Journal of Cyber Health and Computer (JOCHAC)
Volume 2, Issue 1, August 2024
ISSN: 3031-4623, DOI: 10.64163/jochac.v2i1.14

Penerapan Tool *Recovery data* dalam Akuisisi Data Forensik *Flashdrive*

*Muhammad Immawan Aulia[1], Panggah Widiandana [2], Latifah Iriani [3], Muhammad Fauzan Gustafi[4], Muhammad Azam Hasani [5]
[1, 2,5] Informatika, Universitas Islam Mulia Yogyakarta, Yogyakarta, Indonesia
[3] Informatika, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
[4] Sistem Informasi, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
Email: [1 *]muhimmawanaulia16@uim-yogya.ac.id, [2] panggah.widiandana@uim-yogya.ac.id, [3] latifahiriani@sibermu.ac.id, [4] muhammadfauzangustafi@sibermu.ac.id, [5] azamhasanie.2@gmail.com
*Corresponding Author

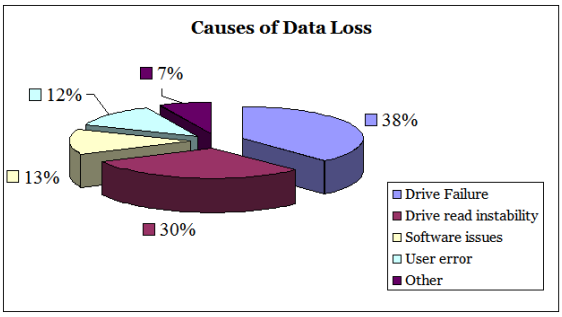
***Abstract*—Di era digital yang serba cepat ini, *flashdrive* menjadi salah satu metode penyimpanan yang paling populer. Saat-saat tertentu, data flashdisk dapat hilang, dan kehilangan data ini dapat membawa konsekuensi yang signifikan baik secara profesional maupun pribadi. Dalam penelitian ini, contoh pemulihan data dari flashdisk yang tidak dapat diakses setelah dicabut secara paksa selama proses transfer data dibahas. Metode forensik statik dan alat Disk Drill, berhasil menemukan sebanyak 7626 file dari partisi yang tidak teralokasikan dengan ukuran total 17,3 GB. Bukti digital yang telah dipulihkan sebanyak 49 files yang disajikan dalam bentuk file dengan berbagai ekstensi, seperti gambar, audio, dokumen, dan arsip. Kemampuan alat pemulihan data yang canggih memungkinkan pemulihan berbagai jenis file, yang meningkatkan peluang untuk menyelamatkan data yang hilang.**

***Keywords*—Pemulihan Data, Flashdisk, Forensik Statik, Disk Drill, Partisi Unallocated**

I. PENDAHULUAN

Data telah menjadi aset yang sangat berharga bagi individu, kelompok, dan bahkan negara di era digital yang serba cepat ini. Data digunakan untuk berbagai tujuan, seperti menyimpan foto pribadi, dokumen penting, dan informasi keuangan yang sensitif. Namun, meskipun data mudah diakses dan disimpan, ada risiko kehilangan data.

Data survei dari perusahaan yang berfokus pada pemulihan data dapat digunakan untuk menyelidiki faktor-faktor utama yang menyebabkan kehilangan data. Kegagalan hard drive adalah penyebab paling umum dari kehilangan data, menyumbang 38% dari semua kasus. Korupsi *software*, yang mungkin termasuk kerusakan yang disebabkan oleh perangkat lunak sistem atau program lain (misalnya, serangan virus), menyumbang 13% dari kehilangan data. Instabilitas membaca drive mencakup situasi di mana kerusakan media atau degradasi mencegah akses ke data pada disk. Selain itu, 12% hilangnya data disebabkan oleh kesalahan manusia. Ini mencakup data yang dihapus secara tidak sengaja dan partisi *hard drive* yang salah. [1].



Gambar 1. Penyebab kehilangan data

Bukti digital sangat penting dalam semua jenis kejahatan, bukan hanya kejahatan komputer, Untuk menghindari hal itu maka diperlukan tindakan seperti menjaga perangkat dalam mode isolasi. Tujuannya adalah untuk menghindari data dari terhapus dan berubah dengan kondisi apa pun. Bukti digital dapat ditemukan di hard drive, flash drive, perangkat seluler.[2].

