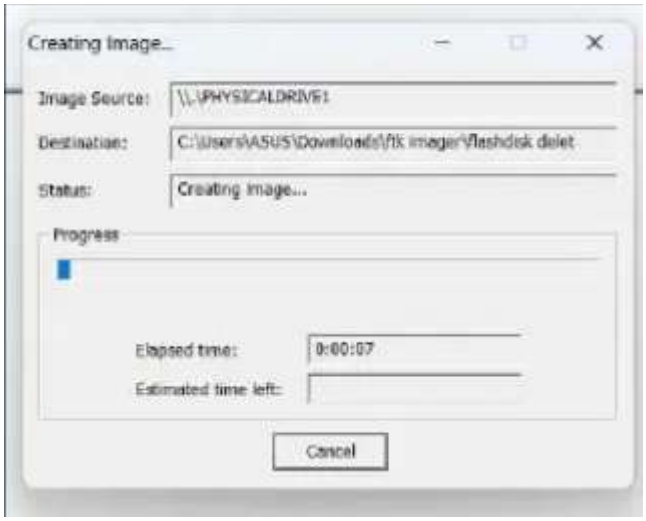
bahwa bukti asli sampai ke penyidik sehingga mereka dapat bertanggung jawab di pengadilan.



Gambar 1. Tahapan Proses Collection

B. Examination

Setelah melakukan tahapan pengumpulan bukti digital dengan menyalin semua data yang ada di media penyimpanan dengan cara imaging, kemudian dari proses tersebut menghasilkan file salinan dengan format RAW untuk FTKImager dan data salinan untuk Autopsy yang akan digunakan pada tahapan analisis. Langkah berikutnya yaitu melakukan pemeriksaan menggunakan aplikasi FTK Imager dengan mengimport file imaging yang telah dihasilkan,dan secara otomatis sistem akan mengekstrak file salinan tersebut untuk dilakukan visualisasi data dan recovery data yang telah dihapus oleh pelaku. Autopsy secara Otomatis setelah pemprosesan langsung pada flashdisk akan menuju Timeline listing dari data-data yang ingin dikembalikan.



Gambar 2. Proses Imaging pada Flasdisk FTK Imager

Setelah proses imaging dengan FTK Imager dan analisis menggunakan Autopsy selesai, hasil yang diperoleh mencakup berbagai aspek penting dalam investigasi digital. Dari FTK Imager, didapatkan salinan forensik berupa file image disk dalam format seperti .dd, .img,atau .E01, yang berisi semua data di perangkat penyimpanan. Sementara itu, Autopsy memberikan analisis mendalam dari disk image tersebut. Hasilnya meliputi data terstruktur berupa daftar file dan folder, meta data file, serta file yang telah dihapus tetapi masih dapat dipulihkan.



Gambar 3. Proses Imaging Autopsy

C. Analysis

Tahapan analisis merupakan poin penting yang harus dilakukan dalam proses penyelidikan forensik. Bukti digital yang telah berhasil dikumpulkan dan dilakukan pemeriksaan secara menyeluruh, selanjutnya dilakukan analisis dengan melakukan evaluasi dan menafsirkan bukti digital untuk memperoleh informasi mengenai aktivitas yang terjadi pada perangkat flashdisk. Dalam penelitian ini, proses digital forensik pada perangkat flashdisk dilakukan sebanyak tiga kali pengujian dengan Delete file pada flashdisk, Quick Format pada file dalam Flashdisk dan Format pada file dalam Flashdisk. Berikut ini merupakan hasil analisis digital forensik pada flashdisk menggunakan FTKImager dan Autopsy yang telah dilakukan.

a. Skenario 1 : Delete File

Pada skenario Delete untuk FTK Imager mendapatkan 35 File data setelah dilakukan pemrosesan pada Flashdisk yang telah dilakukan Delete. Untuk Autopsy hanya mendapatkan 29 File data dari 35 total keseluruhan setelah dilakukan pemrosesan data pada Flashdisk. Selanjutnya dilakukan validasi dengan pencocokan nilai hash (MD5) bukti digital dan hasil pencocokan nilai hash hasil pemulihan dari FTK Imager dan Autopsy.

