



Analisis Perbandingan File Carving Recuva, PhotoRec, dan FTK Imager pada Flashdisk

Mumtaz Imanullah^{1✉}, Eryal Rivano Zistafa², Yustian Servanda³

^{1,2,3} Ilmu Komputer, Universitas Mulia Balikpapan, Kota Balikpapan, 76114, Indonesia

mumtazimanullah@gmail.com

Abstract

Recovering deleted data from flash drives has become a crucial requirement in digital forensics and personal data recovery. This study compares file carving and metadata-based file recovery techniques across three applications: Recuva, PhotoRec, and FTK Imager. Fifty files of various types permanently deleted from an 8GB FAT32-formatted flash drive were tested sequentially across the three applications. Evaluation parameters included the number of recovered files, integrity through hash verification, percentage of openable files, ability to preserve original names, and scanning speed. Recuva's deep scan feature excelled in recovering metadata, including file names and folder hierarchies. PhotoRec achieved the highest recovery volume thanks to its aggressive header and footer detection, but was unable to preserve file names or directory structures. FTK Imager achieved the highest file integrity with the most stable recovery, despite requiring a longer scan time. This study confirms that no application excels in all aspects, so tool selection should be tailored to user priorities.

Keywords: *file recovery, Recuva, PhotoRec, FTK Imager, flashdisk*

Abstrak

Pemulihan data terhapus dari flashdisk menjadi kebutuhan penting dalam forensik digital maupun penyelamatan data pribadi. Penelitian ini membandingkan teknik file carving dan file recovery berbasis metadata pada tiga aplikasi: Recuva, PhotoRec, dan FTK Imager. Sebanyak 20 file beragam jenis dihapus secara permanen dari flashdisk 8 GB berformat FAT32, lalu diuji secara berurutan pada ketiga aplikasi. Parameter evaluasi mencakup jumlah file terpulihkan, integritas melalui verifikasi hash, persentase file yang dapat dibuka, kemampuan mempertahankan nama asli, dan kecepatan pemindaian. Recuva dengan fitur deep scan unggul dalam memulihkan metadata, termasuk nama file dan hierarki folder. PhotoRec mencatatkan kuantitas pemulihan tertinggi berkat deteksi header dan footer yang agresif, namun tidak mampu mempertahankan nama file maupun struktur direktori. FTK Imager menghasilkan integritas file tertinggi dengan pemulihan paling stabil, meski memerlukan waktu pemindaian lebih lama. Penelitian ini menegaskan bahwa tidak ada aplikasi yang unggul di semua aspek, sehingga pemilihan alat sebaiknya disesuaikan dengan prioritas pengguna.

Kata kunci: pemulihan file, Recuva, PhotoRec, FTK Imager, flashdisk

Jutekom is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.



1. Pendahuluan

Perkembangan teknologi informasi saat ini menjadi salah satu pondasi utama dalam kemajuan zaman ke era yang lebih modern. Tak heran tempat penyimpanan tersebut mengalami perubahan dari zaman ke zaman, dari yang awalnya besar dan memakan tempat sampai sekecil flashdisk yang bisa dibawa kemana-mana. Penggunaannya pun masif dan kemudahan akses yang tidak hanya dipakai oleh individu untuk keperluan pribadi, tapi juga bisa dipakai dalam

lingkungan profesional, pendidikan, bahkan penyelidikan hukum [1][2]. Namun dalam kemudahan ini, ada risiko untuk kehilangan data. Penghapusan tidak disengaja, kerusakan fisik, serangan malware, sampai operasi format bisa mengakibatkan data-data tersebut menjadi tidak dapat diakses [3]. Kondisi ini dapat menciptakan teknik pemulihan data, baik untuk keperluan pemulihan data pribadi maupun investigasi forensik digital [4].

