Analisis Perbandingan Tool FTK Imager dan PhotoRec dalam Pemulihan Data *Flashdrive* Berbasis Metode Statik Forensik

Muhammad Immawan Aulia[a,1*], Panggah Widiandana[a,2], Wicaksono Yuli Sulistyo [b,3], Siti Hartinah[a,4], Muhammad Azam Hasani[a,5]

[a] Universitas Islam Mulia Yogyakarta, Jl. Wates No.Km 9, RW.5, Plawonan, Argomulyo, Kec. Sedayu, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55752, Indonesia
[b] Universitas Siber Muhammadiyah, Pakuncen, Wirobrajan, Yogyakarta, Daerah Istimewa Yogyakarta 55253

[1] muhimmawanaulia16@uim-yogya.ac.id*; [2] panggah.widiandana@uim-yogya.ac.id; [3] wicaksono@sibermu.ac.id; [4] siti.hartinah@uim-yogya.ac.id; [5] azamhasanie.2@gmail.com
* Muhammad Immawan Aulia

Submission:29/04/2025, Revision: 02/05/2025, Accepted: 04/05/2025

Abstract

*This study aims to evaluate the effectiveness of two digital forensic tools, **FTK Imager** and **PhotoRec**, in the file recovery process using the static forensic method on a flash drive. The background of this research stems from the need to select forensic tools capable of accurately recovering data while maintaining the integrity of digital evidence, which is crucial in digital investigations. The research was conducted by performing imaging on a flash drive containing test data, followed by a recovery process using both tools. The experimental results show that FTK Imager successfully recovered six audio files and one text file in their entirety, with identical file names and hash values compared to the original digital evidence. In contrast, PhotoRec only managed to recover four audio files and one text file, with two audio files showing different hash values from the originals. Based on these findings, it can be concluded that FTK Imager outperforms PhotoRec in terms of accuracy and reliability in digital data recovery.*
Keywords: Analysis; Tools Comparation; Static Forensics;FTK Imager;PhotoRec

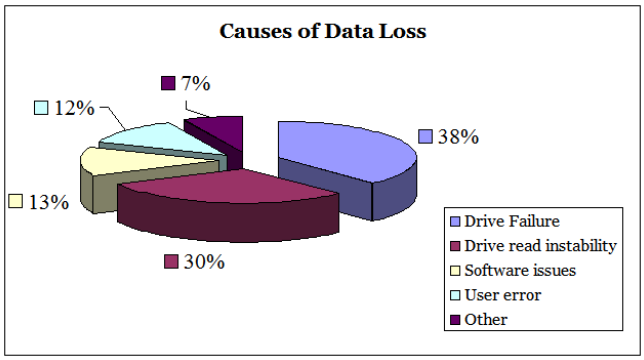
Abstrak

Penelitian ini bertujuan untuk mengevaluasi efektivitas dua perangkat lunak digital forensik, yaitu **FTK Imager** dan **PhotoRec**, dalam proses *recovery* file melalui metode forensik statis pada media penyimpanan *flash drive*. Latar belakang dari penelitian ini didasarkan pada kebutuhan untuk memilih tools forensik yang mampu melakukan pemulihan data secara akurat dan mempertahankan integritas bukti digital, yang sangat krusial dalam proses penyelidikan digital. Penelitian dilakukan dengan melakukan proses *imaging* terhadap *flash drive* yang berisi data uji, kemudian dilakukan proses *recovery* menggunakan kedua tools tersebut. Hasil eksperimen menunjukkan bahwa FTK Imager mampu melakukan *recovery* secara utuh terhadap enam file audio dan satu file teks dengan format nama file dan nilai hash yang identik dengan data asli. Sebaliknya, PhotoRec hanya mampu merekonstruksi empat file audio dan satu file teks, dengan dua file audio menunjukkan perbedaan nilai hash dari file aslinya. Berdasarkan temuan ini, dapat disimpulkan bahwa FTK Imager lebih unggul dalam aspek akurasi dan keandalan pemulihan data digital dibandingkan PhotoRec.
Kata kunci: Analisis; Komparasi Tools, Forensik Statis, FTK Imager, PhotoRec.

1. Pendahuluan

Di era digital yang serba cepat ini, data telah menjadi aset yang sangat berharga bagi individu, kelompok, dan bahkan negara. Data digunakan untuk berbagai tujuan, seperti menyimpan foto pribadi, dokumen penting, dan informasi keuangan yang sensitif. Namun, meskipun data dapat diakses dan disimpan dengan mudah, ada risiko kehilangan data. Survei dari perusahaan yang berfokus pada pemulihan data dapat digunakan untuk menyelidiki faktor-faktor utama yang menyebabkan kehilangan data. Instabilitas membaca drive mencakup situasi di mana kerusakan media atau kerusakan mencegah akses ke data di disk. Selain itu, kesalahan manusia,

yang mencakup data yang dihapus secara tidak sengaja dan partisi *hard drive* atau *flash drive* yang salah sekitar 12% ilustrasi diagram seperti pada Gambar 1. [1].



Gambar 1. Faktor Utama Penyebab Kehilangan Data pada Media Penyimpanan.