Terhapus dan kerusakan file pada sebuah media penyimpanan merupakan hal yang tidak dapat dihindari, baik sengaja ataupun secara tidak sengaja. Kasus digital forensik seperti ini dapat bilang sebagai sebuah kejahatan digital apabila dilakukan dengan tujuan tidak baik atau negatif dalam artian penghapusan barang bukti digital. File yang terhapus sangat berpotensi untuk direcovery menggunakan bidang digital forensik.[3].

Akibatnya, penting bagi kita untuk memahami bahaya kehilangan data dan mengambil tindakan pencegahan yang tepat. Jika hal ini terjadi, memahami cara memulihkan data yang hilang merupakan langkah penting. Dalam proses transfer data, kasus pemulihan data dari flashdisk yang tidak dapat diakses akan dibahas dalam penelitian ini.

II. METODE PENELITIAN

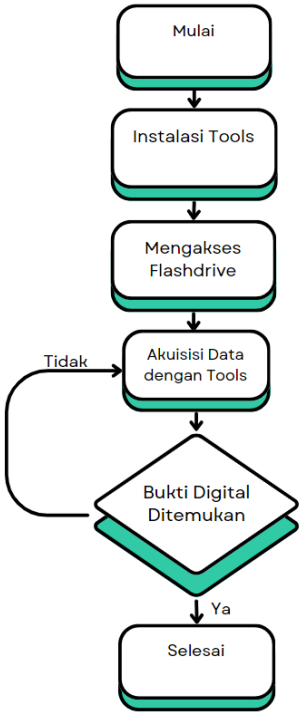
Statik Forensik difokuskan pada pemeriksaan sebuah duplikat yang disebut salinan disk untuk mengeluarkan konten memori, seperti file yang dihapus, riwayat penelusuran web, fragment file, koneksi jaringan, file yang dibuka, riwayat log in pengguna, dll. untuk membuat timeline yang memberikan pandangan, misalnya statika parsial atau ringkasan tentang aktivitas yang dilakukan pada sistem korban sebelum mematikannya. Dalam analisis statis

berbagai jenis perangkat lunak dan perangkat keras seperti Fundl, RegCon digunakan untuk dumping memori dan penyortiran data pembuktian untuk analisis dan tujuan presentasi. Data forensik diperoleh dengan menggunakan berbagai jenis perangkat eksternal seperti USB, eksternal hard drive atau CD, DVD. Kemudian data ini dibawa investigator untuk melakukan berbagai metode agar dapat menganalisis data sebagai bukti secara forensik. [4].

Statik Forensik mengacu pada penyelidikan forensik tradisional yang dilakukan dengan perangkat yang tidak aktif atau tidak berfungsi. Forensik statis berfokus pada pemeriksaan duplikat media penyimpanan mengambil data yang ada, misalnya, seperti file yang dihapus, riwayat situs web, riwayat pengguna, dan riwayat log komputer. Salinan bukti dapat diperoleh dengan menggunakan berbagai jenis media penyimpanan eksternal seperti *Flash disk*, External Hard Drive, dan penyimpanan lainnya. [5][6]. Ilustrasi pada Gambar 2.

Gambar 2. Tahapan Statik Forensik

Gambar 3 adalah Ilustrasi proses akuisisi data pada penelitian.



Gambar 3. *Flowchart* proses akuisisi data pada *flashdrive*

Uraian proses akuisisi data dari flowchart sebagai berikut:

- Melakukan instalasi *tools* Drill Disk untuk melakukan proses *recovery data.*
- Mengakses *Flashdrive* menggunakan laptop.
- Mengoperasikan *tools* untuk *recovery data*.
- Apabila ditemukan bukti digital (file yang terhapus) maka proses *recovery* dapat dilakukan.

III. HASIL DAN PEMBAHASAN

Pada penelitian ini perangkat dan *tools* dengan spesifikasi sebagai berikut:

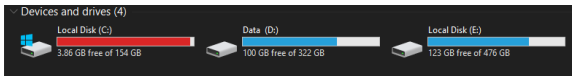
TABEL I. SPESIFIKASI ALAT

Alat	*Merk*	*Spesifikasi*
Laptop	Acer	Acer Aspire E14 E5-422 AMD A6-7310
Flashdrive	Toshiba	8 GB

TABEL II. SPESIFIKASI *TOOLS*

Tools	*Versi*
Drill Disk	5.5.900.0

Dalam mengakses *flashdrive* dilakukan dengan melakukan pengecekan apakah *flashdrive* terdeteksi seperti pada Gambar 4.