Forensik digital merupakan cabang dari ilmu forensik yang berfokus pada identifikasi,

pengumpulan, pemeriksaan, dan analisis bukti digital dari berbagai perangkat elektronik [5]. Dalam konteks flashdisk, pemahaman pada sistem berkas menjadi pondasi utama dalam proses pemulihan data. Pada umumnya, flashdisk menggunakan sistem berkas FAT32 (File Allocation Table 32-bit), menjadikannya pilihan dominan karena kompatibilitas yang lintas sistem operasi [6]. Selama data yang bersangkutan belum ditimpa data baru, isi dari file asli masih dapat dipulihkan dengan teknik tertentu. Hal ini menjadikan flashdisk berformat FAT32 sebagai acuan dasar pemulihan data digital dalam penelitian ini.

Ada dua pendekatan utama dari pemulihan file di media penyimpanan yang sudah terhapus. Pertama, pendekatan berbasis metadata (metadata-based recovery), memanfaatkan informasi sistem berkas yang masih tersisa, seperti entri direktori, tabel alokasi file, serta nama dan atribut file asli. Pendekatan ini efektif apabila struktur metadata belum tertimpa [7]. Kedua, teknik file carving, yaitu metode pemulihan data yang bekerja tanpa bergantung pada metadata sistem berkas. File carving mengidentifikasi file berdasarkan pola header dan footer yang khas dari setiap format file di dalam aliran data mentah pada sektor penyimpanan [7]. Teknik ini sangat berguna ketika tabel alokasi atau entri direktori telah rusak atau tertimpa, namun isi data masih utuh secara fisik di media penyimpanan.

Recuva, dikembangkan oleh Piriform, adalah salah satu aplikasi pemulihan data yang paling populer untuk sistem berbasis Windows. Aplikasi ini bekerja terutama dengan pendekatan berbasis metadata, memanfaatkan entri direktori FAT yang masih tersisa untuk melacak file yang terhapus [9]. Fitur unggulan Recuva adalah kemampuan deep scan yang memungkinkan pemindaian menyeluruh terhadap setiap sektor pada media penyimpanan. Melalui fitur ini, Recuva mampu mempertahankan nama file asli beserta hierarki direktorinya, sehingga menghasilkan struktur pemulihan yang lebih terorganisasi dibandingkan metode carving murni [9]. Kemampuan preservasi metadata ini menjadikan Recuva pilihan yang praktis bagi pengguna awam sekalipun.

PhotoRec, yang merupakan perangkat lunak open-source yang dikembangkan oleh Christophe Grenier dari CGSecurity, menggunakan pendekatan file carving murni berbasis signature [10]. Alih-alih bergantung pada informasi sistem berkas, PhotoRec memindai setiap sektor pada

media penyimpanan dan mengidentifikasi file berdasarkan header dan footer formatnya. PhotoRec mendukung lebih dari 480 format file, menjadikannya salah satu alat pemulihan dengan cakupan terluas yang tersedia secara gratis [10]. Keunggulan utamanya terletak pada kuantitas file yang berhasil dipulihkan, terutama pada kondisi di mana sistem berkas telah rusak parah. Namun, konsekuensi dari pendekatannya yang mengabaikan metadata adalah ketidakmampuan mempertahankan nama file asli dan struktur direktori, sehingga file yang dipulihkan diberi nama generik berdasarkan posisi sektornya [10].

FTK Imager, yang dikembangkan oleh AccessData (kini Exterro), merupakan alat forensik digital profesional yang digunakan secara luas dalam investigasi hukum dan keamanan siber [11]. Berbeda dari dua aplikasi sebelumnya, FTK Imager dirancang dengan orientasi forensik yang kuat, mengutamakan integritas bukti digital melalui verifikasi hash MD5 dan SHA-1 [11]. Aplikasi ini mampu membuat salinan forensik (forensic image) dari media penyimpanan tanpa mengubah data asli, menjaga rantai kepemilikan bukti (chain of custody) yang diperlukan dalam proses hukum. FTK Imager mendukung berbagai format image forensik seperti E01 dan DD, serta dapat menganalisis **file sistem FAT32** secara mendalam untuk memulihkan file yang terhapus dengan tingkat integritas tinggi [11].