Digital forensik adalah bidang ilmu pengatahuan dan teknologi komputer serta metode ilmiah untuk membuktikan kejahatan digital dalam hukum pro justice. Ini mencakup membuktikan kejahatan dengan menggunakan bukti digital, yang berasal dari sumber digital, seperti paket data yang dikirimkan melalui jaringan komputer, untuk memfasilitasi atau melanjutkan rekonstruksi peradilan. Tujuan utama analisis forensik adalah untuk menemukan semua peristiwa, mengetahui dampak mereka pada sistem, mendapatkan bukti yang diperlukan, dan mencegah insiden di masa mendatang dengan menemukan teknik berbahaya yang digunakan.[2].

Untuk menjaga keasliannya, bukti digital dari *flashdrive* harus di-*collect* dengan prosedur yang terstandar. Metode forensik statik menekankan pembuatan salinan *bitwise* dari media asli untuk memastikan bahwa perangkat asli tidak diubah. Untuk menjaga integritas bukti digital, pada prosedur umum pada digital forensik menyarankan agar pemeriksa hanya bekerja pada salinan forensik.

Pemulihan data yang aman merupakan aspek penting dalam forensik tradisional dan forensik digital. Forensik, secara umum, didefinisikan sebagai proses ilmiah untuk mengumpulkan, menganalisis, dan menyajikan bukti fisik dalam konteks hukum, seperti di pengadilan. Sebaliknya, forensik digital menerapkan prinsip yang sama, tetapi berfokus pada kasus yang melibatkan teknologi digital. Bidang ini lebih lanjut dibagi menjadi sub-disiplin seperti forensik komputer, yang berhubungan dengan pemulihan dan analisis data dari sistem komputer; forensik mobile, yang berfokus pada perangkat mobile; dan forensik jaringan, yang melibatkan penyelidikan data dari lingkungan jaringan. Masing-masing sub-disiplin ini menggunakan teknik dan alat khusus untuk memastikan integritas bukti digital dan penerimaannya dalam prosedur hukum. [3].

Ada beberapa hasil penelitian yang melatarbelakangi dilakukannya penelitian ini, yang pertama penelitian Aulia tahun 2024, tools Disk Drill dan metode Forensik Statik digunakan untuk memulihkan data dari flash drive 8 GB yang *unallocated*. Hasilnya menunjukkan bahwa Disk Drill menemukan 7626 file, atau total 17,3 GB. [4]. Pada penelitian yang dilakukan oleh I Putu Agus Eka Pratama yang menggunakan PhotoRec merupakan alat forensik digital yang andal dan efisien dalam melakukan proses pemulihan data, terbukti mampu melakukan pemulihan secara aman dengan mengembalikan seluruh file yang ditargetkan secara lengkap (dengan tingkat keberhasilan 100%). Konsep pemulihan data yang aman pada PhotoRec diterapkan melalui pemberian izin akses root pada seluruh file yang berhasil dipulihkan. Mekanisme keamanan ini memastikan bahwa file yang telah dipulihkan tidak dapat diakses oleh pengguna yang tidak memiliki otorisasi, dan hanya dapat dibuka atau dimodifikasi oleh pengguna yang telah diberikan hak akses yang sesuai, sehingga menjaga kerahasiaan dan integritas data yang dipulihkan. [5]. Penelitian dari Imam Riadi Et al pada media penyimpanan optical (CD/DVD) dengan hasil Temuan dari hasil analisis menggunakan tools FTK Imager menunjukkan bahwa alat ini berhasil memperoleh sepuluh file yang telah terhapus, dengan semua file tersebut memiliki nilai hash yang sesuai dengan data aslinya. Hal ini mengindikasikan tingkat akurasi dan integritas data yang sangat tinggi. Sebaliknya, tools Autopsy hanya berhasil mendeteksi tujuh dari sepuluh file tersebut dan gagal menemukan tiga file dengan ekstensi *.MOV, *.exe, dan *.rar*. Ketidaksesuaian ini secara signifikan memengaruhi kinerja Autopsy dalam proses recovery data. Berdasarkan hasil uji kinerja komparatif yang dilakukan, FTK Imager mendapatkan nilai keberhasilan 100% karena berhasil memulihkan seluruh file yang terhapus beserta nilai hash-nya yang valid. Sementara itu, Autopsy hanya memperoleh skor kinerja sebesar 70% karena tidak dapat mendeteksi tiga file, yang juga tidak memiliki nilai hash akibat ekstensi file yang tidak didukung *(*.MOV, *.exe, dan *.rar). Keterbatasan ini menyoroti kelemahan Autopsy dalam menangani jenis file tertentu selama proses pemulihan data. [6]. Penelitian Imam Riadi Et. Al, ditemukan bahwa DVD-R yang telah diburning menggunakan mode multisession melalui aplikasi Nero, memungkinkan media tersebut dapat diformat dan dianalisis menggunakan tools forensik digital seperti Autopsy. Implementasi tools Autopsy dalam

pengujian ini menunjukkan kemampuannya untuk merestorasi file secara menyeluruh dengan hasil pemulihan yang sangat akurat, dibuktikan dengan nilai hash MD5 yang identik dengan file asli sebelum dilakukan proses eksaminasi. Jenis file yang berhasil direstorasi mencakup berbagai format seperti .pdf, .docx, .pptx, .txt, .mp3, .iso, .jpg, dan .png dengan total keseluruhan sebanyak 29 file. Tingkat keberhasilan proses recovery ini mencapai 100%, menunjukkan bahwa semua file pada DVD-R sebelum diformat berhasil ditemukan kembali tanpa adanya kehilangan data. Jumlah file yang ditemukan oleh tools Autopsy sama persis dengan jumlah file pada DVD-R sebelum dilakukan formatting. Dalam penelitian ini digunakan metode forensik statik, mengingat objek yang diperiksa merupakan media penyimpanan optik, yang bertujuan untuk menjaga keaslian dan integritas barang bukti baik dari segi fisik maupun digital. Melalui hasil review ini, diharapkan dapat memberikan kontribusi dan informasi yang bermanfaat dalam praktik analisis forensik digital, khususnya pada media penyimpanan optikal seperti CD atau DVD. [7].

