Disk carving untuk *Recovery Solid State Drive* Volume ReFS dan NTFS Dengan Fitur TRIM

Tesis

Muhardinata
20917027

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2024

Lembar Pengesahan Pembimbing

Disk carving untuk *Recovery Solid State Drive* Volume ReFS dan NTFS Dengan Fitur TRIM

Muhardinata

20917027

Yogyakarta, Mei, 2024

Pembimbing I	Pembimbing II
Dr. Ahmad Luthfi, M.Kom	Erika Ramadhani, S.T., M.Eng

Lembar Pengesahan Penguji

Disk carving untuk *Recovery Solid State Drive* Volume ReFS dan NTFS Dengan Fitur TRIM

Muhardinata
20917027

Yogyakarta, Mei, 2024

Tim Penguji,

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

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

Irving Vitra Paputungan, S.T., M.Sc., P.hD
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

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

Abstrak

Tujuan utama dari forensik digital adalah untuk mengumpulkan, mengembalikan, dan menganalisis bukti digital, seperti data dari perangkat penyimpanan seperti *Hard Disk Drive* (HDD), *flashdisk*, *Solid State Drive* (SSD), dan semua perangkat penyimpanan yang terhubung ke laptop atau komputer. Saat ini, teknologi komputer semakin membutuhkan kecepatan yang lebih tinggi dalam membaca dan menyalin data. Salah satu jenis penyimpanan yang populer adalah SSD. *Solid State Drive* memiliki fungsi yang beragam, salah satunya adalah kemampuan untuk memindahkan dan menyimpan data dalam format *New Technology File System* (NTFS). Karena kebutuhan akan integritas data dengan ketahanan terhadap kerusakan dan format NTFS yang telah mencapai batas data yang tersedia, Microsoft mengembangkan file sistem terbaru yang tangguh dalam menangani ketersediaan dan integritas data, yaitu *Resilient File System* (ReFS). ReFS memiliki batas penyimpanan data yang lebih besar dan fitur integritas data yang lebih baik dibandingkan dengan NTFS, yang memiliki batasan penyimpanan sebesar 256 terabyte. Perbedaan antara NTFS dan ReFS ini menyebabkan metadata file sistem menjadi faktor penentu dalam investigasi untuk mengambil data yang telah dihapus dari penyimpanan SSD. Umumnya, akuisisi data dari SSD dilakukan pada file sistem berformat NTFS. Oleh karena itu, diperlukan teknik khusus untuk mengakuisisi SSD dengan file sistem berformat ReFS tanpa mematikan sistem operasi yang sedang berjalan. Sistem operasi yang digunakan dalam penelitian ini adalah Windows 11 Enterprise Versi 21H2, yang sudah mendukung format volume ReFS versi 3.7. Hasil dari penelitian ini adalah perbandingan tingkat keberhasilan *recovery* data dari file sistem NTFS dan ReFS pada SSD. Penelitian ini diharapkan dapat memberikan pemahaman baru dalam melakukan *recovery* bukti digital pada SSD dengan file sistem ReFS dan NTFS, yang akan membantu penyidik dalam menjalankan investigasi digital.

Kata kunci

Teknik *Disk carving*, *Solid State Drive*, ReFS, NTFS

Abstract

The primary purpose of digital forensics is to collect, recover, and analyze digital evidence, including data from storage devices such as Hard Disk Drives (HDDs), flash disks, Solid State Drives (SSDs), and all storage devices connected to laptops or computers. Presently, computer technology demands quicker data reading and copying capabilities. One of the popular storage types is the SSD. The Solid State Drive serves various functions, one of which is the ability to move and store data in the New Technology File System (NTFS) format.Due to the need for data integrity with resilience against damage and the NTFS format reaching its data limit, Microsoft has developed the latest resilient file system, the Resilient File System (ReFS), to manage data availability and integrity. ReFS boasts a larger data storage limit and enhanced data integrity features compared to NTFS, which is constrained by a storage limit of 256 terabytes. The disparities between NTFS and ReFS render file system metadata a pivotal factor in investigations involving the recovery of deleted data from SSD storage.Typically, data acquisition from SSDs is conducted on the NTFS-formatted file system. Therefore, specific techniques are necessary to acquire SSDs with ReFS-formatted file systems without the need to shut down the running operating system. The operating system utilized in this research is Windows 11 Enterprise Version 21H2, which supports ReFS Volume Version 3.7. The outcome of this research is a comparison of the success rates of data recovery from NTFS and ReFS file systems on SSDs. This study aims to provide novel insights into digital evidence recovery on SSDs using ReFS and NTFS file systems, thereby assisting investigators in conducting digital investigations.

Kata kunci

Disk carving Technique, Solid State Drive, ReFS, NTFS

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, Mei, 2024

Muhardinata

v

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

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.

Sitasi Publikasi 1

Kontributor	Jenis Kontribusi
Muhardinata	Mendesain eksperimen (60%) Menulis *paper* (70%)
Ahmad Luthfi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)
Erika Ramadhan	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**".

Halaman Persembahan

Saya persembahkan tesis ini untuk:

“Kedua orang tuaku ”

“Kepada adik ku”

“Kepada kakak yang selalu memberikan semangat”

“Teman-temanku”

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur kami panjatkan kepada Allah SWT, Yang Maha Esa, atas limpahan rahmat, petunjuk, serta anugerah-Nya yang melimpah. Shalawat dan salam senantiasa kami curahkan kepada Nabi Muhammad SAW, sebagai teladan bagi seluruh umat manusia.

Pada kesempatan ini, dengan rasa syukur dan kebahagiaan yang mendalam, kami berhasil menyelesaikan tugas akhir berupa thesis dalam rangka meraih gelar Magister Informatika dari Universitas Islam Indonesia (UII). Proses penulisan thesis ini adalah hasil dari upaya dan dedikasi kami dalam eksplorasi dan pemahaman lebih dalam terhadap ilmu informatika.