Sejumlah penelitian sebelumnya telah mengeksplorasi kinerja alat pemulihan data dalam konteks forensik digital. Hafizh (2020) membandingkan Recuva dengan Active File Recovery pada flashdisk dan menemukan bahwa keduanya memiliki keunggulan masing-masing tergantung kondisi media [9]. Pratama (2021) mendemonstrasikan kemampuan PhotoRec dalam memulihkan 2.781 file dari flashdisk berformat FAT32, menegaskan keunggulan kuantitatifnya [10]. Fakhri et al. (2023) membandingkan beberapa alat file carving menggunakan kerangka DFRWS, namun tidak secara spesifik membandingkan ketiga alat yang diteliti dalam studi ini [12]. Matondang et al. (2023) melakukan analisis perbandingan perangkat lunak forensik file carving menggunakan metode NIST, namun cakupannya tidak mencakup evaluasi simultan terhadap Recuva, PhotoRec, dan FTK Imager pada media yang sama [13]. Dasmen et al. (2024) mengimplementasikan PhotoRec untuk pemulihan file pada external storage, tetapi tanpa perbandingan langsung dengan alat lain [14]. Susanti (2025) meneliti efektivitas file carving

dengan Autopsy dan FTK Imager pada flashdisk, namun belum menyertakan Recuva dalam perbandingannya [11]. Dengan demikian, terdapat kesenjangan penelitian berupa belum adanya studi yang secara komprehensif dan sistematis membandingkan Recuva, PhotoRec, dan FTK Imager secara bersamaan dalam satu skenario pengujian terkontrol pada flashdisk berformat FAT32 dengan parameter evaluasi yang terstandarisasi.

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk melakukan analisis perbandingan kinerja tiga aplikasi pemulihan data, yaitu Recuva, PhotoRec, dan FTK Imager, pada flashdisk berformat **FAT32**. Evaluasi dilakukan terhadap lima parameter utama: (1) jumlah file yang berhasil terpulihkan dari total **20 file** yang dihapus secara permanen; (2) integritas file yang diverifikasi melalui pencocokan nilai hash MD5; (3) persentase file yang dapat dibuka dan dibaca secara normal setelah pemulihan; (4) kemampuan aplikasi dalam mempertahankan nama file asli; serta (5) kecepatan pemindaian yang diukur dalam satuan waktu. Hasil penelitian ini diharapkan dapat memberikan panduan praktis bagi pengguna dan investigator forensik digital dalam memilih alat yang paling sesuai dengan kebutuhan spesifik mereka [15].

2. Metodologi Penelitian

Penelitian ini menggunakan metode eksperimen, yaitu pengujian langsung terhadap tiga aplikasi pemulihan data pada flashdisk dalam lingkungan yang terkontrol. Pengujian dilakukan pada flashdisk berformat FAT32 dengan skenario penghapusan file menggunakan metode Shift+Delete. Alur penelitian terdiri atas empat tahapan utama: persiapan alat dan bahan, persiapan dataset, prosedur pengujian, serta pengukuran parameter evaluasi.

2.1. Alat dan Bahan

Perangkat keras yang digunakan dalam penelitian ini terdiri atas satu unit komputer berbasis sistem operasi Windows sebagai platform pengujian, serta satu unit flashdisk 8 GB yang diformat menggunakan sistem berkas FAT32 sebagai media uji. Pemilihan sistem berkas FAT32 didasarkan pada prevalensinya sebagai format default flashdisk serta relevansinya dalam konteks forensik digital [6].

Perangkat lunak yang menjadi objek perbandingan dalam penelitian ini adalah: (1) Recuva versi terbaru (Piriform), dijalankan dalam

mode deep scan; (2) PhotoRec versi terbaru (CGSecurity), dijalankan melalui antarmuka TestDisk; dan (3) FTK Imager versi terbaru (Exterro), digunakan untuk akuisisi forensic image sekaligus pemulihan file. Selain ketiga aplikasi utama tersebut, digunakan juga aplikasi HashMyFiles sebagai instrumen verifikasi nilai hash MD5 untuk mengukur integritas file hasil pemulihan [8].

2.2. Persiapan Dataset

Dataset pengujian terdiri atas 20 file yang mencakup empat kategori format, yaitu dokumen, gambar, audio, dan video. Rincian komposisinya dapat dilihat pada Tabel 1.