Tujuan penelitian adalah untuk mengetahui seberapa baik FTK Imager dan PhotoRec dioperasikan pada flash drive berkapasitas 2 GB. Fokus utama dari penelitian ini adalah jumlah file yang ditemukan, total ukuran data yang berhasil dippulihkan, waktu pemindaian/pemulihan, dan tipe file yang didukung. metode forensik statik diterapkan dalam semua proses akuisisi: perangkat forensik pertama tidak disentuh, gambar forensik dibuat menggunakan media penyimpanan baru yang bersih.[8].

Ada banyak *tools* forensik yang berbeda yang digunakan untuk mendapatkan kembali data yang telah dihapus tersebut. Tools forensik yang biasa digunakan pada media penyimpanan termasuk FTK-Imager, Autopsy, Belkasoft, PhotoRec, dan lainnya[9].

PhotoRec adalah perangkat lunak pemulihan data berkas yang dimaksudkan untuk memulihkan berkas yang hilang, termasuk gambar yang hilang dari memori kamera digital, dokumen, video, dan arsip, serta dari hard disk (Hard Disk Mekanis, Solid State Drive, dll.) dan CD-ROM. PhotoRec mengabaikan sistem berkas dan mencari data yang mendasarinya, sehingga tetap berfungsi meskipun sistem berkas media Anda rusak atau diformat ulang secara signifikan. [10].

Gambar 2. *Tools* PhotoRec

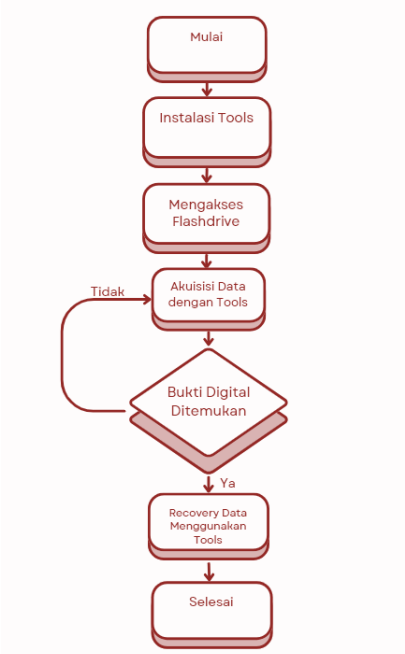
2. Metode Penelitian

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. RegCon digunakan dalam analisis statis berbagai jenis perangkat lunak dan perangkat keras seperti Fundl untuk penyortiran data pembuktian untuk analisis dan presentasi. Dengan menggunakan berbagai jenis perangkat eksternal, seperti USB, *hard drive* eksternal, CD, atau DVD, data forensik diperoleh. Kemudian, para peneliti menggunakan berbagai metode untuk menganalisis data sebagai bukti forensik.[11][12].

Statistik forensik adalah istilah yang mengacu pada penyelidikan forensik tradisional yang dilakukan dengan perangkat yang tidak berfungsi atau tidak aktif. Forensik statis berkonsentrasi pada pemeriksaan duplikat media penyimpanan mengambil data yang ada, seperti riwayat log komputer, riwayat situs web, dan file yang dihapus. Berbagai jenis media penyimpanan eksternal, seperti *flash disk*, *hard drive* eksternal, dan lainnya, dapat digunakan untuk mendapatkan salinan bukti. [13] [14][15]. Ilustrasi pada gambar 3.

Gambar 3. Tahapan pada Statik Forensik

Dalam skenario penelitian ini, seorang wanita muda bernama Lia sedang menjalani program diet dan menggunakan file audio hypnosliming yang disimpan di flash drive-nya sebagai bagian dari metode bantuannya. Namun, secara tidak sengaja, file audio tersebut terhapus dari perangkat penyimpanan. Setelah melakukan pemeriksaan ulang, Lia menyadari bahwa file audio yang baru saja ia coba dengarkan hilang tanpa jejak dan tidak dapat ditemukan lagi di dalam flash drive-nya. Ilustrasi proses akuisisi data yang menggambarkan langkah-langkah untuk mengambil kembali data yang hilang pada penelitian ini dapat dilihat pada Gambar 4.