Kami ingin mengucapkan terima kasih yang tak terhingga kepada semua pihak yang telah memberikan dukungan, panduan, dan kontribusi selama perjalanan penulisan thesis ini. Terutama kepada Bapak/Ibu Dosen Pembimbing kami, Dr. Ahmad Luthfi, M.Kom dan Erika Ramadhani, S.T., M.Eng., yang telah memberikan bimbingan, arahan, dan dorongan luar biasa selama penulisan thesis ini. Bapak/Ibu adalah sosok yang tidak hanya membagikan pengetahuan dan wawasan, tetapi juga menjadi sumber inspirasi dalam perjalanan kami di dunia akademik. Terima kasih atas kesabaran, motivasi, dan dedikasi yang Bapak/Ibu berikan.

Tak lupa, kami juga ingin menyampaikan rasa terima kasih kepada seluruh dosen dan staf pengajar di Program Studi Magister Informatika UII yang telah memberikan ilmu dan pengalaman berharga kepada kami selama studi di UII. Terima kasih atas komitmen Bapak/Ibu dalam memberikan pendidikan yang berkualitas.

Rasa terima kasih kami juga terpancar kepada keluarga kami yang selalu memberikan dukungan, doa, dan semangat dalam setiap langkah perjalanan kami. Keluarga adalah sumber kekuatan dan inspirasi bagi kami. Terima kasih atas cinta, pengertian, dan dukungan tak terbatas yang Bapak/Ibu berikan.

Kami juga ingin mengucapkan terima kasih kepada teman-teman seangkatan dan sesama mahasiswa di Program Studi Magister Informatika UII. Terima kasih atas *disk*usi, kerja sama, dan pengalaman berharga yang kami bagikan bersama. Semua momen ini telah memberikan warna dan kenangan indah selama studi di UII.

Kami sadar bahwa dalam penelitian ini terdapat keterbatasan dan kekurangan. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun untuk perbaikan di masa depan. Semoga hasil dari thesis ini dapat memberikan sumbangan positif dalam pengembangan ilmu pengetahuan dan teknologi di bidang informatika.

Sebagai penutup, kami ingin mengucapkan terima kasih yang tulus kepada Allah SWT, atas segala rahmat dan karunia-Nya yang telah menyertai perjalanan penyelesaian thesis ini. Semoga segala usaha dan perjuangan kami dapat menjadi amal jariyah yang bermanfaat bagi umat dan bangsa.

Kami berharap bahwa thesis ini dapat memberikan kontribusi kecil dalam pengembangan ilmu pengetahuan dan teknologi, terutama dalam bidang informatika. Semoga hasil penelitian yang kami sajikan dapat memberikan wawasan baru, pemahaman yang lebih mendalam, dan solusi yang relevan dalam menghadapi berbagai tantangan dan permasalahan.

Kami juga berharap bahwa thesis ini dapat menginspirasi peneliti dan akademisi lainnya untuk melanjutkan studi lebih lanjut dan mengembangkan konsep-konsep yang kami ajukan. Kami terbuka untuk kemungkinan adanya penelitian lebih mendalam dan pengembangan yang lebih luas di masa depan.

Terakhir, kami mengucapkan terima kasih kepada semua pihak yang telah turut serta mendukung dan membantu kami dalam perjalanan penyelesaian thesis ini. Semoga semua usaha kami dapat bermanfaat dalam perkembangan ilmu pengetahuan dan teknologi, serta membawa manfaat nyata bagi masyarakat dan bangsa.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

MUHARDINATA
Magister Informatika
Universitas Islam Indonesia (UII)

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

SSD	- *Solid State Drive*
ReFS	- *Resilient File System*
NTFS	- *New Technology File System*
HDD	- *Hard Disk Drive*
AVI	- *Audio Video Interleave*
BMP	- bitmap
3gp	- 3rd generation partnership
DOC	- Document
DOCX	- Document XML
ZIP	- Zoning Improvement Plan
RAR	- Roshal Archive
TXT	- text

BAB 1
Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi yang pesat beriringan dengan perkembangan teknik kejahatan siber. Serangan siber memiliki dampak yang besar pada penyimpanan data ((Lv et al., 2023; Mijwil et al., 2023). SSD adalah salah satu alat penyimpanan yang sering digunakan saat ini (Liu et al., 2022a; Lv et al., 2020). SSD memiliki kelebihan dalam kecepatan transfer data, untuk menjaga kinerja dan perpanjangan masa pakai dibuatlah fitur TRIM (Ramadhan & Mualfah, 2020) . Sisi negatifnya fitur TRIM pada SSD akan menandai file pada blok yang telah using (dihapus permanen) di SSD untuk membersihkan file pada blok-blok yang telah usang, membuat file yang telah dihapus permanen menjadi sulit untuk di*recovery* (Pranoto et al., 2020a). Sistem operasi menggunakan file sistem untuk mengatur file-file pengguna agar mudah untuk diakses. File sistem akan secara langsung berhubungan dengan fitur TRIM di SSD. Objek pada penelitian ini adalah File Sistem NTFS dan ReFS. Perbedaan metadata yang signifikan antara file sistem NTFS dan ReFS membuat proses *recovery* data pengguna menjadi lebih sulit untuk dilakukan (Lee et al., 2021).

Karena metadata dari ReFS sangat berbeda dengan NTFS membuat *tool* konvensional tidak memiliki dukungan untuk membaca file-file yang ada didalam volume ReFS sehingga untuk proses *recovery* dibutuhkan pengembangan untuk membaca file sistem gabungan seperti ReFS (Daghmehchi Firoozjaei et al., 2022). Teknik *disk carving* atau file *carving* bisa digunakan untuk proses *recovery* data yang telah dihapus permanen. *Disk carving* dan file *carving* adalah kemampuan untuk mendapatkan kembali file yang telah dihapus atau disembunyikan pada sebuah medium penyimpanan dengan atau tanpa file sistem (Porter et al., 2021; Sari & Mohamad, 2020). Pada penelitian ini akan menggunakan *tool hetman partition recovery* yang sudah mendukung *recovery* dengan teknik *disk carving*.

