AJIE - Asian Journal of Innovation and Entrepreneurship
(e-ISSN: 2477-0574; p-ISSN: 2477-3824)
Vol. 09, Issue. 02, May 2025
DOI: 10.20885/ajie.vol9.iss2.art5

Perbandingan Hasil Recovery File terhadap Penghapusan File menggunakan Perintah Sdelete dan Shift+Delete

Rosi Rahmadi Syahputra [1*], Yudi Prayudi [2]

[1,2] Program Studi Informatika Program Magister, Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta, Indonesia
**Corresponding Email*: 23917005@students.uii.ac.id

ABSTRAK

Pemulihan data yang telah dihapus merupakan aspek penting dalam investigasi digital forensik, terutama dalam mengidentifikasi barang bukti yang relevan. Namun, teknik penghapusan seperti perintah Sdelete mengimplementasikan standar Department of Defense (DoD) 5220.22-M yang dapat menghapus dengan permanen sehingga proses pemulihan bukti digital dari media penyimpanan akan sulit, sedangkan penghapusan menggunakan Shift+Delete hanya menghilangkan referensi *file* tanpa menimpa data, sehingga memungkinkan pemulihan data dengan teknik *file carving*. Penelitian ini menggunakan metode static forensic, di mana data yang ada didalam flashdisk telah dihapus dan dilakukan akuisisi menggunakan FTK Imager sehingga menghasilkan *file imaging* untuk menjaga integritas barang bukti. Setelah itu, *file imaging* diproses menggunakan *tools file carving*. Penelitian ini bertujuan untuk melakukan perbandingan hasil *recovery* yang dihapus menggunakan perintah Sdelete dan kombinasi tombol Shift + Delete dan menilai berdasarkan persentase tertinggi dari hasil tiga *tools file carving*, yaitu Autopsy, Magnet Axiom, dan Photore. Hasil penelitian menunjukkan bahwa *file* yang dihapus menggunakan Sdelete tidak dapat dipulihkan oleh ketiga *tools*, baik dari segi temuan artefak maupun kesesuaian nilai hash, sesuai dengan klaim Microsoft. Sebaliknya, *file* yang telah dihapus menggunakan kombinasi tombol Shift + Delete masih bisa dipulihkan dengan keberhasilan yang bervariasi. PhotoRec memiliki tingkat pemulihan tertinggi (90%), diikuti oleh Autopsy (88%) dan Magnet Axiom (60%). Dari segi kesesuaian nilai hash, PhotoRec mencapai 80%, sementara Autopsy 76% dan Magnet Axiom 50%. Temuan ini mengkonfirmasi bahwa Sdelete efektif dalam menghapus data secara permanen, sementara kombinasi Shift + Delete masih memungkinkan pemulihan dengan tingkat keberhasilan yang beragam. Harapan penulis, penelitian ini bisa menjadi pengetahuan baru bagi penyidik digital forensik dalam hal pemilihan *tools file carving* yang paling sesuai untuk pemulihan bukti digital.

Kata Kunci: Digital Forensik, *File carving*, *Recovery* Data, Sdelete, Static Forensic.

ABSTRACT

The recovery of deleted data is an important aspect of forensic digital investigations, especially in identifying relevant evidence. However, deletion techniques such as the Sdelete command implement the Department of Defense (DoD) 5220.22-M standard which can permanently delete so that the process of recovering digital evidence from storage media will be difficult, while deletion using Shift+Delete only removes file references without overwriting the data, thus allowing data recovery with file carving techniques. This study uses a static forensic method, where the data in the flash drive has been deleted and acquired using FTK Imager so as to produce an imaging file to maintain the integrity of the evidence. After that, the imaging file is processed using file carving tools. This study aims to compare the results of deleted recovery using the Sdelete command and the Shift + Delete key combination and assess based on the highest percentage of the results of three file carving tools, namely Autopsy, Axiom Magnet, and Photore. The results of the study show that files deleted using Sdelete cannot be recovered by the three tools, both in terms of artifact findings and

the suitability of hash values, according to Microsoft's claims. In contrast, files that have been deleted using the Shift + Delete key combination can still be recovered with varying success. PhotoRec has the highest recovery rate (90%), followed by Autopsy (88%) and Axiom Magnet (60%). In terms of hash value suitability, PhotoRec reaches 80%, while Autopsy 76% and Axiom Magnet 50%. These findings confirm that Sdelete is effective in permanently deleting data, while the Shift + Delete combination still allows for recovery with varying success rates. The author hopes that this research can be a new knowledge for digital forensic investigators in terms of selecting the most suitable file carving tools for digital evidence recovery.

Keywords: *Digital Forensik, File carving, Recovery Data, Sdelete, Static Forensic*

1. Pendahuluan

Secara umum, aktivitas kejahatan siber yang telah dilakukan oleh pelaku meninggalkan jejak digital yang dapat dijadikan barang bukti dalam proses penyelidikan (Setiawan et al., 2022). Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE), direvisi pada tahun 2016 dan revisi kedua pada tahun 2024 diberlakukan untuk menangani kasus kejahatan siber memiliki fungsi sebagai alat hukum dalam menangani dan memberikan ganjaran terhadap pelaku kejahatan siber.

Hasil kejahatan siber umumnya disimpan pada media penyimpanan yang digunakan sebagai wadah *file* hasil pencurian, penindasan, penipuan (Agustiono et al., 2024) menjadikannya sebagai barang bukti yang berisi rekam jejak dari aktivitas kejahatan, dimana masih dapat dilakukan tindakan membuka, membaca, mengedit, menghapus dan memformat menggunakan komputer. (Dasmen et al., 2024). Ketika tindakan kejahatan telah dilakukan, untuk menutupi atau menghilangkan jejak, pelaku cenderung melakukan tindakan dengan menghapus dan/atau memformat semua *file* yang telah dikumpulkan dalam aktivitas kejahatan yang dilakukan (Yuwono & W, 2020). Beberapa teknik yang bisa digunakan dalam menghapus data, dapat dengan cara manual, menggunakan kombinasi tombol Shift + Delete atau menggunakan *tools* (Jupriadi Fakhri et al., 2023). Salah satu *tool* hapus yaitu dengan menggunakan perintah Sdelete. Sdelete merupakan *tool* berbasis perintah CMD yang menghapus data dengan menimpa *file* serta mengimplementasikan standar Department of Defense (DoD) 5220.22-M, untuk menghapus informasi dan memastikan data tidak dapat diakses (Microsoft, 2022).

Aktivitas menghilangkan bukti digital dari media penyimpanan dapat diatasi menggunakan *tools file carving* yang dapat melakukan pemulihan data yang dihapus atau diformat dengan mengenali tanda khusus yang ada di dalam struktur data dan melakukan identifikasi keberadaan *file* (Matondang et al., 2023). *File carving* menjadi hal penting dalam penerapan ilmu digital forensik sebagai upaya menemukan informasi yang berada di dalam struktur sistem *file* pada media penyimpanan (Pratama et al., 2021). Teknik ini digunakan untuk melakukan *recovery* data didalam media penyimpanan yang telah dihapus, memungkinkan bagian-bagian *file* yang tersebar pada media penyimpanan untuk disusun kembali menjadi *file* utuh yang dapat diakses (Porter et al., 2021).