Gambar 4. *Flowchart* proses *recovery data* pada *flash drive*

Uraian mengenai proses akuisisi data yang dijelaskan melalui flowchart adalah sebagai berikut:

- Melakukan instalasi tools FTK Imager dan PhotoRec: Langkah pertama adalah menginstal kedua perangkat lunak pemulihan data, FTK Imager dan PhotoRec, yang akan digunakan untuk melakukan pemulihan data dari flash drive yang bermasalah. Proses instalasi ini memastikan bahwa kedua tools siap digunakan untuk langkah-langkah selanjutnya.
- Mengakses Flashdrive menggunakan laptop: Setelah instalasi selesai, langkah berikutnya adalah menghubungkan flash drive yang ingin diperiksa ke laptop. Akses ini diperlukan untuk melakukan proses akuisisi data secara langsung dari media penyimpanan yang terkena masalah.
- Mengoperasikan FTK Imager dan PhotoRec untuk akuisisi data pada partisi di flashdrive: Dalam tahap ini, kedua tools, FTK Imager dan PhotoRec, akan digunakan untuk melakukan akuisisi data pada partisi flash drive yang terhubung. Tools ini bekerja untuk mengekstraksi data yang ada di dalamnya, terutama yang terhapus atau hilang.
- Apabila ditemukan bukti digital (file yang terhapus) maka proses recovery dapat dilakukan: Jika selama proses akuisisi ditemukan file yang terhapus atau data yang dapat dipulihkan, proses recovery akan dilanjutkan. Hal ini memungkinkan pemulihan data yang hilang untuk kembali dalam kondisi yang dapat diakses dan digunakan.

Pada penelitian ini, perangkat keras dan perangkat lunak yang digunakan memiliki spesifikasi sebagai berikut:

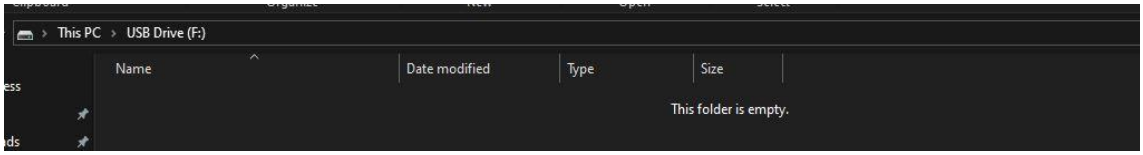
Tabel 1. Spesifikasi *Hardware* dan *Software*

Hardware/Software	Merk/Nama Tools	Spesifikasi/Versi
Laptop	MSI	GF63 Thin
Flash Drive	Toshiba	2GB
Data Recovery Tools	FTK Imager	3.1.2.0.
Data Recovery Tools	PhotoRec	7.3
Sistem Operasi	Windows 10	24H2
Hashing Tools	HashMyFile	2.50

3. Hasil dan Pembahasan

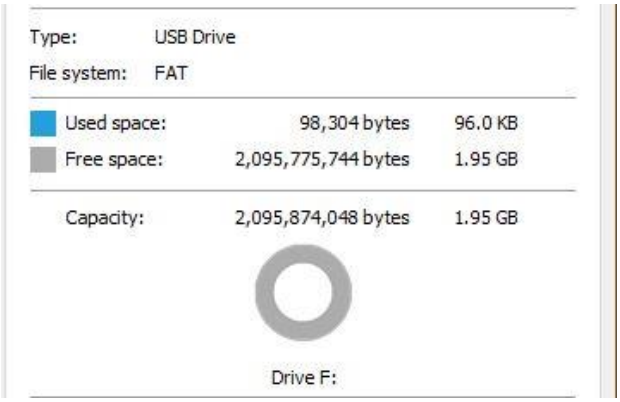
Collection

Saat *flash drive* milik Lia dikoneksikan ke perangkat laptop, tidak ada folder maupun file yang muncul atau dapat diakses melalui tampilan direktori sistem operasi. Kondisi ini menunjukkan bahwa data yang sebelumnya tersimpan di dalam flash drive tidak terlihat oleh sistem secara normal, baik karena terhapus, tersembunyi, atau mengalami kerusakan logis pada struktur penyimpanan. Situasi ini menjadi indikasi awal bahwa diperlukan proses forensik lebih lanjut untuk mengetahui keberadaan atau kemungkinan pemulihan data yang tersembunyi atau terhapus. Tampilan kondisi ini ditunjukkan secara visual pada Gambar 5.



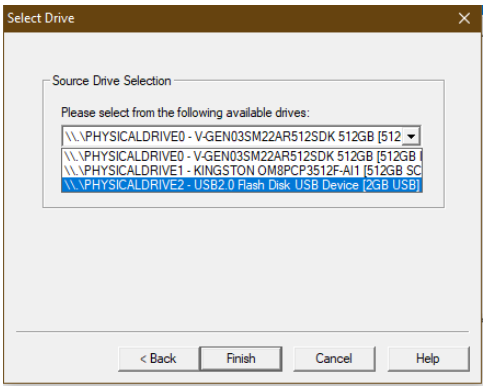
Gambar 5. Flash Drive Kosong

Proses pengecekan kapasitas flash drive dilakukan terlebih dahulu sebelum kegiatan imaging data dimulai, dengan tujuan untuk memastikan bahwa kapasitas penyimpanan perangkat tidak mengalami perubahan, kerusakan, atau manipulasi yang dapat memengaruhi validitas hasil imaging. Langkah ini penting dilakukan guna menjamin keaslian media penyimpanan dan memastikan bahwa seluruh data yang akan di-image benar-benar berasal dari sumber asli tanpa adanya pengurangan atau penambahan ruang penyimpanan. Ilustrasi dari proses ini dapat dilihat pada Gambar 6.