Tabel 1. Komposisi Dataset Pengujian

No.	Kategori	Format	Jumlah
1	Dokumen	.pdf, .docx, .txt	5 file
2	Gambar	.jpg, .png	5 file
3	Audio	.mp3, .wav	5 file
4	Video	.mp4	5 file
Total			20 file

Sebelum proses penghapusan dimulai, nilai hash MD5 dari setiap file dicatat menggunakan HashMyFiles sebagai nilai referensi (baseline). Pencatatan baseline ini menjadi acuan utama dalam pengukuran parameter integritas file pada tahap evaluasi [8].

2.3. Prosedur Pengujian

Flashdisk diformat menggunakan sistem berkas FAT32 untuk memastikan kondisi awal yang bersih. Seluruh 20 file dataset kemudian disalin ke dalam flashdisk, dan nilai hash MD5 dari setiap file diverifikasi ulang untuk memastikan integritas data sebelum penghapusan. Selanjutnya, seluruh 20 file dihapus menggunakan kombinasi tombol Shift+Delete, yang menghapus file secara langsung tanpa menempatkannya di Recycle Bin. Metode ini menandai entri direktori FAT sebagai tersedia namun tidak menimpa data secara fisik pada sektor penyimpanan, sehingga pemulihan masih dimungkinkan selama sektor tersebut belum tertimpa [7].

Setelah penghapusan, ketiga aplikasi dijalankan secara berurutan pada flashdisk yang sama dengan urutan: Recuva, PhotoRec, kemudian FTK Imager. Untuk menghindari kontaminasi antar sesi, flashdisk tidak digunakan untuk aktivitas lain di antara sesi pengujian. Khusus untuk FTK Imager, proses dimulai dengan pembuatan forensic image dari flashdisk dalam format E01, yang kemudian dimuat kembali untuk analisis dan ekstraksi file. Pendekatan ini sesuai dengan

praktik terbaik forensik digital, di mana analisis dilakukan pada salinan image dan bukan pada media asli, guna menjaga integritas barang bukti [11]. Waktu pemindaian pada setiap sesi dicatat menggunakan stopwatch digital, dimulai sejak proses pemindaian diinisiasi hingga daftar file hasil pemulihan selesai ditampilkan oleh aplikasi.

2.4. Parameter Evaluasi

Kinerja setiap aplikasi diukur berdasarkan lima parameter evaluasi yang diadopsi dari kerangka yang digunakan oleh Akintola (2025) [15], sebagai berikut:

2.4.1 Jumlah file terpulihkan,

Dihitung sebagai total file yang berhasil diidentifikasi dan dipulihkan dari 20 file yang dihapus. Parameter ini mencerminkan kemampuan kuantitatif masing-masing aplikasi.

2.4.2 Integritas file (verifikasi hashMD5),

Dilakukan dengan membandingkan nilai hash MD5 file yang dipulihkan terhadap nilai hash MD5 referensi yang dicatat sebelum penghapusan. File dinyatakan utuh apabila nilai hash-nya identik [8].

$$\text{Integritas (\%)} = \frac{\text{File dengan hash MD5 cocok}}{\text{File terpulihkan}} \times 100\%$$

2.4.3 Persentase file dapat dibuka,

Mengukur proporsi file yang dipulihkan dan dapat dibuka serta dibaca secara normal menggunakan aplikasi yang sesuai tanpa pesan error. File yang berhasil dipulihkan namun korup tidak dihitung dalam parameter ini.

$$\text{File bisa dibuka (\%)} = \frac{\text{File dapat dibuka normal}}{\text{File terpulihkan}} \times 100\%$$

2.4.4 Preservasi nama,

Mengevaluasi kemampuan aplikasi dalam mempertahankan nama file asli. Penilaian dilakukan secara dikotomis (ya/tidak) per file, kemudian dihitung persentasenya terhadap total file yang berhasil dipulihkan.

$$\text{Preservasi (\%)} = \frac{\text{File dengan nama terjaga}}{\text{File terpulihkan}} \times 100\%$$