Tabel 2. Pencocokan Hash (MD5) Skenario Delete

No	Nama File	MD-5	FTK Imager	Autopsy
1.	AVI 1	0b229b47c882396df06386e54f17d3ef	Valid	Valid
2.	MP4 1	c8b22df6b2cf78990adbb8feda7142bf	Valid	Valid
3.	MP4 2	03ffd995643c3d5bbf111b6cc88885ff	Valid	Valid
4.	MP3 1	5f43999166c25921b33d86127fe5de21	Valid	Valid
5.	MP3 2	1c7317e44d5a3c0946facafcd81f3207	Valid	Valid

No	Nama File	MD-5	FTK Imager	Autopsy
6.	JPG 1	88b72ff59a9131d654fecfd7ab8fdd41	Valid	Valid
7.	JPG 2	e1fa23ca1381da42b09ef31744282fea	Valid	Valid
8.	JPG 3	008a7761bd65d07fc08b6baab77f4f9f	Valid	Valid
9.	JPG 4	c9eb5831c339a332b53a3bcd6ecb2b26	Valid	Valid
10.	JPG 5	b666c33f60ab28e3f70a1330441fc84a	Valid	Valid
11.	JPG 6	7672c8d478ed339acea1e3ca28844b48	Valid	Valid
12.	JPG 7	a1dde7c2f42cd97815f5041f6a2ede5d	Valid	Valid
13.	JPG 8	149a8f56cd4f1392189bcda7c492e1af	Valid	Valid
14.	JPG 9	0cffcbe7ab826a93299d31756dd1c7a1	Valid	Valid
15.	Excel 1	c91cf1a147009ee53a0fa2acea99e043	Valid	Valid
16.	Excel 2	21475b9e67a77a6bae316e70c707b344	Valid	Valid
17.	PDF 1	9513f260197456864c22cdebf20a1700	Valid	Valid
18.	PDF 2	733539d1a889848a909447d08ccc07c8	Valid	Valid
19.	PDF 3	b646c37cb216e5a9a752562152cf485a	Valid	Valid
20.	PDF 4	4f273c4b8a6d85bea60dffecf42f9adb	Valid	Valid
21.	PPT 1	d41d8cd98f00b204e9800998ecf8427e	Valid	Tidak Valid
22.	PPT 2	d25cd3edc245d0992ecd6c2c3727761e	Valid	Valid
23.	PPT 3	6c3ead801f86311759537d83db33b51a	Valid	Valid
24.	TXT 1	74277a1abc0accc52f05a8287eedec0d	Valid	Valid
25.	Word 1	ef8b2d24a5a1dce105660d857731bc66	Valid	Tidak Valid
26.	Word 2	7aa792a9bcd9c759cbde7da8f54a4ce7	Valid	Tidak Valid
27.	Word 3	3e5288243f0c71ef31a9a269066fcc94	Valid	Tidak Valid
28.	Word 4	71bcbabfb35e96442998c167bb206dcd	Valid	Tidak Valid
29.	Word 5	a4b06de68f267fa8663a9cb81556bb6e	Valid	Tidak Valid
30.	Word 6	e7dd119626d8d991e024ff6b5f5e597c	Valid	Valid
31.	ZIP 1	9f4222cb47b98a2fe3e3da6ba5dfdbd3	Valid	Valid
32.	ZIP 2	2c02c4c57e72cf44ca16223d3050ce3e	Valid	Valid
33.	ZIP 3	4eedb1a104bb106449d178f7b998d107	Valid	Valid
34.	ZIP 4	273d722e495f62524597d84b380da198	Valid	Valid
35.	ZIP 5	be723115491bf8cb616cc83741264b4c	Valid	Valid

b. Skenario 2: Quick Format

Quick Format untuk FTK Imager mendapatkan 0 File data dari 35 total keseluruhan setelah dilakukan pemrosesan pada Flashdisk yang telah dilakukan Delete. Untuk Autopsy mendapatkan 26 File data dari 35 total keseluruhan setelah dilakukan pemrosesan data pada Flashdisk. Selanjutnya dilakukan validasi dengan pencocokan nilai hash (MD5) bukti digital dan hasil pencocokan nilai hash hasil pemulihan dari FTK Imager dan Autopsy.

