**Jurnal Inovasi Komputer (INOKOM), Vol. 2 No. 1, Januari 2026**
https://jurnal.citanusantara.id/index.php/inokom

# Analisis Forensik Digital ISO/IEC 27037 pada *Recovery File* Terhapus Permanen dari *Removable Flash Storage*

Mirza Sutrisno[1]*, Asruddin[2]
[1]Universitas Muhammadiyah Jakarta
[2]Universitas Bung Karno
* E-mail: mirza.sutrisno@umj.ac.id

## ABSTRAK

Penghapusan file secara permanen pada media penyimpanan USB sering dianggap sebagai metode yang mampu menghilangkan data secara menyeluruh. Namun secara teknis, proses tersebut hanya menghapus referensi metadata pada sistem file tanpa menghilangkan data fisik yang tersimpan pada media penyimpanan. Penelitian ini bertujuan untuk menganalisis proses recovery file yang dihapus secara permanen menggunakan pendekatan forensik digital yang mengacu pada standar ISO/IEC 27037. Penelitian dilakukan dengan skenario penghapusan sepuluh file dari flashdisk pada sistem operasi Windows. Proses akuisisi bukti digital dilakukan menggunakan FTK Imager, sedangkan proses pemeriksaan dan recovery file dilakukan menggunakan Autopsy. Hasil penelitian menunjukkan bahwa seluruh file yang dihapus masih dapat direcovery secara utuh karena sektor penyimpanan belum mengalami penimpaan data. Analisis kepatuhan terhadap ISO/IEC 27037 menunjukkan bahwa seluruh tahapan forensik digital yang dilakukan telah memenuhi prinsip keaslian, integritas, dan ketertelusuran bukti digital. Penelitian ini diharapkan dapat menjadi referensi praktis dan akademik dalam penerapan forensik digital berbasis standar internasional pada media penyimpanan lepas.

Kata Kunci : bukti digital, forensik digital, ISO/IEC 27037, pemulihan data

## ABSTRACT

Permanent file deletion on USB storage media is often assumed to completely remove data from the device. Technically, however, this process only deletes file system metadata references while the physical data remains on the storage media until overwritten. This study aims to analyze the file recovery process of permanently deleted files using a digital forensic approach based on the ISO/IEC 27037 standard. The research was conducted using a scenario involving the permanent deletion of ten files from a USB flash drive on a Windows operating system. Digital evidence acquisition was performed using FTK Imager, while examination and file recovery were carried out using Autopsy. The results indicate that all deleted files were successfully recovered because the storage sectors had not been overwritten. The compliance analysis with ISO/IEC 27037 shows that all digital forensic stages were conducted in accordance with the principles of authenticity, integrity, and traceability of digital evidence. This study is expected to serve as a practical and academic reference for the implementation of international standard–based digital forensic investigations on removable storage media.

Keywords: digital evidence, digital forensics, file recovery, ISO/IEC 27037

Jurnal Inovasi Komputer (INOKOM), Vol. 2 No. 1, Januari 2026
https://jurnal.citanusantara.id/index.php/inokom

## PENDAHULUAN DAN TINJAUAN PUSTAKA

Media penyimpanan USB masih banyak digunakan dalam aktivitas sehari-hari, baik untuk kebutuhan personal maupun organisasi. Karakteristiknya yang portabel, murah, dan kompatibel dengan berbagai sistem operasi menjadikan flashdisk sebagai media penyimpanan yang praktis, namun sekaligus rentan terhadap penyalahgunaan. Dalam konteks kejahatan digital, perangkat USB kerap dimanfaatkan sebagai sarana penyimpanan, pemindahan, maupun penghapusan data yang bertujuan untuk menghilangkan jejak digital terkait suatu peristiwa hukum. Salah satu cara yang umum digunakan adalah penghapusan file secara permanen melalui kombinasi tombol *Shift* + *Delete* pada sistem operasi Windows, yang secara umum dipersepsikan sebagai penghapusan data secara total dan tidak dapat dipulihkan.


