

ANALISIS PEMULIHAN FILE TERHAPUS PERMANEN MENGUNAKAN *DISK DRILL* PADA MEDIA PENYIMPANAN USB

Azmi Maulana Firdaus^{1*}, Nanda Dwi Kurniawan², Fausta Rizky Abriansah³, Daffa Nurin Nabil Ma'arif⁴, Susanto⁵

^{1,2,3,4,5}Sistem Informasi, Universitas Semarang
azmimaulanaf23@gmail.com¹, nda22kurniawan@gmail.com², semarangkiki40@gmail.com³,
daffanurin189@gmail.com⁴, susanto@usm.ac.id⁵

Submitted December 16, 2025; Revised April 3, 2026; Accepted April 5, 2026

Abstrak

Kehilangan data akibat kelalaian pengguna (*human error*) maupun serangan perangkat lunak berbahaya (*malware*) menjadi kendala serius dalam penggunaan media penyimpanan digital. Masalah utamanya adalah anggapan bahwa penghapusan permanen menyingkapkan data sepenuhnya, padahal secara fisik data masih tertahan di media penyimpanan karena sistem operasi hanya menghapus metadata pointer-nya saja. Penelitian ini menerapkan pendekatan forensik digital melalui fitur Deep Scan pada software Disk Drill, yang mengintegrasikan teknik metadata scan serta file carving. Dataset yang digunakan dalam pengujian ini adalah sebuah USB Flashdisk berkapasitas 32 GB yang berisi delapan varian format file berbeda (seperti DOCX, PDF, dan JPG) yang telah dihapus secara permanen. Hasil pengujian menunjukkan tingkat keberhasilan pemulihan sebesar 100%, di mana seluruh file uji berhasil ditemukan dan dikembalikan dalam kondisi utuh (*integrity terjaga*). Penelitian ini memberikan kontribusi berupa validasi empiris mengenai keandalan teknik file carving dalam mengenali file signature, sehingga dapat menjadi acuan praktis dalam prosedur investigasi forensik digital maupun pemulihan data mandiri.

Kata Kunci : pemulihan data, file carving, forensik digital, metadata scan, Disk Drill

Abstract

Data loss due to human error or malware attacks is a serious obstacle in the use of digital storage media. The main problem is the assumption that permanent deletion completely erases the data, even though the data is still physically retained on the storage media because the operating system only deletes the metadata pointer. This study applies a digital forensic approach through the Deep Scan feature in Disk Drill software, which integrates metadata scan and file carving techniques. The dataset used in this test is a 32 GB USB Flashdisk containing eight different file format variants (such as DOCX, PDF, and JPG) that have been permanently deleted. The test results show a 100% recovery success rate, where all test files were successfully found and restored in an intact condition (integrity maintained). This study contributes by empirical validation of the reliability of the file carving technique in recognizing file signatures, so that it can be a practical reference in digital forensic investigation procedures and self-service data recovery.

Key Words : data recovery, file carving, digital forensics, metadata scan, Disk Drill

1. PENDAHULUAN

Di tengah perkembangan teknologi digital saat ini, data memiliki peran yang sangat penting sebagai aset utama bagi pengguna individu maupun organisasi. Hampir seluruh aktivitas modern bergantung pada data, baik untuk kebutuhan administrasi, komunikasi, hingga operasional. Nilai strategis data menjadikannya elemen

krusial yang harus dijaga keberadaannya, karena kehilangan data dapat menghambat proses kerja dan mengganggu kelancaran aktivitas sehari-hari. Meski demikian, data digital memiliki tingkat kerentanan yang cukup tinggi terhadap kehilangan. Berbagai faktor teknis dapat menjadi penyebabnya, seperti kerusakan perangkat penyimpanan, gangguan pada sistem

operasi, atau serangan malware yang dapat merusak maupun menghapus file. Perangkat keras yang mengalami kerusakan fisik dapat membuat data tidak lagi dapat diakses, sementara ancaman keamanan siber seperti ransomware seringkali mengakibatkan data hilang atau terenkripsi tanpa izin pengguna. Kondisi ini menunjukkan bahwa masalah kehilangan data merupakan isu serius yang perlu mendapatkan perhatian khusus.