Tabel 3. Pencocokan Hash (MD5) Skenario Quick Format

No	Nama File	MD-5	FTK Imager	Autopsy
1.	AVI 1	0b229b47c882396df06386e54f17d3ef	Tidak Valid	Valid
2.	MP4 1	c8b22df6b2cf78990adbb8feda7142bf	Tidak Valid	Valid
3.	MP4 2	03ffd995643c3d5bbf111b6cc88885ff	Tidak Valid	Tidak Valid
4.	MP3 1	5f43999166c25921b33d86127fe5de21	Tidak Valid	Valid
5.	MP3 2	1c7317e44d5a3c0946facafcd81f3207	Tidak Valid	Valid
6.	JPG 1	88b72ff59a9131d654fecfd7ab8fdd41	Tidak Valid	Valid
7.	JPG 2	e1fa23ca1381da42b09ef31744282fea	Tidak Valid	Valid
8.	JPG 3	008a7761bd65d07fc08b6baab77f4f9f	Tidak Valid	Valid
9.	JPG 4	c9eb5831c339a332b53a3bcd6ecb2b26	Tidak Valid	Valid
10.	JPG 5	b666c33f60ab28e3f70a1330441fc84a	Tidak Valid	Valid
11.	JPG 6	7672c8d478ed339acea1e3ca28844b48	Tidak Valid	Valid
12.	JPG 7	a1dde7c2f42cd97815f5041f6a2ede5d	Tidak Valid	Valid
13.	JPG 8	149a8f56cd4f1392189bcda7c492e1af	Tidak Valid	Valid
14.	JPG 9	0cffcbe7ab826a93299d31756dd1c7a1	Tidak Valid	Valid
15.	Excel 1	c91cf1a147009ee53a0fa2acea99e043	Tidak Valid	Valid
16.	Excel 2	21475b9e67a77a6bae316e70c707b344	Tidak Valid	Valid
17.	PDF 1	9513f260197456864c22cdebf20a1700	Tidak Valid	Valid
18.	PDF 2	733539d1a889848a909447d08ccc07c8	Tidak Valid	Valid
19.	PDF 3	b646c37cb216e5a9a752562152cf485a	Tidak Valid	Valid
20.	PDF 4	4f273c4b8a6d85bea60dffecf42f9adb	Tidak Valid	Valid
21.	PPT 1	d41d8cd98f00b204e9800998ecf8427e	Tidak Valid	Tidak Valid
22.	PPT 2	d25cd3edc245d0992ecd6c2c3727761e	Tidak Valid	Valid
23.	PPT 3	6c3ead801f86311759537d83db33b51a	Tidak Valid	Valid
24.	TXT 1	74277a1abc0accc52f05a8287eedec0d	Tidak Valid	Valid
25.	Word 1	ef8b2d24a5a1dce105660d857731bc66	Tidak Valid	Tidak Valid
26.	Word 2	7aa792a9bcd9c759cbde7da8f54a4ce7	Tidak Valid	Tidak Valid
27.	Word 3	3e5288243f0c71ef31a9a269066fcc94	Tidak Valid	Tidak Valid
28.	Word 4	71bcbabfb35e96442998c167bb206dcd	Tidak Valid	Tidak Valid
29.	Word 5	a4b06de68f267fa8663a9cb81556bb6e	Tidak Valid	Tidak Valid
30.	Word 6	e7dd119626d8d991e024ff6b5f5e597c	Tidak Valid	Valid
31.	ZIP 1	9f4222cb47b98a2fe3e3da6ba5dfdbd3	Tidak Valid	Valid
32.	ZIP 2	2c02c4c57e72cf44ca16223d3050ce3e	Tidak Valid	Valid
33.	ZIP 3	4eedb1a104bb106449d178f7b998d107	Tidak Valid	Tidak Valid
34.	ZIP 4	273d722e495f62524597d84b380da198	Tidak Valid	Tidak Valid

No	Nama File	MD-5	FTK Imager	Autopsy
35.	ZIP 5	be723115491bf8cb616cc83741264b4c	Tidak Valid	Valid

c. Skenario 3: Format

Full Format untuk FTK Imager dan Autopsy sama sama menghasilkan 0 File data ketika dilakukan pemrosesan data dengan skenario Format data pada Flashdisk.