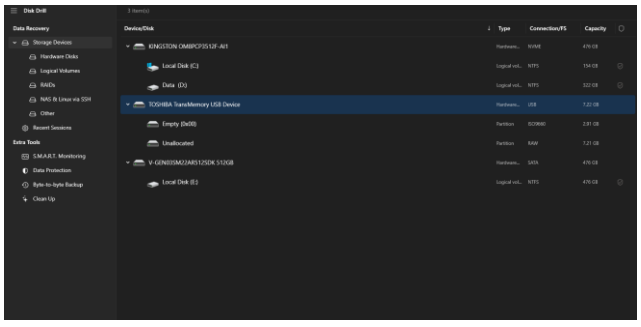


Gambar 4. *Flashdrive* tidak terdeteksi

Setelah dilakukan pengecekan ulang pada *disk management* mendeteksi adanya partisid dari *flashdrive* namun dengan status unallocated seperti pada Gambar 5.

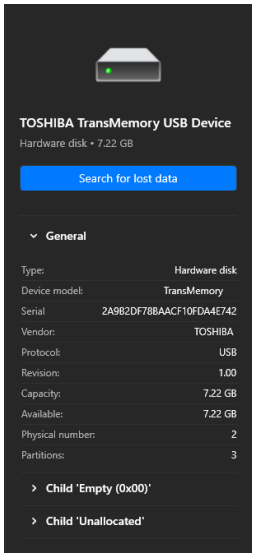
Gambar 5. Partisi *flashdrive* di *Disk Management*

Pada Gambar 6, tampilan *tools* Drill Disk dioperasikan pada sistem operasi windows 10.



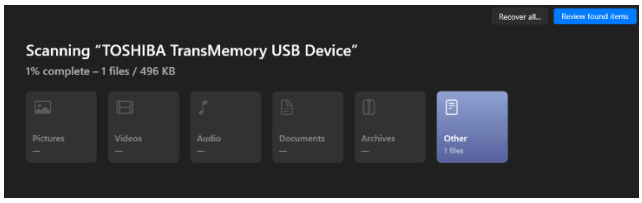
Gambar 6. Tampilan *Tools* Drill Disk

Setelah memilih partisi *flashdrive* yang terdeteksi pada *tools* Drill Disk, tekan tombol *Search for lost data*, seperti pada Gambar 7.



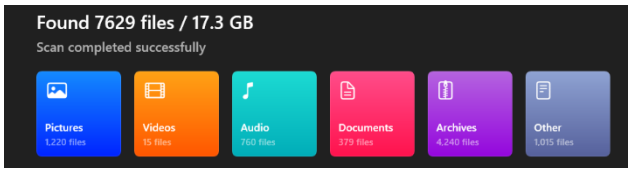
Gambar 7. Fitur Pencarian data yang hilang

Proses berlanjut dari *search for lost data* seperti pada Gambar 8.



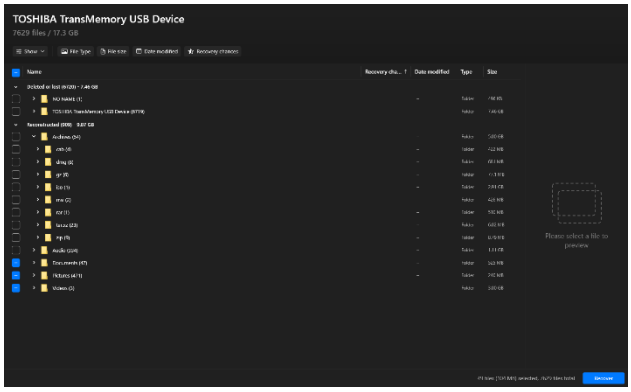
Gambar 8. Proses pencarian data yang hilang

Kemudian proses pencarian data yang hilang pada partisi *flashdrive* seperti pada gambar 9.



