



# **Perbandingan Hasil *Recovery File* Terhadap Penghapusan *File* Menggunakan Perintah Sdelete dan Shift+Delete**

Rosi Rahmadi Syahputra

23917005

*Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer*

*Konsentrasi Forensika Digital*

*Program Studi Informatika Program Magister*

*Fakultas Teknologi Industri*

*Universitas Islam Indonesia*

2025

## Lembar Pengesahan Pembimbing

### Perbandingan Hasil *Recovery File* Terhadap Penghapusan *File* Menggunakan Perintah Sdelete dan Shift+Delete

Rosi Rahmadi Syahputra

23917005



Pembimbing

Dr. Yudi Prayudi, S.Si., M.Kom

## Lembar Pengesahan Penguji

### Perbandingan Hasil *Recovery File* Terhadap Penghapusan *File* Menggunakan Perintah Sdelete dan Shift+Delete

Rosi Rahmadi Syahputra

23917005

Yogyakarta, Agustus 2025

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M. Kom.

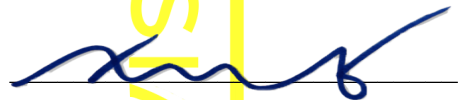
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom.

Anggota I

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Anggota II



08/09/2025

Mengetahui,

Ketua Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia



Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

## Abstrak

### Perbandingan Hasil *Recovery File* Terhadap Penghapusan *File* Menggunakan Perintah Sdelete dan Shift+Delete

Pemulihan data yang telah dihapus merupakan aspek penting dalam investigasi digital forensik, terutama dalam mengidentifikasi barang bukti yang relevan. Penelitian ini melakukan perbandingan terhadap hasil *recovery file* yang dihapus menggunakan perintah Sdelete dan kombinasi tombol Shift+Delete dengan mengevaluasi tiga *tools file carving*, yaitu Autopsy, Magnet Axiom, dan PhotoRec. Sdelete merupakan metode penghapusan penimpaan data berbasis standar *Department of Defense* (DoD) 5220.22-M, sedangkan Shift+Delete hanya menghapus referensi *file* tanpa menimpa data. Hasil penelitian menunjukkan bahwa *file* yang dihapus menggunakan Sdelete tidak dapat dipulihkan oleh ketiga *tools*, baik dari segi temuan artefak maupun nilai *hash*. Jika dibandingkan dengan Sdelete, *file* yang dihapus menggunakan Shift+Delete masih dapat dipulihkan dengan tingkat 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 mengonfirmasi bahwa *tools file carving* yang digunakan pada penelitian ini tidak dapat melakukan *recovery file* jika data tersebut dihapus menggunakan teknik hapus Sdelete dan sebaliknya dapat dilakukan *recovery* jika hanya dihapus menggunakan Shift+Delete.

#### **Kata kunci**

*File carving*, Sdelete, Shift+Delete, *Static Forensic*, Digital Forensik, *Recovery Data*.

## ***Abstract***

### ***Comparison of File Recovery Results Against File Deletion Using Sdelete and Shift+Delete Commands***

*The recovery of deleted data is an important aspect of digital forensic investigations, especially in identifying relevant evidence. This study compares the results of recovery of deleted files using the Sdelete command and the combination of Shift+Delete keys by evaluating three file carving tools, namely Autopsy, Magnet Axion, and PhotoRec. Sdelete is a data overwrite removal method based on the Department of Defense (DoD) standard 5220.22-M, while Shift+Delete only deletes file references without overwriting the data. The results show that files deleted using Sdelete cannot be recovered by all three tools, both in terms of artifact findings and hash values. When compared to Sdelete, files deleted using Shift+Delete can still be recovered with varying degrees of success. PhotoRec has the highest recovery rate (90%), followed by Autopsy (88%) and Magnet Axion (60%). In terms of hash value suitability, PhotoRec achieves 80%, while Autopsy is 76% and Magnet Axion is 50%. This finding confirms that the file carving tools used in this study cannot recover files if the data is deleted using the Sdelete delete technique and vice versa can be recovered if it is only deleted using Shift+Delete.*

### **Keywords**

*File carving, Sdelete, Shift+Delete, Static Forensic, Digital Forensik, Recovery Data.*

## **Pernyataan Keaslian Tulisan**

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Agustus 2025



Rosi Rahmadi Syaliputra, S.Kom



## Daftar Publikasi

### Publikasi yang menjadi bagian dari tesis

Syahputra, R. R., & Prayudi, Y. (2025). Perbandingan Hasil *Recovery File* terhadap Penghapusan *File* menggunakan Perintah Sdelete dan Shift+Delete. *Asian Journal of Innovation and Entrepreneurship*, 09(02).

| Kontributor            | Jenis Kontribusi                                                      |
|------------------------|-----------------------------------------------------------------------|
| Rosi Rahmadi Syahputra | Mendesain eksperimen (60%)<br>Menulis <i>paper</i> (70%)              |
| Yudi Prayudi           | Mendesain eksperimen (40%)<br>Menulis dan mengedit <i>paper</i> (30%) |

## **Halaman Kontribusi**

Berkat kontribusi dari berbagai pihak, alhamdulillah penelitian ini berjalan dan telah selesai. Pihak-pihak yang menjad guru dan telah banyak memberikan saran serta masukan, yang bermula dari sebelum penelitan, seminar proposal, sidang kemajuan hingga sidang pendadaran:

1. Bapak Dr. Yudi Prayudi, S.Si., M.Kom. sebagai Pembimbing I, Bapak Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom. dan Ibu Erika Ramadhani, S.T., M.Eng sebagai dosen penguji proposal, progres dan pendadaran yang telah memberikan arahan-arahannya kepada penulis, sehingga penulisan tesis ini bisa selesai dengan baik dan tepat waktu.
2. Segenap dosen dan seluruh pengurus akademik MI UII yang banyak memberikan waktu serta ilmu selama menempuh masa studi di Magister Informatika Universitas Islam Indonesia.

## Halaman Persembahan

Alhamdulillah, segala puji dan rasa sukur kepada Allah Subhana Wa Ta'ala, Tuhan seluruh alam yang telah memberikan nikmat hidup dan selalu memberikan rahmat-Nya pada seluruh makhluk ciptaan-Nya. Alhamdulillah saya ucapkan baik dari dalam hati maupun secara lisan, karena telah menyelesaikan laporan tesis yang saya persembahkan kepada:

1. Kedua orang tuaku, Bapak Romel dan Ibu Samsi Rumaida yang selalu tak bosan memberikan doa, menjadi *support system*, motivasi dan nasehat dalam keseluruhan hidupku.
2. Saudara-saudariku, Muhammad Alfidri dan Nabilla Nur Rabbani, adikku yang seringkali menanyakan kabar dan juga motivasi kepadaku sebagai kakak mereka.
3. Keluarga besar Amran – Mahani dan Tamrin – Nurmaini.
4. Teman – teman seperjuangan dalam menempuh pendidikan di Jogja dalam suka dan duka yang selalu kebersamai.

## Kata Pengantar

Assalamu'alaikum warahmatullahi wabarakatuh.

Alhamdulillah, puji dan sukur penulis panjatkan kepada Allah sang maha agung karena berkat limpahan kasih sayang serta hidayah-Nya kepada penulis dan ridho-Nya penulis diberi kesempatan untuk dapat menuntaskan tesis ini dengan sebaik mungkin. Tesis dengan judul “Perbandingan Hasil *Recovery File* Terhadap Penghapusan *File* Menggunakan Perintah *Sdelete* dan *Shift+Delete*” disusun sebagai persyaratan kelulusan dibangku perkuliahan pada tingkat magister serta mendapatkan gelar magister komputer. Hasil penulisan ini tidak lepas dari banyak bantuan berbagai pihak dan penulis mengucapkan beribu terimakasih kepada :

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., Selaku Rektor Universitas Islam Indonesia.
2. Bapak Dr. Yudi Prayudi, S.Si., M.Kom., selaku dosen pembimbing 1 yang telah banyak memberikan masukan dan arahan terhadap jalannya penelitian yang penulis lakukan.
3. Bapak Irving Vitra Paputungan, S.T., M.Sc., Ph.D., yang menjadi dosen penguji ketika penulis melakukan sidang proposal, sidang progres.
4. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom yang menjadi dosen penguji sidang pendadaran.
5. Ibu Erika Ramadhani, ST., M.Eng. yang menjadi dosen penguji ketika penulis melakukan sidang proposal dan progres.
6. Teman-teman dari Magister Informatika Fakultas Teknologi Industri Universitas Islam Indonesia dan juga khususnya Konsentrasi Forensika Digital Angkatan XXVIII, Terima kasih banyak sudah saling berjuang dan bekerjasama.

Penulis menyadari masih banyak terdapat kekurangan dalam penyusunan tesis ini dan oleh karena itu penulis kira sangat memerlukan serta berharap masukan, kritik, saran yang membangun.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Rosi Rahmadi Syahputra

Magister Informatika

Universitas Islam Indonesia (UII)

## Daftar Isi

|                                    |      |
|------------------------------------|------|
| Lembar Pengesahan Pembimbing ..... | i    |
| Lembar Pengesahan Penguji.....     | ii   |
| Abstrak .....                      | iii  |
| <i>Abstract</i> .....              | iv   |
| Pernyataan Keaslian Tulisan .....  | v    |
| Daftar Publikasi .....             | vi   |
| Halaman Kontribusi.....            | vii  |
| Halaman Persembahan .....          | viii |
| Kata Pengantar.....                | ix   |
| Daftar Isi .....                   | x    |
| Daftar Tabel.....                  | xiii |
| Daftar Gambar .....                | xiv  |
| Glosarium .....                    | xv   |
| BAB 1 Pendahuluan .....            | 1    |
| 1.1 Latar Belakang.....            | 1    |
| 1.2 Rumusan Masalah.....           | 3    |
| 1.2.1 Pertanyaan Penelitian.....   | 4    |
| 1.3 Batasan Masalah .....          | 4    |
| 1.4 Tujuan Penelitian .....        | 5    |
| 1.5 Manfaat Penelitian .....       | 5    |
| 1.6 Metode Penelitian .....        | 5    |
| 1.7 Sistematika Penulisan .....    | 6    |
| BAB 2 Tinjauan Pustaka .....       | 8    |
| 2.1 Penelitian Terdahulu.....      | 8    |
| 2.2 Konsep Pengetahuan.....        | 16   |
| 2.2.1 Digital Forensik .....       | 16   |

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| 2.2.2 Bukti Digital .....                                                          | 17 |
| 2.2.3 <i>Static Forensic</i> .....                                                 | 17 |
| 2.2.4 <i>File Carving</i> .....                                                    | 18 |
| 2.2.5 Perintah Sdelete .....                                                       | 18 |
| 2.2.6 Kombinasi tombol Shift+Delete .....                                          | 18 |
| 2.2.7 Autopsy.....                                                                 | 19 |
| 2.2.8 Magnet Axiom .....                                                           | 19 |
| 2.2.9 PhotoRec.....                                                                | 20 |
| BAB 3 Metodologi .....                                                             | 21 |
| 3.1 Tahapan Awal.....                                                              | 21 |
| 3.2 Tinjauan Pustaka.....                                                          | 21 |
| 3.3 Persiapan Alat dan Sistem .....                                                | 22 |
| 3.4 Skenario dan Simulasi Kasus.....                                               | 22 |
| 3.5 Akuisisi Menggunakan Metode <i>Static Forensic</i> .....                       | 23 |
| 3.6 <i>Recovery</i> Menggunakan Teknik <i>File Carving</i> .....                   | 23 |
| 3.7 Hasil <i>Output Recovery</i> Flashdisk.....                                    | 23 |
| 3.8 Analisis Perbandingan Hasil <i>Recovery</i> .....                              | 23 |
| 3.9 Hasil Akhir.....                                                               | 24 |
| BAB 4 Hasil dan Pembahasan .....                                                   | 25 |
| 4.1 Tinjauan Pustaka.....                                                          | 25 |
| 4.2 Persiapan Alat dan Sistem .....                                                | 26 |
| 4.3 Skenario dan simulasi Kasus .....                                              | 26 |
| 4.4 Akuisisi Menggunakan Metode <i>Static Forensic</i> .....                       | 30 |
| 4.5 <i>Recovery</i> Menggunakan Teknik <i>File Carving</i> .....                   | 31 |
| 4.6 Hasil <i>Output Recovery</i> Flashdisk.....                                    | 34 |
| 4.6.1 <i>Output File</i> Yang Dihapus Menggunakan Sdelete .....                    | 34 |
| 4.6.2 <i>Output File</i> Yang Dihapus Menggunakan Kombinasi Tombol Shift+Delete .. | 35 |

|                                                       |    |
|-------------------------------------------------------|----|
| 4.7 Analisis Perbandingan Hasil <i>Recovery</i> ..... | 37 |
| 4.8 Hasil .....                                       | 46 |
| BAB 5 Kesimpulan dan Saran.....                       | 48 |
| 5.1 Kesimpulan .....                                  | 48 |
| 5.2 Saran .....                                       | 49 |

## Daftar Tabel

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| Tabel 1.1 <i>Review</i> Penelitian Terdahulu .....                         | 9  |
| Tabel 1.2 Perbandingan Terhadap Penelitian Terdahulu.....                  | 15 |
| Tabel 3.1 Contoh Tabel Hasil Akhir .....                                   | 24 |
| Tabel 4.1 <i>Hardware</i> dan <i>Software</i> .....                        | 26 |
| Tabel 4.2 File Temuan Dan Keidentikan Nilai <i>Hash</i> Autopsy.....       | 34 |
| Tabel 4.3 File Temuan Dan Keidentikan Nilai <i>Hash</i> Magnet Axiom.....  | 35 |
| Tabel 4.4 File Temuan Dan Keidentikan Nilai <i>Hash</i> Photorec .....     | 35 |
| Tabel 4.5 File Temuan Dan Keidentikan Nilai <i>Hash</i> Autopsy .....      | 35 |
| Tabel 4.6 File Temuan Dan Keidentikan Nilai <i>Hash</i> Magnet Axiom.....  | 36 |
| Tabel 4.7 File Temuan Dan Keidentikan Nilai <i>Hash</i> PhotoRec.....      | 36 |
| Tabel 4.8 Artefak Yang Dihapus Menggunakan Perintah Sdelete.....           | 38 |
| Tabel 4.9 Kesesuaian Nilai <i>Hash</i> .....                               | 39 |
| Tabel 4.10 Keseluruhan Artefak Yang Dihapus Menggunakan Shift+Delete ..... | 43 |
| Tabel 4.11 Hasil Analisis Keseluruhan Nilai <i>Hash</i> .....              | 44 |
| Tabel 4.12 Hasil Akhir .....                                               | 46 |

## Daftar Gambar

|                                                                                                |    |
|------------------------------------------------------------------------------------------------|----|
| Gambar 3.1 Alur Metodologi Penelitian .....                                                    | 21 |
| Gambar 4.1 Flashdisk (F:) dalam keadaan kosong.....                                            | 26 |
| Gambar 4.2 Alur Skenario Kasus .....                                                           | 27 |
| Gambar 4.3 <i>File</i> dihapus menggunakan kombinasi tombol Shift+Delete .....                 | 28 |
| Gambar 4.4 <i>File</i> dihapus menggunakan Sdelete .....                                       | 28 |
| Gambar 4.5 Barang bukti flashdisk yang ditemukan diatas meja .....                             | 29 |
| Gambar 4.6 Tampilan utama FTK Imager .....                                                     | 30 |
| Gambar 4.7 Nilai <i>Hash</i> hasil <i>imaging</i> flashdisk.....                               | 31 |
| Gambar 4.8 <i>Recovery completed</i> menggunakan Autopsy .....                                 | 31 |
| Gambar 4.9 Artefak yang berhasil <i>direcovery</i> menggunakan Autopsy.....                    | 32 |
| Gambar 4.10 <i>Recovery completed</i> menggunakan Magnet Axiom .....                           | 32 |
| Gambar 4.11 Artefak yang berhasil <i>direcovery</i> menggunakan Magnet Axiom.....              | 33 |
| Gambar 4.12 <i>Recovery completed</i> menggunakan Photorec .....                               | 33 |
| Gambar 4.13 Artefak yang berhasil <i>direcovery</i> menggunakan PhotoRec.....                  | 34 |
| Gambar 4.14 <i>File recovery</i> menggunakan Autopsy yang tidak dapat diakses.....             | 37 |
| Gambar 4.15 <i>File recovery</i> menggunakan Axiom yang tidak dapat diakses .....              | 38 |
| Gambar 4.16 <i>File recovery</i> menggunakan Photorec yang tidak dapat diakses .....           | 38 |
| Gambar 4.17 Artefak yang ditemukan pada Autopsy .....                                          | 40 |
| Gambar 4.18 <i>File metadata tool</i> Autopsy.....                                             | 40 |
| Gambar 4.19 <i>File</i> yang dapat diakses pada <i>tool</i> Autopsy. ....                      | 41 |
| Gambar 4.20 Artefak yang ditemukan pada Axiom dari hapus Sdelete .....                         | 41 |
| Gambar 4.21 <i>File</i> yang dapat diakses pada <i>tool</i> Axiom dari hapus Shift+Delete..... | 42 |
| Gambar 4.22 Grafik persentase <i>file</i> yang ditemukan .....                                 | 44 |
| Gambar 4.23 Grafik persentase keidentikan nilai <i>hash</i> .....                              | 45 |

## **Glosarium**

|      |                                             |
|------|---------------------------------------------|
| ITE  | - <i>Informasi dan Transaksi Elektronik</i> |
| CMD  | - <i>Command</i>                            |
| SSD  | - <i>Solite State Drive</i>                 |
| API  | - <i>Application Programming Interface</i>  |
| DOD  | - <i>Experience Driven Learning</i>         |
| NTFS | - <i>New Technology File System</i>         |

# BAB 1

## Pendahuluan

### 1.1 Latar Belakang

Serangan siber dalam beberapa tahun terakhir menjadi kerugian bagi banyak warga Indonesia (Septasari, 2023). Bentuk-bentuk kejahatan ini dapat berupa pencurian data, peretasan, penipuan online, penghapusan bukti digital, hingga penyebaran malware (Aini & Lubis, 2024). Secara umum, aktivitas kejahatan siber yang dilakukan oleh pelaku biasanya meninggalkan jejak digital yang dapat dijadikan barang bukti dalam proses penyelidikan (Setiawan et al., 2022). Untuk menangani kasus kejahatan siber, Indonesia memberlakukan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE), yang direvisi pada tahun 2016 dan revisi kedua pada tahun 2024 yang berfungsi sebagai alat hukum dalam menangani dan memberikan ganjaran terhadap pelaku kejahatan siber.

Hasil kejahatan umumnya disimpan pada media penyimpanan yang digunakan sebagai wadah *file* hasil pencurian, penindasan, penipuan, menjadikan *storage* sebagai barang bukti yang berisi rekam jejak dari aktivitas kejahatan (Agustiono et al., 2024). Dalam memuluskan aksi kejahatan, media penyimpanan seringkali digunakan untuk melakukan aktifitas penyimpanan data sehingga memudahkan pelaku mengakses untuk mengedit dan membaca menggunakan komputer (Dasmen et al., 2024). Lalu, ketika tindakan kejahatan telah dilakukan, agar jejak hilang dan tertutupi, pelaku seringkali menghapus atau memilik untuk memformat semua data hasil kejahatan dari dalam media penyimpanan (Yuwono & W, 2020).