Tabel 4. Pencocokan Hash (MD5) Skenario Full Format

No	Nama File	MD-5	FTK Imager	Autopsy
1.	AVI 1	0b229b47c882396df06386e54f17d3ef	Tidak Valid	Tidak Valid
2.	MP4 1	c8b22df6b2cf78990adbb8feda7142bf	Tidak Valid	Tidak Valid
3.	MP4 2	03ffd995643c3d5bbf111b6cc88885ff	Tidak Valid	Tidak Valid
4.	MP3 1	5f43999166c25921b33d86127fe5de21	Tidak Valid	Tidak Valid
5.	MP3 2	1c7317e44d5a3c0946facafcd81f3207	Tidak Valid	Tidak Valid
6.	JPG 1	88b72ff59a9131d654fecfd7ab8fdd41	Tidak Valid	Tidak Valid
7.	JPG 2	e1fa23ca1381da42b09ef31744282fea	Tidak Valid	Tidak Valid
8.	JPG 3	008a7761bd65d07fc08b6baab77f4f9f	Tidak Valid	Tidak Valid
9.	JPG 4	c9eb5831c339a332b53a3bcd6ecb2b26	Tidak Valid	Tidak Valid
10.	JPG 5	b666c33f60ab28e3f70a1330441fc84a	Tidak Valid	Tidak Valid
11.	JPG 6	7672c8d478ed339acea1e3ca28844b48	Tidak Valid	Tidak Valid
12.	JPG 7	a1dde7c2f42cd97815f5041f6a2ede5d	Tidak Valid	Tidak Valid
13.	JPG 8	149a8f56cd4f1392189bcda7c492e1af	Tidak Valid	Tidak Valid
14.	JPG 9	0cffcbe7ab826a93299d31756dd1c7a1	Tidak Valid	Tidak Valid
15.	Excel 1	c91cf1a147009ee53a0fa2acea99e043	Tidak Valid	Tidak Valid
16.	Excel 2	21475b9e67a77a6bae316e70c707b344	Tidak Valid	Tidak Valid
17.	PDF 1	9513f260197456864c22cdebf20a1700	Tidak Valid	Tidak Valid
18.	PDF 2	733539d1a889848a909447d08ccc07c8	Tidak Valid	Tidak Valid
19.	PDF 3	b646c37cb216e5a9a752562152cf485a	Tidak Valid	Tidak Valid
20.	PDF 4	4f273c4b8a6d85bea60dffecf42f9adb	Tidak Valid	Tidak Valid
21.	PPT 1	d41d8cd98f00b204e9800998ecf8427e	Tidak Valid	Tidak Valid
22.	PPT 2	d25cd3edc245d0992ecd6c2c3727761e	Tidak Valid	Tidak Valid
23.	PPT 3	6c3ead801f86311759537d83db33b51a	Tidak Valid	Tidak Valid
24.	TXT 1	74277a1abc0accc52f05a8287eedec0d	Tidak Valid	Tidak Valid
25.	Word 1	ef8b2d24a5a1dce105660d857731bc66	Tidak Valid	Tidak Valid
26.	Word 2	7aa792a9bcd9c759cbde7da8f54a4ce7	Tidak Valid	Tidak Valid
27.	Word 3	3e5288243f0c71ef31a9a269066fcc94	Tidak Valid	Tidak Valid
28.	Word 4	71bcbabfb35e96442998c167bb206dcd	Tidak Valid	Tidak Valid

No	Nama File	MD-5	FTK Imager	Autopsy
29.	Word 5	a4b06de68f267fa8663a9cb81556bb6e	Tidak Valid	Tidak Valid
30.	Word 6	e7dd119626d8d991e024ff6b5f5e597c	Tidak Valid	Tidak Valid
31.	ZIP 1	9f4222cb47b98a2fe3e3da6ba5dfdbd3	Tidak Valid	Tidak Valid
32.	ZIP 2	2c02c4c57e72cf44ca16223d3050ce3e	Tidak Valid	Tidak Valid
33.	ZIP 3	4eedb1a104bb106449d178f7b998d107	Tidak Valid	Tidak Valid
34.	ZIP 4	273d722e495f62524597d84b380da198	Tidak Valid	Tidak Valid
35.	ZIP 5	be723115491bf8cb616cc83741264b4c	Tidak Valid	Tidak Valid

D. Reporting

Pada tahap ini, ahli forensik menyusun laporan teerinci dan lengkap mengenai hasil penyelidikan pada barang bukti flashdisk yang telah dilakukan pada tahap sebelumnya, menggunakan aplikasi FTK Imager dan Autopsy untuk melakukan pemulihan data pada sebuah Flashdisk yang telah melalui 3 tahapan

Proses skenario.x 100%

∑a= Jumlah File yang berhasil diakuisisi

∑n=Jumlah File Asli

Berdasarkan Tabel 2, Tabel 3 dan Tabel 4 didapatkan laporan perbandingan dari hasil pemulihan seluruh data yang telah dilakukan dengan beberapa kondisi seperti skenario Delete, Quick Format, dan Full Format.