Dalam menyelidiki jejak kejahatan yang ditinggalkan pelaku, maka dibutuhkan proses digital forensik yang bertujuan untuk memperoleh, mengumpulkan, memulihkan, melakukan analisis serta menyajikan bukti digital (Julian et al., 2023). Pemulihan data merupakan hal terpenting yang dilakukan oleh penyidik untuk menghasilkan bukti yang sah di pengadilan (Yuwono & W, 2020). Berbagai *tools* pemulihan data baik gratis maupun berbayar dapat digunakan oleh ahli digital forensik. (Abdillah & Prayudi, 2022). Studi kasus penelitian ini adalah aktivitas kejahatan digital dengan melakukan penghapusan barang bukti digital dari media penyimpanan flashdisk menggunakan perintah Sdelete dan Shift + Delete dan menggunakan metode static forensic dalam melakukan akuisisi flashdisk, karena flashdisk merupakan media penyimpanan *non-volatile* sehingga tetap tersimpan meskipun perangkat dimatikan, maka digunakan metode static forensic, yaitu cara analisa forensik yang dilakukan pada media yang tidak aktif atau dalam kondisi *offline*. (Muhardinata et al., 2023).

Beberapa penelitian sebelumnya telah mengkaji perbandingan *tools file carving* dalam hal melakukan *recovery file*. Penelitian yang dilakukan (Fakhri et al., 2023) membandingkan hasil *recovery tools* Foremost dan Scalpel pada objek flashdisk berdasarkan nilai *hash* dan artefak yang ditemukan, dengan hasil penelitian Foremost lebih unggul dari Scalpel. Penelitian serupa oleh (Julian et al., 2023) melakukan perbandingan kinerja *tools file carving* Autopsy, Recuva, Stellar, Puran dan Easus dengan kesimpulan Autopsy berhasil menemukan 83% file. Recuva, puran dan easus sebesar 66% dan stellar berhasil merecovery sebesar 33%.

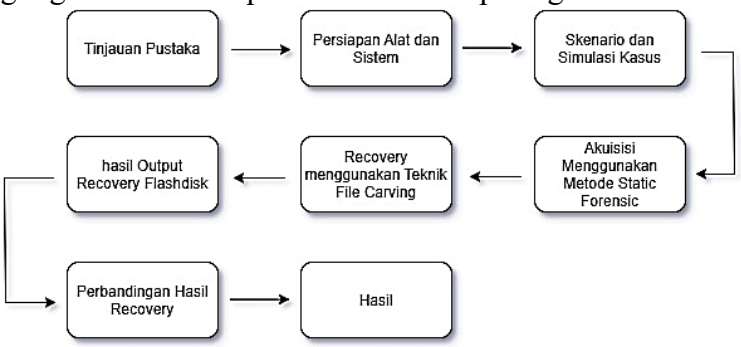
Penelitian lainnya (Rafiq et al., 2022) mengevaluasi Magnet Axiom dan Belkasoft Evidence menggunakan metode NIST terhadap objek Instagram, menunjukkan bahwa Axiom memiliki akurasi *recovery* sebesar 83,3% sedangkan Belkasoft hanya 50%. NIST juga digunakan pada penelitian (Yuladi & Indrayani, 2023) menemukan bahwa Axiom memiliki keunggulan dalam melakukan *recovery* dengan tingkat akurasi sebesar 81,8% dibandingkan MOBILedit yang hanya 72,7%. Penelitian (Matondang et al., 2023) juga membahas perbandingan hasil *recovery* menggunakan *tool* Autopsy, PhotoRec, Scalpel dan Fremost dengan objek menggunakan flashdisk, hasil didapat yaitu PhotoRec menunjukkan kinerja *recovery* sebesar 80%, Autopsy 54,16%, Scalpel 15% dan Foremost 10%.

Meskipun penelitian-penelitian terdahulu tersebut hanya melakukan perbandingan *tools file carving*, penelitian ini mengisi kekosongan literatur yang berkontribusi dengan memberikan analisis komparatif terhadap tiga *tools file carving*, Autopsy, Magnet Axiom dan PhotoRec dalam menghadapi dua skenario penghapusan data yang berbeda, yaitu penghapusan biasa menggunakan kombinasi tombol Shift+Delete dan penghapusan permanen menggunakan perintah Sdelete, dengan mengevaluasi jumlah *file* yang berhasil dipulihkan dan tingkat keidentikan nilai *hash* antar *file*.

2. Metode Penelitian

2.1 Tahapan Penelitian

Alur metodologi yang digunakan untuk penelitian terlihat pada gambar 1.



Gambar 1. Alur Metodologi Penelitian

Tinjauan pustaka sebagai langkah awal yang bertujuan dalam mengumpulkan informasi yang berkaitan dengan beberapa teori mengenai digital forensik, akuisisi, *tools file carving*, sehingga dapat menjangkau tujuan dari penelitian ini. Selanjutnya, setelah alat dan sistem telah disiapkan, peneliti melakukan akuisisi, *recovery file,* dan perbandingan terhadap hasil *recovery tools file carving,* digital forensik dalam memulihkan data yang dihapus menggunakan Sdelete dan Shift + Delete.

Peneliti mengimplementasikan metode static forensic dengan melakukan *imaging* atau pembuatan salinan *bit-by-bit* dari seluruh isi flashdisk agar flashdisk asli dapat disimpan dalam kondisi tidak tersentuh untuk menjaga integritas data. Metode ini dipilih karena relevan dengan flashdisk yang bersifat *non volatile* yang tetap menyimpan data meskipun daya dimatikan. Setelah dilakukan akuisisi menggunakan metode static forensic, peneliti menggunakan teknik *file carving*, *tool* yang digunakan akan melakukan pemindaian pada data yang telah dihapus permanen kemudian akan di recovery secara otomatis. Teknik ini akan melakukan pencarian *file* yang telah dihapus berdasarkan *header* dan *footer* (Sari & Mohamad, 2020).

2.2 Alat dan Sistem

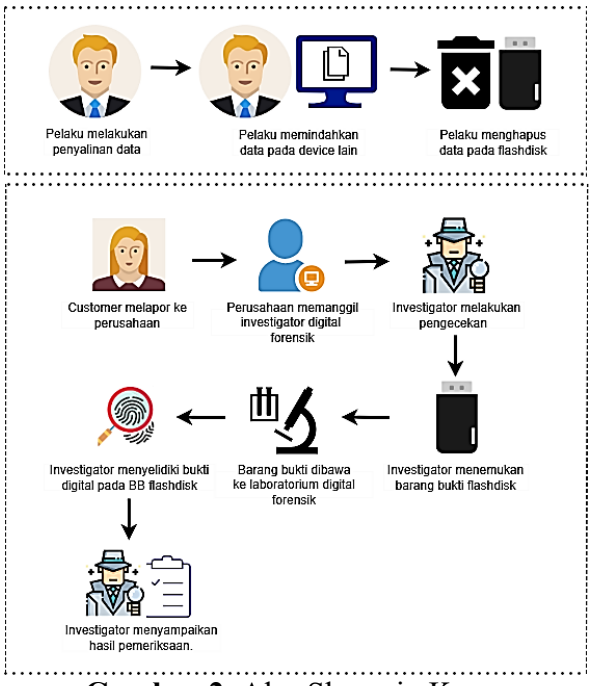
Peneliti mempersiapkan peralatan untuk diterapkan selama proses akuisisi dan *recovery* data secara langsung. Tahap awal mencakup *hardware* dan *software* yang diperlukan untuk menjalankan penelitian ini. Beberapa peralatan yang dipersiapkan ditampilkan pada tabel 1.