Dalam melakukan penghapusan, Ada beberapa teknik yang dapat digunakan, bisa dengan cara hapus manual, hapus permanen dengan menggunakan kombinasi tombol Shift+Delete atau menggunakan *tools* (Jupriadi Fakhri et al., 2023). Salah satu *tool* hapus yaitu 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).

Aktifitas penghapusan pada media penyimpanan dapat diatasi menggunakan teknik *file carving*, teknik yang bekerja dengan melakukan identifikasi terhadap tanda yang ada didalam struktur data yang mengindikasi keberadaan suatu *file* (Matondang et al., 2023) dan teknik ini menjadi penting dalam penerapan investigasi digital forensik karena diperlukan dalam mencari informasi yang tersimpan pada stuktur sistem *file* suatu media penyimpanan

(Pratama et al., 2021). Teknik ini dapat digunakan untuk proses *recovery* data yang telah dihapus secara permanen dan langkah analisis setelah proses *recovery* selesai (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).

Penelitian terdahulu dengan judul Analisis Perbandingan Perangkat Lunak Forensik Digital *File Carving* Menggunakan NIST (Matondang et al., 2023) membahas *recovery* dan perbandingan *tools* pada *recovery file* didalam flashdisk yang dihapus secara permanen, menghasilkan kesimpulan PhotoRec memiliki kemampuan sebanyak 80% dalam melakukan *recovery* pada *file* gambar, video, audio dan dokumen. Penelitian lain dengan judul Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan *Tools* Autopsy dan OSForensics (Fatmah & Indrayani, 2022) menyimpulkan *tool* Autopsy tidak dapat melakukan *recovery* file pada fitur SSD dengan trim *enable* yang memberikan nilai persentase sebesar 0% dan persentase *recovery file* sebesar 100% jika fitur SSD trim dalam keadaan *disable*. Fokus pada penelitian ini adalah mencoba melakukan *recovery* pada SSD dengan fitur TRIM *enable*. Magnet Axiom digunakan pada penelitian *Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method* (Herman et al., 2022) dengan hasil Magnet Axiom lebih unggul dalam mengambil bukti digital.

Penelitian (Yudhana, Riadi, & putra, 2022) menggunakan metode *static forensic* dengan judul Analisis Kinerja Perangkat Lunak *Forensic Imaging* Pada Sistem Operasi Linux Menggunakan Metode *static forensic*, memberikan hasil mengenai analisis dan penggunaan tool DC3DD, Ddrescue dan FTK Imager CLI terhadap barang bukti USB drive yang menyimpulkan bahwa metode akuisisi *static forensic* dapat diterapkan dengan baik serta dapat dilakukan untuk perbandingan *tools file carving*.

Dari literatur terdahulu, belum ada studi komparatif yang menggunakan dua teknik penghapusan Sdelete dan Shift+Delete secara bersamaan dengan *tools file carving*. Sdelete sebagai perintah berbasis CMD diklaim mampu menghapus *file* secara permanen, namun validitas teknis klaim tersebut belum diuji secara sistematis dalam konteks pemulihan *file* menggunakan teknik *file carving*. Oleh karena itu, penelitian ini bertujuan untuk melakukan perbandingan pada hasil *recovery* antar *tools* yang dihapus menggunakan perintah Sdelete

dan Shift+Delete, serta memberikan pengetahuan dari sisi *tools file carving* yang terbaik dalam melakukan *recovery*. Pemilihan teknik penghapusan menggunakan perintah Sdelete dan Shift+Delete karena keduanya mewakili dua kategori penghapusan data, secara standar militer dan secara metode konvensional / *logical delete* yang seringkali ditemukan dalam berbagai kasus investigasi digital forensik (Yuwono & W, 2020). Hasil dari analisis perbandingan *recovery* penting untuk mengetahui ciri atau tanda dari adanya teknik penghapusan tertentu yang telah digunakan pelaku dan studi terdahulu yang lebih banyak fokus pada hapus konvensional seperti kombinasi tombol Shift+Delete.

Studi kasus penelitian ini yakni adanya aktifitas kejahatan digital dengan melakukan penghapusan barang bukti digital dari media penyimpanan flashdisk menggunakan perintah Sdelete dan Shift+Delete. 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).

Kontribusi penelitian ini adalah memberikan bukti empiris bahwa perintah SDelete benar-benar menghilangkan kemungkinan pemulihan data melalui praktik pemulihan *file* menggunakan metode *file carving*. Selain itu, penelitian ini mengisi kesenjangan penelitian sebelumnya dengan membandingkan hasil *recovery file* dengan dua teknik penghapusan berbeda yakni perintah SDelete dan Shift+Delete pada tiga *tools file carving*, sehingga dapat menjadi acuan bagi investigator digital forensik dalam memilih *tools* yang efektif jika dihadapkan dengan kasus penghapusan konvensional.

*Tools forensic* yang digunakan yaitu FTK Imager, Autopsy, Magnet Axiom dan PhotoRec. Data atau bukti digital yang digunakan sebagai pengujian terdiri dari jenis *file* dokumen, gambar, audio, video dan arsip dengan ekstensi .pdf, .docx, .jpg, .png, .mp3, .avi dan .zip. Pada masing-masing ekstensi dengan jumlah *file* sebanyak 5 *file*. Pada tahap akhir, dilakukan perbandingan untuk menentukan *tools* yang secara persentase paling baik dalam melakukan pemulihan data.

## 1.2 Rumusan Masalah

Penghapusan *file* menjadi teknik yang sering digunakan pelaku kejahatan siber untuk menghilangkan jejak digital dari media penyimpanan. Perintah Sdelete, yang dikembangkan oleh Microsoft menerapkan standar DoD 5220.22-M, diklaim dapat menghapus *file* secara permanen dengan menimpa data berulang kali, sehingga tidak dapat dipulihkan. Di sisi lain, teknik Shift+Delete menghapus *file* secara langsung tanpa melalui Recycle Bin, tetapi tidak

melakukan penimpaan data secara fisik, sehingga memungkinkan *file* masih dapat *direcovery* dengan metode forensik tertentu. Dalam konteks penyelidikan forensik digital, penting untuk mengetahui bagaimana performa berbagai *tools file carving* dalam memulihkan *file* dari media penyimpanan yang telah mengalami penghapusan dengan teknik hapus yang berbeda.

### 1.2.1 Pertanyaan Penelitian

Pertanyaan penelitian didasarkan dari rumusan masalah yang telah ditulis diatas tersebut. Agar masalah menjadi butiran-butiran pertanyaan sebagai motor penggerak penelitian untuk dijawab, maka pertanyaan didalam penelitian sebagai berikut :

1. Apakah *file* yang dihapus menggunakan perintah Sdelete dan kombinasi Shift+Delete dapat dipulihkan kembali menggunakan *tools file carving* Autopsy, Magnet Axiom, dan PhotoRec?
2. Bagaimana tingkat keberhasilan masing-masing *tools* dalam memulihkan *file* berdasarkan jumlah artefak yang dapat diakses dan kesesuaian nilai *hash* dengan *file* asli? Serta *tools* mana yang memiliki tingkat persentase keberhasilan paling tinggi?
3. Apa perbedaan karakteristik hasil *recovery* antara *file* yang dihapus menggunakan Sdelete dan Shift+Delete, ditinjau dari dapat diaksesnya artefak, dan validitas nilai *hash*?

### 1.3 Batasan Masalah

Peneliti memberi batasan masalah agar fokus pada tema dalam penelitian ini. Batasan masalah tersebut terdiri dari :

- a. Media penyimpanan yang digunakan untuk penyalinan *file* yakni Flashdisk.
- b. Penelitian ini berfokus untuk melakukan perbandingan hasil *recovery tools file carving* terhadap penghapusan *file* menggunakan perintah Sdelete dan Shift +Delete dan tidak membahas secara eksplisit alasan teknis mengapa suatu *tools* berhasil atau tidak dalam melakukan *recovery tools*.
- c. *Tools file carving* yang digunakan adalah FTK Imager, Autopsy, Magnet Axiom dan PhotoRec yang dapat berjalan pada sistem operasi Windows.
- d. Bukti digital masing-masing ekstensi dengan jumlah 5 *file*, yaitu:
  1. *File* dokumen dengan ekstensi .pdf dan .docx
  2. *File* gambar dengan ekstensi .jpg dan .png

3. *File* audio dengan ekstensi .mp3 dan .wav
  4. *File* video dengan ekstensi .mp4 dan .avi
  5. *File* arsip dengan ekstensi .zip dan .rar
- e. Validasi bukti digital didasarkan pada kesamaan nilai *hash* MD5, antara bukti digital asli dan hasil temuan.
  - f. Parameter penilaian kinerja *tools file carving* yaitu pada temuan artefak yang dapat dibuka / diakses dan kesesuaian pada nilai *hash* pada masing-masing artefak.
  - g. Metode akuisisi data yang digunakan adalah *static forensic*.

#### 1.4 Tujuan Penelitian

Penelitian ini memiliki tujuan untuk melakukan perbandingan hasil *recovery* dari masing-masing *tools file carving* dalam melakukan *recovery file* yang dihapus menggunakan teknik penghapusan data perintah *Sdelete* dan kombinasi tombol Shift+Delete.

#### 1.5 Manfaat Penelitian

Harapan besarnya, penelitian ini dapat memberikan pengetahuan yang berguna kepada pembaca secara umum, investigator, peneliti, mahasiswa. Manfaat dari apa yang didapat dalam penelitian ini terdiri dari :

- a. Memastikan kinerja *tools file carving* dalam melakukan *recovery file* dan bagaimana perbandingan hasil dari masing-masing data yang telah dihapus menggunakan teknik hapus yang berbeda.
- b. Penelitian ini memberikan wawasan tentang bagaimana hasil *recovery file* jika dihadapkan pada permasalahan *file* yang dihapus menggunakan metode penipaan *file* yang mengadopsi standar DOD 5220.22-M
- c. Peningkatan pemahaman tentang daya hapus menggunakan perintah *Sdelete* dan kombinasi Shift+Delete serta mengidentifikasi beberapa tantangan teknis dalam pemulihan data, seperti adanya *file* yang *corrupt* sehingga tidak dapat diakses hingga *file* yang tidak ditemukan.

#### 1.6 Metode Penelitian

Penelitian ini perlu disusun langkah-langkah penyelesaian secara sistematis, adapun sistematika metodologi yang digunakan pada penelitian ini adalah sebagai berikut:

### 1. Identifikasi Masalah

Pada tahapan ini peneliti mengidentifikasi dan menemukan masalah dari jurnal-jurnal penelitian terbaru yang terkait kejahatan yang penghapusan terhadap barang bukti digital.

### 2. Menetapkan Tujuan Penelitian

Tahapan selanjutnya dengan menentukan tujuan yang ingin dicapai dari penelitian yang sesuai dengan latar belakang penelitian.

### 3. Menentukan Objek Penelitian

Peneliti melakukan penentuan terhadap objek penelitian, objek tersebut adalah hasil dari *recovery file* yang telah dilakukan penghapusan menggunakan teknik hapus yang berbeda.

### 4. Studi Literatur

Peneliti melakukan studi literatur dalam mengumpulkan informasi, melakukan peninjauan dan menganalisis dari berbagai informasi yang telah ada, seperti jurnal, buku, artikel resmi. Dalam meninjau literatur yang ada, peneliti dapat mencari celah dan menemukan area yang belum diteliti serta mendapatkan keterbaruan penelitian.

### 5. Pengujian dan Analisis Sistem

Setelah masalah, tujuan, objek penelitian, dan keterbaruan penelitian ditentukan, penelitian ini melakukan pengujian menggunakan *tools file carving*. Teknik hapus yang digunakan adalah perintah Sdelete dan kombinasi tombol Shift+Delete. Analisis dilakukan setelah seluruh hasil didapat.

## 1.7 Sistematika Penulisan

Untuk memberikan kerangka konseptual dan memfasilitasi proses penyusunan penelitian ini, disusun sistematika penulisan dengan struktur sebagai berikut:

### **BAB I Pendahuluan**

Bab ini secara detail berisi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

### **BAB II Tinjauan Pustaka**

Pada bab ini berisi teori-teori yang menjadi landasan terkait dengan kebutuhan didalam penelitian ini.

### **BAB III Metodologi Penelitian**

Bab metodologi memuat langkah-langkah pendekatan dalam penyelesaian masalah penelitian dari awal sampai dengan hasil.

#### **BAB IV Hasil**

Hasil dari penelitian dituliskan didalam bab ini. Hasil penelitian sesuai dengan praktik dari penerapan teknik-teknik yang digunakan.

#### **BAB V Penutup**

Sebagai bagian penutup, bab ini memuat kesimpulan dari keseluruhan proses hingga hasil penelitian. Dalam bab ini, disampaikan juga rekomendasi yang bisa menjadi acuan untuk penelitian lanjutan di masa mendatang.

## BAB 2

### Tinjauan Pustaka

Tinjauan pustaka peneliti sajikan dalam dua bagian yaitu penelitian terdahulu dan konsep pengetahuan, yang terdapat dibawah ini:

#### 2.1 Penelitian Terdahulu

*Recovery file carving* menggunakan *tools* menjadi teknik yang telah digunakan oleh investigator dalam melakukan pemulihan *file* yang telah dihapus dari penyimpanan perangkat. Banyak *tools* yang dapat digunakan dalam memulihkan data, diantaranya yakni Autopsy, Magnet Axiom dan PhotoRec. Sebelum melakukan *recovery*, terlebih dahulu investigator digital forensik melakukan akuisisi data. Akuisisi berguna agar menghasilkan salinan seluruh isi perangkat dimana salinan akan menjadi *file image*. *File image* ini nantinya yang akan menjadi bahan dalam melakukan *recovery* data.

Teknik *file carving* telah dilakukan pada penelitian-penelitian sebelumnya, seperti pada penelitian (Matondang et al., 2023) yang menguji PhotoRec, Autopsy, dan Scalpel terhadap flashdisk yang diformat dan dihapus secara permanen. Hasilnya menunjukkan PhotoRec memiliki tingkat keberhasilan *recovery* tertinggi hingga 80% pada *file* gambar, video, audio, dan dokumen. Namun, penelitian ini hanya fokus pada *logical deletion* (Shift+Delete atau format *drive*) dan tidak mempertimbangkan metode *secure deletion* yang menggunakan teknik penimpaan data (*overwrite*). Hal ini menjadi keterbatasan penting karena *logical deletion* masih menyisakan artefak di *storage*, sedangkan *secure deletion* seperti Sdelete menghapus data secara permanen. Penelitian lain oleh (Fatmah & Indrayani, 2022) menemukan bahwa Autopsy gagal memulihkan *file* pada SSD dengan fitur TRIM aktif (0%) dan hanya berhasil (100%) jika TRIM dinonaktifkan. Temuan ini menyoroti pengaruh signifikan teknologi *storage* terhadap keberhasilan *recovery*. Meskipun demikian, penelitian ini terbatas pada SSD dengan skenario penghapusan TRIM, sementara media penyimpanan berbasis flashdisk dengan metode penghapusan aman seperti Sdelete belum dieksplorasi.

(Herman et al., 2022) mengevaluasi Magnet Axiom untuk memulihkan artefak digital dari aplikasi media sosial. *Tools* ini terbukti unggul dalam akuisisi artefak aplikasi, namun tidak fokus pada pemulihan *file* yang dihapus di *storage* fisik. Artinya, efektivitas Magnet Axiom dalam konteks *recovery file* yang dihapus dari media penyimpanan eksternal seperti flashdisk masih belum teruji. (Yudhana, Riadi, & putra, 2022) menekankan efektivitas metode *static forensic* menggunakan tools DC3DD, ddrescue, dan FTK Imager

CLI untuk akuisisi data dari USB *drive*. Penelitian ini membuktikan bahwa *metode static forensic* penting untuk menjaga integritas bukti, tetapi tidak membahas evaluasi *tools file carving* terhadap *file* yang dihapus dengan teknik penghapusan aman seperti Sdelete. Selain itu, (Julian et al., 2023) menunjukkan Autopsy mampu memulihkan data hingga 81,42% pada flashdisk yang diformat. Akan tetapi, studi ini masih terbatas pada penghapusan standar dan tidak menguji performa *tools* saat metadata dan isi data telah ditimpa.

Dari penelitian sebelumnya, dapat disimpulkan sebagian besar studi lebih menekankan pada pemulihan data setelah penghapusan konvensional. Keterbatasan ini menciptakan celah penelitian yang signifikan terutama untuk memahami keefektifan *tools file carving* serta perbandingan hasil jika kedua teknik hapus berbeda. Penelitian ini hadir untuk mengisi *gap* tersebut dengan membandingkan performa tiga *tools file carving* (Autopsy, Magnet Axiom dan PhotoRec) terhadap dua metode penghapusan *file*, yaitu perintah Sdelete dan kombinasi tombol Shift+Delete. Fokus utama penelitian ini adalah mengevaluasi kemampuan *recovery tools* pada media penyimpanan flashdisk, sekaligus menganalisis integritas data hasil *recovery* dengan membandingkan nilai *hash file* asli dan *file* hasil pemulihan. Berikut rangkuman penelitian terdahulu yang berkaitan dengan metode, *tools* dan objek pada tabel 1.1.