Gambar 1. Siklus Pemulihan Data Forensik

Pada gambar 1 menunjukkan siklus pemulihan data pada forensik digital. Penghapusan file secara permanen *Shift* + *Delete* pada sistem operasi Windows tidak berarti menghilangkan data secara fisik dari media penyimpanan. Sistem file pada sistem operasi Windows, seperti FAT32 dan NTFS, hanya menghapus referensi metadata file dan menandai sektor penyimpanan sebagai ruang kosong yang dapat digunakan kembali. Selama sektor penyimpanan tersebut belum tertimpa oleh data baru (*overwritten*), sisa data (*data remnants*) masih dapat diidentifikasi dan dipulihkan menggunakan teknik forensik digital. Kondisi ini menjadi sangat relevan dalam proses pembuktian di persidangan, di mana keberadaan atau ketiadaan suatu file digital dapat berpengaruh langsung terhadap penilaian fakta hukum.

Sejumlah penelitian sebelumnya telah mengkaji fenomena pemulihan data yang dihapus secara permanen. (R dkk., 2025) menjelaskan bahwa penghapusan file pada media penyimpanan tidak menghilangkan data secara langsung, melainkan hanya menghapus struktur logisnya. Penelitian oleh (Pratama, 2021) menunjukkan bahwa artefak digital yang telah dihapus masih dapat dipulihkan secara forensik selama

belum terjadi penumpukan data, dengan tingkat keberhasilan yang bergantung pada metode akuisisi dan analisis yang digunakan. Selain itu, (Singh dkk., 2025) menegaskan bahwa pemulihan data dari media penyimpanan eksternal, seperti USB flashdisk, harus dilakukan dengan pendekatan forensic sound agar hasil analisis dapat dipertanggungjawabkan secara ilmiah dan hukum.

Dalam konteks pembuktian di persidangan, keberhasilan pemulihan data saja tidak cukup untuk menjamin diterimanya bukti digital. Proses penanganan bukti sejak tahap identifikasi hingga analisis harus memenuhi prinsip validitas, integritas, dan *chain of custody*. (Nortjé & Myburgh, 2019) menekankan bahwa integritas dan *chain of custody* adalah syarat kunci agar bukti digital dapat diterima di pengadilan; data tidak boleh diubah, pemeriksaan dilakukan pada duplikat forensik, dan seluruh proses harus terdokumentasi.

Untuk menjawab tantangan tersebut, ISO/IEC 27037 hadir sebagai standar internasional yang memberikan pedoman dalam proses identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital. Standar ini bertujuan untuk memastikan bahwa setiap tahapan penanganan bukti digital dilakukan secara sistematis, terdokumentasi, dan mampu menjaga integritas data asli. Penelitian yang dilakukan oleh (Alawi dkk., 2025) menunjukkan bahwa penerapan standar forensik yang terstruktur, termasuk ISO/IEC 27037, dapat meningkatkan kredibilitas hasil investigasi forensik digital serta memperkuat posisi bukti digital dalam proses hukum.

Selain aspek standar, perangkat lunak forensik juga memegang peranan penting dalam proses investigasi. FTK Imager banyak digunakan dalam tahap akuisisi karena kemampuannya menghasilkan *bit-by-bit image* dan melakukan verifikasi integritas data menggunakan nilai hash (Sitima, 2024). Autopsy sebagai platform forensik berbasis open-source menyediakan fitur analisis sistem file dan pemulihan data yang luas, termasuk pada media penyimpanan USB (Singh dkk., 2025). Penggunaan kedua perangkat lunak ini secara bersamaan dinilai efektif dalam mendukung proses investigasi forensik yang sesuai dengan prinsip standar internasional.

Meskipun penelitian sebelumnya telah banyak membahas keberhasilan pemulihan file yang dihapus secara permanen dari media penyimpanan USB, sebagian besar studi tersebut masih berfokus pada aspek teknis file *recovery* dan evaluasi kemampuan perangkat lunak forensik tanpa mengkaji secara mendalam kesesuaian proses tersebut terhadap standar internasional yang mengatur keabsahan bukti digital. Penelitian oleh (Alawi dkk., 2025) menegaskan potensi pemulihan data, namun belum secara eksplisit mengaitkan prosedur pemulihan tersebut dengan penerapan ISO/IEC 27037. Selain itu, kajian yang secara khusus mengintegrasikan skenario penghapusan *Shift* + *Delete* pada sistem operasi Windows dengan analisis kepatuhan terhadap standar forensik serta implikasinya terhadap penerimaan bukti di persidangan masih sangat terbatas. Oleh karena itu, terdapat celah penelitian yang signifikan dalam mengkaji bagaimana penerapan ISO/IEC 27037 secara praktis pada proses pemulihan file USB menggunakan FTK Imager dan Autopsy dapat menjamin integritas, validitas, dan kekuatan pembuktian bukti digital dalam konteks hukum.