Penelitian sebelumnya pernah membahas *recovery* menggunakan *tool* scalpel yang tersedia di linux dengan media penyimpanan *Flashdisk* dan File sistem FAT32 telah membuktikan bahwa data dapat di*recovery* dengan tingkat keberhasilan 100% untuk 20 file dokumen dan 90% untuk file gambar (Yuwono et al., 2019). Penelitian lain yang sejenis juga pernah membahas perbandingan antara *tool* FTKImager, TSK Recover *Tool* dan *tool Foremost Recover*, *TestDisk* lebih unggul di linux dengan media penyimpanan *Flashdisk*

menunjukkan hasil lebih banyak data yang bisa *direcovery* (Abdillah & Prayudi, 2022). Pada penelitian tentang kasus *recovery* disebutkan bahwa metode lama yang digunakan untuk *recovery* data dengan aman pada *Flashdisk* atau HDD yang tidak mendukung TRIM(non SSD) tidak selalu berfungsi pada SSD yang sudah mendukung TRIM, hal ini disebabkan fitur TRIM yang digunakan untuk menjaga tidak terjadi penurunan kinerja SSD dengan cara membersihkan data yang dihapus permanen (Hepisuthar & Priyankasharma, 2021).

Penelitian yang membahas untuk *recovery* tentang SSD yang terfrozen dijadikan barang bukti digital dengan metode *static forensic* menyatakan hasil pemeriksaan dari SSD yang ter-Frozen oleh *software* pembeku *drive* seperti *shadow* defender terbukti berpengaruh tidak semua file bisa diperbaiki sepenuhnya dari 85 file yang bisa diperbaiki sepenuhnya hanya 25 file (Riadi et al., 2018). Penelitian sejenis membahas SSD NVMe file sistem NTFS dengan fungsi TRIM yang *enable* dan *disable*. SSD NVMe dengan fungsi TRIM dijadikan bukti digital dengan metode *live* forensic menyatakan hasil dari *imaging* dengan *tool* FTK Imager Portable dan *tools* test*disk* dapat melakukan *recovery* secara langsung terhadap fungsi TRIM *disable* dan *enable*. Hasil hash MD5 SSD NVMe TRIM *disable* identik sementara TRIM *enable* tidak identik dengan file aslinya. Pada TRIM *disable* dengan *tool* autopsy dan test*disk* data 100% berhasil *direcovery* dan pada *tool* Belkasoft 3% berhasil dipulihkan, sedangkan TRIM *enable* tidak ada file yang dapat *direcovery* secara utuh, sayangnya penelitian ini belum melakukan *recovery* pada file sistem yang berbeda seperti ReFS (Pranoto et al., 2020b).

Metode *live* forensik adalah cara analisa forensik ketika sistem sedang berjalan. Metode yang dilakukan dan teori pendekatannya hampir sama dengan proses forensik statistik atau tradisional, namun pada proses forensik tradisional ketikan sistem mati proses akan terhenti dan bisa membuat ada data yang tidak bisa ditemukan pada proses forensik tradisional. Ini memberikan keunggulan dibandingkan dengan metode forensik tradisional yang tidak memiliki kemampuan untuk mengakses dan menyelidiki komputer dalam kondisi hidup guna menemukan bukti dan informasi yang terkandung di dalamnya. Namun, perlu diingat bahwa terdapat beberapa kerugian dalam menggunakan pendekatan *live* forensik ini. Setiap komputer memiliki sistem operasi yang unik dan lingkungan yang berbeda, yang dapat mengakibatkan perlunya analisis ulang terhadap data mentah yang diperoleh. Selain itu, metode *live* forensik juga memiliki potensi untuk mengganggu integritas barang bukti, terutama jika terjadi kesalahan dalam proses pelaksanaannya.

Pengujian implementasi SSD pada Fitur TRIM *disable* dan *enable* dengan perspektif sistem operasi juga pernah dilakukan dan menunjukkan hasil penelitian yaitu pada konfigurasi TRIM *enable* di windows 11 volume NTFS, Linux Ubuntu volume ext4, dan MacOS Catalina volume APFS tidak ada satu pun file yang bisa di*recovery*. Pada konfigurasi TRIM *disable* di windows 11 volume NTFS 85,7% file berhasil di*recovery*, sedangkan pada Linux Ubuntu volume ext4 dan MacOS Catalina volume APFS tidak ada file yang berhasil di*recovery,* hal ini membuktikan file sistem juga memiliki pengaruh besar dalam kasus *recovery*(Ramadhan & Mualfah, 2020).

Menurut analisis literatur dari penelitian sebelumnya, yang menjadi dasar dukungan untuk penelitian ini, selalu ditemukan pengujian pada *Solid State Drive* (SSD) forensik menggunakan alat-alat yang umum digunakan dalam proses *recovery* data. Sayangnya, penelitian sebelumnya belum berhasil dalam melakukan *recovery* data pada SSD dengan fitur TRIM yang di*enable,* dan hal ini membuktikan bahwa fitur TRIM selalu menjadi tantangan besar dalam dunia forensik. Sementara di sisi perangkat lunak, terus dikembangkan berbagai jenis file sistem dengan metadata yang berbeda guna menunjang kebutuhan perangkat keras.

Oleh karena itu, penelitian ini mencoba menggunakan teknik *disk carving* untuk proses *recovery* data file pada SSD. Objek yang akan diukur dalam penelitian ini adalah file sistem NTFS dan ReFS. Parameter yang akan digunakan dalam penelitian ini meliputi tingkat keberhasilan *recovery* dari teknik *disk carving* terhadap SSD dengan file sistem NTFS dan ReFS.

1.2 Rumusan Masalah

Permasalahan dirumuskan menjadi:

a. Apakah fungsi TRIM *enable* berpengaruh kepada tingkat keberhasilan *recovery* file yang telah dihapus permanen dalam volume NTFS dan ReFS?

b. Apakah SSD volume ReFS dan NTFS bisa dibaca oleh *tool* forensik yang sudah mendukung teknik *disk carving* dan mampu me*recovery* data yang telah dihapus permanen saat TRIM *disable*?

1.3 Tujuan Penelitian

a. Tujuan penelitian ini untuk mengevaluasi pengaruh TRIM *enable* terhadap tingkat keberhasilan *recovery* file yang telah dihapus permanen dalam volume NTFS dan ReFS.

b. Penelitian ini juga bertujuan untuk mengevaluasi apakah SSD yang menggunakan file sistem ReFS dan NTFS dapat diproses oleh *tool* forensik yang mendukung teknik *disk carving*. Tujuannya adalah untuk mengetahui apakah *tool* forensik tertentu seperti hetman dapat mengatasi tantangan dalam pemrosesan file sistem yang berbeda, terutama dalam konteks pemulihan data yang telah dihapus permanen saat TRIM *disable*.