Tabel 1.1 *Review Penelitian Terdahulu*

| No. | Judul                                                                     | Metode, <i>framework</i> ,<br><i>Tools</i> , Objek                                                                                   | Hasil Penelitian                                                                                                             |
|-----|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 1   | Perbandingan <i>Tools</i> Forensik pada Aplikasi Dompet Digital           | <i>framework</i> : DFRWS<br><i>Tools</i> : Autopsy dan Belkasoft Evidence Center.<br>Objek: <i>Software</i> Android (Dompet Digital) | Autopsy lebih baik dalam menemukan data aktivitas transaksi pada aplikasi dompet digital daripada Belkasoft Evidence Center. |
| 2   | Analisa Kinerja Aplikasi Digital Forensik Autopsy untuk Pengembalian Data | <i>Framework</i> : NIST dan metode <i>static forensic</i><br><i>Tools</i> : Autopsy dan hash compare<br>Objek: FlashDisk             | Sebanyak 81,42% data berhasil dipulihkan menggunakan Autopsy, data tersebut bersumber dari flashdisk yang diformat.          |

Tabel 1.1 *Review Penelitian Terdahulu (Lanjutan)*

| No. | Judul                                                                                                                                                         | Metode, <i>framework</i> ,<br><i>Tools</i> , Objek                                                                                                                                                             | Hasil Penelitian                                                                                                                                                                                                                                          |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | Menggunakan<br>Metode NIST SP<br>800-86                                                                                                                       |                                                                                                                                                                                                                |                                                                                                                                                                                                                                                           |
| 3   | <i>Digital Forensic<br/>Signal Instant<br/>Messages Services<br/>in Case of<br/>Cyberbullying<br/>using Digital<br/>Forensic Research<br/>Workshop Method</i> | <i>framework</i> : DFWRS<br><i>Tools</i> : MOBILedit<br>Forensic Express Pro,<br>Belkasoft Evidence<br>Center, dan SQLite DB<br>Browser<br>Objek: <i>Software</i><br>Android (Signal Instant<br>Messenger)     | Penelitian ini mengungkapkan<br>bahwa perundungan daring<br>dilakukan oleh 4 orang, dengan 2<br>sebagai korban, dan 1 sebagai<br>saksi                                                                                                                    |
| 4   | Analisis<br>Perbandingan<br>Perangkat Lunak<br>Forensik Digital<br>untuk <i>File carving</i><br>dalam Mengungkap<br>Barang Bukti<br>Digital                   | <i>Framework</i> : National<br>Institute of Justice (NIJ)<br><i>Tools</i> : Autopsy,<br>PhotoRec, Scalpel, dan<br>Foremost<br>Objek : flashdisk                                                                | Hasil terhadap evaluasi kinerja<br>recovery menghasilkan Photorec<br>dengan kinerja tertinggi yaitu<br>90,8%, diikuti dengan Autopsy<br>dengan persentase sebesar<br>64,17%, Foremost memiliki<br>kinerja 30% dan Scalpel memiliki<br>kinerja sebesar 0%. |
| 5   | <i>Mobile Forensic<br/>Tools for Digital<br/>Crime<br/>Investigation:<br/>Comparison and<br/>Evaluation</i>                                                   | <i>framework</i> : DFRWS<br><i>Tools</i> : MOBILedit<br>Forensic Express, DB<br>Browser, Oxygen<br>Forensic Detective, dan<br>Final Mobile Forensic<br>Objek: <i>Software</i><br>Android (MiChat<br>Messenger) | Final Mobile Forensic memiliki<br>skor indeks tertinggi sebesar 100%<br>dalam penelitian ini, menunjukkan<br>bahwa alat ini memiliki kinerja<br>terbaik dalam mengumpulkan<br>bukti digital                                                               |

Tabel 1.1 *Review Penelitian Terdahulu (Lanjutan)*

| No. | Judul                                                                                                                              | Metode, <i>framework</i> ,<br><i>Tools</i> , Objek                                                                                        | Hasil Penelitian                                                                                                                                                                                                         |
|-----|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6   | Analisis Perbandingan Perangkat Lunak Forensik Digital <i>File carving</i> Menggunakan NIST                                        | <i>Framework</i> : NIST<br><i>Tools</i> : Autopsy, PhotoRec, Scalpel, dan Foremost<br>Objek : Flashdisk                                   | Hasil menunjukkan <i>tool</i> Photorec memenuhi skenario dengan kinerja <i>recovery</i> sebesar 80%. Sedangkan kinerja <i>tool</i> Autopsy sebesar 54,16%, Scalpel sebesar 15% dan terakhir adalah Foremost sebesar 10%. |
| 7   | <i>Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method</i>                             | <i>Framework</i> : NIST<br><i>Tools</i> : Magnet Axiom dan MOBILedit Forensics<br>Objek: Software Android (WhatsApp dan Instagram)        | Magnet Axiom lebih unggul dalam mengambil bukti digital dari aplikasi Instagram dan WhatsApp, terutama ketika bukti digital berupa video yang berdurasi lebih dari 20 menit.                                             |
| 8   | <i>Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework</i>                         | <i>framework</i> : ACPO<br><i>Tools</i> : MOBILedit Forensic Express dan FTK Imager<br>Objek: Software Android (IMO Messenger)            | MOBILedit Forensic Express menghasilkan ekstraksi sebesar 0,75%, sedangkan FTK Imager menghasilkan ekstraksi sebesar 0,25%.                                                                                              |
| 9   | Akuisisi Bukti Digital Pada Aplikasi Michat di Smartphone Menggunakan Metode National Institute of Standards and Technology (NIST) | <i>Framework</i> : NIST<br><i>Tools</i> : MobilEdit Forensik dan Wondershare Dr.Fone<br>Objek: <i>Software</i> Android (MiChat Messenger) | Hasil menunjukkan MobileEdit berhasil melakukan <i>recovery</i> data sebanyak 40 dari 41 data yang disiapkan dan Wondershare Dr. Fone terbilang mampu <i>merecovery</i> sebanyak 23 data dari 41 data.                   |

Tabel 1.1 *Review Penelitian Terdahulu (Lanjutan)*

| No. | Judul                                                                                                                   | Metode, <i>framework</i> ,<br><i>Tools</i> , Objek                                                                                                                 | Hasil Penelitian                                                                                                                                                                                                                                         |
|-----|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10  | <i>Forensic Tools Comparison on File carving using Digital Forensics Research Workshop Framework</i>                    | <i>framework</i> : Digital Forensics Research Workshop (DFRWS).<br><i>Tools</i> : Foremost dan Scalpel.<br>Objek : Flashdisk                                       | Hasilnya, Foremost lebih unggul dari Scalpel, sehingga direkomendasikan dalam proses memperoleh bukti digital pada Flashdisk.                                                                                                                            |
| 11  | Teknik <i>Disk Carving</i> untuk <i>Solid State Drive</i> Volume ReFS dan NTFS dengan Fitur TRIM                        | Metode: Forensika Langsung yang mengikuti Standar Nasional Indonesia (SNI) 27037:2014<br>Tools: Portable FTK Imager, Hetman Partition Recovery, HxD<br>Objek : SSD | Data pada SSD dengan fitur TRIM aktif pulih sebanyak 9% di volume NTFS. Volume ReFS data yang berhasil pulih 0%. Akan tetapi, ketika TRIM nonaktif keseluruhan data dapat pulih pada volume NTFS, sedangkan volume ReFS hanya 74% data yang terpulihkan. |
| 12  | Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST) | <i>Framework</i> : NIST<br><i>Tools</i> : MOBILedit Forensic Express, Belkasoft, dan Autopsy<br>Objek: Software Android (Viber).                                   | MOBILedit Forensic Express dan Belkasoft memberikan hasil bukti digital dengan persentase 100% untuk akun, kontak, gambar, dan video.                                                                                                                    |
| 13  | Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android                                          | <i>Framework</i> : NIST<br><i>Tools</i> : Magnet AXIOM, MobileEdit Express, Autopsy, signal-back, dan signalbackup-tools                                           | <i>Tool</i> Magnet Axiom, MobileEdit dan Autopsy belum mampu membaca database aplikasi android signal Messenger yang terenkripsi. Sedangkan ketiga                                                                                                       |

Tabel 1.1 *Review Penelitian Terdahulu (Lanjutan)*

| No. | Judul                                                                                                                               | Metode, <i>framework</i> ,<br><i>Tools</i> , Objek                                                                   | Hasil Penelitian                                                                                                                                                                                                                    |
|-----|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | dengan metode NIST                                                                                                                  | Objek: Software Android (Signal Messenger)                                                                           | <i>tools</i> tersebut jika berhadapan pada dekripsi database data dari Signalbackup-tools data tidak dapat menampilkan panggilan suara dan panggilan video.                                                                         |
| 14  | Forensik Mobile pada Layanan Media Sosial LinkedIn                                                                                  | <i>Framework</i> : NIST<br><i>Tools</i> : Autopsy, Andriller, Root Browser Apps, dan MOBILedit<br>Objek:             | Andriller mengungkapkan spesifikasi dan rekam jejak komunikasi data, MOBILedit menemukan log activity, Autopsy memunculkan <i>file</i> terhapus, dan Root Browser mengidentifikasi <i>file</i> tersembunyi melalui proses forensik. |
| 15  | Perbandingan <i>Forensic Tools</i> pada Instagram Menggunakan Metode NIST                                                           | <i>Framework</i> : NIST<br><i>Tools</i> : Magnet Axiom dan Belkasoft Evidence<br>Objek: Software Android (Instagram) | Magnet Axiom berhasil mencapai tingkat akurasi sebesar 83.3%, sementara Belkasoft Evidence hanya mencapai 50%.                                                                                                                      |
| 16  | Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology | <i>Framework</i> : NIST<br><i>Tools</i> : Autopsy, Recuva, Stellar, Puran dan Easus.<br>Objek : flashdisk            | Autopsy berhasil menemukan 83% <i>file</i> . Lalu pada tool Recuva, puran, dan easus memiliki kesamaan dalam <i>recovery</i> , yakni sebesar 66%. terakhir, tool stellar berhasil melakukan <i>recovery</i> sebesar 33%.            |

Tabel 1.1 *Review Penelitian Terdahulu* (Lanjutan)

| No. | Judul                                                                                                          | Metode, <i>framework</i> ,<br><i>Tools</i> , Objek                                     | Hasil Penelitian                                                                                                                                                                                                                                        |
|-----|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17  | Analisis Dan Perbandingan <i>Tools</i> Forensik Menggunakan Metode NIST Dalam Penanganan Kasus Kejahatan Siber | <i>Framework</i> : NIST<br><i>Tools</i> : MOBILedit Forensics Express dan Magnet Axiom | Hasil menyebutkan bahwa <i>tool</i> Magnet Axiom lebih unggul ketimbang MOBILedit. Magnet Axiom mampu melakukan <i>recovery</i> dengan nilai keakuratan sebesar 81,8% sedangkan MOBILedit Forensic sebesar menghasilkan nilai keakuratan sebesar 72,7%. |

Peneliti melakukan perbandingan terhadap penelitian terdahulu untuk mendapatkan keterbaruan penelitian yang dijlankan ini. Lalu, mencari solusi atas penelian terdahulu, sehingga peneliti dapat melihat dari berbagai sudut pandang seperti objek yang diteliti, metode yang digunakan, *framework*, serta *tools* yang digunakan dalam penelitian. Keseluruhan penelitian terdahulu dipaparkan secara terperinci dengan jelas pada tabel 1.2

Tabel 1.2 Perbandingan Terhadap Penelitian Terdahulu

| Metode                                          |                                                                                                          |                                               |                                       |          |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------|---------------------------------------|----------|
|                                                 | Static forensic [2, 17]                                                                                  |                                               |                                       |          |
|                                                 | Live Forensic [11]                                                                                       |                                               |                                       |          |
| Objek                                           | Judul Penelitian                                                                                         |                                               | Tool                                  |          |
| Software Android (Dompet Digital) [1]           | Perbandingan hasil recovery file terhadap penghapusan file menggunakan perintah Sdelete dan Shift+Delete |                                               | Autopsy [1, 2, 4, 6, 12, 13, 14, 16]  |          |
| Flashdisk [2, 4, 6, 10, 16]                     |                                                                                                          |                                               | PhotoRec [4, 6]                       |          |
| Software Android (Signal Instant Messenger) [3] |                                                                                                          |                                               | Magnet Axiom [7, 13, 15]              |          |
| Software Android (MiChat Messenger) [5]         |                                                                                                          |                                               | Belkasoft Evidence [1, 3, 12, 15]     |          |
| Software Android (WhatsApp dan Instagram) [7]   |                                                                                                          |                                               | Andriller [14]                        |          |
| Software Android (IMO Messenger) [8]            |                                                                                                          |                                               | Root Browser Apps [14]                |          |
| Software Android (MiChat Messenger) [9]         |                                                                                                          |                                               | MOBILedit [3, 5, 7, 8, 9, 12, 13, 14] |          |
| SSD [11]                                        |                                                                                                          |                                               | signalbackup-tools [13]               |          |
| Software Android (Viber) [12]                   |                                                                                                          |                                               | Hetman Partition Recovery [11]        |          |
| software Android (Signal Messenger) [13]        |                                                                                                          |                                               | FTK Imager [8, 11]                    |          |
| Software Android (LinkedIn) [14]                |                                                                                                          |                                               | HxD [11]                              |          |
| Software Android (Instagram) [15]               |                                                                                                          |                                               | Foremost [4, 6, 10, ]                 |          |
| Software desktop perintah CMD (Sdelete)         |                                                                                                          |                                               | Scalpel [4, 6, 10,                    |          |
|                                                 | DFRWS [1, 3, 5, 10]                                                                                      | NIST [2, 6, 7, 9, 12, 13, 14, 14, 15, 16, 17] | NIJ [4]                               | ACPO [8] |
| Framework                                       |                                                                                                          |                                               |                                       |          |

Tabel 1.1 dan 1.2 oleh peneliti dilakukan sebagai upaya dalam mendapatkan keterbaruan penelitian, memilah dan memilih solusi yang ditawarkan yang dapat dilihat baik dari objek yang diteliti, metode serta *tools* yang diterapkan dalam penelitian, sehingga dari upaya tersebut dihasilkan beberapa poin yaitu :

- a. Berdasarkan metode, penelitian ini menggunakan metode *static forensic* sama dengan penelitian pada tabel nomor 2 dan 17.
- b. Berdasarkan *tools* yang digunakan, peneliti menggunakan beberapa *tools* seperti FTK Imager, Autopsy, Magnet Axiom dan Photorec yang sama dengan penelitian pada tabel :
  - FTK Imager tabel 8 dan 11
  - Autopsy tabel 1, 2, 4, 6, 12, 13, 14 dan 16
  - Magnet Axiom tabel 7, 13 dan 15
  - PhotoRec tabel 4 dan 6
- c. Penelitian ini menggunakan *file* yang telah dipersiapkan dan dilakukan penyalinan pada flashdisk lalu dihapus menggunakan perintah Sdelete yang membedakan dari penelitian sebelumnya dan menggunakan kombinasi tombol Shift+Delete sebagai perbandingan keefektifan penghapusan.

Setelah meninjau berbagai penelitian terdahulu, ditemukan bahwa pembahasan terkait perbandingan hasil *recovery* fokus utama pada *tools* dalam melakukan *recovery* data pada *storage* saja. Berdasarkan hasil peninjauan oleh peneliti, maka penelitian ini mengambil bagian pada bagaimana *tools* yang secara persentase paling banyak direkomendasikan oleh peneliti sebelumnya dapat melakukan *recovery* pada *storage* yang terisi *file-file* yang telah dilakukan upaya penghapusan menggunakan Sdelete dan Shift+Delete.

## **2.2 Konsep Pengetahuan**

### **2.2.1 Digital Forensik**

Digital forensik serangkaian cara yang berfokus dalam hal melakukan pengumpulan bukti digital, analisis temuan, dan pelaporan bukti-bukti digital dari berbagai *device* elektronik yang memiliki *storage*. Ilmu ini memiliki peran penting dalam peradilan kejahatan digital dengan memastikan bahwa bukti digital dapat diperiksa dan divalidasi secara ilmiah untuk digunakan dalam proses hukum (Santos et al., 2024). Digital forensik tidak hanya digunakan

dalam investigasi kriminal tetapi juga dalam kasus perdata, perselisihan bisnis, serta keamanan siber (Horan & Saiedian, 2021). Dalam praktiknya, penyidik digital forensik menggunakan berbagai teknik untuk memperoleh dan menganalisis bukti digital guna memperkuat atau melemahkan bukti dalam suatu kasus (Aisyah et al., 2022). Oleh karena itu, metode yang digunakan harus sesuai dalam menangani bukti digital dengan akurat.

### **2.2.2 Bukti Digital**

Bukti digital menjadi informasi dalam bentuk elektronik yang dapat digunakan untuk membuktikan suatu kejadian dalam investigasi (Citra Dewi et al., 2023). Bukti ini dapat ditemukan dalam berbagai format, seperti *file* teks, gambar atau video, metadata, rekaman audio, serta jejak digital dari komunikasi daring. Temuan bukti digital yang valid dapat menjadi faktor penentu dalam berbagai kasus hukum, baik dalam investigasi kriminal, perselisihan perdata, maupun keamanan siber (Prasetya & Priyana, 2021). Oleh karena itu, keberhasilan dalam memulihkan bukti digital yang telah dihapus menjadi sangat penting dalam proses investigasi.

### **2.2.3 Static Forensic**

Dalam hal melakukan rangkaian pengumpulan bukti digital, terdapat dua metode utama, yaitu *Live Forensic* dan *static forensic*. *Live Forensic* digunakan ketika perangkat dalam keadaan menyala untuk memperoleh bukti dari sistem yang sedang berjalan, seperti memori RAM, koneksi jaringan, atau aktivitas pengguna (Utami et al., 2021). Teknik ini berguna untuk menangkap data yang bersifat *volatile* atau mudah hilang setelah perangkat dimatikan. Sementara itu, *static forensic* dilakukan pada perangkat dalam keadaan mati dengan cara melakukan ekstraksi dan analisis bukti digital dari media penyimpanan (Santoso & Sulaksono, 2022). Metode ini memastikan bahwa bukti tidak berubah selama proses investigasi karena menggunakan pencitraan (*imaging*) bit-per-bit untuk mendapatkan salinan data yang utuh (Riadi et al., 2020) dan memastikan bahwa bukti digital tetap terjaga dalam kondisi aslinya (Iqbal & Soewito, 2020). Dalam konteks penelitian ini, metode *static forensic* lebih relevan karena fokusnya adalah pada pemulihan data dari media penyimpanan yang bersifat *non-volatile* yang telah dilakukan penghapusan *file* menggunakan metode hapus tertentu.

#### 2.2.4 File Carving

Salah satu teknik utama dalam pemulihan data digital forensik adalah *file carving*, metode yang digunakan dalam melakukan *recovery file* dimana *file* dengan sengaja dihapus dari median penyimpanan, bahkan jika informasi sistem *file* sudah hilang (Boiko et al., 2023). Teknik ini bekerja dengan mengidentifikasi pola spesifik dalam struktur *file*, seperti *header*, *footer*, dan struktur data internal, untuk merekonstruksi *file* yang masih tersimpan dalam sektor penyimpanan meskipun telah dihapus oleh sistem operasi. *File carving* diperlukan karena keunggulannya dalam mengambil data dari penyimpanan seperti harddisk, flashdisk, perangkat seluler walaupun dalam keadaan terhapus (Alzaabi & Al Shibli, 2025). Oleh karena itu, *file carving* digunakan dalam penelitian ini untuk menguji efektivitas *tools* forensik dalam memulihkan *file* yang telah dihapus menggunakan teknik hapus perintah Sdelete dan Shift+Delete.

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*.

#### 2.2.5 Perintah Sdelete

SDelete merupakan utilitas penghapusan aman (*secure deletion*) berbasis *Command Line* yang dikembangkan oleh Microsoft. alat ini menggunakan metode *overwrite* berbasis standar DoD 5220.22-M yang menimpa data berulang kali untuk memastikan *file* tidak dapat direkonstruksi kembali (Microsoft, 2022). Sdelete bekerja dengan menghapus dan menimpa ruang kosong pada *disk* sehingga *file* yang sebelumnya dihapus tidak dapat direkonstruksi. Selain itu, Sdelete menggunakan teknik pengacakan nama *file* sebelum dihapus, sehingga lebih sulit bagi *tools* pemulihan untuk mengenali jejak *file* yang dihapus. Pengguna dapat menentukan jumlah *overwrite pass* menggunakan opsi perintah -p, serta memilih untuk membersihkan *free space* dengan perintah -c atau menuliskan nol dengan perintah -z. Meskipun data termusnahkan, nama *file* lama tetap tidak terhapus dari struktur direktori, hanya konten fisiknya saja yang di *overwrite* secara aman.