Tabel 1. *Hardware* dan *software*

No	Nama Perangkat	Keterangan
1	Laptop Lenovo seri Thinkpad L480	*Hardware*
2	FlashDisk 8 GB	*Hardware*
3	HashMy*Files*	*Tool Hashing*
4	Sdelete.exe	*Tool Delete*
5	AccessData FTK Imager v4.7.1.2	*Tool Imaging*
6	Autopsy v4.21.0	*Tool File Carving*
7	Magnet AXIOM Examine v5.4.0.26185	*Tool File Carving*
8	PhotoRec 7.2	*Tool File Carving*

2.3 Skenario Kasus

Saat flashdisk ditemukan, flashdisk dinyatakan kosong setelah dilakukan pengecekan, flashdisk tersebut dianggap mencurigakan menyimpan bukti yang telah dihapus oleh pelaku kejahatan. Karena kecurigaan tersebut, dilakukan proses akuisisi menggunakan metode static forensic. Untuk mendapatkan *file imaging*, penyidik menggunakan *tool* FTK Imager. Hasil *imaging* tersebut dilakukan *working copy* agar *file* asli *imaging* tidak rusak dan *file working copy imaging* tersebut digunakan sebagai sumber data untuk dilakukan *recovery file.* Selanjutnya, *file working copy* dibuka melalui *tool file carving* Autopsy, Magnet Axiom dan PhotoRec untuk dilakukan proses *recovery.*



Gambar 2. Alur Skenario Kasus

Berikut alur skenario kasus berdasarkan pada gambar 2 yang bermula dari tindakan yang dilakukan oleh pelaku. Langkah – langkah yang dilakukan pelaku:

1. Pelaku melakukan penyalinan data dari komputer perusahaan menggunakan flashdisk.
2. Hasil *file* salinan data perusahaan dipindahkan pelaku pada *device* lain.
3. Untuk menghilangkan jejak pelaku menghapus keseluruhan data yang ada didalam flashdisk menggunakan perintah Sdelete. Karena Sdelete memerlukan proses dan waktu dalam penghapusan, untuk mempercepat penghilangan bukti pelaku menghapus data-data lainnya menggunakan kombinasi tombol Shift + Delete.

Selanjutnya, *customer* perusahaan merasa dirugikan karena datanya telah digunakan dalam pembuatan akun pinjaman online dan *customer* hanya memberikan data pribadi termasuk Gmail tersebut pada perusahaan Dango. Oleh sebab itu, *customer* melapor pada perusahaan dan perusahaan menindak lanjuti dengan memanggil investigator digital forensik. Setelah surat investigasi diterima oleh investigator, langkah – langkah yang dilakukan investigator yaitu :

1. Investigator melakukan pengecekan pada perusahaan.
2. Setelah dilakukan pengecekan, investigator menemukan barang bukti flashdisk diatas meja salah satu karyawan dan mengamankannya.
3. Flashdisk dibawa ke laboratorium digital forensik untuk dilakukan penyelidikan.
4. Investigator melakukan akuisisi pada flashdisk menggunakan komputer laboratorium digital forensik dan *tool* menggunakan FTK Imager.
5. Setelah dilakukan *imaging* dan mendapatkan hasil *image* dari flashdisk, dilakukan pemeriksaan serta melakukan analisis menggunakan *tools file carving.*
6. Investigator menuliskan hasil dan menyampaikan hasil keseluruhan dari temuan yang ada didalam flahsdisk kepada pihak perusahaan.

Secara garis besar terdapat tiga tahapan dalam simulasi kasus penelitian ini:

1. Penyalinan dan penghapusan *file* : Penyalinan *file* dilakukan sebagai data untuk dilakukan penghapusan berdasarkan folder yang telah dibuat. Folder tersebut diberi nama sdeleteCMD dan shift+delete. Selanjutnya, folder dihapus menggunakan perintah Sdelete dan kombinasi tombol shift+delete.
2. Melakukan static forensic terhadap flashdisk : Pada flashdisk yang telah kosong, dilakukan proses *imaging* menggunakan *Tool* FTK untuk mendapatkan *file Imaging* serta membuat *working copy file imag*ing.
3. Melakukan *recovery* dan analisis : *File working copy* dilakukan *recovery* menggunakan *tools* Autopsy, Magnet Axiom dan PhotoRec. Hasil *recovery* digunakan untuk melakukan analisis data.

2.4 Kriteria Penilaian dan Data Uji

Dalam melakukan penilaian terhadap *tools file carving* berdasarkan dua kriteria, yaitu jumlah *file* yang dapat diakses dan keidentikan nilai *hash* setelah data yang telah disiapkan dilakukan penghapusan menggunakan hapus Sdelete dan hapus shift+delete. Adapun waktu yang diperlukan oleh masing-masing *tools* dalam melakukan proses *recovery* hanya sebagai informasi tambahan dan tidak digunakan sebagai kriteria dalam penilaian *tools*.

Data uji yang disiapkan dalam penelitian ini masing-masing berjumlah 5 *file* pada setiap ekstensi *file*, yang terdiri dari *file* dokumen yang berekstensi .pdf dan .docx, ekstensi *file* gambar yakni .jpg dan .png, ekstensi *file* audio yakni .mp3 dan .wav, ekstensi *file* video yakni .mp4 dan .avi dan ekstensi *file* arsip yakni .zip dan .rar.

3. Hasil dan Pembahasan

3.1 Akuisisi Menggunakan Metode Static Forensic

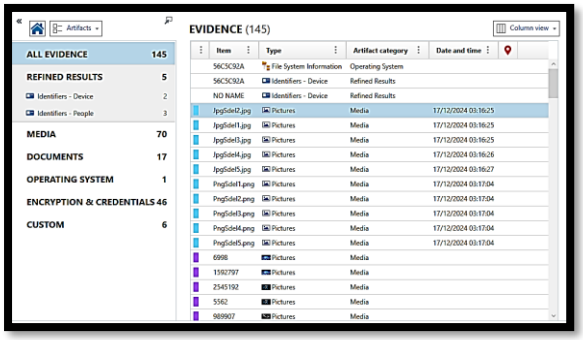
Proses akuisisi dimulai dengan pembuatan *image bit-by-bit* dari flashdisk yang berkapasitas 8 GB menggunakan FTK Imager yang bertujuan untuk membuat salinan digital dari seluruh isi flashdisk yang kemudian digunakan sebagai dasar untuk proses analisis lebih lanjut, sementara flashdisk asli disimpan untuk menjaga keutuhan barang bukti. Setelah proses akuisisi, FTK Imager memberikan informasi berupa nilai *hash* (MD5 dan SHA-1) flashdisk. Setelah proses akuisisi selesai, *file image* dari flashdisk kemudian digunakan dalam tahap *recovery* menggunakan *tools file carving*.