1.4 Batasan Masalah

a. Penelitian ini berfokus pada akurasi *recovery* SSD TRIM terhadap dua format volume berbeda yaitu ReFS dan NTFS.
b. Pada penelitian ini hanya menggunakan teknik *disk carving* untuk melakukan *recovery* dengan *tool* hetman partition *recovery*.
c. Menggunakan metode *live* forensik untuk melakukan akuisisi bertujuan untuk mendapatkan file data yang telah dihapus permanen lebih banyak.

1.5 Manfaat Penelitian

Beberapa manfaat penelitian ini dapat diidentifikasi sebagai berikut:

a. *Optimisasi* keberhasilan *recovery* data: Penelitian ini memberikan wawasan tentang bagaimana pengaturan TRIM *enable* dan *disable* memengaruhi keberhasilan pemulihan data pada file sistem NTFS dan ReFS. Hal ini dapat membantu praktisi forensik dan pengguna SSD untuk mengoptimalkan proses pemulihan data dengan mempertimbangkan pengaturan TRIM.
b. Peningkatan pemahaman tentang file sistem NTFS dan ReFS: Temuan penelitian menggambarkan perbedaan dalam cara file sistem NTFS dan ReFS menangani file-file kecil dan penghapusan data. Ini membantu memperdalam pemahaman tentang karakteristik masing-masing sistem file dan implikasinya terhadap pemulihan data.
c. Evaluasi *tool* forensik: Penelitian ini juga melakukan evaluasi terhadap beberapa alat forensik, seperti FTK Imager dan Hetman Partition Recovery, dalam pemulihan data pada file sistem NTFS dan ReFS. Informasi ini bermanfaat bagi praktisi forensik untuk memilih alat yang sesuai dengan kebutuhan mereka.
d. Identifikasi tantangan teknis: Penelitian mengidentifikasi beberapa tantangan teknis dalam pemulihan data, seperti fragmentasi logis pada file sistem ReFS dan absennya file terfragmentasi pada file sistem NTFS. Ini membantu menyadari area-area di mana alat dan teknik pemulihan data masih perlu ditingkatkan.

BAB 2
Landasan Teori

2.1 Penelitian Terdahulu

Forensika digital merupakan sebuah sub divisi dalam ilmu forensik yang memanfaatkan pengetahuan ilmiah untuk menghimpun, menganalisis, mencatat, dan menyajikan informasi digital yang terkait dengan tindak kejahatan siber di konteks peradilan (Alshumrani et al., 2023). Penyidik memanfaatkan forensika digital dalam menghimpun bukti dari berbagai jenis perangkat digital. Terdapat beragam peralatan dan metode yang dapat diterapkan untuk mencari bukti digital yang cenderung sulit diidentifikasi, termasuk bukti yang telah dihapus, terkunci, atau ter samarkan (Khairunnisak & Widodo, 2023). SSD dan ReFS merupakan tantangan baru dalam digital forensik. Dalam menyelesaikan kasus yang berhubungan dengan SSD format volume NTFS dan ReFS diperlukan teknik *recovery* yang tidak harus menggunakan database metadata file sistem agar membantu mempermudah mengumpulkan barang bukti digital untuk keperluan investigasi. Telah banyak penelitian dalam digital forensik yang membahas tentang *storage* dan file sistem.

Penelitian sebelumnya *Recovery* data file menggunakan *tool* scalpel yang tersedia di linux dengan media penyimpanan *Flashdisk* dan File sistem FAT32 terbukti data dapat di*recovery* dengan tingkat keberhasilan 100% untuk 20 file dokumen dan 90% untuk file gambar (Yuwono et al., 2019). Penelitian lain yang sejenis juga pernah membahas perbandingan antara *tool* FTKImager, TSK Recover *Tool* dan *tool* Foremost Recover, TestDisk lebih unggul di linux dengan media penyimpanan *Flashdisk* menunjukkan hasil lebih banyak data yang bisa *direcovery* menggunakan *tool* dengan teknik file *carving* (Abdillah & Prayudi, 2022). Pada laporan penelitian sebelumnya telah dibahas tentang kasus *recovery* membahas metode lama yang digunakan untuk *recovery* data dengan aman pada *Flashdisk* atau HDD konvensional tidak selalu berfungsi pada SSD. *Solid state drive* memiliki fitur TRIM yang akan memberikan informasi ke sistem untuk menandai kemudian membersihkan blok usang tempat data yang telah dihapus permanen agar kinerja SSD tidak menurun (Hepisuthar & Priyankasharma, 2021).

Dimulailah penelitian untuk *recovery* tentang SSD pada kasus terfrozen dijadikan barang bukti digital dengan metode static forensic menyatakan hasil pemeriksaan dari SSD yang ter-Frozen oleh *software* pembeku drive seperti *shadow defender* terbukti berpengaruh tidak semua file bisa diperbaiki sepenuhnya dari 85 file yang bisa diperbaiki sepenuhnya

hanya 25 file, penelitian ini belum membahas tentang pengaruh fungsi TRIM terhadap kasus *recovery* file dari SSD (Riadi et al., 2018).

Penelitian selanjutnya SSD NVMe menggunakan file sistem NTFS dengan fungsi TRIM yang *enable* dan *disable*. SSD NVMe dengan fungsi TRIM tersebut dijadikan bukti digital dengan metode *live* forensic menyatakan hasil dari *imaging* dengan *tool* FTK Imager Portable dan *tools* test*disk* dapat melakukan *recovery* secara langsung terhadap fungsi TRIM *disable* dan *enable*. Hasil hash MD5 SSD NVMe TRIM *disable* identik sementara TRIM *enable* tidak identik dengan file aslinya. Pada TRIM *disable* dengan *tool* autopsy dan test*disk* data 100% kemudian pada *tool* Belkasoft 3% berhasil dipulihkan sedangkan TRIM *enable* tidak ada satupun data dapat dipulihkan, penelitian ini berfokus pada metode *live* forensik kemudian pada penelitian ini menyebutkan dibutuhkan analisis hasi*l recovery* pada file sistem yang berbeda metadata seperti ReFS (Pranoto et al., 2020a).