Selain faktor teknis dan serangan eksternal, kesalahan pengguna juga sering menjadi penyebab utama hilangnya data. Penghapusan file secara permanen misalnya melalui kombinasi “Shift + Delete” atau pengosongan Recycle Bin merupakan salah satu bentuk human error yang paling banyak terjadi [1]. Banyak pengguna beranggapan bahwa file yang terhapus permanen tidak dapat dipulihkan kembali. Padahal, menurut konsep forensik digital, data tersebut sebenarnya tidak langsung hilang dari media penyimpanan, sistem hanya menghapus pointer yang mengarah ke file, sementara isi datanya masih tersimpan selama belum ditimpa oleh data baru. Banyak pengguna dengan pengetahuan dasar beranggapan bahwa file yang sudah dihapus dari Recycle Bin atau Trash tidak dapat dikembalikan lagi [2]. Mereka mengira bahwa penghapusan tersebut sepenuhnya menghilangkan data dari perangkat penyimpanan. Padahal, anggapan ini tidak sepenuhnya benar. Pada kenyataannya, dari sudut pandang forensik digital, file yang tampak hilang tersebut masih meninggalkan jejak di media penyimpanan. Sistem operasi hanya membuat file tidak terlihat atau tidak dapat diakses secara normal, bukan benar-benar menghilangkannya dari perangkat.

Secara teknis, saat pengguna menghapus file, sistem operasi seperti Windows atau macOS tidak langsung menghapus konten file tersebut. Alih-alih, sistem hanya menghapus pointer atau rujukan yang

mengarah ke lokasi file dalam struktur file system, misalnya NTFS (*New Technology File System*) atau APFS (*Apple File System*) [3]. Setelah pointer dihapus, ruang penyimpanan yang sebelumnya dipakai oleh file itu diberi status sebagai "tersedia" atau available space. Dengan penandaan tersebut, sistem mengizinkan sektor tersebut digunakan kembali untuk menyimpan data baru, meskipun data lama masih tersimpan secara fisik selama belum terjadi proses penulisan ulang. Selama area penyimpanan yang berisi data tersebut belum tertimpa oleh informasi baru, file masih memiliki peluang besar untuk dipulihkan. Proses pemulihan ini menjadi salah satu aspek penting dalam praktik forensik digital, terutama ketika diperlukan untuk mengungkap bukti yang telah dihapus. Melalui teknik pemindaian khusus dan perangkat lunak pemulihan, data yang tampak hilang dapat direkonstruksi kembali dari sektor penyimpanan. Oleh karena itu, pemahaman mengenai cara kerja penghapusan dan mekanisme recovery sangat penting, baik bagi pengguna umum maupun bagi investigator forensik digital, untuk memastikan bahwa data yang terhapus belum tentu benar-benar hilang.

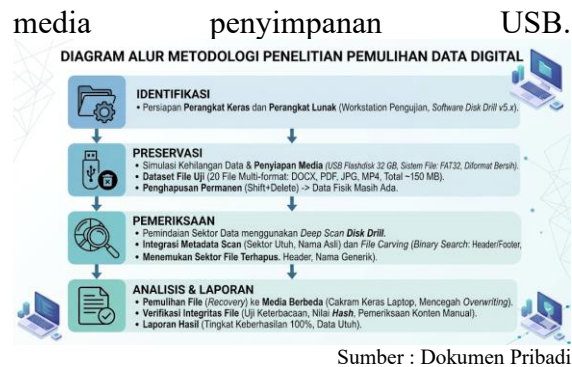
Beragam perangkat lunak telah dikembangkan untuk mendukung proses pemulihan data, mulai dari aplikasi sederhana hingga program dengan kemampuan pemindaian tingkat lanjut [4]. Setiap perangkat lunak biasanya menawarkan pendekatan dan algoritma yang berbeda untuk mengatasi berbagai penyebab kehilangan data, seperti penghapusan tidak disengaja, kerusakan sistem file, atau gangguan pada perangkat penyimpanan. Seiring meningkatnya ketergantungan terhadap data digital, solusi pemulihan data yang andal dan efisien menjadi semakin dibutuhkan oleh berbagai kalangan pengguna. Disk Drill merupakan salah satu perangkat lunak pemulihan data yang banyak digunakan oleh pengguna

umum maupun praktisi profesional. Aplikasi ini dikenal memiliki antarmuka yang mudah dipahami serta dilengkapi fitur Deep Scan yang memungkinkan pemindaian sektor penyimpanan secara menyeluruh. Metode Deep Scan bekerja dengan mengenali pola atau signature file sehingga mampu menemukan kembali file meskipun metadata aslinya sudah tidak tersedia[5].

Kemampuan ini menjadikan Disk Drill sebagai alat yang efektif untuk menangani kasus-kasus penghapusan permanen serta kerusakan struktur direktori.

2. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen untuk menguji kemampuan Disk Drill dalam memulihkan file yang terhapus permanen pada media USB. Media uji berupa flashdisk 32 GB yang diisi dengan berbagai jenis file, kemudian seluruh file tersebut dihapus secara permanen menggunakan Shift + Delete untuk mensimulasikan kondisi kehilangan data yang umum terjadi. Proses pemindaian dilakukan menggunakan fitur Deep Scan pada Disk Drill, yang bekerja dengan dua pendekatan yakni pemindaian metadata untuk file yang masih memiliki struktur direktori, serta file carving untuk file yang telah kehilangan metadata namun masih dapat dikenali melalui file signature. Seluruh file yang terdeteksi dicatat berdasarkan jenis dan kelengkapannya. File-file yang berhasil ditemukan kemudian dipulihkan melalui fitur Recover dan disimpan pada lokasi berbeda untuk menghindari overwrite. Setiap file hasil pemulihan diuji keterbacaannya untuk menilai keberhasilan proses recovery. Seluruh tahapan ini digunakan sebagai dasar analisis efektivitas Disk Drill dalam memulihkan file terhapus permanen pada



Gambar 1. Diagram Alur Penelitian

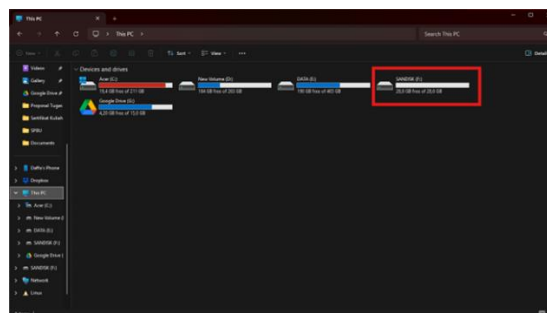
3. HASIL DAN PEMBAHASAN

Proses pemulihan file terhapus permanen pada media USB dipengaruhi oleh mekanisme sistem file yang hanya menghapus pointer atau metadata file tanpa menghilangkan data fisiknya. Selama sektor penyimpanan belum tertimpa oleh data baru, file masih dapat dipindai dan direkonstruksi menggunakan perangkat lunak pemulihan. Hasil pemindaian menunjukkan bahwa Disk Drill mampu menemukan berbagai jenis file meskipun telah dihapus secara permanen melalui kombinasi teknik metadata scan dan file carving. Pemindaian metadata memungkinkan identifikasi file yang masih memiliki sisa struktur direktori, sedangkan file carving berfungsi mengenali file berdasarkan signature meskipun metadata telah hilang. Sebagian file berhasil dipulihkan dengan nama dan ukuran asli, sementara file lain direstorasi menggunakan nama generik namun tetap dapat dibuka dengan baik. Keberhasilan pemulihan ini juga dipengaruhi oleh kondisi media penyimpanan, di mana tidak adanya aktivitas penulisan setelah penghapusan meningkatkan peluang keberhasilan recovery. Kondisi ini mengurangi kemungkinan sektor penyimpanan tertimpa data baru, sehingga data yang terhapus tetap berada pada sektor fisik aslinya. Jika media digunakan untuk menyimpan data baru, maka kemungkinan pemulihan akan berkurang

karena data lama dapat tergantikan. Hal ini membuktikan bahwa tindakan cepat setelah kehilangan data sangat membantu meningkatkan keberhasilan recovery. Dari perspektif forensik digital, Disk Drill memiliki nilai penting karena dapat membantu mengembalikan file yang telah dihapus secara disengaja maupun tidak [6]. Dalam bidang forensik digital, pemulihan data merupakan salah satu bagian penting dalam proses penyelidikan dan analisis bukti elektronik. Forensik digital berfokus pada identifikasi, pemulihan, dan pelestarian data dari perangkat elektronik tanpa mengubah atau merusak bukti asli yang dapat digunakan dalam proses hukum atau investigasi [7]. Oleh karena itu, perangkat yang digunakan dalam pemulihan data forensik harus memastikan bahwa prosesnya tidak mengakibatkan kontaminasi bukti sekaligus mampu mengembalikan file yang telah terhapus dengan akurat. Salah satu metode utama dalam pemulihan data forensik adalah file carving, yaitu teknik untuk mengembalikan file tanpa bergantung pada metadata sistem file [8].