Jurnal Inovasi Komputer (INOKOM), Vol. 2 No. 1, Januari 2026
https://jurnal.citanusantara.id/index.php/inokom

## METODE/EKSPERIMEN

Penelitian ini menggunakan pendekatan forensik digital dengan mengacu pada pedoman ISO/IEC 27037 untuk memastikan bahwa seluruh proses penanganan bukti digital dilakukan secara sistematis, terstandarisasi, dan dapat dipertanggungjawabkan secara hukum.


Gambar 2. Tahapan Forensik Digital Berbasis Standar ISO/IEC 27037

Gambar 2 menjelaskan tentang tahapan forensik digital berbasis standar ISO/IEC 27037 yang dapat dijelaskan sebagai berikut:

1. Identifikasi Bukti Digital
   Menentukan media penyimpanan USB sebagai objek penelitian serta mengidentifikasi jenis file yang menjadi fokus investigasi, yaitu file audio, video, dan tangkapan layar percakapan WhatsApp yang diduga telah dihapus secara permanen.
2. Preservasi Bukti
   Melakukan pengamanan terhadap media USB untuk menjaga keutuhan dan integritas bukti digital, serta memastikan bahwa data asli tidak mengalami perubahan selama proses investigasi.
3. Akuisisi Bukti Digital
   Membuat salinan forensik (*forensic image*) dari media USB menggunakan FTK Imager dalam format RAW, sehingga seluruh isi media, termasuk ruang tidak

teralokasi, dapat dianalisis. Keaslian salinan forensik diverifikasi menggunakan nilai hash MD5 dan SHA1.

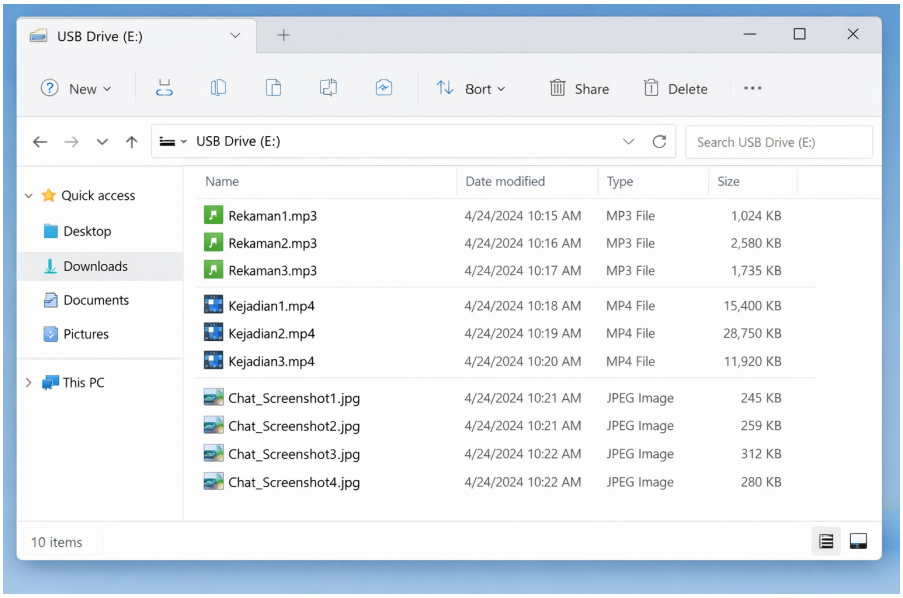
4. Pemeriksaan dan Analisis
   Melakukan analisis terhadap *image* forensik menggunakan Autopsy untuk mengidentifikasi struktur sistem file, artefak digital, dan file yang berpotensi dipulihkan dari ruang penyimpanan yang telah dihapus.
5. Recovery dan Dokumentasi
   Melakukan proses pemulihan (*recovery*) terhadap file-file yang telah dihapus secara permanen dan menyimpan hasilnya secara terstruktur. Seluruh proses dan hasil *recovery* didokumentasikan sebagai bagian dari laporan forensik untuk mendukung validitas bukti digital.