3.2 Recovery Menggunakan Teknik File Carving

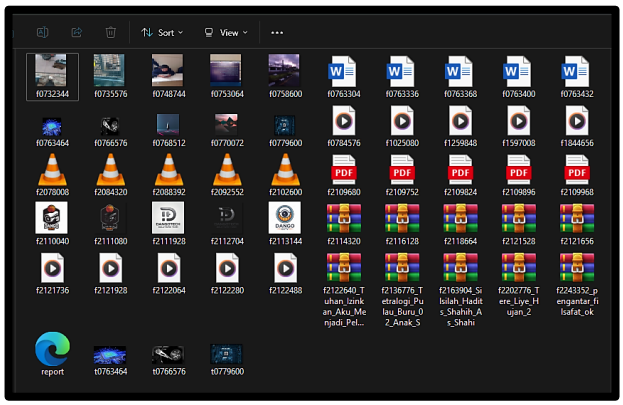
Teknik *file carving* dalam proses ini memanfaatkan *tools* Autopsy, Magnet Axiom, dan PhotoRec untuk mengembalikan beberapa jenis *file* gambar, dokumen, video, audio, dan arsip. Hasil *recovery* dianalisis berdasarkan jumlah *file* yang berhasil ditemukan dan kesesuaian nilai *hash* dengan *file* asli untuk menilai setiap *tools*. Autopsy memiliki kemampuan untuk mengenali struktur sistem *file* secara menyeluruh, termasuk *file* media yang terekam, metadata seperti Exif, serta menyusun

tampilan artefak secara visual terorganisir dalam bentuk *timeline* dan *thumbnail* (Nayak, 2024). Magnet Axiom melakukan *recovery* awal dengan parsing metadata sistem *file*, kemudian dilanjutkan dengan proses *post-process carving* untuk mendeteksi artefak yang tidak terstruktur, meskipun demikian, pendekatan yang digunakan tidak sepenuhnya berbasis *signature* (Siamukulule, 2024). Berbeda dari *tools* lainnya, PhotoRec menggunakan metode *file carving* berbasis *signature*, yaitu dengan mengenali pola *header* dan *footer file* secara langsung dari blok data, tanpa bergantung pada struktur sistem *file* (cgsecurity, 2024).

Gambar 3. Hasil *Tool* Autopsy



Gambar 4. Hasil *Tool* Magnet Axiom



Gambar 5. Hasil *Tool* PhotoRec

Sebagaimana pada gambar 3, Autopsy memelukan waktu 2 jam 28 menit 27 detik dan berhasil melakukan *recovery file* dengan *images* sebanyak 824 artefak, video 20 artefak, audio 30 artefak, archives 19 artefak, PDF 18 artefak, office 6 artefak. Sementara itu pada gambar 4, Magnet Axiom memerlukan waktu 6 menit, dengan hasil *recovery* terdiri dari refined result sebanyak 5, media sebanyak 70, documents sebanyak 17, operating system sebanyak 1, encryption & credentials sebanyak 46 dan costum sebanyak 6. Hasil dari *recovery* terakhir yakni pada gambar 5 menggunakan PhotoRec yang tidak memiliki fitur mencatat waktu, dengan hasil keseluruhan *recovery* sebanyak 54 artefak. Meskipun waktu yang diperlukan dalam melakukan recovery dicatat, informasi ini tidak dijadikan kriteria dalam penilaian *tools*.

3.3 Hasil *Output Recovery* flashdisk

Penulis menuangkan hasil pada tabel 2 dan tabel 3. Hasil ditulis menjadi 3 kategori yaitu, jumlah artefak yang ditemukan, *file* tidak dapat diakses dan *file* tidak ditemukan. Dalam menemukan artefak, penulis menggunakan fitur pada *tool* Autopsy dan Magnet Axiom seperti *search* dan *tag* sebagai penandaan artefak. Sedangkan *tool* PhotoRec tidak memiliki fitur tersebut, karena hasil hanya dalam bentuk folder yang keseluruhan isinya memuat langsung artefak-artefak yang telah ditemukan.

Tabel 2. *File* temuan dan keidentikan nilai *hash* hapus menggunakan Sdelete

Tools	Nama File	Format File	Jumlah artefak ditemukan	Keidentikan nilai hash
Autopsy	Gambar	Jpg	*File* tidak dapat diakses	Tidak identik
		Png	*File* tidak dapat diakses	Tidak identik
	Dokumen	Docx	*File* tidak ditemukan	Tidak ditemukan
		Pdf	*File* tidak dapat diakses	Tidak identik
	Audio	Mp3	*File* tidak dapat diakses	Tidak identik
		Wav	*File* tidak dapat diakses	Tidak identik
	Video	Mp4	*File* tidak dapat diakses	Tidak identik
		Avi	*File* tidak dapat diakses	Tidak identik
	Arsip	Rar	*File* tidak dapat diakses	Tidak identik
		Zip	*File* tidak dapat diakses	Tidak identik
Magnet Axiom	Gambar	Jpg	*File* tidak dapat diakses	Tidak identik
		Png	*File* tidak dapat diakses	Tidak identik
	Dokumen	Docx	*File* tidak ditemukan	Tidak ditemukan
		Pdf	*File* tidak dapat diakses	Tidak identik
	Audio	Mp3	*File* tidak dapat diakses	Tidak identik
		Wav	*File* tidak dapat diakses	Tidak identik
	Video	Mp4	*File* tidak dapat diakses	Tidak identik
		Avi	*File* tidak dapat diakses	Tidak identik
	Arsip	Rar	*File* tidak ditemukan	Tidak ditemukan
		Zip	*File* tidak ditemukan	Tidak ditemukan
PhotoRec	Gambar	Jpg	*File* tidak ditemukan	Tidak ditemukan
		png	*File* tidak ditemukan	Tidak ditemukan
	Dokumen	Docx	*File* tidak ditemukan	Tidak ditemukan
		Pdf	*File* tidak ditemukan	Tidak ditemukan
	Audio	Mp3	*File* tidak ditemukan	Tidak ditemukan
		Wav	*File* tidak ditemukan	Tidak ditemukan
	Video	Mp4	*File* tidak ditemukan	Tidak ditemukan
		Avi	*File* tidak ditemukan	Tidak ditemukan
	Arsip	Rar	*File* tidak ditemukan	Tidak ditemukan
		Zip	*File* tidak ditemukan	Tidak ditemukan

Dari pencarian dan hasil, didapati bahwa data yang dihapus menggunakan perintah Sdelete seperti yang tertuang pada tabel 2 tidak ditemukan satupun artefak yang dapat diakses / dibuka. Sdelete melakukan pengrusakan pada *file* sehingga artefak yang ditemukan tidak dapat diakses dengan kondisi *corrupt*.

Tabel 3. *File* temuan dan keidentikan nilai *hash* pada hapus menggunakan Shift + Delete

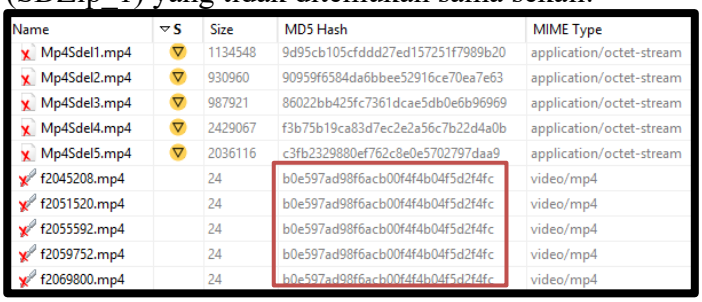
Tools	Nama File	Format File	Jumlah artefak ditemukan	Keidentikan nilai hash
Autopsy	Gambar	Jpg	5 artefak	5 *file* identik
		Png	5 artefak	5 *file* identik
	Dokumen	Docx	5 artefak	5 *file* identik
		Pdf	5 artefak	5 *file* identik
	Audio	Mp3	5 artefak	3 *file* identik
		Wav	5 artefak	5 *file* identik
	Video	Mp4	*File* tidak ditemukan	Tidak ditemukan
		Avi	5 artefak	5 *file* identik
	Arsip	Rar	5 artefak	1 *file* identik
		Zip	4 artefak	4 *file* identik