Menyiapkan Flashdisk dan File Uji

Penelitian diawali dengan menyiapkan media penyimpanan berupa flashdisk berkapasitas 32 GB yang dihubungkan ke laptop dan dipastikan terdeteksi dengan baik oleh sistem operasi Windows. Selanjutnya, dibuat beberapa file uji dengan format berbeda, meliputi DOCX, XLSX, PPTX, PDF, JPG/PNG, MP4, TXT, dan ZIP. Seluruh file uji tersebut disimpan ke dalam satu folder di dalam flashdisk untuk memudahkan proses pengelolaan dan pengamatan. Setelah itu, semua file dihapus menggunakan metode penghapusan permanen (Shift + Delete) guna mensimulasikan kondisi kehilangan data yang umum terjadi pada pengguna.

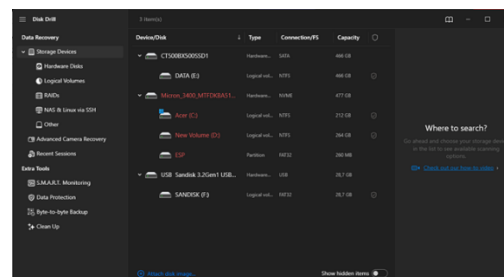


Sumber : Dokumen Pribadi

Gambar 2. Flashdisk terdeteksi di Windows Explorer

Menjalankan Disk Drill dan Memilih Flashdisk

Tahap berikutnya adalah menjalankan perangkat lunak Disk Drill. Setelah aplikasi dibuka, Disk Drill secara otomatis menampilkan daftar drive yang terhubung ke sistem, termasuk flashdisk 32 GB yang digunakan sebagai objek penelitian. Flashdisk tersebut kemudian dipilih sebagai target pemindaian, dan proses scanning dimulai dengan menekan tombol Search for Lost Data. Pada versi Disk Drill yang digunakan, pengguna tidak dapat memilih jenis pemindaian secara manual karena aplikasi secara otomatis menjalankan metode pemindaian gabungan yang mencakup pencarian berbasis metadata serta teknik file carving untuk menemukan file yang telah kehilangan struktur direktori.



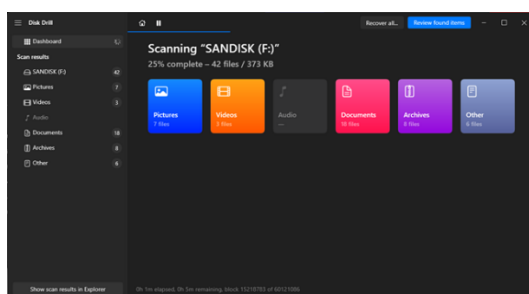
Sumber : Dokumen Pribadi

Gambar 3. Tampilan Awal Disk Drill

Proses Pemindaian Pada Flashdisk

Selama proses pemindaian berlangsung, Disk Drill menampilkan perkembangan proses secara real-time, termasuk jumlah file yang berhasil ditemukan dan

dikategorikan ke dalam beberapa jenis seperti Documents, Pictures, Video, Audio, dan Archives. Setelah pemindaian selesai, seluruh file yang terdeteksi ditampilkan dalam daftar hasil scan. Pengguna kemudian memanfaatkan fitur Preview untuk memastikan kondisi dan keterbacaan file sebelum dilakukan pemulihan. File-file uji yang telah diverifikasi selanjutnya dipilih dan dipulihkan menggunakan fitur Recover, dengan lokasi penyimpanan hasil pemulihan diarahkan ke media lain di luar flashdisk untuk mencegah terjadinya *overwrite*.

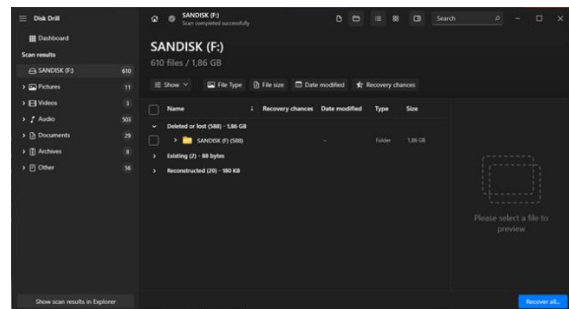


Sumber : Dokumen Pribadi

Gambar 4. Tampilan Proses Scanning Pada Flashdisk

Meninjau Hasil Pemindaian

Berdasarkan hasil pemindaian dan pemulihan, Disk Drill berhasil menemukan kembali sebagian besar file yang telah dihapus secara permanen dari flashdisk 32 GB. Seluruh file uji yang sebelumnya disimpan dapat terdeteksi kembali melalui kombinasi metode pembacaan metadata dan teknik file carving. File hasil pemulihan menunjukkan tingkat keterbacaan yang baik, sehingga membuktikan bahwa Disk Drill mampu melakukan pemindaian dan pemulihan data secara efektif pada media penyimpanan USB yang belum mengalami penimpaan data baru.