## HASIL DAN PEMBAHASAN

Penelitian ini difokuskan pada investigasi dengan menggunakan simulasi 10 file digital yang tersimpan pada sebuah media penyimpanan *USB flashdisk*, terdiri atas 3 file audio, 3 file video, dan 4 file hasil tangkapan layar (*screenshot*) percakapan WhatsApp. File-file tersebut disimulasikan telah dihapus secara permanen menggunakan metode *Shift* + *Delete* pada sistem operasi Windows. Seluruh tahapan penelitian dilakukan dengan mengacu pada prinsip *forensic soundness* dan pedoman ISO/IEC 27037 agar hasil investigasi dapat dipertanggungjawabkan secara teknis dan hukum.

1. Identifikasi Bukti Digital

Tahap identifikasi bertujuan untuk menentukan dan mengenali objek yang berpotensi mengandung bukti digital. Pada tahap ini, media USB diidentifikasi sebagai potential digital evidence karena diduga menyimpan atau pernah menyimpan file audio, video, dan tangkapan layar percakapan WhatsApp yang relevan dengan kasus. Sebagai gambaran file yang disimulasikan dapat dilihat pada gambar 3 di bawah ini.



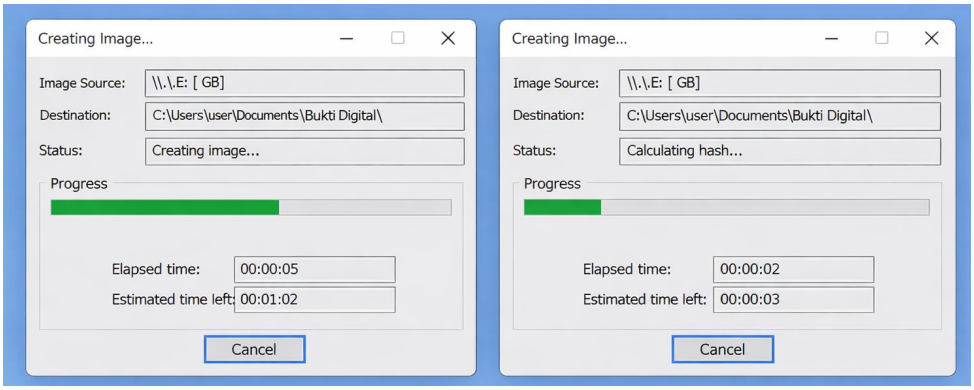

Gambar 3. File Simulasi *USB Drive*

Proses identifikasi meliputi pencatatan jenis perangkat, kapasitas penyimpanan, sistem file yang digunakan, serta kondisi fisik media penyimpanan. Selain itu,

dilakukan klasifikasi awal terhadap jenis file yang akan dianalisis guna menentukan pendekatan pemeriksaan dan pemulihan data yang tepat.

2. Preservasi Bukti
Tahap preservasi dilakukan untuk menjaga keutuhan dan integritas bukti digital agar tidak mengalami perubahan sejak pertama kali diidentifikasi. Media USB diamankan dan dilindungi dari aktivitas baca-tulis yang tidak sah. Dalam tahap ini, prinsip *do not alter original evidence* diterapkan dengan memastikan bahwa seluruh proses analisis dilakukan terhadap salinan forensik (*forensic image*), bukan terhadap media asli. Setiap tindakan yang dilakukan pada bukti didokumentasikan sebagai bagian dari *chain of custody* untuk menjamin transparansi dan akuntabilitas proses investigasi.