Magnet Axiom	Gambar	Jpg	5 artefak	5 *file* identik
		Png	5 artefak	5 *file* identik
	Dokumen	Docx	5 artefak	5 *file* identik
		Pdf	5 artefak	0 *file* identik
	Audio	Mp3	*File* tidak ditemukan	Tidak ditemukan
		Wav	*File* tidak ditemukan	Tidak ditemukan
	Video	Mp4	5 artefak	5 *file* identik
		Avi	5 artefak	5 *file* identik
	Arsip	Rar	*File* tidak ditemukan	Tidak ditemukan
		Zip	*File* tidak ditemukan	Tidak ditemukan
PhotoRec	Gambar	Jpg	5 artefak	5 *file* identik
		png	5 artefak	5 *file* identik
	Dokumen	Docx	5 artefak	5 *file* identik
		Pdf	5 artefak	5 *file* identik
	Audio	Mp3	5 artefak	4 *file* identik
		Wav	5 artefak	5 *file* identik
	Video	Mp4	*File* tidak ditemukan	Tidak ditemukan
		Avi	5 artefak	5 *file* identik
	Arsip	Rar	5 artefak	1 *file* identik
		Zip	5 artefak	5 *file* identik

Namun, pada *file* yang dihapus menggunakan shift+delete, terdapat artefak yang berhasil di recovery tanpa *corrupt* seperti *file* yang dihapus menggunakan Sdelete. *Tools* mampu menemukan artefak dalam kondisi dapat diakses / dapat dibuka.

3.4 Analisis Perbandingan Hasil Recovery

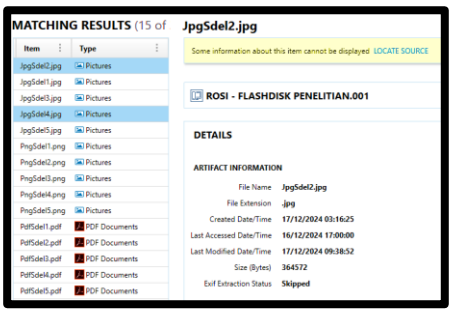
Peneliti menemukan adanya beberapa *file* yang tidak berhasil dipulihkan, baik dari metode penghapusan Sdelete maupun Shift + Delete. *Recovery* menggunakan Autopsy, dengan *file* yang telah dihapus menggunakan perintah Sdelete yakni *file* DOCX tidak ditemukan sama sekali. Sementara itu, untuk *file* yang dihapus menggunakan kombinasi tombol Shift + Delete antaranya MP4, yang mengalami kerusakan dan memiliki nilai *hash* yang sama untuk seluruh *file* MP4 (terlihat pada gambar 6) dan *file* ZIP (SDZip_1) yang tidak ditemukan sama sekali.



Name	S	Size	MD5 Hash	MIME Type
Mp4Sdel1.mp4		1134548	9d95cb105cfddd27ed157251f7989b20	application/octet-stream
Mp4Sdel2.mp4		930960	90959f6584da6bbee52916ce70ea7e63	application/octet-stream
Mp4Sdel3.mp4		987921	86022bb425fc7361dcae5db0e6b96969	application/octet-stream
Mp4Sdel4.mp4		2429067	f3b75b19ca83d7ec2e2a56c7b22d4a0b	application/octet-stream
Mp4Sdel5.mp4		2036116	c3fb2329880ef762c8e0e5702797daa9	application/octet-stream
f2045208.mp4		24	b0e597ad98f6acb00f4f4b04f5d2f4fc	video/mp4
f2051520.mp4		24	b0e597ad98f6acb00f4f4b04f5d2f4fc	video/mp4
f2055592.mp4		24	b0e597ad98f6acb00f4f4b04f5d2f4fc	video/mp4
f2059752.mp4		24	b0e597ad98f6acb00f4f4b04f5d2f4fc	video/mp4
f2069800.mp4		24	b0e597ad98f6acb00f4f4b04f5d2f4fc	video/mp4

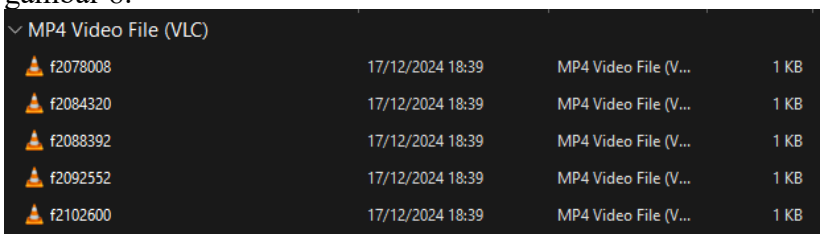
Gambar 6. *File recovery* menggunakan Autopsy yang tidak dapat diakses

Tool lainnya yakni Magnet Axiom menunjukkan hasil yang berbeda. Hasil *recovery* menunjukkan, untuk *file* yang dihapus menggunakan Sdelete, *file* dengan format DOCX, ZIP, dan RAR tidak dapat ditemukan dan *file* lainnya ditemukan namun tidak dapat diakses seperti terlihat pada gambar 7. Adapun untuk *file* yang dihapus menggunakan Shift + Delete, beberapa format *file* yang tidak ditemukan antara lain MP3, WAV, RAR, dan ZIP, yang menunjukkan bahwa Magnet Axiom memiliki keterbatasan dalam menangani *recovery file* dari beberapa jenis format yang telah dihapus.



Gambar 7. *File recovery* menggunakan Axiom yang tidak dapat diakses

Hasil PhotoRec menunjukkan bahwa hapus menggunakan Sdelete tidak ditemukan artefak sama sekali dan hapus menggunakan Shift + Delete *file* dengan format MP4 tidak dapat diakses yang dapat dilihat pada gambar 8.



Gambar 8. *file recovery* menggunakan PhotoRec yang tidak dapat diakses

Adapun daftar temuan artefak yang ditemukan dan kesesuaian nilai *hash* dibuat menjadi tabel yang dapat dilihat pada pada tabel 4 berikut:

Tabel 4. Artefak yang dihapus menggunakan perintah Sdelete

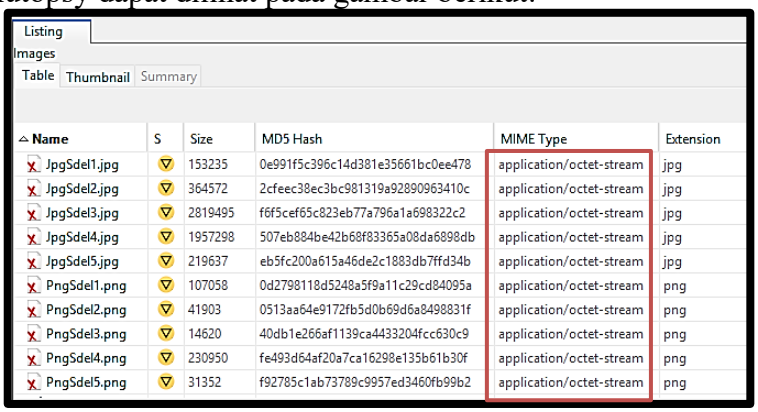
Variable		**Tools**		
Tipe *File*	**Format *File***	**Autopsy**	**Axiom**	**PhotoRec**
Gambar	Jpg	*File* tidak dapat diakses	*File* tidak dapat diakses	*File* tidak ditemukan
	png	*File* tidak dapat diakses	*File* tidak dapat diakses	*File* tidak ditemukan
Dokumen	Docx	*File* tidak ditemukan	*File* tidak ditemukan	*File* tidak ditemukan
	Pdf	*File* tidak dapat diakses	*File* tidak dapat diakses	*File* tidak ditemukan
Audio	Mp3	*File* tidak dapat diakses	*File* tidak dapat diakses	*File* tidak ditemukan
	Wav	*File* tidak dapat diakses	*File* tidak dapat diakses	*File* tidak ditemukan
Video	Mp4	*File* tidak dapat diakses	*File* tidak dapat diakses	*File* tidak ditemukan
	Avi	*File* tidak dapat diakses	*File* tidak dapat diakses	*File* tidak ditemukan
Arsip	Rar	*File* tidak dapat diakses	*File* tidak ditemukan	*File* tidak ditemukan
	Zip	*File* tidak dapat diakses	*File* tidak ditemukan	*File* tidak ditemukan
Total *File* yang dapat diakses		**0 *file***	**0 *file***	**0 *file***

Total *file* pada tabel 4, menginformasikan bahwa tidak ada satupun *file* yang ditemukan dalam keadaan dapat diakses. Selanjutnya, untuk kesesuaian nilai *hash* dapat dilihat pada tabel 5.