2.4.5 Kecepatan pemindaian,

Diukur dalam detik dari awal hingga akhir proses pemindaian dalam satu kali pengukuran per aplikasi.

t = waktu pemindaian satu sesi (detik)

3. Hasil dan Pembahasan

3.1.1 Hasil Pengujian

Pengujian dilakukan terhadap 20 file dataset (5 dokumen, 5 gambar, 5 audio, 5 video) yang dihapus menggunakan metode Shift+Delete pada flashdisk berformat FAT32. Hasil pengujian terhadap ketiga aplikasi disajikan pada Tabel 2.

Tabel 2. Hasil Perbandingan Kinerja Recuva, PhotoRec, dan FTK Imager

Parameter	Recuva	PhotoRec	FTK Imager
Jumlah file terpulihkan	20/20	19/20	20/2
Integritas hash MD5	100%	84.21%	100%
File dapat dibuka	100%	100%	100%
Preservasi nama file	10%	0%	10%

3.1.2 Pembahasan

a) Jumlah File Terpulihkan

Recuva dan FTK Imager berhasil memulihkan seluruh 20 file dataset (100%), sementara PhotoRec hanya memulihkan 19 dari 20 file (95%). Satu file yang gagal dipulihkan oleh PhotoRec adalah file berformat .txt. Kegagalan ini sejalan dengan karakteristik file carving berbasis signature yang digunakan PhotoRec, file teks polos (.txt) tidak memiliki header dan footer yang khas seperti format biner (misalnya .jpg atau .mp4), sehingga sulit dikenali oleh algoritma carving [10]. Hasil ini menunjukkan bahwa keunggulan kuantitas PhotoRec lebih terlihat pada file dengan struktur biner yang jelas, bukan pada seluruh jenis format file.

b) Integritas File (Hash MD5)

FTK Imager dan Recuva mencatatkan integritas hash sempurna (100%), yang berarti seluruh file yang dipulihkan oleh kedua aplikasi tersebut identik secara bit-per-bit dengan file aslinya. PhotoRec mencatatkan integritas lebih rendah (84,21%), dengan 3 dari 19 file yang dipulihkan memiliki nilai hash berbeda dari aslinya. Berdasarkan data pengujian, ketiga file tersebut berasal dari kategori audio (.mp3), mengindikasikan bahwa proses carving berbasis header-footer pada PhotoRec rentan mengalami kesalahan batas data (boundary error) pada file dengan struktur kompresi audio, sehingga sebagian byte data turut terpotong atau tercampur dengan sektor file lain [7]. Temuan ini memperkuat klaim bahwa pendekatan berbasis metadata (Recuva) dan forensic imaging (FTK Imager) lebih unggul dalam menjaga integritas data dibandingkan carving murni, sejalan dengan tujuan FTK Imager yang memang dirancang

untuk keperluan forensik dengan standar verifikasi hash yang ketat [11].

c) Persentase File Dapat Dibuka

Ketiga aplikasi mencatatkan hasil yang identik pada parameter ini, seluruh file yang berhasil dipulihkan (20 file untuk Recuva dan FTK Imager, 19 file untuk PhotoRec) dapat dibuka dan dibaca secara normal tanpa pesan error (100%). Menariknya, meskipun PhotoRec memiliki 3 file dengan hash tidak cocok, file-file tersebut tetap dapat dibuka secara normal. Ini menunjukkan bahwa kerusakan data pada level byte tidak selalu berdampak pada kemampuan file untuk dibaca oleh aplikasi terkait, khususnya pada format yang memiliki toleransi terhadap distorsi kecil seperti file audio.

d) Preservasi Nama File

Parameter ini menjadi pembeda paling signifikan antar ketiga aplikasi. Recuva dan FTK Imager hanya mampu mempertahankan nama file asli pada 2 dari 20 file (10%), yaitu pada file berformat .docx. Sementara file lain (.pdf, .txt, .jpg, .png, .mp3, .wav, .mp4) mengalami perubahan nama, ditandai dengan karakter awal nama file yang berubah menjadi simbol seperti garis bawah (_) pada Recuva atau tanda seru (!) pada FTK Imager. Pola ini mengindikasikan bahwa karakter pertama nama file pada entri direktori/MFT tertimpa marker penghapusan, sehingga tidak dapat direkonstruksi sepenuhnya meskipun sisa nama file masih terbaca [6]. PhotoRec tidak mempertahankan nama file sama sekali (0%), karena seluruh file dipulihkan dengan nama generik berbasis ID sektor (misalnya f0447728), sesuai dengan karakteristik file carving yang tidak bergantung pada metadata sistem berkas [10].