Metode *live* forensik adalah cara analisa forensik ketika sistem sedang berjalan. Metode yang dilakukan dan teori pendekatannya hampir sama dengan proses forensik statistik atau tradisional, namun pada proses forensik tradisional ketikan sistem mati proses akan terhenti dan bisa membuat ada data yang tidak bisa ditemukan pada proses forensik tradisional. Pelaksanaan *live* forensik dilakukan saat perangkat komputer atau barang bukti masih dalam keadaan aktif. Ini memberikan keunggulan dibandingkan dengan metode forensik tradisional yang tidak memiliki kemampuan untuk mengakses dan menyelidiki komputer dalam kondisi hidup guna menemukan bukti dan informasi yang terkandung di dalamnya. Namun, perlu diingat bahwa terdapat beberapa kerugian dalam menggunakan pendekatan *live* forensik ini. Setiap komputer memiliki sistem operasi yang unik dan lingkungan yang berbeda, yang dapat mengakibatkan perlunya analisis ulang terhadap data mentah yang diperoleh. Selain itu, metode *live* forensik juga memiliki potensi untuk mengganggu integritas barang bukti, terutama jika terjadi kesalahan dalam proses pelaksanaannya.

Pengujian implementasi SSD pada Fitur TRIM *disable* dan *enable* dengan perspektif sistem operasi juga dilakukan menunjukkan hasil penelitian yaitu pada konfigurasi TRIM *enable* di windows 11 volume NTFS, Linux Ubuntu volume ext4, dan MacOS Catalina volume APFS tidak ada satupun file yang bisa *direcovery*. Pada konfigurasi TRIM *disable* di windows 11 volume NTFS 85,7% file berhasil di*recovery*, sedangkan pada Linux Ubuntu volume ext4 dan MacOS Catalina volume APFS tidak ada file yang berhasil di *recovery*, penelitian ini sudah menguji pengaruh pada fitur TRIM di berbagai sistem operasi dengan

berbagai file sistem dan belum berhasil melakukan *recovery* pada file sistem yang berbeda metadata seperti ext4 dan APFS (Ramadhan & Mualfah, 2020). Menurut analisis literatur dari penelitian sebelumnya, yang menjadi dasar dukungan untuk penelitian ini, selalu ditemukan pengujian pada *Solid State Drive* (SSD) forensik menggunakan alat-alat yang umum digunakan dalam proses *recovery* data. Sayangnya, masih sedikit penelitian sebelumnya yang membahas pengaruh antara file sistem dan fitur TRIM SSD pada tingkat keberhasilan *recovery* file yang telah dihapus permanen, selain itu peneliti sebelumnya belum berhasil me*recovery* SSD dengan file sistem yang berbeda metadata. Penelitian ini diharapkan dapat memberikan referensi untuk penyidik pada kasus SSD dan file sistem. Tabel 2.1 – 2.2 akan mengulas lebih detail tema-tema penelitian yang berkaitan dengan penelitian ini.

Tabel 2.1 Ulasan Kritis Tema

No.	Peneliti	Tujuan	Pendekatan/Metode Penelitian	Area Penelitian	Hasil Penelitian
1.	(Yuwono et al., 2019)	Perbandingan *tool* scaple, foremost dan autopsy untuk *recovery*	Pendekatan teknik akuisisi NIST dan untuk melakukan *recovery* menggunakan teknik file *carving*.	*Recovery* pada *Flashdisk* file sistem FAT 32	Scaple menunjukkan akurasi tertinggi file data dapat di*recovery* dengan tingkat keberhasilan 100% untuk 20 file dokumen dan 90% untuk file gambar.
2.	(Soni et al., 2019)	Implementasi *framework* SNI untuk mengakuisisi mesin virtual server	Metode akuisisi *live forensics*	mesin virtual	Pada penelitian ini menunjukkan metode SNI 27037:2014 bisa digunakan untuk melakukan akuisisi penyimpanan pada mesin virtual.
3.	(Hepisuthar & Priyankasharma, 2021)	Melakukan studi perbandingan antara SSD, HDD, dan SSHD	Pendekatan penelitian ini berdasarkan pada perangkat keras berfokus pada bagian komponen PCB dan perangkat lunak berfokus pada fitur yang mendukung kinerja penyimpanan seperti TRIM dan *garbage collection.*	SSD, HDD, SSHD	menunjukkan bahwa SSD tidak menjalankan penyimpanan data seperti HDD. SSD menggunakan fitur TRIM dan *garbage collection* karena setiap bit data disimpan dalam *floating gate transistor rather*, sementara HDD hanya perlu menimpa data lama dengan data baru karena menggunakan piringan magnetik untuk menyimpan data.
4.	(Pranoto et al., 2020a)	Pemeriksaan dan analisis pada SSD NVMe dengan fitur TRIM	*live forensics*	SSD dengan fitur TRIM pada file sistem NTFS	Dengan beragam *tool* pada TRIM *disable* data file 100% berhasil dipulihkan sementara saat TRIM *dienable* data file 0% berhasil dipulihkan.

Tabel 2.2 Ulasan Kritis Tema (Lanjutan)

No.	Peneliti	Tujuan	Pendekatan/Metode Penelitian	Area Penelitian	Hasil Penelitian
5.	(Lee et al., 2021)	Membandingkan cara kerja file sistem NTFS dan ReFS dalam merekam perubahan data file.	*Revers enginering*	ReFS *journaling* dan file log	Diketahui bahwa artefak dari ReFS terkait melakukan rekam perubahan pada suatu file sangat berbeda dengan yang dimiliki NTFS. NTFS menggunakan $Logfile dan $UsnJrnl sementara ReFS menggunakan Log Record dan USN_RECORD_V3 sebagai data base yang mencatat perubahan yang terjadi pada satu file.
6.	(Ramadhan & Mualfah, 2020)	Penelitian ini bersifat eksperimental bertujuan untuk mengetahui pengaruh fitur TRIM di berbagai sistem operasi	NIJ	SSD TRIM objek eksperimental sistem operasi windows, linux dan macintos	Penelitian ini berhasil membuktikan dengan metode NIJ bahwa Fitur TRIM akan memiliki pengaruh besar pada kasus forensik *recovery* data file. Dari sistem operasi windows, linux dan macintos tidak ada file yang bisa dipulihkan saat fitur TRIM *enable*.
7.	(Fatmah & Indrayani, 2022)	Menganalisa pengaruh fitur TRIM dengan *tools* autopsy dan OSForensics untuk kebutuhan *recovery*.	SNI Acquisition 27037:2014	*Recovery* SSD TRIM	Penelitian ini membuktikan bahwa fitur TRIM memiliki pengaruh besar dibuktikan dengan *tool* autopsy dan OSForensics belum berhasil *recovery* file pada SSD dengan TRIM yang di*enable*.
8.	(Abdillah & Prayudi, 2022)	Perbandingan Data *Recovery* Menggunakan *Tools* Forensik Berbasis Open Source Pada Linux	*Live* forensic	*Recovery Flashdisk*	Penelitian ini menunjukkan kinerja *tool* yang menggunakan metode Foremost Recover dan Test*Disk* lebih unggul, sayangnya belum dibahas tentang kasus *Recovery* pada fitur TRIM dari SSD yang akan mempengaruhi keberhasilan *recovery* secara signifikan.