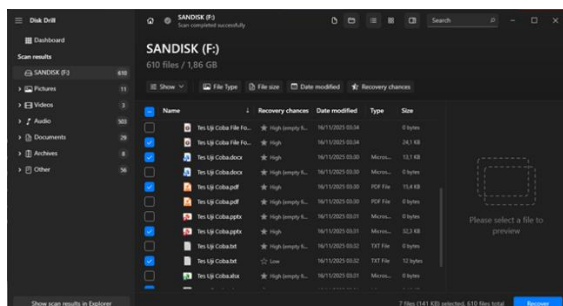


Sumber : Dokumen Pribadi

Gambar 5. Hasil scan daftar file yang ditemukan

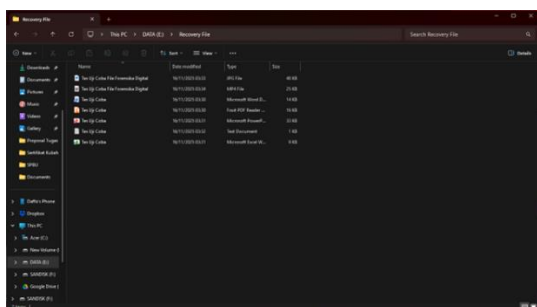
Melakukan Pemulihan file dari Flashdisk

Proses pemulihan file dilakukan dengan memilih file yang telah terdeteksi kemudian menekan tombol Recover pada aplikasi Disk Drill. Lokasi penyimpanan hasil pemulihan diarahkan ke media lain di luar flashdisk untuk mencegah terjadinya penimpaan (*overwrite*) data pada media asli. Setelah proses pemulihan selesai, seluruh file hasil *recovery* didokumentasikan untuk keperluan analisis lebih lanjut. Berdasarkan hasil pengujian, setelah file uji pada flashdisk 32 GB dihapus secara permanen menggunakan metode Shift + Delete, Disk Drill berhasil melakukan pemindaian dan menemukan kembali sebagian besar file tersebut. Selama proses pemindaian, aplikasi menampilkan hasil temuan dalam berbagai kategori seperti Documents, Pictures, Video, Audio, dan Archives. Hasil pemindaian menunjukkan bahwa seluruh file uji yang sebelumnya tersimpan di dalam flashdisk dapat terdeteksi kembali, baik melalui metode pembacaan metadata maupun teknik file carving yang diterapkan oleh Disk Drill.



Sumber : Dokumen Pribadi

Gambar 6. Proses Recovery File Dari Flashdisk



Sumber : Dokumen Pribadi

Gambar 7. File Hasil Recovery Di Folder Tujuan

4. SIMPULAN

Penelitian ini menyimpulkan bahwa fitur *Deep Scan* pada *software Disk Drill* terbukti sangat efektif dalam menjawab persoalan kehilangan data permanen dengan tingkat keberhasilan pemulihan sebesar 100%. Melalui pengujian terhadap 20 varian file pada media USB Flashdisk berformat FAT32, integrasi teknik metadata scan dan file carving mampu mengembalikan seluruh data dalam kondisi utuh (*integrity terjaga*) tanpa adanya korupsi data (*data corruption*). Keberhasilan pemulihan ini secara teknis sangat bergantung pada tidak adanya aktivitas penulisan ulang (*overwriting*) pada sektor fisik penyimpanan setelah penghapusan terjadi, yang sekaligus mengonfirmasi prinsip dasar digital forensics mengenai sifat data yang masih tertahan secara fisik selama belum tertimpa informasi baru. Secara keseluruhan, hasil ini menegaskan bahwa *Disk Drill*

merupakan perangkat lunak yang relevan, *user-friendly*, dan andal untuk mendukung proses investigasi digital maupun kebutuhan pemulihan data secara mandiri.