Tabel 5. kesesuaian nilai *hash*

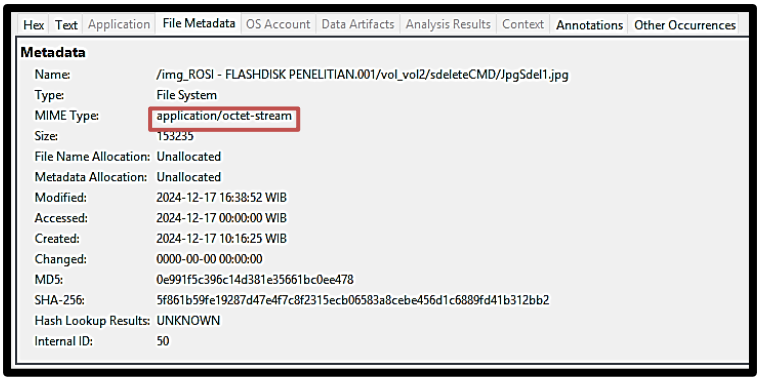
Variable		Tools		
Tipe *File*	**Format *File***	**Autopsy**	**Axiom**	**PhotoRec**
Gambar	Jpg	Tidak identik	Tidak identik	Tidak ditemukan
	png	Tidak identik	Tidak identik	Tidak ditemukan
Dokumen	Docx	Tidak ditemukan	Tidak ditemukan	Tidak ditemukan
	Pdf	Tidak identik	Tidak identik	Tidak ditemukan
Audio	Mp3	Tidak identik	Tidak identik	Tidak ditemukan
	Wav	Tidak identik	Tidak identik	Tidak ditemukan
Video	Mp4	Tidak identik	Tidak identik	Tidak ditemukan
	Avi	Tidak identik	Tidak identik	Tidak ditemukan
Arsip	Rar	Tidak identik	Tidak ditemukan	Tidak ditemukan
	Zip	Tidak identik	Tidak ditemukan	Tidak ditemukan
Total *File* yang identik		**0 identik**	**0 identik**	**0 identik**

Pada tabel 4, ditulis sebagian besar *file* yang telah di recovery dengan temuan "file tidak dapat diakses" yang tetap memiliki nilai *hash.* Namun, nilai *hash* tersebut tidak satupun yang identik dengan nilai *hash* pada *file* yang aslinya, menginformasikan bahwa *file* temuan tidak satupun yang identik dengan nilai *hash*nya. Hasil *capture file* yang dihapus menggunakan Sdelete dan di*recovery* menggunakan *tool* Autopsy dapat dilihat pada gambar berikut:



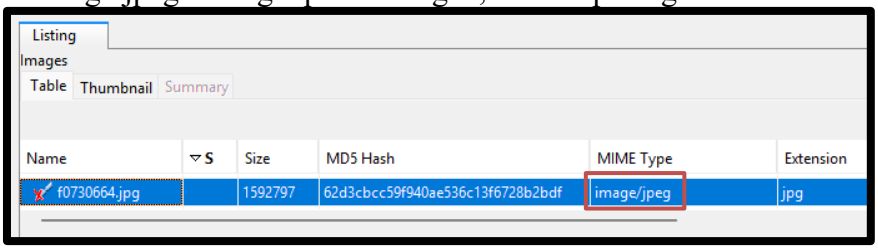
Gambar 9. Artefak yang tidak dapat diakses pada Autopsy

Gambar 9 menunjukkan keseluruhan *file* memiliki MIME type yaitu application/octet-stream. Selanjutnya, jika *file* tersebut dilihat berdasarkan File Metadata, maka akan terlihat sebagaimana pada gambar 10.



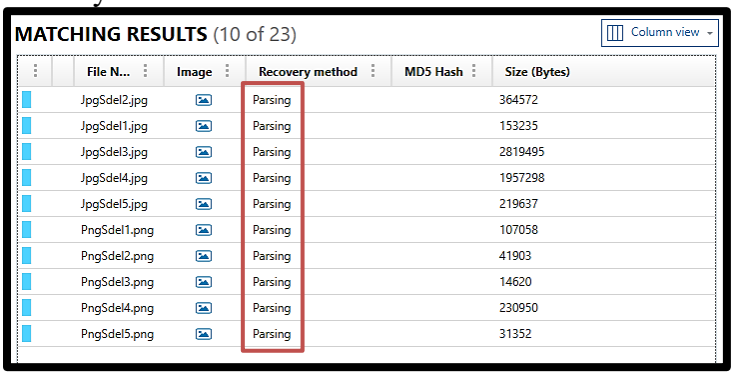
Gambar 10. *File* metadata *tool* Autopsy

Berbeda pada *file* gambar yang dihapus menggunakan shift+delete yang dapat diakses memiliki MIME Type yaitu image/jpeg. Sebagai perbandingan, terlihat pada gambar 11 berikut:



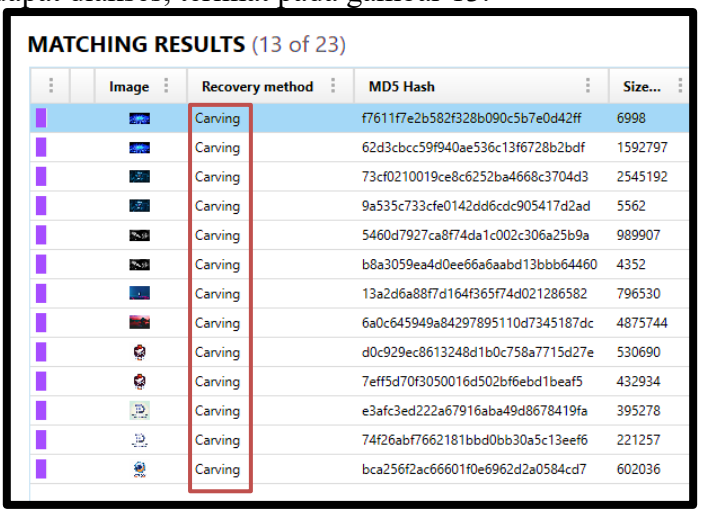
Gambar 11. *file* yang dapat diakses pada Autopsy

Selanjutnya, penelitian ini mencoba melihat perbandingan *recovery* data pada *tool* Magnet Axiom Examine. Pada *tool* ini, terdapat perbedaan dalam sisi *recovery method* yang digunakan secara otomatis saat setelah recovery selesai.



Gambar 12. Artefak yang ditemukan pada Axiom dari hapus Sdelete

Dari gambar 12, *file* yang ditemukan merupakan *file* yang dihapus menggunakan perintah Sdelete namun tidak dapat diakses dan menginformasikan Recovery Method yang digunakan yaitu "Parsing". Berbeda dengan Recovery Method pada *file* yang dihapus menggunakan Shift + Delete yaitu "Carving" dan *file* ini dapat diakses, terlihat pada gambar 13.