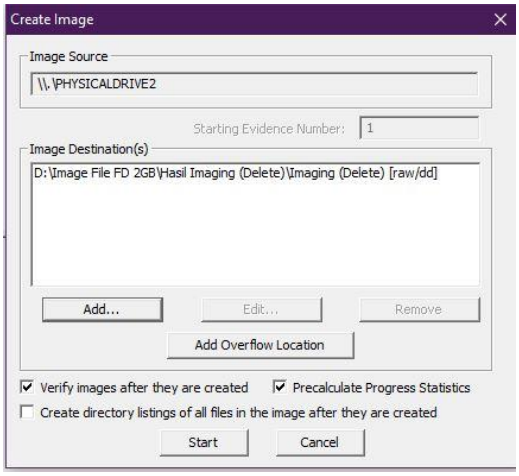
Gambar 6. Kapasitas flash drive

Pada Gambar 7 ditampilkan proses pelaksanaan imaging menggunakan perangkat lunak forensik FTK Imager, di mana langkah awal yang dilakukan adalah memilih media target, yaitu *flash drive* Toshiba berkapasitas 2GB, melalui opsi '*Physical Drive*'. Pemilihan ini dilakukan untuk memastikan bahwa seluruh data, termasuk data tersembunyi, file yang telah dihapus, serta struktur partisi, dapat direkam secara menyeluruh dalam bentuk citra digital (image) yang utuh. Proses ini merupakan bagian penting dalam metode forensik statis, karena bertujuan untuk memperoleh salinan *bit-per-bit* dari media penyimpanan asli tanpa mengubah data sumber.



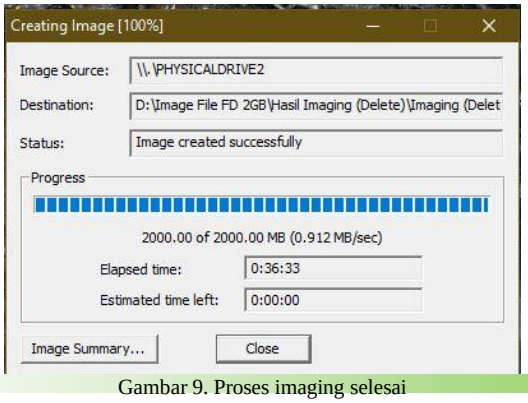
Gambar 7. Pemilihan storage untuk dilakukan proses Imaging Data

Langkah selanjutnya dalam proses imaging adalah menentukan ekstensi atau format file hasil imaging yang akan digunakan. Pada tahap ini, dipilih tipe *raw/dd* sebagai format output, yang merupakan format citra digital mentah yang umum digunakan dalam proses forensik karena tidak melakukan kompresi ataupun enkripsi terhadap data asli. Pemilihan format ini bertujuan untuk menjaga integritas data dan memudahkan kompatibilitas dengan berbagai perangkat lunak forensik lainnya dalam tahap analisis lanjutan. Setelah format ditentukan, proses imaging akan dilanjutkan secara otomatis oleh FTK Imager, seperti yang ditampilkan pada Gambar 8.



Gambar 8. Pemilihan ekstensi file imaging

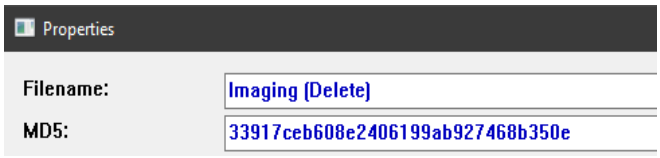
Setelah seluruh parameter dan pengaturan imaging ditentukan, langkah berikutnya adalah menekan tombol *'Start'* untuk memulai proses pembuatan citra digital dari *flash drive*. Proses imaging ini berjalan secara otomatis hingga seluruh sektor pada perangkat tersalin secara menyeluruh ke dalam file *image* berformat *raw/dd*. Dalam pengujian ini, proses tersebut memakan waktu kurang lebih 36 menit dan 33 detik untuk menyelesaikan penyalinan data dari flash drive Toshiba berkapasitas 2GB. Lamanya proses bergantung pada kondisi perangkat, kecepatan sistem, dan jumlah data yang tersembunyi atau sudah terhapus. Visualisasi proses ini dapat dilihat secara jelas pada Gambar 9.



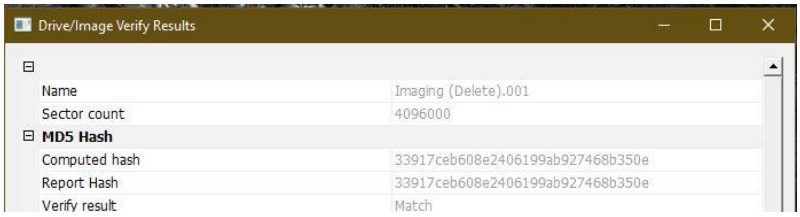
Gambar 9. Proses imaging selesai

Examination

Tahap penting berikutnya setelah proses imaging selesai adalah melakukan dokumentasi terhadap nilai hash dari file hasil imaging. Dokumentasi ini bertujuan untuk memastikan integritas dan keaslian data, sekaligus mencegah terjadinya manipulasi atau perubahan informasi pada file citra digital tersebut. Untuk keperluan ini, digunakan tools tambahan bernama HashMyFile, yang berfungsi untuk menghasilkan nilai hash dari file image menggunakan algoritma tertentu, seperti MD5 Nilai hash yang dihasilkan kemudian dicatat dan dibandingkan secara cermat untuk memastikan bahwa file image yang dianalisis identik dengan data asli yang telah di-*image*. Proses pencocokan hash ini didokumentasikan dan ditampilkan secara rinci pada Gambar 10 dan Gambar 11.