#### 2.2.6 Kombinasi tombol Shift+Delete

Dalam penelitian ini, disamping menggunakan perintah Sdelete sebagai upaya penghapusan data, juga digunakan teknik hapus lain yang tidak menggunakan metode penimpaan data.

Kombinasi tombol Shift+Delete digunakan karena teknik hapus ini melakukan penghapusan data secara permanen dengan melakukan penghapusan tanpa melalui *recycle bin*. Teknik Shift+Delete termasuk dalam kategori *logical deletion*, yaitu penghapusan *file* dengan cara menghapus entri *file* dari tabel direktori pada sistem *file*, tanpa melakukan penimpaan pada sektor data. Akibatnya, konten *file* fisik tetap berada di media penyimpanan sampai sektor tersebut ditimpa oleh data baru (Agustiono et al., 2024). Oleh karena itu, meskipun *file* dihapus secara permanen dari antarmuka pengguna (tidak melalui *recycle bin*), metode ini masih memungkinkan pemulihan menggunakan teknik *file carving* selama blok memori belum di-*overwrite*.

### **2.2.7 Autopsy**

Autopsy merupakan salah satu alat digital forensik yang digunakan dalam melakukan pemulihan data, merupakan *platform open source* yang dikembangkan oleh Sleuth Kit. Alat ini dirancang sebagai solusi untuk menganalisis media digital secara cepat, menyeluruh, efisien dan memiliki modul otomatis yang dapat dijalankan paralel, pencarian kata kunci, pencocokan *hash*, pemulihan *file* melalui teknik *file carving*, analisis *timeline*, ekstraksi metadata (Sleuth Kit Labs, 2025). 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 *thumbnail* (Nayak, 2024).

### **2.2.8 Magnet Axiom**

Sama seperti Autopsy, Magnet Axiom merupakan salah satu alat yang digunakan dalam melakukan *recovery file* yang telah dihapus dari media penyimpanan. Magnet Axiom melakukan proses pemulihan data melalui dua tahapan, yaitu *parsing-only* yang mengekstraksi metadata dan artefak yang mudah ditemukan, serta *post-process carving* yang menerapkan teknik *file carving* setelah proses *parsing* untuk memulihkan *file* yang terhapus (Magnet Forensics, 2022). Pada tahap awal, Magnet Axiom memanfaatkan metadata sistem *file*, kemudian dilanjutkan dengan proses *post-process carving* untuk mendeteksi artefak yang tidak terstruktur. Namun demikian, pendekatan yang digunakan tidak sepenuhnya bergantung pada metode berbasis *signature* (Siamukulule, 2024).

### 2.2.9 PhotoRec

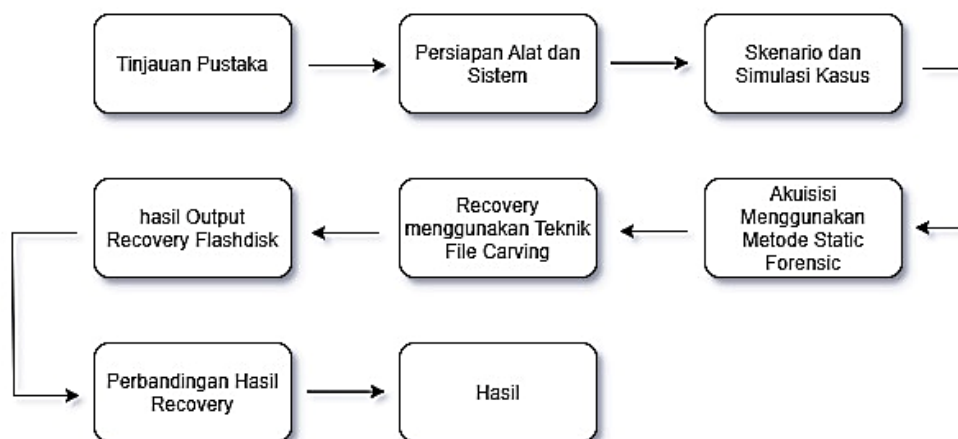
Berbeda dari *tools file carving* lainnya, PhotoRec merupakan alat pemulihan data *open source* lintas *platform* yang dirancang untuk memulihkan beragam jenis *file* dari media penyimpanan, termasuk hard disk, SSD, CD-ROM, *drive* memori USB dan memori kamera digital, meskipun struktur sistem *filenya* rusak atau terformat. Cara kerjanya adalah dengan mengabaikan sistem *file* dan melakukan *signature-based carving*, menemukan *file* berdasarkan *signature* yang telah dikenali, seperti *header* JPEG, mengikuti validasi struktur *file* untuk memastikan hasil yang akurat. PhotoRec mendukung ratusan tipe format *file* (sekitar 480 ekstensi), bersifat *read only* demi keamanan data, dan tersedia secara gratis di banyak sistem operasi (CGsecurity, 2024).

## BAB 3

### Metodologi

#### 3.1 Tahapan Awal

Perbandingan hasil *recovery* masing-masing *tools file carving* dalam melakukan *recovery file* yang dihapus menjadi tujuan dalam penelitian ini. Untuk mencapai tujuan dan menjawab pertanyaan penelitian, diperlukan langkah-langkah penelitian agar dapat menyelesaikan masalah. Sebagai langkah penyelesaian masalah, penelitian ini dilakukan melalui beberapa tahapan yang dipilih agar relevan dengan permasalahan, langkah-langkah terbagi menjadi persiapan alat, skenario simulasi kasus, akuisisi data, proses, hasil dan perbandingan hasil *recovery*. Berikut langkah demi langkah yang diterapkan didalam peneltian ini, terlihat pada gambar 3.1.



Gambar 3.1 Alur metodologi penelitian.

#### 3.2 Tinjauan Pustaka

Tinjauan pustaka sebagai modal awal yang bertujuan dalam melakukan pengumpulan informasi yang sesuai dengan topik penelitian. Sumber pustaka berasal dari jurnal, paper, artikel, penemuan penelitian sebelumnya dan situs yang berasal dari internet yang sesuai dengan konteks penelitian. Sehingga, mampu mengantarkan kepada tujuan akhir dari penelitian ini.

### 3.3 Persiapan Alat dan Sistem

Penelitian ini menggunakan teknik *file carving* untuk melakukan *recovery* flashdisk. Supaya penelitian dapat berjalan dengan baik, diperlukan alat dan sistem pada komputer sebagai perlengkapan untuk menunjang penelitian. Berikut ini persiapan yang akan digunakan :

1. Laptop Lenovo seri Thinkpad L480 dengan spesifikasi :
  - a. Processor : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz 1.90 GHz
  - b. Memory : 480 GB SSD / 16 GB RAM
  - c. Sistem Operasi : Windows 11 Pro 64-bit
2. Flash Disk Mikuso 8 GB
3. HashMyFiles
4. Sdelete.exe
5. AccessData FTK Imager v4.7.1.2
6. Autopsy v4.21.0
7. Magnet AXIOM Examine v5.4.0.26185
8. PhotoRec 7.2

### 3.4 Skenario dan Simulasi Kasus

Skenario dilakukan berawal dari data yang disalin kedalam flashdisk berupa *file-file* yang telah disiapkan. Data tersebut dibagi menjadi *file* yang dihapus menggunakan perintah Sdelete dan *file* yang dihapus menggunakan kombinasi tombol Shift+Delete. Studi kasus yang terjadi yakni seluruh data yang ada didalam flashdisk kosong dan dicurigai telah dilakukan penghapusan dengan teknik tertentu untuk menghilangkan barang bukti. Data tersebut dibutuhkan sebagai bukti yang kuat di meja pengadilan bahwa telah dilakukan upaya penyalahgunaan data. Untuk menganalisa flashdisk yang telah kosong tersebut, maka dibutuhkan bantuan ahli digital forensik sebagai upaya dalam mengembalikan data, menguak kejahatan yang dilakukan serta mencocokkan antara data asli dan data yang telah dihapus dari dalam flashdisk.

Data atau bukti digital yang digunakan sebagai pengujian pada skenario dan simulasi kasus terdiri dari jenis *file* berdasarkan literatur yang menyebut format-format tersebut merupakan jenis *file* yang paling sering muncul dalam konteks kejahatan digital yakni *file* dengan ekstensi .pdf, .docx, .jpg, .png, .mp3, .avi dan .zip, dimana format ini termasuk dalam kategori media *file* berstruktur kompleks yang merupakan target utama dalam proses *file carving* karena kerentanan terhadap fragmentasi (Boiko et al., 2023). Jumlah total *file* yang digunakan dalam pengujian yakni 50 *file* dengan masing-masing ekstensi berjumlah 5 *file*

sebagaimana diperkenankan pada ISO/IEC 17025:2017, Pasal 7.2.2 yang menyatakan bahwa tingkat validasi disesuaikan dengan ruang lingkup aplikasi. Karena pada penelitian ini bersifat komparatif dan eksploratif, maka jumlah 5 *file* cukup untuk mengukur pola hasil pemulihan perbandingan hasil *recovery file*.

### 3.5 Akuisisi Menggunakan Metode *Static Forensic*

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.

### 3.6 *Recovery* Menggunakan Teknik *File Carving*

Dengan teknik *file carving*, *tool* yang digunakan akan melakukan pemindaian pada data yang telah dihapus permanen kemudian akan *direcovery* secara otomatis. Teknik ini akan melakukan pencarian *file* yang telah dihapus berdasarkan *header* dan *footer* (Sethi, 2024).

### 3.7 Hasil *Output Recovery* Flashdisk

Setelah proses *recovery* selesai, artefak yang berhasil dipulihkan dikelompokkan berdasarkan masing-masing teknik penghapusan yaitu penghapusan menggunakan Sdelete dan penghapusan permanen menggunakan kombinasi Shift+Delete. Hasil dicatat pada tabel berdasarkan nama *tools*, nama *file*, format *file* dan jumlah artefak temuan. Selain itu, hasil dicatat pada tabel sebagai validasi kesesuaian *hash* yang dilakukan untuk memastikan bahwa *file* yang dipulihkan sesuai dengan *file* aslinya. Nilai *hash* hasil *recovery* setiap *file* yang dipulihkan dilakukan pengecekan keidentikan dengan nilai *hash file* aslinya menggunakan *tool* HashMyFiles. Rancangan tabel akan dibuat dalam dua tabel, yaitu *output File Yang Dihapus Menggunakan Sdelete* dan *output File Yang Dihapus Menggunakan Shift+Delete*.

### 3.8 Analisis Perbandingan Hasil *Recovery*

Dalam melakukan pengukuran kemampuan terhadap *tools*, digunakan rumus perhitungan yang akan menghasilkan angka persentase pemulihan data. Hasil persentase diperoleh dari perhitungan *file* yang ditemukan dari penggunaan *tools file carving*. Rumus perhitungan (rumus 3.1) yang digunakan adalah sebagai berikut: (Yuladi & Indrayani, 2023).

$$Par = \frac{\sum ar0}{\sum arT} \times 100\% = XX\% \quad (3.1)$$

Keterangan :

Par merupakan angka indeks persentase

ar0 merupakan jumlah *file* yang terdeteksi.

arT merupakan jumlah keseluruhan *file* yang digunakan.

Perhitungan dilakukan berdasarkan hasil *output recovery* yang telah dilakukan, evaluasi kinerja seluruh *tools file carving* dalam mengambil bukti digital dari media penyimpanan flashdisk ditampilkan dalam dua tabel, yaitu analisis *recovery* hasil penghapusan Sdelete dan analisis *recovery* hasil penghapusan Shift+Delete.

### 3.9 Hasil

Setelah keseluruhan langkah-langkah penelitian selesai, hasil setiap perhitungan persentase dari analisis ditulis kedalam tabel. Tabel hasil akhir sebagai informasi nilai persentase perhitungan masing-masing *tools file carving* dalam melakukan *recovery file*. Tabel hasil sebagaimana terlihat pada tabel 3.1.

Tabel 3.1 Contoh Tabel Hasil Akhir

| Nama <i>Tools</i> | Nilai persentase         |                        |
|-------------------|--------------------------|------------------------|
|                   | Pengembalian <i>File</i> | Kesesuaian <i>Hash</i> |
| Autopsy           | xx                       | xx                     |
| Magnet Axiom      | xx                       | xx                     |
| PhotoRec          | xx                       | xx                     |

## BAB 4

### Hasil dan Pembahasan

#### 4.1 Tinjauan Pustaka

Peneliti mengkaji hasil *recovery* perangkat lunak forensik digital dalam memulihkan data yang dihapus menggunakan perintah Sdelete dan kombinasi tombol Shift+Delete. Sdelete sebuah utilitas yang dirancang untuk menghapus data secara permanen sesuai dengan standar DOD 5220.22-M. Selain itu, Sdelete merupakan alat penghapusan data permanen yang mengimplementasikan penipaan data berulang untuk memastikan data tidak dapat dipulihkan (Microsoft, 2022). Digital forensik cabang ilmu untuk mengungkap kasus-kasus kejahatan digital yang berfokus pada pengumpulan, analisis, dan pelaporan bukti digital bertujuan untuk memberikan pilihan dan rekomendasi kepada hakim untuk mengungkap kasus pidana (Yudhana et al., 2022).

Salah satu pendekatan akuisisi yang digunakan adalah *static forensic*, yaitu analisis media penyimpanan dalam kondisi tidak aktif, berbeda dengan *live forensic* yang dilakukan pada perangkat aktif (Santoso & Sulaksono, 2022). Teknik *file carving* merupakan metode pemulihan data tanpa informasi *file system*, yang mengidentifikasi struktur data berdasarkan *header* dan *footer file* dan memungkinkan pemulihan data yang dihapus atau rusak, bahkan ketika metadata *file system* telah hilang (Garfinkel & McCarrin, 2015). Penelitian-penelitian terdahulu memberikan gambaran efektivitas berbagai *tools* digital forensik. PhotoRec tercatat memiliki tingkat keberhasilan hingga 80% dalam memulihkan berbagai jenis *file* (Matondang et al., 2023). Autopsy menunjukkan hasil yang baik pada media penyimpanan dengan fitur TRIM nonaktif, namun tidak berhasil memulihkan data dari SSD dengan fitur TRIM aktif (Fatmah & Indrayani, 2022). Sementara itu, Magnet Axiom terbukti unggul dalam mengambil artefak digital dari aplikasi media sosial, terutama *file* multimedia (Herman et al., 2022). Selain itu, metode *static forensic* telah terbukti andal dalam menganalisis perangkat penyimpanan USB, terutama dalam menjaga integritas bukti digital (Yudhana et al., 2022).

Sebagian besar penelitian sebelumnya hanya berfokus pada pemulihan data secara umum tanpa melakukan pengujian terhadap teknik penghapusan lainnya yang menggunakan penipaan data. Microsoft mengklaim bahwa data yang dihapus dengan Sdelete tidak dapat dipulihkan. Penelitian ini bertujuan untuk melakukan perbandingan hasil pada *file* yang dihapus menggunakan Sdelete dan Shift+Delete sebagai upaya pembandingan daya hapus,

serta membandingkan hasil *recovery tool file carving* terbaik berdasarkan temuan dan kesesuaian nilai *hash file* hasil pemulihan. *Tools file carving* yang digunakan sebagai *recovery* yaitu Autopsy, Magnet Axiom dan PhotoRec.

## 4.2 Persiapan Alat dan Sistem

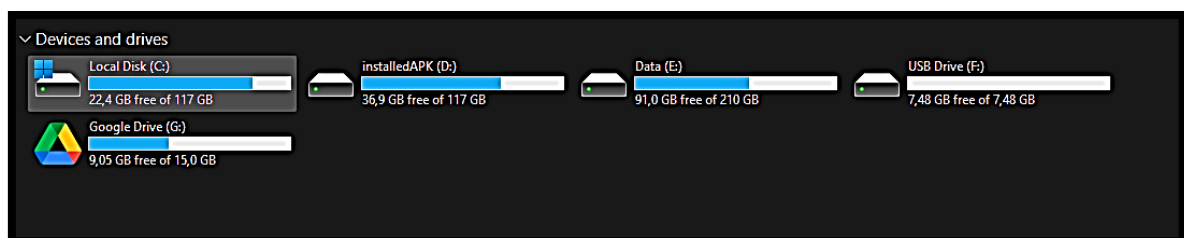
Persiapan peralatan serta sistem diterapkan selama proses akuisisi dan *recovery* data secara langsung. Tahap awal mencakup penyiapan *hardware* dan *software* yang diperlukan untuk menjalankan penelitian ini. Beberapa peralatan yang harus dipersiapkan ditampilkan pada tabel 4.1.

Tabel 4.1 *Hardware Dan Software*

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

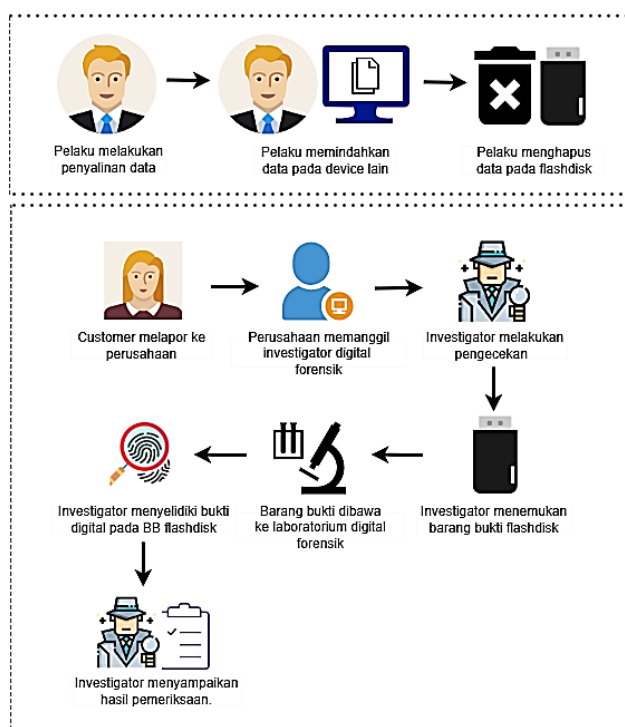
## 4.3 Skenario dan simulasi Kasus

Dalam simulasi kasus, dilakukan penyalinan data kedalam flashdisk berupa *file-file* dokumen (docx dan pdf), gambar (jpg dan png), audio (mp3), video (mp4), arsip (zip dan rar) yang dibuat menjadi dua folder, yaitu folder yang nantinya digunakan untuk dihapus menggunakan Sdelete dan folder yang digunakan sebagai data yang dihapus menggunakan kombinasi tombol Shift+Delete. Saat flashdisk ditemukan, dengan nama USB Drive (F:) dilihat isinya, kondisi flashdisk tersebut telah kosong, dapat dilihat pada gambar 4.1.



Gambar 4.1 Flashdisk (F:) dalam keadaan kosong.