2.2 Konsep Pengetahuan

2.2.1 Digital Forensik

Digital forensik merujuk pada rangkaian prosedur untuk mengumpulkan, mengidentifikasi, mengekstraksi, dan mendokumentasikan bukti elektronik dari berbagai peranti elektronik, yang nantinya dapat digunakan sebagai bukti yang sah dalam proses hukum (Salih & Ibrahim, 2023). Proses digital forensik umumnya dibagi menjadi empat tahapan utama, yang membantu para profesional forensik digital dalam mengumpulkan, menganalisis, dan menyajikan bukti digital (Freiling et al., 2018), Keempat tahapan tersebut adalah :

1. Pengumpulan Informasi (*Acquisition*):

   Pada tahap ini, ahli forensik digital mengumpulkan semua informasi yang relevan dari berbagai sumber, seperti perangkat keras, perangkat lunak, jaringan, dan dokumen terkait. Pengumpulan informasi harus dilakukan dengan hati-hati dan tanpa merusak data asli.

2. Analisis (*Analysis*):

   Tahap analisis melibatkan pemeriksaan mendalam terhadap data yang dikumpulkan untuk mengidentifikasi bukti digital yang signifikan. Ini mencakup *recovery* data yang terhapus, identifikasi aktivitas yang mencurigakan, dan rekonstruksi peristiwa yang terjadi. Metode analisis dapat mencakup teknik-teknik seperti pemeriksaan file, analisis register sistem, dan *recovery* metadata.

3. Identifikasi (*Identification*):

   Pada tahap ini, ahli forensik digital mengidentifikasi dan menetapkan bukti yang relevan dari hasil analisis. Identifikasi dapat mencakup pengenalan pola, pencocokan data, dan pembuatan hubungan antar berbagai elemen bukti. Proses identifikasi membantu dalam memahami kronologi kejadian dan hubungan antar entitas digital yang terlibat.

4. Pemaparan (*Presentation*):

   Tahap pemaparan melibatkan penyajian temuan forensik secara jelas dan komprehensif. Ahli forensik perlu menyusun laporan forensik yang rinci, termasuk metodologi yang digunakan, temuan utama, dan kesimpulan. Laporan ini harus disusun sedemikian rupa sehingga dapat dimengerti oleh pihak yang tidak memiliki latar belakang teknis. Pemaparan juga dapat melibatkan kesaksian di pengadilan jika hasil forensik digunakan sebagai bukti dalam proses hukum. Keempat tahapan ini membantu memastikan bahwa proses digital forensik dilakukan secara sistematis, akurat, dan dapat diterima sebagai bukti di pengadilan atau dalam konteks investigasi lainnya.

Dalam ranah digital forensik, proses *recovery* file yang telah dihapus permanen memiliki peran penting dalam mengungkap bukti-bukti krusial yang dapat digunakan dalam proses hukum. Berbagai teknik dan metode telah dikembangkan untuk memfasilitasi proses ini. Dalam penelitian sebelumnya, ditemukan bahwa teknik *recovery* file, seperti *disk carving,* telah berhasil dalam mengembalikan data yang secara sengaja dihapus dari sistem penyimpanan digital (Abdillah & Prayudi, 2022; Yuwono et al., 2019). Selain itu, analisis terhadap jurnal (journaling) file sistem juga telah menunjukkan efektivitasnya dalam mendapatkan informasi terkait sejarah penghapusan file yang dapat mendukung proses *recovery* (Lee et al., 2021). Namun, terdapat keterbatasan tertentu terkait dengan keefektifan teknik jurnal file sistem, terutama ketika berhadapan dengan sistem file yang kompleks dan format penyimpanan yang lebih baru.

2.2.2 *Live* Forensik

Dalam praktiknya, *Live* Forensik melibatkan penggunaan teknik dan alat yang dapat mengidentifikasi, mengekstraksi, dan menganalisis data yang masih tersimpan dalam sistem aktif, termasuk data yang telah dihapus. Dengan menggunakan teknik *Live* Forensik, analis dapat mengakses area memori yang sedang digunakan oleh sistem operasi, serta melakukan *monitoring* terhadap aktivitas sistem saat ini. Proses ini memungkinkan untuk mendapatkan akses langsung ke data yang tidak dapat diakses melalui metode forensik tradisional (Rahman & Khan, 2015).

Namun, *Live* forensik memiliki beberapa keterbatasan, terutama terkait dengan kemungkinan gangguan terhadap integritas bukti digital dan keakuratan analisis. Kecenderungan setiap sistem komputer memiliki lingkungan yang berbeda-beda bisa menjadi tantangan dalam melakukan analisis ulang terhadap data mentah yang diperoleh. Selain itu, terdapat risiko potensial dalam hal memodifikasi atau mengubah data selama proses ekstraksi yang dapat mengurangi keabsahan bukti digital di pengadilan. Oleh karena itu, penggunaan teknik *Live* Forensik harus dilakukan dengan hati-hati dan memperhatikan pedoman serta prosedur yang berlaku dalam praktik forensik digital (Pradhana et al., 2021).