Hasil ini menegaskan bahwa preservasi nama file bukan hanya bergantung pada pendekatan teknik (metadata-based vs carving), tetapi juga pada sejauh mana sistem berkas FAT32 menyimpan sisa informasi direktori setelah penghapusan. Bahkan aplikasi berbasis metadata seperti Recuva dan FTK Imager pun mengalami keterbatasan yang sama ketika karakter penanda penghapusan ikut menimpa bagian dari nama file asli.

3.1.3 Diskusi Umum

Secara keseluruhan, hasil pengujian menunjukkan bahwa tidak ada aplikasi yang unggul di seluruh parameter secara mutlak:

- Recuva dan FTK Imager menunjukkan performa yang hampir identik pada keempat

parameter, dengan unggul pada jumlah file terpulihkan, integritas hash, dan preservasi nama dibandingkan PhotoRec.

- PhotoRec, meskipun mencatatkan jumlah file terpulihkan yang sedikit lebih rendah dan integritas hash yang lebih rendah, tetap mampu mengembalikan isi file secara terbaca (100% dapat dibuka), namun mengorbankan seluruh informasi nama file asli.
- Parameter preservasi nama file menjadi titik lemah ketiga aplikasi secara umum pada skenario Shift+Delete di FAT32, dengan tingkat keberhasilan tertinggi hanya 10%.

Temuan ini relevan dengan praktik forensik digital, karena menunjukkan bahwa rekonstruksi metadata file (nama dan struktur) merupakan tantangan tersendiri yang terpisah dari keberhasilan rekonstruksi isi/konten file, sehingga investigator perlu mempertimbangkan kombinasi alat atau metode tambahan apabila identitas asli file menjadi krusial dalam suatu kasus [9].

4. Kesimpulan

Dari hasil penelitian ini, membandingkan dari 3 kinerja aplikasi pemulihan data, yaitu Recuva, PhotoRec, dan FTK Imager pada flashdisk berformat FAT32. Skenario penghapusan file menggunakan metode Shift+Delete dari dataset 20 file. Dari hasil pengujian menunjukkan bahwa Recuva dan FTK Imager telah memulihkan seluruh 20 file dengan hasil persentase 100%, integritas hash MD5 sempurna (100%), sementara aplikasi PhotoRec hanya memulihkan 19 file dari 20 file (95%) dengan integritas hash sebesar 84,21%. Akibat tiga file audio yang mengalami kesalahan pada proses carving. Pada parameter persentase file dapat dibuka, ketiga aplikasi mencatatkan hasil yang identik, yaitu seluruh file yang berhasil dipulihkan dapat dibuka dan dibaca secara normal (100%), meskipun beberapa file pada PhotoRec memiliki nilai hash yang tidak cocok dengan aslinya.

Pada parameter preservasi nama file, Recuva dan FTK Imager hanya mampu mempertahankan nama file asli pada 2 dari 20 file (10%), sementara PhotoRec tidak mempertahankan nama file sama sekali (0%) karena seluruh file dipulihkan dengan nama generik berbasis ID sektor. Berdasarkan temuan tersebut, dapat disimpulkan bahwa tidak ada aplikasi yang unggul di seluruh parameter secara mutlak. Recuva dan FTK Imager menunjukkan performa yang hampir identik dan lebih unggul dibandingkan PhotoRec pada aspek

jumlah file terpulihkan, integritas hash, dan preservasi nama file, sementara PhotoRec tetap mampu mengembalikan isi file secara terbaca meskipun mengorbankan informasi nama file asli. Preservasi nama file menjadi titik lemah ketiga aplikasi pada skenario pengujian ini, dengan tingkat keberhasilan tertinggi hanya 10%.