Tabel 5. Laporan Perbandingan FTK Imager dan Autopsy

Skenario	FTK Imager	Autopsy	Rata-Rata Waktu Proses Pemulihan File	
			FTK Imager	Autopsy
Delete	100 %	82,8 %	18 Menit 06 Detik	32 Menit 16 Detik
Quick Format	0 %	74,3 %	10 Menit 37 Detik	53 Menit 20 Detik
Full Format	0 %	0 %	-	-

KESIMPULAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa efektivitas file carving sangat bergantung pada jenis alat forensik dan metode penghapusan data. FTK Imager terbukti lebih unggul dalam memulihkan data yang dihapus dengan metode delete (100% berhasil), sementara Autopsy lebih efektif dalam menangani kasus quick format (74.3% berhasil). Namun, kedua alat tersebut tidak mampu memulihkan data yang telah diformat secara penuh (full format). Kecepatan pemrosesan FTK Imager juga lebih baik dibandingkan Autopsy pada semua skenario. Untuk penelitian selanjutnya, disarankan untuk mengeksplorasi kombinasi penggunaan kedua alat tersebut secara sinergis untuk meningkatkan tingkat pemulihan data, menguji pada berbagai jenis media penyimpanan dengan kapasitas dan sistem file yang berbeda, serta mengembangkan metode atau algoritma baru yang dapat menangani pemulihan data dari perangkat yang telah mengalami full format.

REFERENSI

Analisis yuridis mengenai pembuktian. (2022). Analisis yuridis mengenai pembuktian Pasal 44 UU No. 11 Tahun 2008. *Lex Privatum, 10*(2), 1–14.

Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. *Technology and Economics Law Journal*, *2*(2), 3.

Dasmen, R. N., Rahman, A., Putra, D. A., & Saputra, M. (2024). Analisis digital forensik recovery file yang dihapus menggunakan tools Autopsy dengan metode National Institute of Justice. *Jurnal Ilmiah KOMPUTASI, 23*(2), 213–218.

Ilham, M. (2025). Efektivitas penggunaan alat bukti elektronik: Studi kasus UU ITE dan praktik peradilan di Indonesia. *PLR: Philippine Law Review / Jurnal Hukum, 12*(1), 55–72.

Kumar, V., & Kumar, S. (2023). Digital forensics challenges in portable storage devices: A review of methods and countermeasures. *Forensic Science International: Digital Investigation, 45,* 301588. https://doi.org/10.1016/j.fsidi.2023.301588

Matondang, J., Maulana, I., & Carudin. (2023). Analisis perbandingan perangkat lunak forensik digital file carving menggunakan NIST. *Innovative: Journal of Social Science Research,* 2154–2165.

Optimizing the use of digital forensics and information technology in legal proceedings: Barriers and opportunities. (2024). *IJLCJ: International Journal of Law, Crime and Justice, 11*(2), 150–170.

Rahman, M., Alasmary, W., Alshammari, R., & Karim, R. (2022). Portable storage device misuse: Risks and prevention in organizational settings. *Journal of Information Security and Applications, 65,* 103123. https://doi.org/10.1016/j.jisa.2021.103123

Ramesh, A., & Gupta, M. (2020). Forensic acquisition and analysis of USB flash drives: Techniques and challenges. *Digital Investigation, 33,* 300995. https://doi.org/10.1016/j.diin.2020.300995

Riadi, I., Fadlil, A., & Aulia, M. I. (2020). Investigasi bukti digital optical drive menggunakan metode National Institute of Standard and Technology (NIST). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 820–828.*

Singh, R., & Kapoor, A. (2021). Impact of portable digital storage devices on productivity and cybersecurity. *International Journal of Computer Applications, 183*(3), 15–22. https://doi.org/10.5120/ijca2021921411

Subarzah, N. A. (2023). Kekuatan pembuktian alat bukti elektronik dalam tindak pidana pencucian uang terkait UU ITE. *Krisna Law Journal, 9*(3), 89–110.

Tamhidah, M. A. R. (2023). Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu dan Kejahatan Siber. *Innovative: Journal Of Social Science Research*, *3*(6), 9133–9147.

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). *Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.*

Wang, J., & Yan, Z. (2019). Trends in flash memory storage: Opportunities and security issues. *Future Generation Computer Systems, 98,* 641–653. https://doi.org/10.1016/j.future.2019.04.031

Yuwono, D. T., Juhairiah, S., & Sonedi. (2019). Analisis file carving pada file system dengan metode National Institute of Standards and Technology (NIST). *Prosiding SNRT (Seminar Nasional Riset Terapan),* 85–92. Politeknik Negeri Banjarmasin.