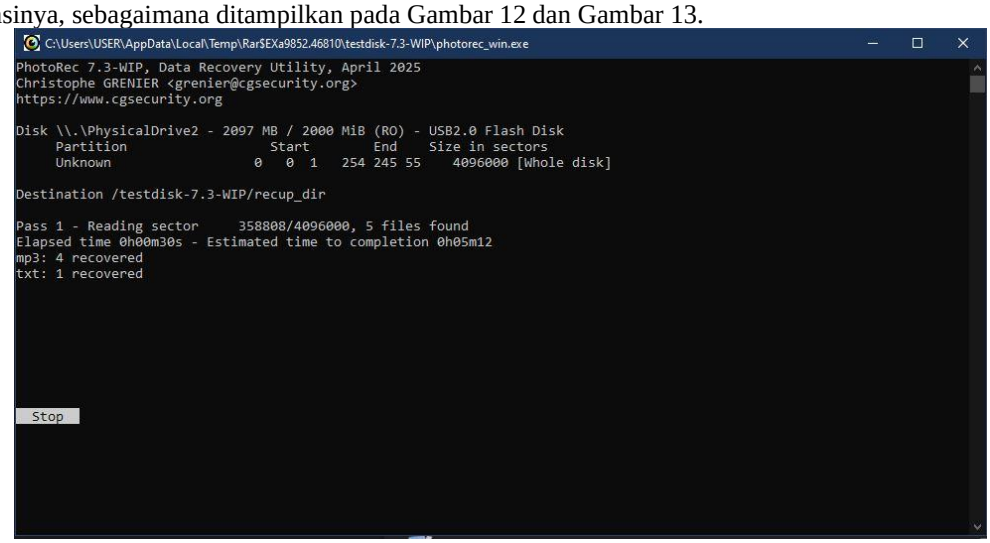


Gambar 10. Nilai Hash dari HashMyFile



Gambar 11. Nilai Hash dari FTK Imager

Kecocokan nilai hash antara file hasil imaging dengan nilai hash awal merupakan indikator utama bahwa proses imaging telah dilakukan dengan benar dan tanpa adanya perubahan atau manipulasi data. Hal ini menjadi landasan penting dalam memastikan bahwa file image yang dihasilkan memiliki validitas dan dapat diterima secara legal sebagai bukti dalam proses forensik digital pada penelitian ini. Setelah integritas data terverifikasi, tahap selanjutnya adalah melakukan proses *recovery* atau pemulihan data dari file image tersebut. Proses ini dilakukan dengan menggunakan dua perangkat lunak forensik, yakni FTK Imager dan PhotoRec, yang masing-masing memiliki pendekatan serta mekanisme kerja yang berbeda dalam mendeteksi dan memulihkan file. Hasil pemulihan data dari kedua tools tersebut kemudian dianalisis dan dibandingkan untuk melihat efektivitas serta akurasinya, sebagaimana ditampilkan pada Gambar 12 dan Gambar 13.

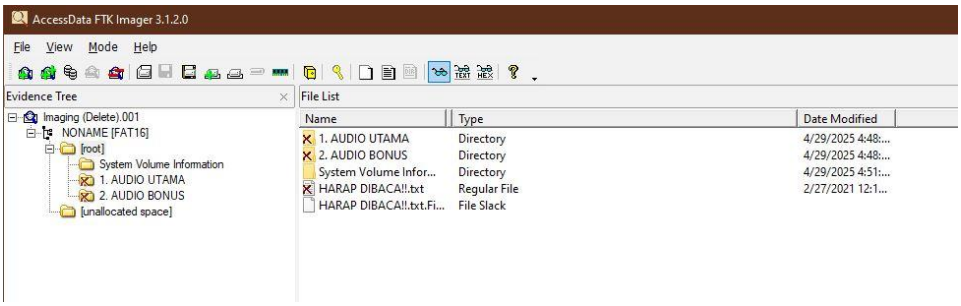


Gambar 12. Hasil Recovery PhotoRec

Analysis

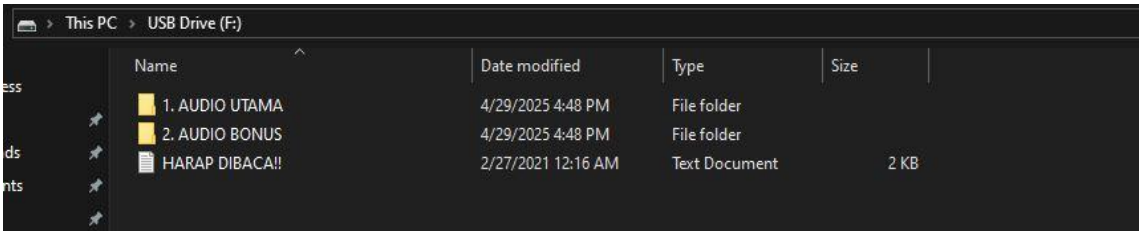
Berdasarkan hasil yang ditunjukkan pada Gambar 12, proses *recovery* menggunakan PhotoRec menghasilkan total lima file, yang terdiri dari empat file berformat .mp3 dan satu file berformat .txt. Meskipun jumlah file yang berhasil dipulihkan cukup signifikan, tidak ditemukan adanya struktur folder atau direktori seperti pada data aslinya. Sebaliknya, pada hasil recovery menggunakan FTK Imager sebagaimana ditampilkan pada Gambar 13, ditemukan struktur data yang lebih lengkap dan terorganisir. FTK Imager berhasil