Gambar 13. *file* yang dapat diakses pada *tool* Axiom dari hapus shift+delete

Namun, pada PhotoRec hanya menghasilkan artefak secara langsung yang tersimpan pada folder. Folder tersebut berisi keseluruhan artefak hasil *recovery* dan untuk *file* yang dihapus menggunakan Sdelete tidak ditemukan sama sekali artefak. Setelah melakukan perbandingan yang dilakukan pada temuan-temuan *file* yang dapat diakses dan tidak dapat diakses, peneliti menghitung keseluruhan hasil pada *file* yang dapat diakses yang dalam hal ini adalah hasil penghapusan menggunakan Shift + Delete, sebagai berikut:

Tabel 6. Keseluruhan artefak yang dihapus menggunakan Shift + Delete

Variable		**Tools**		
Tipe *File*	**Format *File***	**Autopsy**	**Magnet Axiom**	**PhotoRec**
Gambar	Jpg	5 artefak	5 artefak	5 artefak
	png	5 artefak	5 artefak	5 artefak
Dokumen	Docx	5 artefak	5 artefak	5 artefak
	Pdf	5 artefak	5 artefak	5 artefak
Audio	Mp3	5 artefak	*file* tidak ditemukan	5 artefak
	Wav	5 artefak	*file* tidak ditemukan	5 artefak
Video	Mp4	*file* tidak ditemukan	5 artefak	*File* tidak dapat diakses
	Avi	5 artefak	5 artefak	5 artefak
Arsip	Rar	5 artefak	*file* tidak ditemukan	5 artefak
	Zip	4 artefak	*file* tidak ditemukan	5 artefak
Total *File* yang dapat diakses		**44 *file***	**30 *file***	**45 *file***

Berdasarkan keseluruhan hasil analisis yang ada didalam Tabel 6, dilakukan evaluasi kinerja seluruh *tools file carving* dalam me*recovery file* menggunakan rumus berikut:

$$Par = \frac{\sum ar0}{\sum arT} \times 100\% = XX\% \quad (1)$$

Pada rumus (1), dengan keterangan yaitu Par merupakan angka indeks persentase, ar0 merupakan jumlah *file* yang terdeteksi dan arT merupakan jumlah keseluruhan *file* yang digunakan (Yuladi & Indrayani, 2023). Berikut adalah perhitungan persentase dalam mengukur kemampuan *recovery* masing-masing *tools file carving*.

Nilai persentase *tool* Autopsy $Par = \frac{44}{50} \times 100\% = 88\%$ (2)

Nilai persentase *tool* Axiom $Par = \frac{30}{50} \times 100\% = 60\%$ (3)

Nilai persentase *tool* PhotoRec $Par = \frac{45}{50} \times 100\% = 90\%$ (4)

Selanjutnya setelah dilakukan analisis keseluruhan arterak yang ditemukan dan dilakukan perhitungan menggunakan rumus (1) untuk artefak yang telah berhasil di recovery, selanjutnya dilakukan hal yang serupa menggunakan rumus yang sama pada hasil analisis keseluruhan nilai *hash,* dapat dilihat pada tabel 7.

Tabel 7. Hasil analisis keseluruhan nilai *hash*

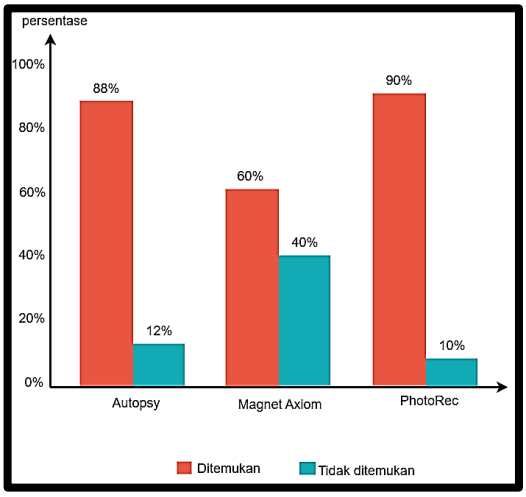
Variable		***Tools***		
Tipe *File*	**Format *File***	**Autopsy**	**Axiom**	**PhotoRec**
Gambar	Jpg	5 *file* identik	5 *file* identik	5 *file* identik
	png	5 *file* identik	5 *file* identik	5 *file* identik
Dokumen	Docx	5 *file* identik	5 *file* identik	5 *file* identik
	Pdf	5 *file* identik	0 *file* identik	5 *file* identik
Audio	Mp3	3 *file* identik	Tidak ditemukan	4 *file* identik
	Wav	5 *file* identik	Tidak ditemukan	5 *file* identik
Video	Mp4	Tidak ditemukan	5 *file* identik	Tidak ditemukan
	Avi	5 *file* identik	5 *file* identik	5 *file* identik
Arsip	Rar	1 *file* identik	Tidak ditemukan	1 *file* identik
	Zip	4 *file* identik	Tidak ditemukan	5 *file* identik
Total *File* yang identik		**38 *file***	***25 file***	**40 *file***

Persentase keidentikan *hash* Autopsy $Par = \frac{38}{50} \times 100\% = 76\%$ (5)

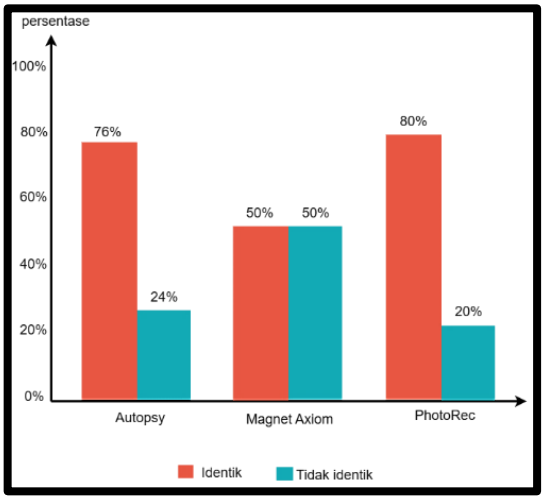
Persentase keidentikan *hash* Axiom $Par = \frac{25}{50} \times 100\% = 50\%$ (6)

Persentase keidentikan *hash* PhotoRec $Par = \frac{40}{50} \times 100\% = 80\%$ (7)

Dari keseluruhan hasil perhitungan pada artefak yang ditemukan dan dapat diakses oleh masing-masing *tools file carving*, peneliti membuat grafik persentase berdasarkan *file* temuan dan keidentikan nilai *hash*. Grafik dapat dilihat pada gambar 14 dan gambar 15.



Gambar 14. grafik persentase *file* yang ditemukan



Gambar 15. grafik persentase keidentikan nilai *hash*

3.5 Hasil

Dalam proses pemulihan data, PhotoRec menunjukkan tingkat keberhasilan tertinggi dengan 90% *file* berhasil dipulihkan dan 80% *file* memiliki nilai *hash* yang identik dengan *file* aslinya. Selanjutnya, Autopsy dengan 88% tingkat keberhasilan pemulihan dan 76% kesesuaian nilai *hash*. Di Posisi terakhir, Magnet Axiom memiliki tingkat pemulihan terendah, yaitu 60% *file* berhasil dipulihkan dan 50% *file* memiliki kesesuaian nilai *hash*, Sebagaimana dapat dilihat pada Tabel 8.