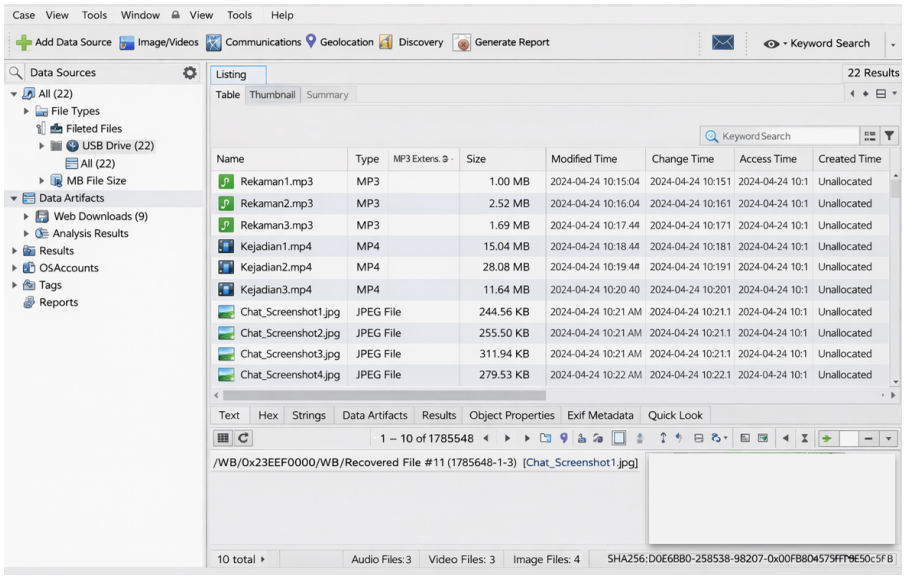
3. Akuisisi Bukti Digital
Akuisisi bukti digital dilakukan menggunakan FTK Imager dengan metode *bit-by-bit imaging* untuk menghasilkan salinan forensik dalam format RAW (dd). Metode ini memungkinkan seluruh isi media penyimpanan, termasuk ruang tidak teralokasi (*unallocated space*), ikut terakuisisi sehingga peluang pemulihan file yang telah dihapus dapat dimaksimalkan. Berikut dijelaskan pada gambar 4 proses imaging dan laporan kode hash.



Gambar 4. Proses Imaging dan Laporan Kode Hash

Pada gambar 4 menunjukan proses dan hasil imaging. Setelah proses selesai, dilakukan verifikasi integritas data menggunakan nilai hash MD5 dan SHA1. Nilai hash antara media asli dan image forensik dibandingkan untuk memastikan bahwa salinan forensik identik dengan sumber aslinya dan tidak mengalami perubahan selama proses akuisisi.

4. Pemeriksaan dan Analisis
Tahap pemeriksaan dan analisis dilakukan terhadap image forensik menggunakan perangkat lunak Autopsy yang disajikan pada gambar 5.




Gambar 5. Hasil *Recovery Data*

Pada gambar 5 menunjukan bahwa sistem file dianalisis untuk mengidentifikasi artefak digital yang berkaitan dengan file audio, video, dan tangkapan layar percakapan WhatsApp. Analisis mencakup pemeriksaan metadata file, lokasi penyimpanan, serta status file apakah masih teralokasi atau telah berada pada ruang tidak teralokasi. Selain itu, dilakukan pencarian artefak pendukung seperti *file headers, file signatures, dan timestamps* untuk membantu proses identifikasi dan validasi file yang akan di*recovery*.

5. *Recovery* dan Dokumentasi

Tahap *recovery* dilakukan dengan memanfaatkan fitur file *recovery* pada Autopsy untuk memulihkan file-file yang telah dihapus secara permanen. Proses pemulihan difokuskan pada 10 file target sesuai dengan kategori yang telah ditentukan. File hasil recovery kemudian disimpan secara terstruktur pada direktori My Documents dengan subfolder File Recovery guna memudahkan pengelolaan dan pelacakan hasil. Seluruh proses *recovery* didokumentasikan secara rinci, meliputi waktu pemulihan, jenis file yang berhasil dipulihkan, tingkat keutuhan file, serta hasil verifikasi integritas pasca-*recovery*. Dokumentasi ini berfungsi sebagai dasar pelaporan forensik dan mendukung kekuatan pembuktian bukti digital di persidangan. Adapun hasil analisis bukti digital dapat dilihat pada Tabel 1.