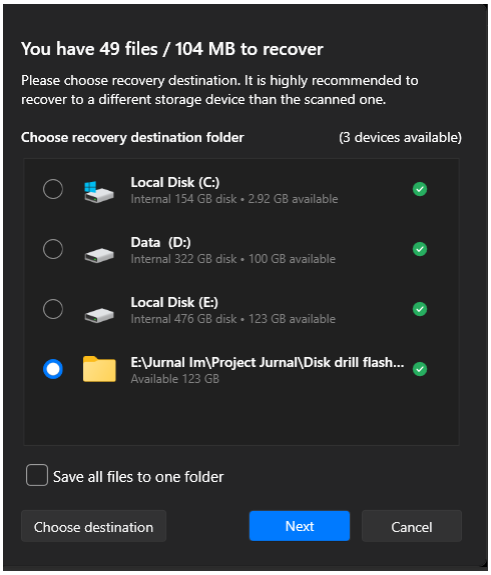
Gambar 9. Proses pencarian data yang hilang selesai

Pilih data yang ingin dipulihkan dan tekan tombol *recover* seperti pada Gambar 10.



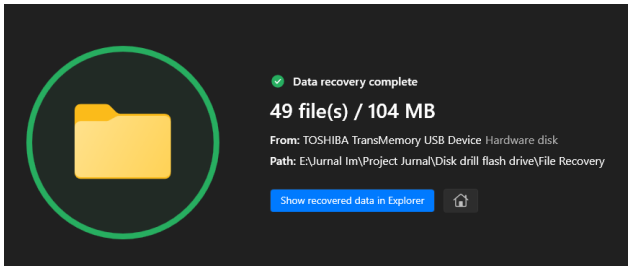
Gambar 10. Pemilihan data yang ingin dipulihkan

Tampilan proses selanjutnya untuk melakukan proses *recovery data* dari sejumlah data yang sudah dipilih sebelumnya, seperti pada Gambar 11.



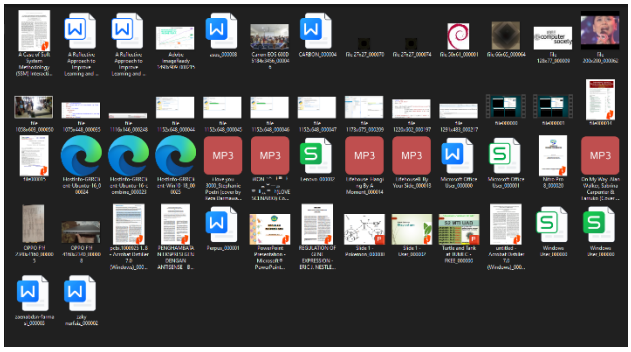
Gambar 11. Memilih *folder destination* untuk file *recovery*

Tampilan apabila proses *recovery* selesai seperti pada gambar 12.



Gambar 12. Proses *recovery* selesai

Hasil dari *recovery data* disajikan pada tampilan *folder* seperti pada Gambar 13.



Gambar 13. Data yang berhasil di*recovery*

IV. KESIMPULAN

Memulihkan data dari flashdisk yang tidak dapat diakses setelah dicabut secara paksa dapat dicapai dengan menggunakan metode Forensik Statik yang tepat dan alat pemulihan data yang sesuai. Studi kasus ini menunjukkan bahwa alat pemulihan data yang populer, Disk Drill, dapat memulihkan 7629 file berukuran 17,3 GB dari partisi yang tidak teralokasikan pada flashdisk yang rusak serta berhasil memulihkan 49 file terpilih dengan beragam ekstensi. Drill disk dapat membantu dalam investigasi digital dan pemulihan

data dalam berbagai situasi karena dapat memulihkan berbagai jenis file, termasuk dokumen, arsip, gambar, dan audio.

REFERENSI

[1] David M. Smith, Michael L. Williams (2007). https://www.deepspar.com/wp-data-loss.html. diakses 25 Juni 2024.

[2] Kessler, G.C., "Anti-Forensics and the Digital Investigator".2007

[3] Saudi, M. M. "An overview of disk imaging tool in computer forensics". SANS Institute. 2001

[4] Mamoona, R., Khan, M.N.A. (2013). "Exploring Static and Live Digital Forensics: Methods, Practices and Tools". International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013 ISSN 2229-5518

[5] Aulia, I. Riadi, and A. Fadlil, "Storage Forensic Optical drive Menggunakan Metode Statik," Semnastek 2019, no. 2013, pp. 756–761, 2019.

[6] I. Riadi, A. Fadlil, and M. I. Aulia, "Review Proses Forensik Optical drive Menggunakan Metode National Institute of Justice (NIJ)" J. Tek. Inform. dan Sist. Inf., vol. 8, no. 3, pp. 107–118, 2019.