Karena flashdisk dinyatakan kosong setelah dilakukan pengecekan, flashdisk tersebut dianggap mencurigakan menyimpan bukti yang telah dihapus oleh pelaku kejahatan. Karena kecurigaan tersebut, dilakukan proses *static forensic*. Proses *static forensic* memungkinkan penyidik digital forensik untuk melakukan analisis pasca akuisisi dilakukan, sehingga memungkinkan mengumpulkan informasi dari dalam flashdisk dan mencari *file-file* yang dianggap mencurigakan menggunakan *tools file carving*. Dengan proses tersebut, *static forensic* sebagai pembukti yang menjadi kunci dalam dan memperkuat kasus dalam investigasi kejahatan. Proses pertama yang dilakukan adalah dengan melakukan *imaging* flashdisk 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*. Setelah dilakukan *imaging*, lalu *file working copy* dibuka melalui *tool file carving* Autopsy, Magnet Axiom dan Photorec untuk dilakukan proses *recovery*.



Gambar 4.2 Alur skenario kasus.

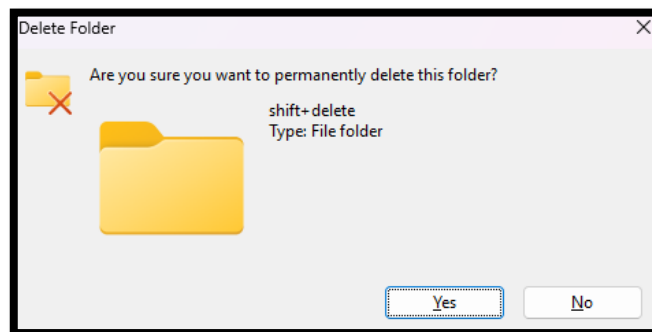
Berikut alur skenario kasus berdasarkan pada gambar 4.2 yang bermula dari tindakan yang dilakukan oleh pelaku. Langkah – langkah yang dilakukan pelaku:

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 seperti pada gambar 4.3. Karena Sdelete memerlukan proses dan waktu dalam penghapusan, untuk mempercepat penghilangan bukti pelaku menghapus data-data lainnya menggunakan kombinasi tombol Shift+Delete, terlihat pada gambar 4.4.

```
C:\Users\rosir>sdelete -s -r -p 3 F:\sdeleteCMD  
  
SDelete v2.05 - Secure file delete  
Copyright (C) 1999-2023 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

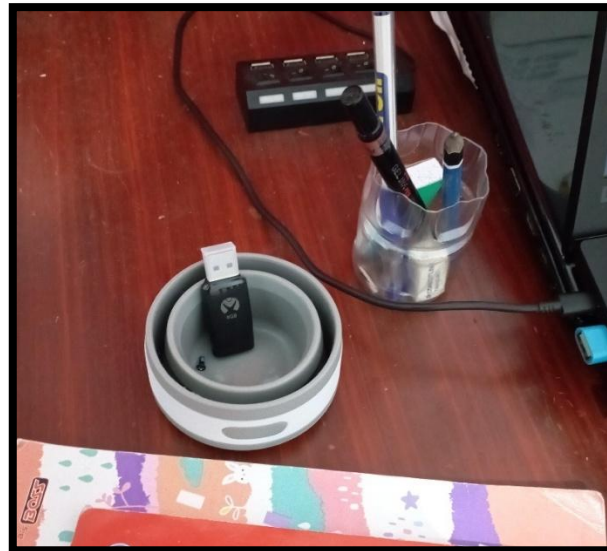
Gambar 4.3 File dihapus menggunakan Sdelete.



Gambar 4.4 File dihapus menggunakan kombinasi tombol Shift+Delete.

Data yang didapat oleh pelaku digunakan untuk aktifitas kejahatan dengan memanfaatkan data informasi *customer*. Lalu, *customer* merasa ada keganjilan dalam notifikasi Gmailnya, sebab notifikasi tersebut berupa tagihan pinjaman *online*. Merasa bahwa data *customer* telah bocor dan disalah gunakan, oleh kareba data serta Gmail yang digunakan hanya diperuntukkan administrasi perusahaan Dango. Oleh sebab itu, *customer* melapor pada perusahaan Dango dan perusahaan menindak lanjuti dengan memanggil investigator digital forensik.

Setelah surat untuk melakukan investigasi diterima oleh investigator, Investigator melakukan pengecekan pada perusahaan dan menemukan flashdisk yang berserakan dan tertinggal di meja kerja pelaku. Ditemukan bahwa flashdisk tersebut berkapasitas 8 giga byte, yang terlihat pada gambar 4.5. Selanjutnya investigator melakukan langkah-langkah forensik untuk mendapatkan bukti.



Gambar 4.5 Barang bukti flashdisk yang ditemukan diatas meja.

Langkah – langkah yang dilakukan investigator :

1. Flashdisk diamankan dan dibawa ke laboratorium digital forensik untuk dilakukan penyelidikan.
2. Investigator melakukan akuisisi pada flashdisk menggunakan komputer laboratorium digital forensik dan *tool* menggunakan FTK Imager.
3. Setelah dilakukan *imaging* dan mendapatkan hasil *image* dari flashdisk, dilakukan pemeriksaan serta melakukan analisis menggunakan *tools file carving*.
4. Investigator menuliskan hasil dan menyampaikan hasil keseluruhan dari temuan yang ada didalam flashdisk kepada pihak perusahaan.

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

6. Penyalinan dan penghapusan *file*

Penjelasan : penyalinan *file* dilakukan sebagai data untuk dilakukan penghapusan. *File* disalin berdasarkan masing-masing pada *folder* sesuai dengan teknik penghapusan. Setelah data tersalin, lalu masing-masing *folder* dilakukan penghapusan menggunakan Sdelete untuk folder Sdelete CMD dan Shift+Delete untuk folder Shift+Delete.

7. Melakukan *static forensic* terhadap flashdisk

Penjelasan : pada flashdisk yang telah kosong, dilakukan proses *imaging*. *Tool* FTK Imager disiapkan dan digunakan untuk *static forensic*. *Imaging* untuk

mendapatkan salinan identik data atau salinan lengkap dari flashdisk secara bit – per – bit. *Imaging* memungkinkan analisis dilakukan dari salinan *file* tersebut agar tidak merusak integritas flashdisk serta menjaga barang bukti dari kerusakan.

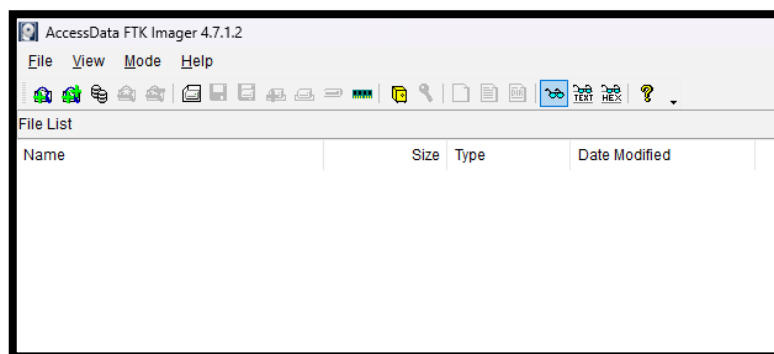
8. Melakukan *recovery* dan analisis

Penjelasan: *file working copy* akan digunakan pada masing-masing *tools file carving*. *Tools* yang digunakan yaitu Autopsy, Magnet Axiom dan Photorec. Hasil *recovery* digunakan untuk melakukan analisis data.

#### 4.4 Akuisisi Menggunakan Metode *Static Forensic*

Akuisisi data langkah awal yang sangat penting dalam proses investigasi digital forensik untuk memastikan integritas dan keaslian barang bukti. Akuisisi data menggunakan metode *static forensic* yang diterapkan pada media penyimpanan flashdisk yang telah dilakukan penghapusan *file* menggunakan perintah Sdelete dan menggunakan Shift+Delete. Metode ini dipilih karena flashdisk dalam kondisi tidak aktif selama proses akuisisi, sehingga risiko data yang termodifikasi pada barang bukti dapat dihindari.

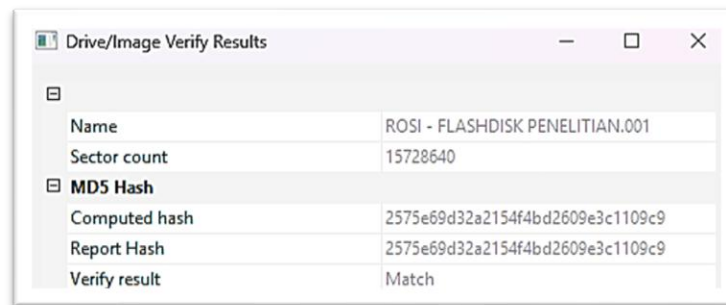
Proses akuisisi dimulai dengan pembuatan *image bit-by-bit* dari flashdisk menggunakan perangkat lunak forensik, yaitu FTK Imager, terlihat pada gambar 4.6. Tahapan ini bertujuan untuk membuat salinan digital dari seluruh isi flashdisk, termasuk data yang tidak teralokasi. Salinan digital tersebut kemudian digunakan sebagai dasar untuk proses analisis lebih lanjut, sementara flashdisk asli disimpan dalam kondisi aman untuk menjaga keutuhan barang bukti.



Gambar 4.6 Tampilan utama FTK Imager.

Setelah proses akuisisi, FTK Imager memberikan informasi berupa nilai *hash* (MD5) flashdisk, seperti pada gambar 4.7. Nilai *hash* yang identik menunjukkan bahwa salinan digital adalah representasi yang *valid* dari media penyimpanan asli. Proses ini dilakukan

sesuai dengan standar *Digital Forensic Investigation Framework* untuk memastikan langkah-langkah yang diambil dapat diterima dalam konteks hukum.

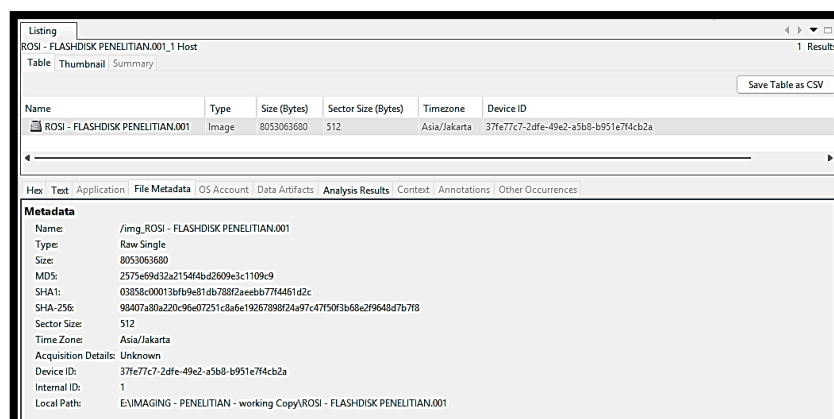


Gambar 4.7 Nilai *hash* hasil *imaging* flashdisk.

Setelah proses akuisisi selesai, hasil *image* flashdisk kemudian digunakan dalam tahap *recovery* data menggunakan *tools file carving* yang telah ditentukan dalam penelitian ini.

#### 4.5 Recovery Menggunakan Teknik *File Carving*

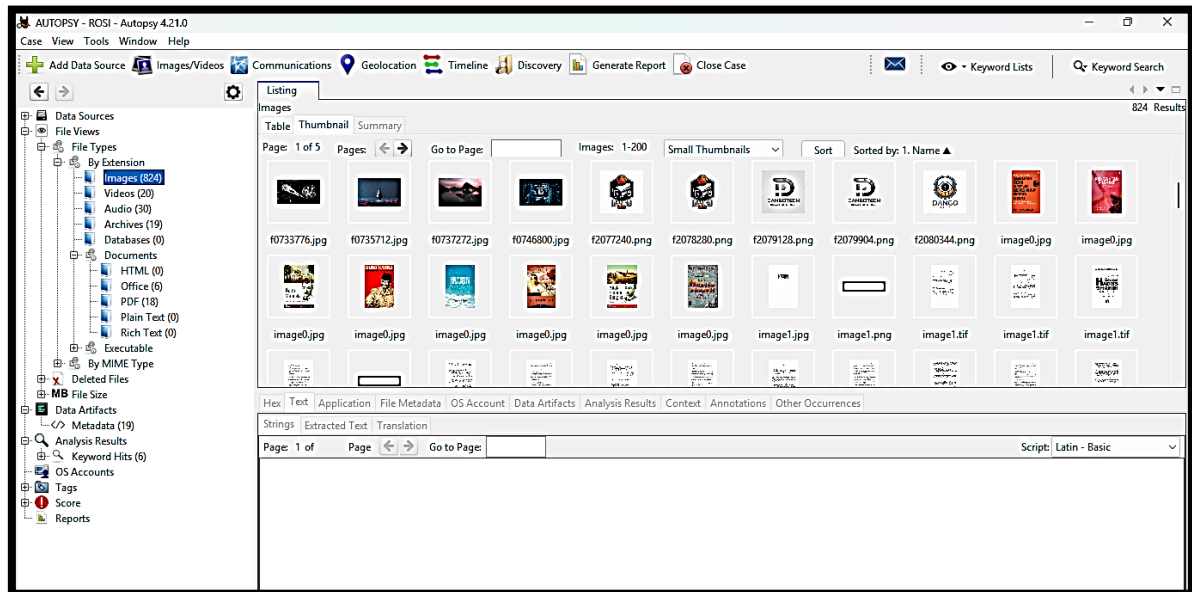
*Recovery* data dilakukan menggunakan teknik *file carving* untuk memulihkan *file* yang dihapus menggunakan perintah *Sdelete*. Proses ini memanfaatkan *tools file carving* Autopsy, Magnet Axion, dan PhotoRec untuk melakukan *recovery file* dokumen, gambar, audio, video, dan arsip. Hasil *recovery* dianalisis berdasarkan jumlah *file* yang berhasil ditemukan dan kesesuaian nilai *hash* dengan *file* asli untuk menilai setiap *tools*.



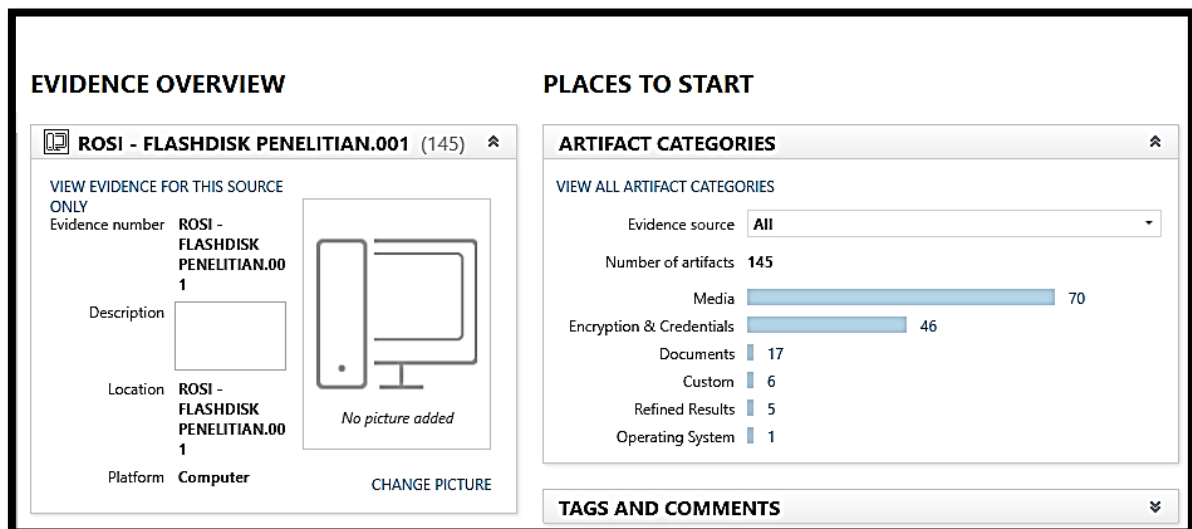
Gambar 4.8 *Recovery completed* menggunakan Autopsy.

Pada gambar 4.8, terlihat hasil menggunakan *tool* Autopsy berhasil melakukan *recovery file* dengan beberapa jenis data. Terdapat *images* dengan jumlah 824 artefak, *videos*

20 artefak, audio 30 artefak, archives 19 artefak, PDF 18 artefak, office 6 artefak. Hasil dapat dilihat pada gambar 4.9.

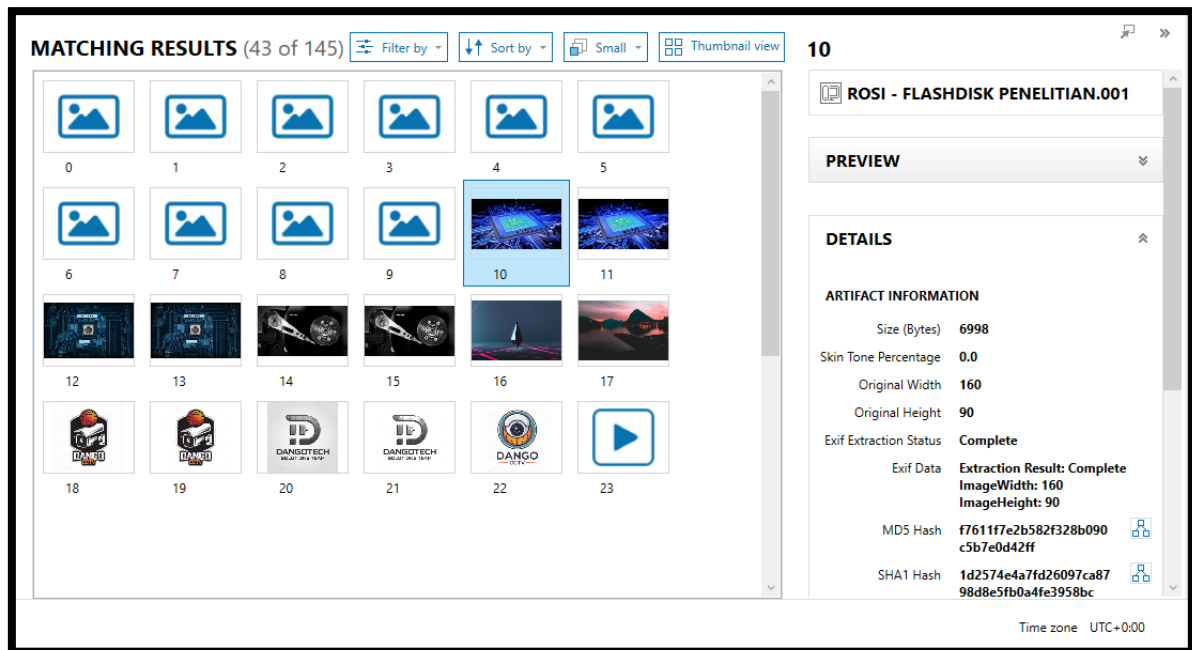


Gambar 4.9 Artefak yang berhasil *discovery* menggunakan Autopsy.

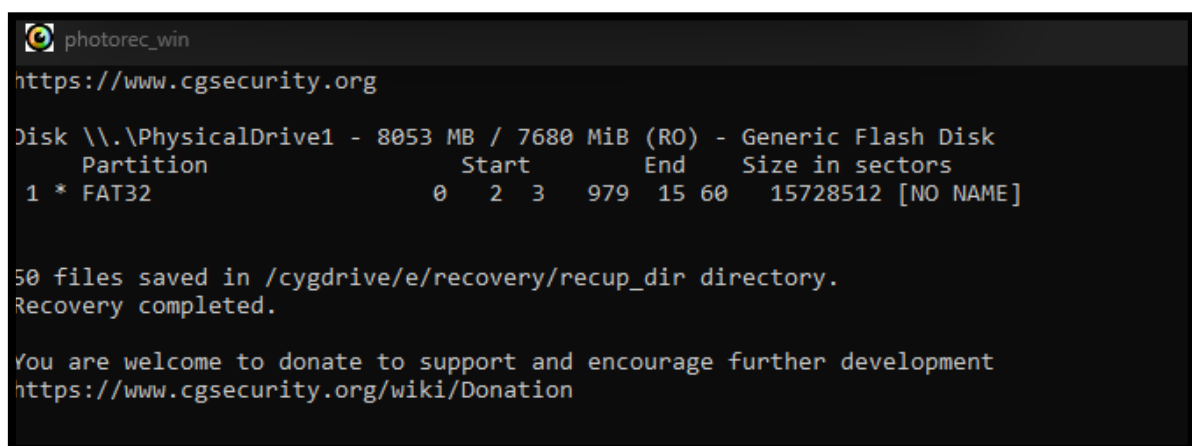


Gambar 4.10 *Recovery completed* menggunakan Magnet Axiom.

Hasil *recovery* pada gambar 4.10 dan 4.11 yang didapat dari *tool* Magnet Axiom yaitu dengan jumlah total 145 artefak. Artefak ini terdiri dari media sebanyak 70, *encryption & credentials* sebanyak 46, *documents* sebanyak 17, *costum* sebanyak 6, *refined result* sebanyak 5 dan *operating system* sebanyak 1.

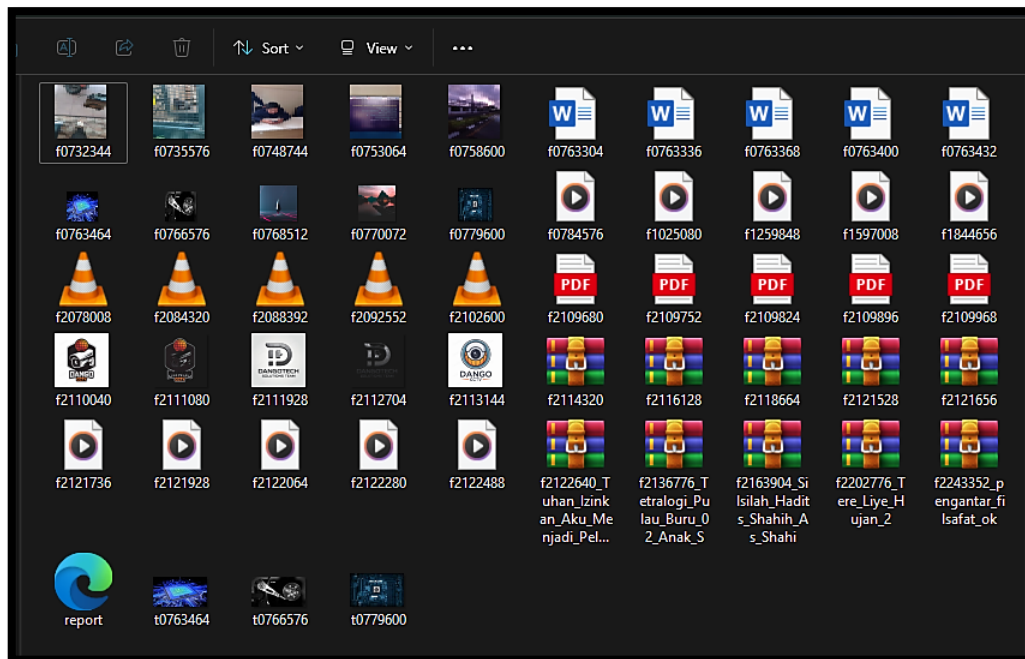


Gambar 4.11 Artefak yang berhasil direcovery menggunakan Magnet Axiom.



Gambar 4.12 *Recovery completed* menggunakan PhotoRec.

Lalu, gambar 4.12 menginformasikan bahwa *recovery* berhasil dengan hasil dari *recovery* terakhir menggunakan *tool* PhotoRec mendapat total 54 artefak sebagaimana pada gambar 4.13, dengan masing-masing ekstensi *file* yang telah dihapus.



Gambar 4.13 Artefak yang berhasil *direcovery* menggunakan PhotoRec.

Keseluruhan hasil *recovery* ini, pada sub-bab selanjutnya oleh penulis dimasukkan kedalam tabel hasil *output recovery* dan dilakukan dianalisis berdasarkan *file-file* yang dihapus.

## 4.6 Hasil Output Recovery Flashdisk

### 4.6.1 Output File Yang Dihapus Menggunakan Sdelete

Tabel 4.2 File Temuan Dan Keidentikan Nilai Hash Autopsy

| <i>Tools</i> | <i>Nama File</i> | <i>Format File</i> | Jumlah artefak ditemukan        | Keidentikan nilai hash |
|--------------|------------------|--------------------|---------------------------------|------------------------|
| Autopsy      | Gambar           | Jpg                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              |                  | Png                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              | Dokumen          | Docx               | <i>File</i> tidak ditemukan     | Tidak ditemukan        |
|              |                  | Pdf                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              | Audio            | Mp3                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              |                  | Wav                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              | Video            | Mp4                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              |                  | Avi                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              | Arsip            | Rar                | <i>File</i> tidak dapat diakses | Tidak identik          |
|              |                  | Zip                | <i>File</i> tidak dapat diakses | Tidak identik          |

Tabel 4.3 *File* Temuan Dan Keidentikan Nilai *Hash* Magnet Axiom

| <i>Tools</i> | <i>Nama File</i> | <i>Format File</i> | <b>Jumlah artefak ditemukan</b> | <b>Keidentikan nilai hash</b> |
|--------------|------------------|--------------------|---------------------------------|-------------------------------|
| Magnet Axiom | Gambar           | Jpg                | <i>File</i> tidak dapat diakses | Tidak identik                 |
|              |                  | Png                | <i>File</i> tidak dapat diakses | Tidak identik                 |
|              | Dokumen          | Docx               | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              |                  | Pdf                | <i>File</i> tidak dapat diakses | Tidak identik                 |
|              | Audio            | Mp3                | <i>File</i> tidak dapat diakses | Tidak identik                 |
|              |                  | Wav                | <i>File</i> tidak dapat diakses | Tidak identik                 |
|              | Video            | Mp4                | <i>File</i> tidak dapat diakses | Tidak identik                 |
|              |                  | Avi                | <i>File</i> tidak dapat diakses | Tidak identik                 |
|              | Arsip            | Rar                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              |                  | Zip                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |

Tabel 4.4 *File* Temuan Dan Keidentikan Nilai *Hash* PhotoRec

| <i>Tools</i> | <i>Nama File</i> | <i>Format File</i> | <b>Jumlah artefak ditemukan</b> | <b>Keidentikan nilai hash</b> |
|--------------|------------------|--------------------|---------------------------------|-------------------------------|
| PhotoRec     | Gambar           | Jpg                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              |                  | png                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              | Dokumen          | Docx               | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              |                  | Pdf                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              | Audio            | Mp3                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              |                  | Wav                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              | Video            | Mp4                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              |                  | Avi                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              | Arsip            | Rar                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |
|              |                  | Zip                | <i>File</i> tidak ditemukan     | Tidak ditemukan               |

#### 4.6.2 *Output File* Yang Dihapus Menggunakan Kombinasi Tombol Shift+Delete

Tabel 4.5 *File* Temuan Dan Keidentikan Nilai *Hash* Autopsy

| <i>Tools</i> | <i>Nama File</i> | <i>Format File</i> | <b>Jumlah artefak ditemukan</b> | <b>Keidentikan nilai hash</b> |
|--------------|------------------|--------------------|---------------------------------|-------------------------------|
| 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                |

Tabel 4.5 *File* Temuan Dan Keidentikan Nilai *Hash* Autopsy (Lanjutan)

| <i>Tools</i> | <i>Nama File</i> | <i>Format File</i> | <b>Jumlah artefak ditemukan</b> | <b>Keidentikan nilai hash</b> |
|--------------|------------------|--------------------|---------------------------------|-------------------------------|
|              | Video            | Wav                | 5 artefak                       | 5 file identik                |
|              |                  | Mp4                | File tidak ditemukan            | Tidak ditemukan               |
|              | Arsip            | Avi                | 5 artefak                       | 5 file identik                |
|              |                  | Rar                | 5 artefak                       | 1 file identik                |
|              |                  | Zip                | 4 artefak                       | 4 file identik                |

Tabel 4.6 *File* Temuan Dan Keidentikan Nilai *Hash* Magnet Axiom

| <i>Tools</i> | <i>Nama File</i> | <i>Format File</i> | <b>Jumlah artefak ditemukan</b> | <b>Keidentikan nilai hash</b> |
|--------------|------------------|--------------------|---------------------------------|-------------------------------|
| 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               |

Tabel 4.7 *File* Temuan Dan Keidentikan Nilai *Hash* PhotoRec

| <i>Tools</i> | <i>Nama File</i> | <i>Format File</i> | <b>Jumlah artefak ditemukan</b> | <b>Keidentikan nilai hash</b> |
|--------------|------------------|--------------------|---------------------------------|-------------------------------|
| 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                |

#### 4.7 Analisis Perbandingan Hasil *Recovery*

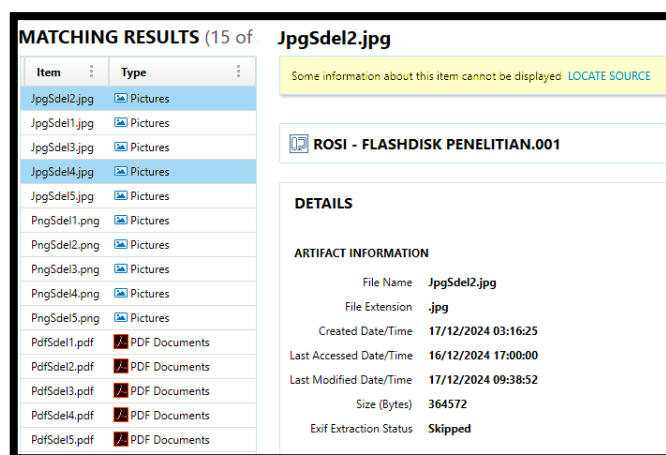
Setelah dilakukan *recovery file*, peneliti melakukan proses ke tahap selanjutnya yaitu melakukan analisis terhadap *file* yang telah berhasil dilakukan *recovery*. Peneliti membuat daftar temuan kedalam bentuk tabel artefak yang ditemukan dan kesesuaian nilai *hash*. Hasil analisis pemulihan data menggunakan tiga *tools file carving*, yaitu Autopsy, Magnet Axiom, dan PhotoRec, ditemukan adanya beberapa *file* yang tidak berhasil dipulihkan, baik dari metode penghapusan Shift+Delete maupun Sdelete.

Pada pemulihan menggunakan Autopsy, hasil *recovery* menunjukkan bahwa *file* yang dihapus menggunakan Shift+Delete yang tidak dapat dipulihkan di antaranya MP4, yang mengalami kerusakan dan memiliki *hash value* yang sama untuk seluruh *file* yang dapat dilihat pada gambar 4.14, serta *file* ZIP (SDZip\_1), yang tidak ditemukan sama sekali. Sementara itu, untuk *file* yang dihapus menggunakan Sdelete yakni *file* DOCX tidak ditemukan sama sekali.

| Name           | ▼ S | Size    | MD5 Hash                         | MIME Type                |
|----------------|-----|---------|----------------------------------|--------------------------|
| ✖ Mp4Sdel1.mp4 | ▼   | 1134548 | 9d95cb105cfddd27ed157251f7989b20 | application/octet-stream |
| ✖ Mp4Sdel2.mp4 | ▼   | 930960  | 90959f6584da6bbe52916ce70ea7e63  | 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 4.14 *File recovery* menggunakan Autopsy yang tidak dapat diakses.

Sementara itu, pemulihan menggunakan Magnet Axiom menunjukkan hasil yang berbeda. Hasil *recovery* menunjukkan bahwa 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 4.15.



Gambar 4.15 *File recovery* menggunakan Axiom yang tidak dapat diakses.

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.

PhotoRec, berbeda dengan kedua *tools* sebelumnya, hasil *recovery* menunjukkan bahwa hapus menggunakan Shift+Delete, *file* dengan format MP4 tidak dapat diakses dan hasil dari hapus menggunakan Sdelete tidak ditemukan artefak sama sekali, seperti terlihat pada gambar 4.16.

| MP4 Video File (VLC) |                  |                      |      |  |
|----------------------|------------------|----------------------|------|--|
| f2078008             | 17/12/2024 18:39 | MP4 Video File (V... | 1 KB |  |
| f2084320             | 17/12/2024 18:39 | MP4 Video File (V... | 1 KB |  |
| f2088392             | 17/12/2024 18:39 | MP4 Video File (V... | 1 KB |  |
| f2092552             | 17/12/2024 18:39 | MP4 Video File (V... | 1 KB |  |
| f2102600             | 17/12/2024 18:39 | MP4 Video File (V... | 1 KB |  |

Gambar 4.16 *File recovery* menggunakan Photorec yang tidak dapat diakses.

Adapun temuan dapat dilihat pada tabel berikut:

Tabel 4.8 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 |

Tabel 4.8 Artefak Yang Dihapus Menggunakan Perintah Sdelete (Lanjutan)

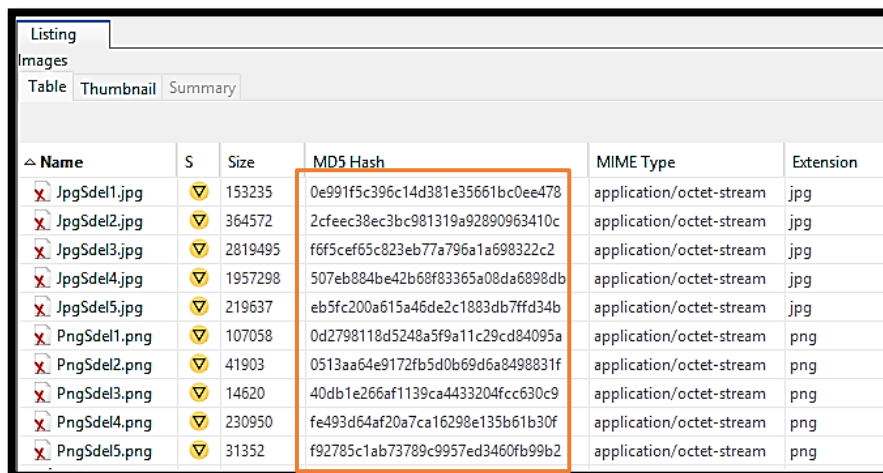
| <i>Variable</i>                      |     | <i>Tools</i>                    |                                 |                             |
|--------------------------------------|-----|---------------------------------|---------------------------------|-----------------------------|
|                                      | Pdf | <i>File</i> tidak dapat diakses | <i>File</i> tidak dapat diakses | <i>File</i> tidak ditemukan |
| Audio                                | Mp3 | <i>File</i> tidak dapat diakses | <i>File</i> tidak dapat diakses | <i>File</i> tidak ditemukan |
|                                      | Wav | <i>File</i> tidak dapat diakses | <i>File</i> tidak dapat diakses | <i>File</i> tidak ditemukan |
| Video                                | Mp4 | <i>File</i> tidak dapat diakses | <i>File</i> tidak dapat diakses | <i>File</i> tidak ditemukan |
|                                      | Avi | <i>File</i> tidak dapat diakses | <i>File</i> tidak dapat diakses | <i>File</i> tidak ditemukan |
| Arsip                                | Rar | <i>File</i> tidak dapat diakses | <i>File</i> tidak ditemukan     | <i>File</i> tidak ditemukan |
|                                      | Zip | <i>File</i> tidak dapat diakses | <i>File</i> tidak ditemukan     | <i>File</i> tidak ditemukan |
| <b>Total File yang dapat diakses</b> |     | <b>0 file</b>                   | <b>0 file</b>                   | <b>0 file</b>               |

Total *file* yang tidak dapat diakses pada tabel 4.8, menginformasikan bahwa tidak ada satupun *file* yang ditemukan dalam keadaan dapat diakses yang merupakan hasil dari *file-file* yang telah dihapus oleh perintah Sdelete. Sdelete sebelum menghapus melakukan pengacakan nama lalu bekerja dengan cara menimpa data. Data yang diacak, dihapus dan telah ditimpa ini membuat Autopsy tidak mengenali struktur sistem *file*, Magnet Axiom tidak menemukan metadata maupun *tools* dan juga pada metode *file carving* berbasis *signature* yakni PhotoRec juga tidak ditemukan. Lalu, untuk kesesuaian nilai *hash* dapat dilihat pada tabel 4.9.

Tabel 4.9 Kesesuaian Nilai *Hash*

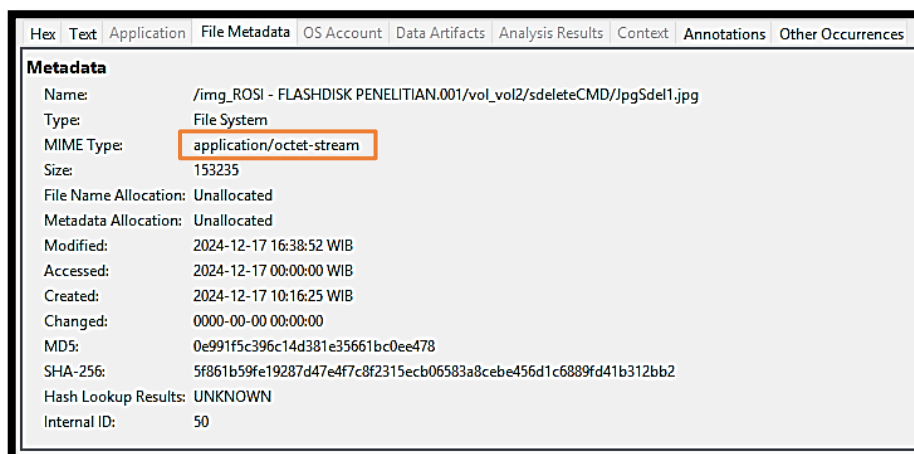
| <i>Variable</i>                |                    | <i>Tools</i>     |                  |                  |
|--------------------------------|--------------------|------------------|------------------|------------------|
| <b>Tipe File</b>               | <b>Format File</b> | <b>Autopsy</b>   | <b>Axiom</b>     | <b>Photorec</b>  |
| 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  |
| <b>Total File yang identik</b> |                    | <b>0 identik</b> | <b>0 identik</b> | <b>0 identik</b> |

Pada tabel 4.8, ditulis sebagian besar *file* yang telah *direcovery* 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 *direcovery* menggunakan *tool* Autopsy dapat dilihat pada gambar 4.17 berikut:



| Name         | S | Size    | MD5 Hash                         | MIME Type                | Extension |
|--------------|---|---------|----------------------------------|--------------------------|-----------|
| JpgSdel1.jpg | ✓ | 153235  | 0e991f5c396c14d381e35661bc0ee478 | application/octet-stream | jpg       |
| JpgSdel2.jpg | ✓ | 364572  | 2cfeec38ec3bc981319a92890963410c | application/octet-stream | jpg       |
| JpgSdel3.jpg | ✓ | 2819495 | f6f5cef65c823eb77a796a1a698322c2 | application/octet-stream | jpg       |
| JpgSdel4.jpg | ✓ | 1957298 | 507eb884be42b68f83365a08da6898db | application/octet-stream | jpg       |
| JpgSdel5.jpg | ✓ | 219637  | eb5fc200a615a46de2c1883db7ffd34b | application/octet-stream | jpg       |
| PngSdel1.png | ✓ | 107058  | 0d2798118d5248a5f9a11c29cd84095a | application/octet-stream | png       |
| PngSdel2.png | ✓ | 41903   | 0513aa64e9172fb5d0b69d6a8498831f | application/octet-stream | png       |
| PngSdel3.png | ✓ | 14620   | 40db1e266af1139ca4433204fcc630c9 | application/octet-stream | png       |
| PngSdel4.png | ✓ | 230950  | fe493d64af20a7ca16298e135b61b30f | application/octet-stream | png       |
| PngSdel5.png | ✓ | 31352   | f92785c1ab73789c9957ed3460fb99b2 | application/octet-stream | png       |

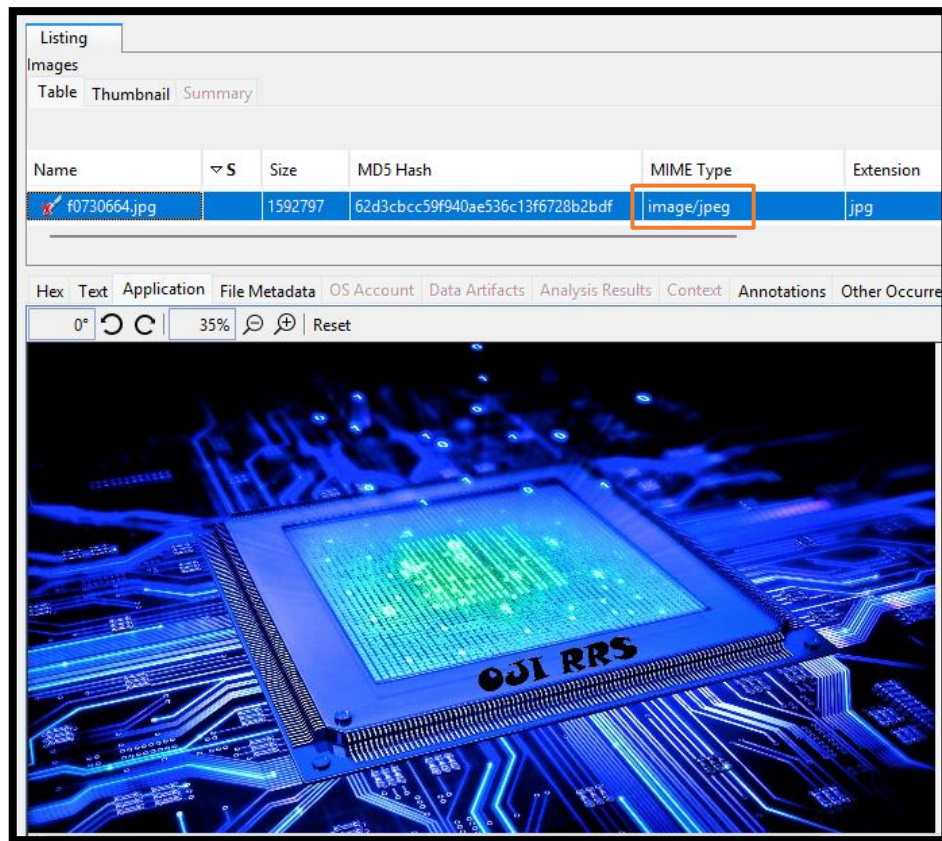
Gambar 4.17 Artefak yang ditemukan pada Autopsy.



| Metadata              |                                                                       |
|-----------------------|-----------------------------------------------------------------------|
| Name:                 | /img_ROSI - FLASHDISK PENELITIAN.001/vol_vol2/sdeleteCMD/JpgSdel1.jpg |
| Type:                 | File System                                                           |
| MIME Type:            | application/octet-stream                                              |
| Size:                 | 153235                                                                |
| File Name Allocation: | Unallocated                                                           |
| Metadata Allocation:  | Unallocated                                                           |
| Modified:             | 2024-12-17 16:38:52 WIB                                               |
| Accessed:             | 2024-12-17 00:00:00 WIB                                               |
| Created:              | 2024-12-17 10:16:25 WIB                                               |
| Changed:              | 0000-00-00 00:00:00                                                   |
| MD5:                  | 0e991f5c396c14d381e35661bc0ee478                                      |
| SHA-256:              | 5f861b59fe19287d47e4f7c8f2315ecb06583a8cebe456d1c6889fd41b312bb2      |
| Hash Lookup Results:  | UNKNOWN                                                               |
| Internal ID:          | 50                                                                    |

Gambar 4.18 *file* metadata *tool* Autopsy.

Pada gambar 4.17 dan gambar 4.18, keseluruhan *file* yang terlihat pada gambar memiliki MIME *type* yaitu *application/octet-stream*. Bukan hanya pada gambar, akan tetapi pada keseluruhan *file* yang dihapus menggunakan perintah Sdelete juga memiliki MIME *type* yang sama. Berbeda pada *file* gambar yang dapat diakses memiliki MIME *type* yaitu *image/jpg*. Sebagai perbandingan, dapat dilihat pada gambar 4.19 berikut:



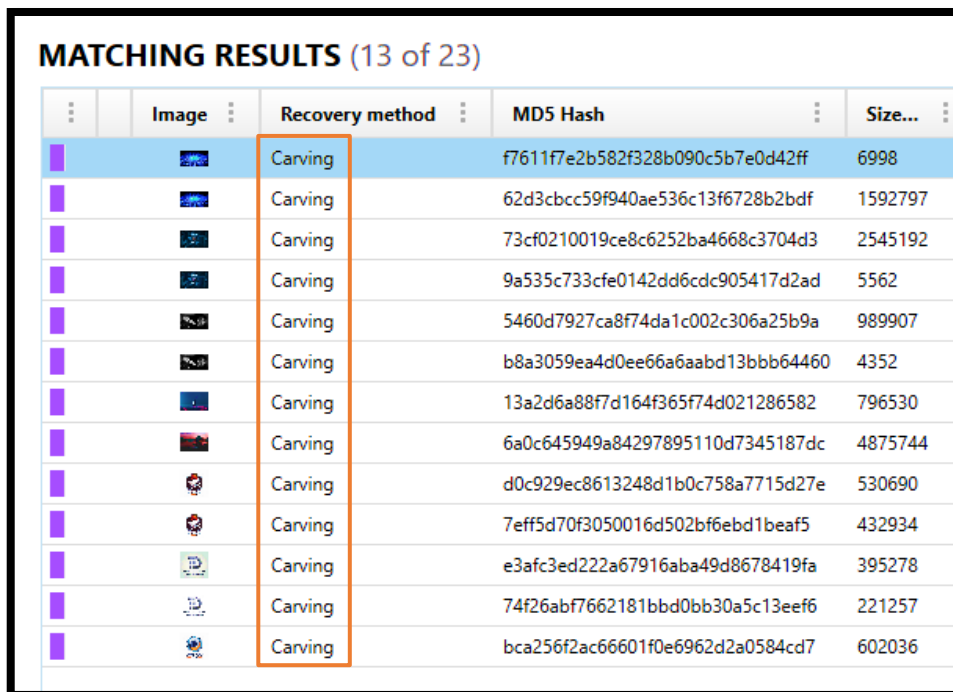
Gambar 4.19 File yang dapat diakses pada tool Autopsy.

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

| MATCHING RESULTS (10 of 23) |              |       |                 |          |              | Column view |
|-----------------------------|--------------|-------|-----------------|----------|--------------|-------------|
|                             | File N...    | Image | Recovery method | MD5 Hash | Size (Bytes) |             |
|                             | JpgSdel2.jpg |       | Parsing         |          | 364572       |             |
|                             | JpgSdel1.jpg |       | Parsing         |          | 153235       |             |
|                             | JpgSdel3.jpg |       | Parsing         |          | 2819495      |             |
|                             | JpgSdel4.jpg |       | Parsing         |          | 1957298      |             |
|                             | JpgSdel5.jpg |       | Parsing         |          | 219637       |             |
|                             | PngSdel1.png |       | Parsing         |          | 107058       |             |
|                             | PngSdel2.png |       | Parsing         |          | 41903        |             |
|                             | PngSdel3.png |       | Parsing         |          | 14620        |             |
|                             | PngSdel4.png |       | Parsing         |          | 230950       |             |
|                             | PngSdel5.png |       | Parsing         |          | 31352        |             |

Gambar 4.20 Artefak yang ditemukan pada Axiom dari hapus Sdelete.

Dari gambar 4.20 *file* yang ditemukan merupakan *file* yang dihapus menggunakan perintah Sdelete dan menginformasikan *Recovery Method* yang digunakan yaitu *parsing*. Berbeda dengan *recovery method* pada *file* yang dihapus menggunakan Shift+Delete yaitu *Carving* dapat dilihat pada gambar 4.21.



|  | Image | Recovery method | MD5 Hash                         | Size... |
|--|-------|-----------------|----------------------------------|---------|
|  |       | Carving         | f7611f7e2b582f328b090c5b7e0d42ff | 6998    |
|  |       | Carving         | 62d3cbcc59f940ae536c13f6728b2bdf | 1592797 |
|  |       | Carving         | 73cf0210019ce8c6252ba4668c3704d3 | 2545192 |
|  |       | Carving         | 9a535c733cfe0142dd6cdc905417d2ad | 5562    |
|  |       | Carving         | 5460d7927ca8f74da1c002c306a25b9a | 989907  |
|  |       | Carving         | b8a3059ea4d0ee66a6aabd13bbb64460 | 4352    |
|  |       | Carving         | 13a2d6a88f7d164f365f74d021286582 | 796530  |
|  |       | Carving         | 6a0c645949a84297895110d7345187dc | 4875744 |
|  |       | Carving         | d0c929ec8613248d1b0c758a7715d27e | 530690  |
|  |       | Carving         | 7eff5d70f3050016d502bf6ebd1beaf5 | 432934  |
|  |       | Carving         | e3afc3ed222a67916aba49d8678419fa | 395278  |
|  |       | Carving         | 74f26abf7662181bbd0bb30a5c13eef6 | 221257  |
|  |       | Carving         | bca256f2ac66601f0e6962d2a0584cd7 | 602036  |

Gambar 4.21 *File* yang dapat diakses pada *tool* Axiom dari hapus Shift+Delete.

Jika dilihat dari hasil *recovery*, perbandingan dari masing-masing *recovery file* ini terletak pada teknik *tools file carving* dalam melakukan *recovery* yang dihadapkan pada metode hapus yang berbeda pula. Autopsy, Magnet Axiom dan PhotoRec tidak dapat memulihkan file dikarenakan perintah Sdelete menghapus dan melakukan penimpanan data dengan karakter acak data, sehingga header dan footer, metadata tidak dikenali oleh ketiga *tools file carving* ini dengan instrumen teknik *recovery*nya yang tidak menemukan artefak utuh. Berbeda dengan metode hapus Shift+Delete, yang menurut beberapa penelitian terdahulu yang hanya menghilangkan *file*, namun metadata dan isi *file* masih tersimpan didalam *disk*.

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, sehingga diharapkan menghasilkan persentase keberhasilan *tool* dalam melakukan *recovery* pada data yang dapat diakses.

Tabel 4.10 Keseluruhan Artefak Yang Dihapus Menggunakan Shift+Delete

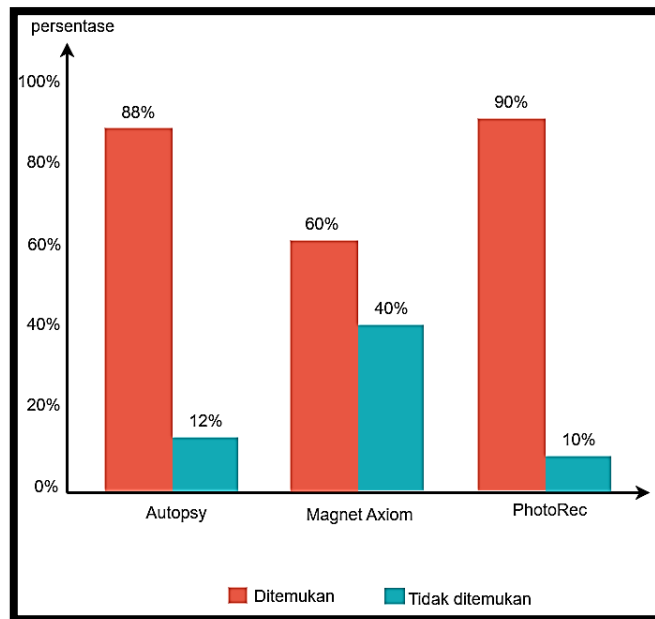
| <i>Variable</i>                      |                    | <i>Tools</i>                |                             |                                 |
|--------------------------------------|--------------------|-----------------------------|-----------------------------|---------------------------------|
| <b>Tipe File</b>                     | <b>Format File</b> | <b>Autopsy</b>              | <b>Magnet Axiom</b>         | <b>Photorec</b>                 |
| 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                   | <i>file tidak ditemukan</i> | 5 artefak                       |
|                                      | Wav                | 5 artefak                   | <i>file tidak ditemukan</i> | 5 artefak                       |
| Video                                | Mp4                | <i>file tidak ditemukan</i> | 5 artefak                   | <i>File tidak dapat diakses</i> |
|                                      | Avi                | 5 artefak                   | 5 artefak                   | 5 artefak                       |
| Arsip                                | Rar                | 5 artefak                   | <i>file tidak ditemukan</i> | 5 artefak                       |
|                                      | Zip                | 4 artefak                   | <i>file tidak ditemukan</i> | 5 artefak                       |
| <b>Total file yang dapat diakses</b> |                    | <b>44 file</b>              | <b>30 file</b>              | <b>45 file</b>                  |

Berdasarkan hasil analisis yang tercantum dalam Tabel 4.10, dilakukan evaluasi kinerja seluruh *tools file carving* dalam *merecovery file* dari Flashdisk. Rumus 3.1 digunakan sebagai pengukuran atas kemampuan masing-masing *tools*. Berikut adalah perhitungan persentase untuk mengukur kemampuan *recovery* masing-masing *tools file carving*.

$$\text{Nilai persentase tool Autopsy} \quad Par = \frac{44}{50} \times 100\% = 88\%$$

$$\text{Nilai persentase tool Axiom} \quad Par = \frac{30}{50} \times 100\% = 60\%$$

$$\text{Nilai persentase tool PhotoRec} \quad Par = \frac{45}{50} \times 100\% = 90\%$$



Gambar 4.22 Grafik persentase *file* yang ditemukan.

Pada gambar 4.22 terlihat grafik persentase *file* yang ditemukan, lalu setelah dilakukan analisis keseluruhan artefak yang ditemukan dan dilakukan perhitungan menggunakan rumus 3.1 untuk artefak yang telah berhasil *direcovery*, selanjutnya dilakukan hal yang serupa menggunakan rumus yang sama. Untuk hasil analisis keseluruhan nilai *hash*, dapat dilihat pada tabel 4.11.

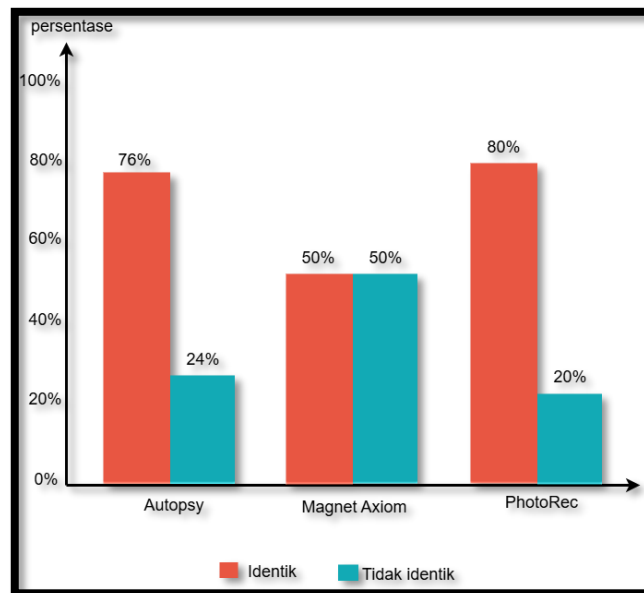
Tabel 4.11 Hasil Analisis Keseluruhan Nilai *Hash*

| <i>Variable</i>                       |                    | <i>Tools</i>          |                       |                       |
|---------------------------------------|--------------------|-----------------------|-----------------------|-----------------------|
| <b>Tipe File</b>                      | <b>Format File</b> | <b>Autopsy</b>        | <b>Axiom</b>          | <b>Photorec</b>       |
| Gambar                                | Jpg                | 5 <i>file</i> identik | 5 <i>file</i> identik | 5 <i>file</i> identik |
|                                       | png                | 5 <i>file</i> identik | 5 <i>file</i> identik | 5 <i>file</i> identik |
| Dokumen                               | Docx               | 5 <i>file</i> identik | 5 <i>file</i> identik | 5 <i>file</i> identik |
|                                       | Pdf                | 5 <i>file</i> identik | 0 <i>file</i> identik | 5 <i>file</i> identik |
| Audio                                 | Mp3                | 3 <i>file</i> identik | Tidak ditemukan       | 4 <i>file</i> identik |
|                                       | Wav                | 5 <i>file</i> identik | Tidak ditemukan       | 5 <i>file</i> identik |
| Video                                 | Mp4                | Tidak ditemukan       | 5 <i>file</i> identik | Tidak ditemukan       |
|                                       | Avi                | 5 <i>file</i> identik | 5 <i>file</i> identik | 5 <i>file</i> identik |
| Arsip                                 | Rar                | 1 <i>file</i> identik | Tidak ditemukan       | 1 <i>file</i> identik |
|                                       | Zip                | 4 <i>file</i> identik | Tidak ditemukan       | 5 <i>file</i> identik |
| <b>Total <i>file</i> yang identik</b> |                    | <b>38 <i>file</i></b> | <b>25 <i>file</i></b> | <b>40 <i>file</i></b> |

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

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

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



Gambar 4.23 Grafik persentase keidentikan nilai *hash*.

Dari grafik persentase *file* temuan pada gambar 4.22 dan grafik persentase keidentikan nilai *hash* pada gambar 4.23, ketiga *tools* sama-sama memiliki kesuksesan dalam melakukan *recovery* pada file dengan ekstensi Jpg, Png, Docx, Pdf dan Avi. Autopsy dan PhotoRec lemah daripada Magnet Axiom dalam *recovery file* dengan ekstensi Mp4 sedangkan unggul dalam *recovery file* berekstensi Mp3, Wav, Rar dan Zip dan Magnet Axiom cenderung lebih lemah.

#### 4.8 Hasil

Dari proses sampai dengan analisis yang telah dilakukan, tidak ditemukan satupun artefak yang dapat diakses ketika *file* percobaan dihapus menggunakan perintah Sdelete. Autopsy tidak dapat menemukan artefak dengan ekstensi *file* .docx, sedangkan artefak lainnya ditemukan namun tidak dapat diakses. *Recovery Magnet Axiom* tidak dapat menemukan artefak dengan ekstensi *file* .docx, .rar, dan .zip sedangkan artefak lainnya ditemukan namun tidak dapat diakses. Lain halnya dengan PhotoRec yang tidak menemukan satupun artefak maupun *file* dalam kondisi tidak dapat diakses.