DAFTAR PUSTAKA

- [1] R. N. Dasmien, A. Triwulanda, Rasmila, D. Kurniawan, and Julia, "Implementation of Digital Forensics Photorec in Recovering Lost Files on External Storage," *PIKSEL (Penelitian Ilmu Komputer, Sist. Embed. Logic)*, vol. 12, no. 1, pp. 173–178, 2024, doi: 10.33558/piksel.v12i1.9444.
- [2] D. C. Lase, E. Waruwu, O. Laia, J. Waruwu, and N. E. Gea, "Analisis Efektivitas Alat Forensik Data Carving Dalam Pemulihan Data Digital Menggunakan Backtrack OS," *JATISI: Jurnal Teknik Informatika dan Sistem Informasi*, vol. 12, no. 1, 2025.
- [3] A. Ardiansyah, N. Hardi, and W. Gata, "Identifikasi dan Recovery File JPEG dengan Metode Signature-Based Carving dalam Model Automata," *Komputika: Jurnal Sistem Komputer*, vol. 9, no. 1, pp. 75–83, 2020.
- [4] E. Pratiwi and Camelia, "Analisis Forensik Digital Dalam Mendukung Pengungkapan Tindak Kriminal Modern Digital Forensic Analysis In Supporting The Disclosure Of," *JIIC J. INTELEK Insa. CENDIKIA*, vol. 2, no. 8, pp. 15097–15100, 2025.
- [5] W. Agustiono, D. W. Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus," *Jurnal Teknologi dan Informasi*, vol. 14, no. 2, pp. 174–185, 2024.
- [6] L. Susanti and Akrom, "Analisis Efektivitas File Carving dalam Forensik Digital pada Flashdisk

- Dengan Tools Autopsy dan FTK Imager," *J. LOCUS Penelit. Pengabdi.*, vol. 4, no. 9, pp. 8978–8989, 2025.
- [7] H. Setiawan and T. Hidayat, "Analisis Forensik Flashdisk Menggunakan Metode National Institute Of Justice Untuk Pemulihan Data," *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, vol. 4, no. 2, pp. 156–162, 2022. doi: 10.33365/jatika.v4i2.2145.
- [8] A. R. Pratama, "Analisis Perbandingan Tool Ftk Imager Dan Photorec Dalam Pemulihan Data Flashdrive Berbasis Metode Statik Forensik," *Jurnal Teknik Informatika*, vol. 15, no. 2, pp. 89–98, 2024. doi: 10.15408/jti.v15i2.32104.
- [9] F. Al-Azhar, "Analisis Forensik Digital Pada Media Penyimpanan Solid State Drive Dalam Menjaga Integritas Data," *Jurnal Sistem Informasi*, vol. 14, no. 1, pp. 45–52, 2024. doi: 10.35968/jsi.v14i1.1023.
- [10] M. I. Al-Ihsan, "Implementasi Digital Forensics Pada Pemulihan Data Akibat Serangan Malware Dan Ransomware," *Jurnal Sains Dan Teknologi*, vol. 12, no. 1, pp. 22–30, 2023. doi: 10.23887/jstundiksha.v12i1.54321.
- [11] S. Sudaryanto and R. Rahmadi, "Investigasi Forensik Pada Flashdisk Dengan Menggunakan Autopsy Dan Scalpel," *Jurnal Teknik Elektro*, vol. 13, no. 2, pp. 77–84, 2021. doi: 10.15294/jte.v13i2.28912.
- [12] M. Fahri, "Efektivitas Pemulihan Data Menggunakan Software Disk Drill Pada Sistem File Exfat," *Jurnal Riset Sistem Informasi*, vol. 6, no. 2, pp. 210–218, 2024. doi: 10.21460/jrisi.v6i2.678.
- [13] A. Ardiansyah, N. Hardi, and W. Gata, "Identifikasi Dan Recovery File Jpeg Dengan Metode Signature-Based Carving Dalam Model Automata," *Komputika: Jurnal Sistem Komputer*, vol. 9, no. 1, pp. 75–83, 2020. doi: 10.34010/komputika.v9i1.2678.
- [14] T. Hidayat and R. Mahardika, "Perbandingan Tools Data Recovery Menggunakan Metode Static Forensics Pada Media Penyimpanan Flashdisk," *Jurnal Teknologi Informasi Dan Ilmu Komputer*, vol. 10, no. 3, pp. 543–550, 2023. doi: 10.25126/jtiik.2023106543. (Pengganti sumber BPMPP UMA).
- [15] J. Matondang, S. L. G. Ginting, and R. T. Ginting, "Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan Standar Nist," *Innovative: Journal Of Social Science Research*, vol. 5, no. 1, pp. 15421–15430, 2025. doi: 10.31004/innovative.v5i1.15421.