Tabel 8. Hasil Akhir

Nama tools	Nilai Persentase	
	Pengembalian *File*	**Kesesuaian Hash**
Autopsy	88%	76%
Magnet Axiom	60%	50%
PhotoRec	90%	80%

Keunggulan PhotoRec ini dapat dijelaskan oleh metode pemulihan yang digunakan, yaitu *file carving* berbasis *signature*, yang memungkinkan pemindaian langsung terhadap blok data untuk menemukan *file* berdasarkan pola *header* dan *footer*. Hal ini menjelaskan mengapa PhotoRec berhasil memulihkan artefak *file* meskipun dilakukan penghapusan dengan Shift+Delete, di mana struktur *file* masih tersisa sebagian, namun gagal sepenuhnya saat metadata benar-benar dihapus oleh Sdelete. Autopsy sendiri bekerja berdasarkan analisis metadata dari sistem *file* dan cocok digunakan ketika struktur *file* system masih tersedia. Magnet Axiom, dengan metode parsing metadata dan post-process carving, namun hasil pemulihannya tidak optimal karena tetap mengandalkan metadata sistem *file* pada tahap awal.

Selain itu, format *file* juga menjadi faktor penting. PhotoRec berhasil memulihkan *file* dengan format gambar dan dokumen (misalnya .jpg, .png, .docx, .pdf) secara konsisten karena *file-file* tersebut memiliki struktur *signature* yang kuat dan mudah dikenali, berbeda dengan format seperti .mp4 yang cenderung kompleks dan rawan fragmentasi. Hal ini turut mempengaruhi keberhasilan

carving. Sementara itu, hasil eksperimen menunjukkan bahwa penghapusan menggunakan Sdelete terbukti jauh lebih efektif dibandingkan Shift+Delete dalam mencegah *recovery*. Hal ini karena Sdelete menimpa isi *file* dan menghapus metadata secara permanen sesuai dengan standar DoD 5220.22-M, sehingga, baik Autopsy, Magnet Axiom, maupun PhotoRec, tidak ada yang berhasil memulihkan *file* yang dihapus dengan metode ini. Sebaliknya, *file* yang dihapus dengan Shift+Delete masih dapat dipulihkan karena metode ini hanya menghapus entri *file* dari sistem *file* tanpa menimpa isi data secara fisik.

4. Kesimpulan

Berdasarkan penelitian yang telah diselesaikan, dari data yang telah dihapus menggunakan perintah Sdelete, *tools file carving* (Autopsy, Magnet Axiom dan PhotoRec) tidak dapat melakukan *recovery file* yang dapat diakses. Selanjutnya, data yang dihapus menggunakan kombinasi tombol Shift + Delete masih bisa dipulihkan dan diakses dengan tingkat keberhasilan yang bervariasi. Autopsy menunjukkan tingkat persentase pengembalian *file* sebesar 88% dan keidentikan nilai *hash* sebesar 76%. Magnet Axiom memiliki tingkat keberhasilan pengembalian *file* sebesar 60% dan keidentikan nilai *hash* sebesar 50%. Selanjutnya pada PhotoRec memiliki tingkat keberhasilan pengembalian *file* sebesar 90% dan keidentikan nilai *hash* sebesar 80%. Berdasarkan tingkat persentase, PhotoRec paling unggul dari kedua *tools,* disusul oleh Autopsy dan yang terakhir Magnet Axiom dalam hal *recovery file* dan keidentikan nilai *hash*.

Referensi

Abdillah, M. F., & Prayudi, Y. (2022). Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux. *International Journal of Advanced Computer Science and Applications*, *13*(9), 633–639. https://doi.org/10.14569/IJACSA.2022.0130975

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

cgsecurity. (2024). *PhotoRec*. https://www.cgsecurity.org/

Dasmen, R. N., Triwulanda, A., Rasmila, R., Kurniawan, D., & Julia, J. (2024). Implementation of Digital Forensics PhotoRec in Recovering Lost Files on External Storage. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *12*(1), 173–178. https://doi.org/10.33558/piksel.v12i1.9444

Fakhri, L. J., Riadi, I., & Yudhana, A. (2023). Forensic Tools Comparison on File Carving using Digital Forensics Research Workshop Framework. *Scientific Journal of Informatics*, *10*. http://journal.unnes.ac.id/nju/index.php/sji

Julian, D., Wijaya, A., & Sutabri, T. (2023). Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology. *Digital Transformation Technology (Digitech)*, *3*. https://doi.org/10.47709/digitech.v3i1.2727

Jupriadi Fakhri, L., Riadi, I., & Yudhana, A. (2023). Forensic Tools Comparison on File Carving using Digital Forensics Research Workshop Framework. *Scientific Journal of Informatics*, *10*(4). https://doi.org/10.15294/sji.v10i4.46901

Matondang, J., Maulana, I., & Carudin. (2023). Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST. *Innovative: Journal Of Social Science Research*, *3*. https://j-innovative.org/index.php/Innovative

Microsoft. (2022). *SDelete v2.05*. https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete

Muhardinata, M., Luthfi, A., & Ramadhani, E. (2023). Teknik Disk Carving untuk Recovery Solid State Drive Volume ReFS dan NTFS dengan Fitur TRIM. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *6*(11), 9507–9515. https://doi.org/10.54371/jiip.v6i11.3133

Nayak, S. C. (2024). *Data Recovery Beyond the Obvious Using Digital Forensic Techniques*. Montclair State Unversity.

Porter, K., Nordvik, R., Toolan, F., & Axelsson, S. (2021). Timestamp prefix carving for filesystem metadata extraction. *Forensic Science International: Digital Investigation*, *38*, 301266. https://doi.org/10.1016/j.fsidi.2021.301266

Pratama, A. K., Carudin, C., & Yusup, D. (2021). Analisis Perbandingan Perangkat Lunak Forensik Digital untuk File Carving dalam Mengungkap Barang Bukti Digital. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, *6*(2), 109–120. https://doi.org/10.32528/justindo.v6i2.5101

Rafiq, I. A., Riadi, I., & Herman. (2022). Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(2), 134–142. https://doi.org/10.14421/jiska.2022.7.2.134-142

Sari, S. A., & Mohamad, K. M. (2020). A Review of Graph Theoretic and Weightage Techniques in File Carving. *Journal of Physics: Conference Series*, *1529*(5), 052011. https://doi.org/10.1088/1742-6596/1529/5/052011

Setiawan, I., Rusydi, I., Rahmawati, A., & Hasanah, S. (2022). Jejak Digital Sebagai Alat Bukti Penunjuk Menurut Pasal 184 Kitab Undang Undang Hukum Acara Pidana. *Jurnal Ilmiah Galuh Justisi*, *10*(1), 119. https://doi.org/10.25157/justisi.v10i1.7236

Siamukulule, M. (2024). A Deep Dive into Magnet AXIOM's Workflow: Exploring the Roles of AXIOM Process and AXIOM Examine in Digital Evidence Acquisition and Analysis. *International Journal for Multidisciplinary Research (IJFMR)*, *6*(6).

Yuladi, A. I., & Indrayani, R. (2023). Analisis dan Perbandingan Tools Forensik menggunakan Metode NIST Dalam Penanganan Kasus Kejahatan Siber. *Jurnal Teknologi Terpadu*, *9*(2), 95–100. https://doi.org/10.54914/jtt.v9i2.636

Yuwono, D. T., & W, Y. (2020). Analisis Perbandingan File Carving Dengan Metode Nist. *Jurnal Sains Komputer dan Teknologi Informasi*, *2*(2), 1–6. https://doi.org/10.33084/jsakti.v2i2.1472