Tabel 1. Hasil Analisis Bukti Digital

| No | Nama File | Jenis Bukti | Format | Ukuran File | Waktu Dibuat | Status Recovery | Hasil Analisis |
|---|---|---|---|---|---|---|---|
| 1 | Rekaman 1.mp3 | Rekaman suara | MP3 | 1.00 MB | 24-04-2024 10:15 | Berhasil | File audio utuh, dapat diputar normal, metadata terbaca |
| 2 | Rekaman 2.mp3 | Rekaman suara | MP3 | 2.52 MB | 24-04-2024 10:16 | Berhasil | Tidak ada kerusakan data, isi suara jelas |
| 3 | Rekaman 3.mp3 | Rekaman suara | MP3 | 1.69 MB | 24-04-2024 10:17 | Berhasil | Struktur file valid, hash sesuai |
| 4 | Kejadian1.mp4 | Video kejadian | MP4 | 15.04 MB | 24-04-2024 10:18 | Berhasil | Video dapat diputar penuh tanpa frame rusak |
| 5 | Kejadian2.mp4 | Video kejadian | MP4 | 28.08 MB | 24-04-2024 10:19 | Berhasil | Audio dan visual sinkron, metadata konsisten |
| 6 | Kejadian3.mp4 | Video kejadian | MP4 | 11.64 MB | 24-04-2024 10:20 | Berhasil | Tidak ditemukan indikasi manipulasi |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | Chat_Screenshot1.jpg | Screenshot WhatsApp | JPG | 244.56 KB | 24-04-2024 10:21 | Berhasil | Gambar utuh, teks percakapan terbaca jelas |
| 8 | Chat_Screenshot2.jpg | Screenshot WhatsApp | JPG | 255.50 KB | 24-04-2024 10:21 | Berhasil | Metadata EXIF tersedia |
| 9 | Chat_Screenshot3.jpg | Screenshot WhatsApp | JPG | 311.94 KB | 24-04-2024 10:21 | Berhasil | Resolusi dan konten sesuai |
| 10 | Chat_Screenshot4.jpg | Screenshot WhatsApp | JPG | 279.53 KB | 24-04-2024 10:22 | Berhasil | File autentik, tidak terkompresi ulang |

Hasil analisis pada Tabel 1 disimpulkan berhasil mengidentifikasi dan memulihkan seluruh bukti digital yang tersimpan dalam media penyimpanan, dengan tingkat keberhasilan *recovery* sebesar 100%. Bukti digital yang diperoleh terdiri dari file audio, video, dan gambar yang berada dalam kondisi utuh serta dapat diakses tanpa mengalami kerusakan.

Tidak ditemukan adanya indikasi perubahan, manipulasi, maupun kehilangan data selama seluruh rangkaian proses forensik digital dilakukan. Oleh karena itu, bukti digital yang berhasil di*recovery* dapat dinyatakan autentik, valid, dan dapat dipertanggungjawabkan secara ilmiah maupun hukum. Hasil penelitian ini menunjukkan bahwa penggunaan metode imaging forensik dan analisis menggunakan FTK Imager serta Autopsy efektif dalam mendukung proses investigasi forensik digital.

## PENUTUP

Penelitian ini membuktikan bahwa penerapan imaging forensik menggunakan FTK Imager dan analisis menggunakan Autopsy efektif dalam memulihkan dan memverifikasi bukti digital dari media penyimpanan USB Drive, dengan seluruh bukti audio, video, dan gambar berhasil di*recovery* secara utuh serta menunjukkan konsistensi nilai hash yang menjamin integritas dan keaslian data, sehingga hasil analisis dapat dipertanggungjawabkan secara ilmiah maupun hukum.

Penelitian selanjutnya disarankan untuk memanfaatkan lebih dari satu perangkat lunak forensik digital, memperluas objek penelitian pada berbagai jenis media penyimpanan dan artefak aplikasi, serta menerapkan otomatisasi atau kecerdasan

buatan dalam proses analisis guna meningkatkan efisiensi dan kekuatan pembuktian forensik digital.

## UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dan kontribusi dalam pelaksanaan penelitian ini.

## DAFTAR PUSTAKA

Alawi, H. S., Riadi, I., & Sunardi, S. (2025). Improving Credibility of Digital Evidence Investigation in E-Commerce Fraud Cases using ISO/IEC 27037. *International Journal of Advances in Data and Information Systems*. https://doi.org/10.59395/ijadis.v6i2.1408

Nortjé, J. G. J., & Myburgh, D. (2019). The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa. *Potchefstroom Electronic Law Journal*. https://doi.org/10.17159/1727-3781/2019/v22i0a4886

Pratama, I. (2021). Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: A Proof of Concept. *International Journal of Science, Technology & Management*. https://doi.org/10.46729/ijstm.v2i4.256

R, N., A, V., & P, A. (2025). Recovery of Deleted Files: Challenges and Techniques. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2025.v07i02.41088

Singh, V., Nikam, A., Singh, R., & Mehta, D. (2025). Advancements in Digital Forensics: Emerging Tools and Techniques. *Journal of Information Systems Engineering and Management*. https://doi.org/10.52783/jisem.v10i43s.8364

Sitima, J. (2024). Understanding Digital Forensic Tools: Their Features, Applicability and Key Short Comings. A Compendium. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2024.v06i06.30026