2.2.3 SNI 37037:2014

SNI 27037:2014, berjudul "Teknologi Informasi – Teknik Keamanan – Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital," merupakan standar forensik digital yang mengadopsi secara keseluruhan isi dokumen dari ISO 27037:2012

dengan metode *republikasi-reprint* (Pranoto et al., 2020a). Dengan demikian, standar nasional Indonesia ini mencakup pedoman dan prosedur yang sama seperti ISO 27037:2012 dalam hal identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital. Metode *republikasi-reprint* menunjukkan bahwa isi dokumen tersebut diterapkan kembali tanpa perubahan signifikan, sehingga konsistensi dengan standar internasional dapat dipertahankan.

Penanganan bukti digital, termasuk aktivitas Identifikasi, Pengumpulan, Akuisisi, dan Preservasi. Semua langkah ini merupakan tahap-tahap krusial yang memerlukan penanganan hati-hati guna memastikan integritas bukti tetap terjaga. Metodologi yang diterapkan dalam proses pengumpulan barang bukti digital memiliki dampak signifikan terhadap validitas penerimaan bukti di pengadilan. Selain memfokuskan pada bukti digital, standar ini juga mencakup pedoman umum untuk mengumpulkan bukti non-digital, yang nantinya akan mendukung analisis barang bukti digital yang potensial.

SNI ini mengidentifikasi empat peran utama dalam keseluruhan proses investigasi forensik digital, yaitu *Digital Evidence First Responder (DEFRs), Digital Evidence Specialist (DESs), Incident Response Specialist, dan Forensic Laboratory Managers*. Standar ini bertujuan untuk memberikan jaminan dan panduan kepada keempat aktor tersebut, memastikan manajemen bukti yang efektif, sehingga metodologi yang diterapkan dapat diakui dan diterima secara global.

Menurut SNI 27037:2014, identifikasi merupakan proses holistik yang mencakup pencarian, pengenalan, dan dokumentasi seluruh potensi barang bukti digital. Proses identifikasi harus secara spesifik mengenali media penyimpanan digital dan perangkat pemrosesan yang mengandung bukti digital yang relevan dalam suatu kasus. Proses ini juga mencakup kegiatan yang memberikan prioritas pada barang bukti yang dikumpulkan berdasarkan tingkat volatilitas atau kerentanan bukti digital terhadap kerusakan atau kehilangan data yang memiliki volatilitas tinggi, atau mudah rusak dan hilang, harus diidentifikasi untuk memastikan prioritas utama dalam proses pengumpulan dan akuisisi. Tujuannya adalah untuk meminimalkan kerusakan terhadap barang bukti digital yang potensial dan memastikan akuisisi bukti yang optimal.

Dalam konteks pengumpulan, SNI 27037:2014 menjelaskan bahwa pengumpulan adalah proses penanganan barang bukti digital di mana peralatan yang diindikasikan sebagai barang bukti potensial dipindahkan dari lokasi kejadian ke laboratorium atau lokasi

terkendali lainnya untuk diakuisisi dan dianalisis. Proses ini mencakup pemisahan peralatan hidup dan mati di lokasi kejadian karena tindakan yang diperlukan dapat bervariasi.

Proses pengumpulan juga memerlukan dokumentasi yang teliti, termasuk pemayetan atau pembungkusan barang bukti untuk pengiriman ke laboratorium. Penting bagi petugas *First Responder* untuk menjalankan proses ini dengan hati-hati, termasuk pengumpulan barang bukti potensial seperti kertas yang diindikasikan sebagai *password*, karena barang bukti dapat hilang jika tidak ditangani dengan cermat.

Tahap selanjutnya adalah akuisisi, yang SNI 27037:2014 menggambarkan sebagai proses pembuatan salinan barang bukti digital dan dokumentasi metodologi serta kegiatan yang dilakukan. Petugas akuisisi harus memilih metode sesuai dengan situasi, biaya, dan waktu, serta mendokumentasikan keputusan tersebut. Metode yang dipilih harus dapat di replikasi dan diverifikasi untuk memastikan hasil salinan identik dengan barang bukti asli. Dalam situasi di mana verifikasi tidak mungkin dilakukan, seperti saat terjadi kesalahan sektor selama proses akuisisi, petugas harus memilih metode untuk melakukan akuisisi ulang, mendokumentasikannya, dan memberikan justifikasi atas keputusan tersebut. Jika tidak memungkinkan atau tidak diperbolehkan untuk membuat salinan utuh dari barang bukti asli, misalnya karena ukuran sumber data yang besar, izin *logical acquisition* diberikan. Metode ini hanya membuat salinan data tertentu, folder, atau lokasi tertentu, dengan memperhatikan bahwa data yang terhapus atau di *unallocated space* tidak akan ikut tersalin. *Logical acquisition* juga dapat diterapkan pada sistem yang tidak boleh dimatikan.

Tahap berikutnya yang diatur oleh SNI 27037:2014 adalah preservasi. Menurut standar ini, preservasi adalah proses untuk melindungi barang bukti digital dan perangkat digital yang berpotensi mengandung bukti digital dari kerusakan atau kehilangan. Proses preservasi harus dimulai sejak identifikasi perangkat digital yang memuat bukti digital potensial hingga seluruh proses penanganan barang bukti digital (Sudyana et al., 2023).

2.2.4 *Teknik Carving*

Disk Carving atau *Carving* file adalah teknik dalam bidang forensik digital yang digunakan untuk mengembalikan atau *recovery* data yang hilang atau terhapus dari suatu media penyimpanan, seperti hard drive, SSD, atau kartu memori. Teknik ini memungkinkan analis forensik untuk mengidentifikasi dan merekonstruksi file yang telah dihapus, baik secara sengaja maupun tidak sengaja. *Carving* file bekerja dengan cara mencari pola karakteristik tertentu yang menunjukkan adanya file yang hilang atau terhapus di dalam media

penyimpanan (Povar & Bhadran, 2011; Sari & Mohamad, 2020). Perbandingan kinerja perangkat lunak forensik sumber terbuka dalam pengambilan data, seperti Scalpel, Foremost, dan Autopsy, telah dilakukan menggunakan metode National Institute of Standards Technology (NIST). Proses pengujian dilaksanakan melalui teknik file *carving*, dan evaluasi dilakukan berdasarkan tingkat keberhasilan (akurasi) alat forensik. Scalpel menggunakan teknik *carving* file dengan pengindeksan *header* dan *footer*, serta menerapkan algoritma pencocokan ulang. Sementara itu, Foremost hanya melakukan pencarian berdasarkan potongan memori tanpa menerapkan algoritma pencocokan ulang. Autopsy, di sisi lain, dapat mengembalikan file sesuai dengan versi aslinya sebelum hilang, namun tidak memiliki kemampuan untuk memperbaiki file yang rusak (Yuwono et al., 2019).