Daftar Rujukan

- [1] Sitorus J. A., Sinaga H., Situmorang M. D., Naipospos M. I., Gunawan I. (2025). "Analisis Pengaruh Memori Eksternal Terhadap Penyimpanan Data Pada Laptop". *Jurnal Penelitian Nusantara*, 1(11), 43-46.
- [2] Kusuma A. W., Alwi E. I., Ramdaniah R. (2024). "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)". *CyberSecurity dan Forensik Digital*, 7(1), 18-24.
- [3] Putra G. A. A. P., Sukerti N. K., Putra N. M. D. K. (2024). "Simulasi Investigasi pada FlashDisk dalam Mengungkap Pesan pada Kasus Perdagangan Narkoba Menggunakan Metode Steganografi". *Prosiding Seminar Hasil Penelitian Informatika dan Komputer*, 1(3), 340-345.
- [4] Anjani D., Novianti D., Ningsih R. (2020). "Pelatihan Penyelamatan Dan Perbaikan Data Pada Penyimpanan Flashdisk Untuk Guru Sekolah Dasar 19 Pal Merah, Jakarta Barat". *Jurnal Pengabdian Masyarakat (Mattawang)*, 1(2), 99-103.
- [5] Johari M., Bernadisman D., Rachma N., Dwiartmodjo H. (2025). "Sistem Forensik Digital". [Online]. Website: <https://books.google.co.id/books?id=JbDPEQAAQBAJ&lpg=PA1&ots=DN4IsKEECv&dq=forensik%20digital%20sistem%20berkas%20fat32&lr&pg=PR2#v=onepage&q=forensik%20digital%20sistem%20berkas%20fat32&f=false>
- [6] Sulaksono P. M., Santoso B. (2022). "Static Forensic Pada USB Mass Storage Menggunakan Forensic Toolkit Imager". *Jurnal Komputer Terapan*, 8(1), 132-142.
- [7] Muhardinata, Luthfi A., Ramadhani E. (2023). "Teknik Disk Carving untuk Recovery Solid State Drive Volume ReFS dan qui dengan Fitur TRIM". *Jurnal Ilmiah Ilmu Pendidikan*, 6(11), 9507-9515.
- [8] Anjelina R., Noviyanti (2024). "Analisis Forensik Dengan Menerapkan Metadata Dan Hash Studi Kasus Pada Rekaman Video". *Jurnal Informatik (IFTK)*, 20(3), 118-124.
- [9] Hafizh E. N. A. (2020). "Analisis Perbandingan Software Recuva dan Active File Recovery Dalam Mencari Bukti Digital pada Flashdisk".
- [10] Pratama P. A. E. (2021). Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept. *International Journal of Science, Technogoly, & Management*, 2(4), 1189-1196.
- [11] Susanti L. (2025). Analisis Efektivitas File Carving dalam Forensik Digital pada Flashdisk Dengan Tools Autopsy dan FTK Imager. *Jurnal Locus: Penelitian & Pengabdian*, 4(9), 8978-8989.
- [12] Fakhri La J., Riadi I., Yudhana A. (2023). "Forensic Tools Comparison on File Carving using Digital Forensics Research Workshop Framework". *Scientifi Journal of Informatics*, 10(4), 571-582.
- [13] Matondang J. Maulana I., Carudin (2023). "Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST". *Journal Of Social Science Research*, 3(4), 2154-2165.
- [14] Dasmen R. N., Triwulanda A., Rasmila, Kurniawan D. (2024). "Implementation of Digital Forensics Photorec in Recovering Lost Files on External Storage". *Penelitian Ilmu Komputer Sistem Embedded and Logic (Piksel)*, 12(1), 173-178.
- [15] Akintola G. B. (2025). "Assessing the Performance of Forensic File Recovery Tools on Deleted File from a USB Device". *DS Journal of Cyber Security*, 3(2), 1-15.