mengembalikan tiga folder serta dua file di dalamnya, yang menunjukkan kemampuannya dalam mempertahankan struktur asli dari sistem file yang direkonstruksi. Perbedaan ini menunjukkan bahwa FTK Imager memiliki keunggulan dalam memulihkan tidak hanya file individual, tetapi juga konteks penyimpanan aslinya, yang sangat penting dalam analisis forensik digital untuk memahami kronologi dan lokasi data secara lebih akurat



Gambar 13. Hasil recovery FTK Imager

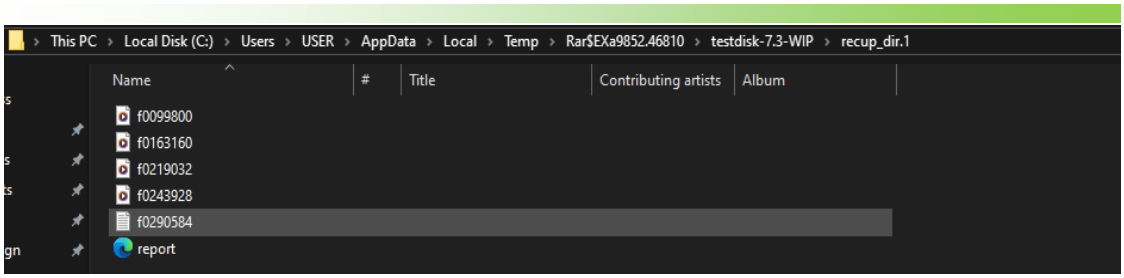
Setelah proses *recovery* selesai dilakukan dan data diekspor, hasil yang diperoleh menunjukkan adanya dua folder yang berhasil dipulihkan beserta satu file teks. Kedua folder yang dipulihkan masing-masing berisi file audio berformat .mp3, dengan total enam file audio yang dapat ditemukan di dalamnya. Hal ini menunjukkan bahwa FTK Imager berhasil mengembalikan tidak hanya file individual, tetapi juga struktur folder yang ada pada media penyimpanan asli, sehingga data yang dipulihkan memiliki susunan yang lebih terorganisir dan mudah untuk dianalisis lebih lanjut. Gambar 14 dan 15 menunjukkan visualisasi dari hasil *recovery* tersebut, yang memperlihatkan bahwa seluruh file dan folder telah dipulihkan dengan baik, dan siap untuk digunakan dalam proses analisis lebih lanjut



Gambar 14. Hasil Eksport recovery file FTK Imager

Gambar 15. File audio dari *flash drive*

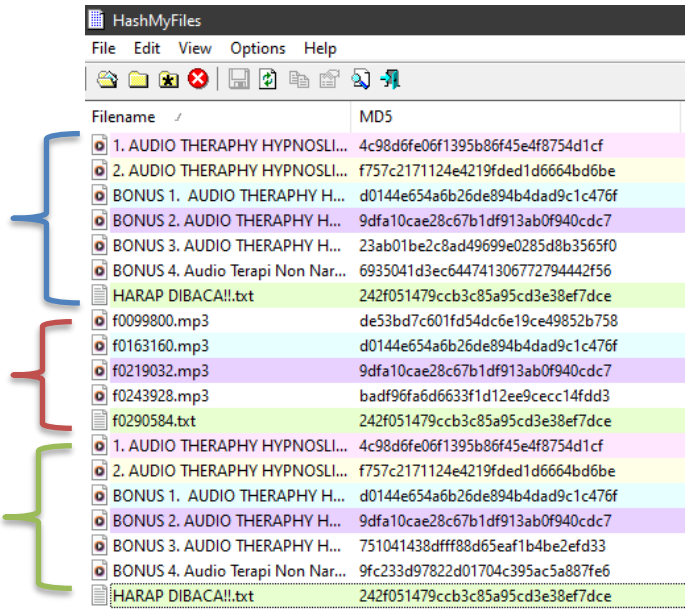
Sebagai perbandingan, hasil *recovery* menggunakan tools PhotoRec disimpan pada folder dengan path "C:\Users\USER\AppData\Local\Temp\Rar$EXa9852.46810\testdisk-7.3-WIP\recup_dir.1". Folder ini berisi file-file yang telah dipulihkan dari media penyimpanan yang teridentifikasi. Meskipun data yang dipulihkan dapat ditemukan, struktur dan organisasi file tidak serapi yang diperoleh dari FTK Imager, dan tidak ada folder atau pengelompokan file yang sesuai dengan struktur aslinya. Gambar 16 menunjukkan hasil ekspor tersebut, yang memperlihatkan file yang berhasil dipulihkan namun dengan penyusunan yang lebih acak, serta penamaan file yang kurang terorganisir, hal ini dapat mempengaruhi efisiensi dalam proses analisis lebih lanjut