Ketiga *tools* tidak mampu melakukan *recovery file* ketika dihadapkan dengan metode hapus yang menggunakan teknik penipaan data. Sehingga, *file* yang telah dihapus tidak dapat direkonstruksi oleh *tools file carving*. Hasil menunjukkan perbedaan ketika hapus yang digunakan adalah Shift+Delete yang tidak menggunakan teknik penipaan data. Shift+Delete hanya menghapus entri *file* dari tabel direktori pada sistem *file* tanpa melakukan penipaan pada sektor data (dijelaskan pada sub bab 2.2.6), membuat *tools file carving* dapat melakukan *recovery file* dengan hasil seperti terlihat pada tabel berikut:

Tabel 4.12 Hasil Akhir

| Nama <i>tools</i> | Nilai Persentase         |                        |
|-------------------|--------------------------|------------------------|
|                   | Pengembalian <i>File</i> | Kesesuaian <i>Hash</i> |
| Autopsy           | 88%                      | 76%                    |
| Magnet Axiom      | 60%                      | 50%                    |
| PhotoRec          | 90%                      | 80%                    |

Perhitungan untuk artefak yang dapat diakses menggunakan rumus persentase 3.1 dengan hasil perhitungan yang terlihat pada tabel 4.12. Hasil menunjukkan PhotoRec memiliki performa lebih baik dari *tools* lainnya dengan kemampuan memulihkan sebanyak 45 *file* dengan nilai *hash* yang identik sebanyak 40 *file*, dan hanya *file* dengan ekstensi .mp4 yang tidak ditemukan. Perbedaan cukup signifikan karena cara kerja PhotoRec yang menggunakan *signature based carving* dan mengabaikan sistem *file* (dijelaskan pada subbab 2.2.9), dengan menentukan ukuran blok, membaca blok demi blok untuk menemukan *file* berdasarkan *signature* yang telah dikenali seperti *header .jpeg* dan mengikuti validasi struktur *file* untuk keakuratan hasil.

Autopsy diperingkat kedua dengan 44 *file* yang dapat dipulihkan dan 38 *file* nilai *hash* yang identik dengan keseluruhan *file* berekstensi .mp4 tidak ditemukan dan ekstensi .zip satu *file* tidak ditemukan. Cara kerja Autopsy berbeda dari Photorec. Autopsy bekerja

dengan mengenali struktur sistem *file* secara menyeluruh (dijelaskan pada subbab 2.2.7) termasuk metadata seperti exif dan pemulihan bergantung pada metadata. Pada penelitian ini *file* temuan yang awalnya dihapus menggunakan Shift+Delete tidak ikut menghilangkan *file* metadata. Karena Shift+Delete hanya menghapus entri *file* dari sistem operasi dan tidak menghilangkan/menimpa konten *file* fisik, sehingga Autopsy dapat memulihkan artefak-artefak yang masih memiliki metadata tersebut.

Lalu, yang terakhir yaitu Magnet Axiom dengan 30 *file* dapat dipulihkan dan 25 *file* nilai *hash* yang identik. *File* dengan ekstensi .mp3, .wav, .rar, .zip tidak ditemukan. Mekanisme pemulihan data Axiom dimulai dari *parsing* metadata, kemudian dilanjutkan dengan *post-process carving*. Akibatnya, ketika metadata telah terhapus atau tidak tersedia, jumlah *file* yang dapat dipulihkan berkurang signifikan. Selain itu, cakupan format *carving* yang lebih terbatas dibandingkan PhotoRec juga turut memengaruhi rendahnya hasil pemulihan.

Perbedaan persentase yang cukup signifikan ini menunjukkan bahwa variasi algoritma dan pendekatan pemulihan antar *tools* menjadi faktor utama, di mana PhotoRec lebih unggul dalam kasus penghapusan konvensional, sementara Autopsy terbatas pada metadata, dan Magnet Axiom kurang optimal untuk *file carving* pada flashdisk

## BAB 5

### Kesimpulan dan Saran

#### 5.1 Kesimpulan

Berdasarkan penelitian yang telah diselesaikan, maka ditarik kesimpulan:

1. Dari data yang telah dihapus menggunakan perintah Sdelete, *tools file carving* (Autopsy, Magnet Axiom dan Photorec) tidak dapat melakukan *recovery file* yang dapat diakses menunjukkan bahwa Sdelete mampu menimpa data secara menyeluruh sesuai dengan standar Dod 5220.22-M.
2. Penggunaan kombinasi tombol Shift+Delete untuk menghapus *file* masih bisa dipulihkan dan diakses dengan 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%. Lalu pada Photorec memiliki tingkat keberhasilan pengembalian *file* sebesar 90% dan keidentikan nilai *hash* sebesar 80%.
3. 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*.
4. Secara keseluruhan penelitian ini melakukan perbandingan hasil *recovery* pada *file* yang dihapus menggunakan perintah Sdelete dan hapus Shift+Delete, dengan tingkat keberhasilan *recovery* yang berbeda-beda untuk tiap *tools*. Hasil dari perhitungan menunjukkan bahwa PhotoRec memiliki kinerja terbaik dan penelitian ini memberikan rekomendasi bahwa PhotoRec adalah *tools* paling efektif untuk *recovery file* yang dihapus menggunakan Shift+Delete, sementara tidak ada *tools* yang mampu merecovery *file* yang dihapus menggunakan perintah Sdelete karena proses penimpaan datanya.
5. Penelitian ini berkontribusi pada bidang digital forensik dengan mempertegas keterbatasan *tools file carving* pada data yang dihapus dengan metode *secure deletion* yakni perintah SDelete dengan membandingkan hasil *recovery* pada teknik penghapusan yang berbeda dan memberikan rekomendasi *tools* paling efektif pada kasus penghapusan konvensional yang menggunakan Shift+Delete.

## 5.2 Saran

Penelitian ini berfokus pada hasil *recovery file tools file carving* serta keefektifan penghapusan perintah *Sdelete* dalam melakukan penghapusan dengan penimpanan data secara permanen. Untuk penelitian selanjutnya dapat dilakukan dengan membandingkan akurasi *tools file carving* pada penyimpanan lainnya seperti SSD dengan fitur trim *enable* yang dilakukan perbandingan penghapusan menggunakan beberapa teknik hapus *file*.

## Daftar Pustaka

- 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>
- Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Jurnal Hukum*, 05. <https://doi.org/10.54209/judge.v5i02.566>
- Aisyah, N., Putra, A. S., Safrizal, S., Valentino, V. H., Zikriah, Z., Prasetyo, B. S., Susanti, D., & Nurhayati, N. (2022). Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi dan Sistem Komputer*, 6(1), 22–27. <https://doi.org/10.55886/infokom.v6i1.452>
- Alzaabi, M., & Al Shibli, A. (2025). A Review of JPEG File Carving: Challenges, Techniques, and Future Directions. *Applied Computing Journal*, 372–385. <https://doi.org/10.52098/acj.20255124>
- Boiko, M., Moskalenko, V., & Shovkopliash, O. (2023). Advanced file carving: Ontology, models and methods. *Radioelectronic and Computer Systems*, 3, 204–216. <https://doi.org/10.32620/reks.2023.3.16>
- CGsecurity. (2024). *PhotoRec*. <https://www.cgsecurity.org/>
- Citra Dewi, N., Sutabri, T., & Putrawansyah, F. (2023). Analisis Penyadapan Pada Telegram Dengan Network Forensic. *JIKO (Jurnal Informatika dan Komputer)*, 7(2), 183. <https://doi.org/10.26798/jiko.v7i2.789>

- 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>
- Fatmah, N., & Indrayani, R. (2022). Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics. *Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD*, 5(2), 185–192.
- Garfinkel, S. L., & McCarrin, M. (2015). Hash-based carving: Searching media for complete files and file fragments with sector hashing and hashdb. *Digital Investigation*, 14, S95–S105. <https://doi.org/10.1016/j.diin.2015.05.001>
- Herman, Riadi, I., & Rafiq, I. A. (2022). Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method. *International Journal of Safety and Security Engineering*, 12(06), 707–713. <https://doi.org/10.18280/ijssse.120606>
- Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy*, 1(4), 580–596. <https://doi.org/10.3390/jcp1040029>
- Iqbal, M., & Soewito, B. (2020). Digital Forensics on Solid State Drive (SSD) with Trim Feature Enabled and Deep Freeze Configuration Using Static Forensic Methods and ACPO Framework. *International Journal of Computer Science and Information Security (IJCSIS)*, 18. <https://doi.org/10.5281/ZENODO.4428140>
- 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>
- Magnet Forensics. (2022). Magnet Forensics. *Digital Evidence Processing: Parsing-Only Processing and Post-Process Carving*. <https://www.magnetforensics.com/>
- 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 University.
- 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>
- Prasetya, W., & Priyana, P. (2021). Pertimbangan Hakim Atas Penghadiran Bukti Digital Forensik dalam Perkara Kejahatan Fraud. *Wajah Hukum*, 5(2), 448. <https://doi.org/10.33087/wjh.v5i2.472>
- 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>

- Riadi, I., Sunardi, S., & Hadi, A. (2020). Analisis Bukti Digital Trim Enable SSD NVMe Menggunakan Metode Static Forensics. *JUITA: Jurnal Informatika*, 8(1), 65. <https://doi.org/10.30595/juita.v8i1.6584>
- Santos, H. D., Martins, T. D. S., Barreto, J. A. D., Nakamura, L. H. V., Ranieri, C. M., Grande, R. E. D., Filho, G. P. R., & Meneguette, R. I. (2024). ChaSAM: An Architecture Based on Perceptual Hashing for Image Detection in Computer Forensics. *IEEE Access*, 12, 104611–104628. <https://doi.org/10.1109/ACCESS.2024.3435027>
- Santoso, B. S., & Sulaksono, P. M. (2022). Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager. *Jurnal Komputer Terapan*, 8(1), 132–142. <https://doi.org/10.35143/jkt.v8i1.5334>
- Septasari, D. (2023). Cyber Security and The Challenge of Society 5.0 Era in Indonesia. *Aisyah Journal of Informatics and Electrical Engineering Universitas Aisyah Pringsewu*, 5(2).
- Sethi, P. C. (2024). FILE CARVING: ANALYZING DATA RETRIEVAL IN DIGITAL FORENSICS. *International Journal Of Creative Research Thoughts (IJRT)*, 12(4).
- 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).
- Sleuth Kit Labs. (2025). *Autopsy Digital Forensics*. <https://www.autopsy.com/>

- Utami, S. D., Carudin, C., & Ridha, A. A. (2021). Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik. *Cyber Security dan Forensik Digital*, 4(1), 24–32. <https://doi.org/10.14421/csecurity.2021.4.1.2416>
- Yudhana, A., Riadi, I., & putra, budi. (2022). Analisis Kinerja Perangkat Lunak Forensic Imaging Pada Sistem Operasi Linux Menggunakan Metode Static Forensic. *Insect (Informatics and Security): Jurnal Teknik Informatika*, 8(1), 38–47. <https://doi.org/10.33506/insect.v8i1.1962>
- Yudhana, A., Riadi, I., & Putra, B. (2022). Digital Forensic on Secure Digital High Capacity using DFRWS Method. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 6(6), 1021–1027. <https://doi.org/10.29207/resti.v6i6.4615>
- 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>

## LAMPIRAN

Hasil wawancara dengan AKBP Bakti Andriyono, Direktur Direktorat Perawatan Tahanan dan Barang Bukti Polda DIY.

1. Apakah hasil ini menurut Bapak relevan dengan praktik investigasi hukum?

Jawaban :

Hasil penelitian ini tetap memiliki relevansi yang signifikan dalam praktik investigasi hukum. Artefak digital yang ditemukan meskipun telah dihapus menggunakan perintah Sdelete memang tidak serta merta dapat langsung dijadikan barang bukti sah di persidangan. Namun, artefak tersebut dapat berperan penting sebagai petunjuk awal dalam proses investigasi. Artinya, temuan tersebut berfungsi sebagai titik masuk bagi penyidik untuk melacak bukti-bukti lain yang lebih kuat dan *valid*. Agar dapat memiliki kekuatan pembuktian di pengadilan, bukti digital yang diajukan harus dapat dipastikan identik dengan yang asli, baik dari sisi konten maupun nilai *hash*. Dengan demikian, meskipun artefak hasil pemulihan tidak langsung sah sebagai alat bukti, kehadirannya tetap krusial sebagai bagian dari proses investigasi.

2. Bagaimana pandangan Bapak terhadap efektivitas *tools* (Autopsy, Magnet Axiom, PhotoRec) jika digunakan dalam praktik investigasi nyata?

Jawaban :

Mengenai efektivitas *tools* forensik yang digunakan dalam penelitian ini, efektivitas yang utama bukan sekadar jumlah *file* yang dapat dipulihkan, melainkan sejauh mana hasil pemulihan tersebut identik dengan *file* aslinya. Identitas *file* dapat dibuktikan melalui kesesuaian nilai *hash*. Dalam praktik investigasi nyata, hasil yang identik inilah yang sangat dibutuhkan karena dapat dijadikan barang bukti sah di pengadilan. Dengan demikian, *tools* seperti Autopsy, Magnet Axiom, dan PhotoRec memiliki potensi untuk digunakan secara efektif, asalkan hasilnya dapat dipertanggungjawabkan secara ilmiah dan menghasilkan temuan yang benar-benar sesuai dengan kondisi awal sebelum dihapus.

3. Menurut Bapak, bagaimana dampak perbedaan hasil antara Shift+Delete dan perintah SDelete terhadap pembuktian di pengadilan? Apakah bukti digital yang dipulihkan sebagian (tidak utuh) masih bernilai di persidangan?

Jawaban :

Terkait dengan perbedaan teknik penghapusan, barang bukti yang tidak utuh atau hanya sebagian dapat dipulihkan, pada dasarnya tidak dapat langsung dijadikan bukti sah di pengadilan. *File* yang hanya sebagian terpulihkan atau mengalami kerusakan hanya berfungsi sebagai petunjuk awal untuk mengarahkan penyidik dalam menemukan bukti yang lebih lengkap. Agar suatu bukti dapat bernilai hukum di persidangan, maka bukti digital tersebut harus memenuhi kesesuaian dengan aspek *tempus* (waktu kejadian) dan *locus* (tempat kejadian perkara). Oleh sebab itu, meskipun hasil pemulihan dari *file* yang dihapus menggunakan kombinasi tombol Shift+Delete lebih memungkinkan dibanding perintah Sdelete, jika data yang diperoleh tidak utuh, nilainya tetap terbatas pada tahap investigasi, bukan pembuktian akhir.

4. Apa saran Bapak agar penelitian ini lebih bermanfaat untuk penegakan hukum?

Jawaban :

Sebagai saran, pentingnya pengembangan lebih lanjut terhadap teknologi atau *tools* yang mampu melakukan *recovery file* yang dihapus dengan metode penimpaan data (*overwrite*) seperti yang dilakukan oleh Sdelete. Hal ini penting karena teknik penghapusan modern semakin canggih, dan pelaku kejahatan siber seringkali berkemungkinan menggunakan metode penghapusan yang dirancang agar data tidak bisa dipulihkan kembali. Dengan adanya pengembangan *tools* baru yang mampu menembus keterbatasan ini, penelitian tidak hanya bermanfaat dalam lingkup akademik, tetapi juga memiliki dampak langsung dalam mendukung aparat penegak hukum untuk mengungkap kasus-kasus kejahatan digital yang lebih kompleks.

Hasil wawancara dengan Bapak Ali Nupiah, Advokat / Pengacara di kabupaten Bengkulu Utara

1. Apakah hasil ini menurut Bapak relevan dengan praktik investigasi hukum?

Jawaban :

Relevansi hasil penelitian ini erat dengan praktik investigasi hukum. Beliau menjelaskan bahwa agar suatu perkara dapat dinaikkan ke pengadilan, syarat seperti alat bukti harus terpenuhi. Dalam konteks barang bukti digital, temuan hasil forensik yang *valid* juga termasuk ke dalam kategori untuk melanjutkan perkara. Namun, jika bukti tidak memadai atau tidak dapat diverifikasi, maka perkara tidak dapat diajukan ke persidangan. Hal ini

menunjukkan bahwa hasil penelitian yang membahas kemampuan pemulihan data digital memiliki kaitan langsung dengan proses hukum, terutama dalam memastikan kecukupan alat bukti.

2. Bagaimana pandangan Bapak terhadap efektivitas *tools* (Autopsy, Magnet Axiom, PhotoRec) jika digunakan dalam praktik investigasi nyata?

Jawaban :

keefektifan suatu *tools* dalam praktik investigasi nyata harus diukur dari sejauh mana hasil pemulihan dapat dipastikan keasliannya.

3. Menurut Bapak, bagaimana dampak perbedaan hasil antara Shift+Delete dan perintah SDelete terhadap pembuktian di pengadilan? Apakah bukti digital yang dipulihkan sebagian (tidak utuh) masih bernilai di persidangan?

Jawaban :

Perbedaan hasil antara penghapusan dengan Shift+Delete dan Sdelete berimplikasi besar terhadap nilai pembuktian. Jika hasil pemulihan dapat diakses secara utuh, maka bukti tersebut berpotensi digunakan dalam proses persidangan. Namun, bukti digital yang tidak utuh, *corrupt*, atau hanya sebagian dipulihkan, tidak memiliki nilai sebagai barang bukti di pengadilan. Bukti semacam itu hanya bisa menjadi indikasi awal, tetapi tidak cukup kuat untuk memperkuat perkara. Analoginya seperti foto wajah di medsos yang sudah diedit atau ditutupi stiker; meskipun masih ada konten di dalamnya, bukti tersebut tidak dapat dipertanggungjawabkan kebenarannya. Hal yang sama berlaku untuk *file* hasil pemulihan Sdelete yang *corrupt*, sehingga tidak dapat digunakan untuk mengajukan perkara.

4. Apa saran Bapak agar penelitian ini lebih bermanfaat untuk penegakan hukum?

Jawaban :

Hasil penelitian akan lebih bermanfaat apabila mampu menjawab persoalan di lapangan, yaitu bagaimana menghadirkan bukti digital yang sah dan dapat dipertanggungjawabkan di persidangan. Oleh karena itu, penelitian sebaiknya tidak hanya berfokus pada aspek teknis pemulihan data, tetapi juga mengaitkannya dengan standar pembuktian hukum yang berlaku, termasuk peran ahli forensik dalam menjelaskan validitas temuan.