Gambar 16. Hasil *Export* dari PhotoRec

Reporting

Tahapan terakhir dalam proses ini adalah mencocokkan nilai hash antara file asli yang ditemukan pada hasil imaging dengan file hasil *recovery* yang diperoleh dari kedua tools, FTK Imager dan PhotoRec. Proses pencocokan ini dilakukan untuk memastikan bahwa data yang telah dipulihkan tidak mengalami perubahan atau kerusakan dan tetap memiliki integritas yang sama dengan data asli. Untuk tujuan ini, digunakan alat HashMyFile yang memungkinkan pengguna untuk menghitung dan membandingkan nilai hash dari masing-masing file, baik file asli maupun file hasil recovery. Proses verifikasi ini sangat penting untuk mengonfirmasi keabsahan dan keakuratan data yang telah dipulihkan. Hasil pencocokan nilai hash ini dapat dilihat secara rinci pada Gambar 17.



Gambar 17. Nilai Hash file asli (biru)dan file hasil recovery dari PhotoRec (Merah) dan FTK Imager (Hijau)

4. Kesimpulan

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa FTK Imager menunjukkan kinerja yang sangat baik dalam proses pemulihan data, berhasil mengembalikan enam file audio dan satu file teks dengan format nama file dan nilai hash yang identik dengan data asli, menunjukkan keandalan dan integritas dalam pemulihan data digital. Sementara itu, PhotoRec, meskipun berhasil memulihkan empat file audio dan satu file teks, menunjukkan perbedaan nilai hash pada dua file audio, yang mengindikasikan adanya ketidaksesuaian atau kerusakan pada sebagian data yang dipulihkan. Hal ini menunjukkan bahwa FTK Imager lebih unggul dalam hal pemulihan data yang lebih akurat dan lengkap dibandingkan dengan PhotoRec. Jika dibandingkan dengan hasil penelitian terdahulu yang menggunakan metode Forensik Statik dan alat pemulihan Disk Drill, yang berhasil mengembalikan lebih dari 7.600 file dengan ukuran total 17,3 GB, dan berbagai jenis file, termasuk audio, dapat disimpulkan bahwa baik FTK Imager maupun Disk Drill memiliki kemampuan pemulihan yang sangat baik. Namun, FTK Imager lebih unggul dalam hal akurasi nilai hash dan integritas data dibandingkan dengan PhotoRec. Penelitian ini mengonfirmasi bahwa pemilihan alat pemulihan yang tepat sangat berpengaruh pada kualitas dan akurasi data yang dipulihkan dalam konteks forensik digital.

5. Daftar Pustaka

[1] David M. Smith, Michael L. Williams (2007). https://www.deepspar.com/wp-data-loss.html.
[2] Muhammad N.F., Rusydi U., Anton Y. Analisis Live Forensics untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary, Jurnal Ilmiah ILKOM. 2016; 8(3):242–247.
[3] K.P. Chow, S. Shenoi, Advances in Digital Forensics VI, IFIP AICT 337 International Federation for Information Processing,2010, pp. 297–311.
[4] M. I. Aulia, P. . Widiandana, L. Iriani, M. F. Gustafi, dan M. A. Hasani, "Penerapan Tool Recovery data dalam Akuisisi Data Forensik Flashdrive: Indonesia", *JOCHAC*, vol. 2, no. 1, hlm. 50–53, Agu 2024.
[5] I. P. A. E. Pratama, "Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept", *International Journal of Science, Technology & Management*, vol. 2, no. 4, pp. 1189-1196, Jul. 2021.
[6] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)", *J. RESTI (Rekayasa Sist. Teknol. Inf.)* , vol. 4, no. 5, pp. 820-828, Oct. 2020.
[7] 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.
[8] Aulia, I. Riadi, and A. Fadlil, "Storage Forensic Optical drive Menggunakan Metode Statik," Semnastek 2019, no. 2013, pp. 756–761, 2019.
[9] PhotoRec By. CGSecurity : https://www.cgsecurity.org/wiki/photoRec
[10] N.A.Muhammad, "Digital Forensik:Panduan Praktis Investigasi Komputer".Jakarta:Salemba Infotek.2012.
[11] Mamoona, R., Khan, M.N.A. "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
[12] I. Riadi, S. Sunardi, S. Sahiruddin, Perbandingan Tool Forensik Data Recovery Berbasis Android menggunakan Metode NIST, Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 7, 2020.
[13] R. N. Dasmen, A. Triwulanda, R. Rasmila, D. Kurniawan, and J. Julia, "Implementation of Digital Forensics Photorec in Recovering Lost Files on External Storage", *PIKSEL*, vol. 12, no. 1, pp. 173–178, Mar. 2024.
[14] Aidil Wijaya Kusuma, Erick Irawadi Alwi, and Ramdaniah Ramdaniah, "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)", *csecurity*, vol. 7, no. 1, pp. 18–24, Nov. 2024.
[15] Abd Rahman Ahmad, "Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 7, Jan. 2023, doi: https://doi.org/10.14569/ijacsa.2023.0140784.