Proses *carving* file melibatkan pencarian dan ekstraksi data berdasarkan pola karakteristik khusus, seperti *header* file atau tanda tangan tertentu yang mengidentifikasi awal atau akhir dari suatu file. Teknik ini memungkinkan untuk mendapatkan kembali file yang telah dihapus bahkan jika informasi metadata telah terhapus atau rusak. Dengan menggunakan algoritma khusus, analis dapat mengumpulkan potongan-potongan data yang tersebar di media penyimpanan dan kemudian menggabungkannya kembali untuk *recovery* file yang hilang secara keseluruhan (Sari & Mohamad, 2020). selain *teknik carving* terdapat teknik lain yang bisa digunakan untuk *recovery* data antara lain adalah sebagai berikut:

1. *Recovery* dengan *Backup*: Teknik ini melibatkan penggunaan salinan data yang disimpan di lokasi terpisah sebagai sumber *recovery* jika data asli hilang atau rusak. *Backup* biasanya termasuk dalam strategi *recovery* data yang terencana dan terjadwal.
2. *Recovery* dengan *Disk Imaging*: Teknik ini melibatkan pembuatan salinan (image) dari media penyimpanan yang rusak atau terformat. Dengan menggunakan image ini, teknisi IT dapat mencoba *recovery* data dari salinan tersebut tanpa merusak data asli.
3. *Recovery dari Backup Cloud*: Jika data disimpan di layanan *cloud* dengan fitur *backup*, *recovery* dapat dilakukan dengan mengunduh kembali data dari penyimpanan *cloud*.

Carving merupakan salah satu teknik yang sangat penting dalam praktik forensik digital, terutama ketika data penting atau bukti yang relevan telah dihapus atau disamarkan oleh pelaku kejahatan. Namun, penting untuk diingat bahwa proses *carving* memerlukan keahlian teknis yang mendalam dan pemahaman yang baik tentang struktur file, sehingga memerlukan penggunaan perangkat lunak dan alat forensik digital yang canggih untuk mendukung proses tersebut. Dalam praktiknya, teknik *carving* sering digunakan sebagai metode terakhir untuk *recovery* data yang hilang ketika teknik lain, seperti *recovery* dengan

Backup, telah gagal memberikan hasil yang memadai (Porter et al., 2021; Sadikin & Sari, 2020).

Sejumlah faktor memengaruhi kinerja alat forensik dalam proses *carving* (Abdillah & Prayudi, 2022; Jupriadi Fakhri et al., 2023), antara lain:

1. Jenis sistem berkas yang diterapkan pada media penyimpanan yang akan *dicarving*.
2. Besarnya media penyimpanan yang akan *dicarving*.
3. Keadaan media penyimpanan yang akan *dicarving*, apakah masih dalam kondisi optimal atau telah mengalami kerusakan.
4. Kualitas algoritma yang dimanfaatkan oleh alat forensik dalam melaksanakan pengcarvingan berkas.
5. Kapabilitas alat forensik dalam menangani berkas yang terfragmentasi atau terhapus secara tidak utuh.
6. Tingkat kecepatan dalam proses *recovery* berkas, keandalan jumlah berkas yang berhasil dipulihkan, dan persentase keakuratan berkas yang dipulihkan.

Terdapat perbedaan penting dalam proses *disk carving* antara SSD (Solid-State Drive) dan *hard drive* tradisional berbasis piringan magnetik (non-SSD). SSD menggunakan teknologi penyimpanan *flash memory* dengan struktur internal yang kompleks dan metode pengelolaan data yang berbeda, seperti pengoptimalan dan *redistribusi* data otomatis, serta memiliki teknik penghapusan data melalui fitur TRIM yang dapat mempengaruhi proses *disk carving* dengan kemungkinan sulitnya pemulihan data yang telah dihapus. Di sisi lain, *hard drive* tradisional memiliki struktur sederhana dengan sektor-sektor fisik yang dapat diakses langsung, serta tidak memiliki fitur khusus seperti TRIM pada SSD, sehingga data yang dihapus masih dapat dipulihkan dengan teknik *disk carving*, terutama jika sektor-sektor tersebut belum ditulis ulang dengan data baru (Hepisuthar & Priyankasharma, 2021). Selain itu, SSD memiliki kinerja yang lebih cepat dan kompleksitas fragmentasi data yang tinggi dibandingkan *hard drive*, yang dapat memengaruhi proses pemindaian dan pemulihan data saat melakukan *disk carving* (Alghafli & Martin, 2016; Munegowda et al., 2014).

2.2.5 *Solid State Drive*

Solid State Drive (SSD) adalah jenis media penyimpanan data non-volatile yang digunakan dalam berbagai perangkat elektronik, termasuk laptop, komputer desktop, dan perangkat mobile. Berbeda dengan *Hard Disk Drive* (HDD) yang menggunakan piringan magnetik berputar, SSD menggunakan sirkuit terpadu semikonduktor untuk menyimpan data secara

elektronik. Teknologi SSD telah mendapatkan popularitas karena kecepatan akses data yang lebih tinggi, waktu respons yang lebih cepat, dan ketahanan fisik yang lebih baik dibandingkan dengan HDD konvensional (Liu et al., 2022b) .

SSD terdiri dari sejumlah *chip* memori *flash* NAND (Not AND) yang digunakan untuk menyimpan data. *Chip* memori *flash* ini dapat mengakses data dengan kecepatan tinggi dan secara efisien, tanpa ada pergerakan mekanis yang diperlukan seperti pada HDD. Selain itu, SSD cenderung lebih tahan terhadap kejutan fisik dan getaran, karena tidak memiliki komponen bergerak yang rentan terhadap kerusakan. Hal ini membuat SSD menjadi pilihan utama dalam banyak aplikasi yang membutuhkan kinerja tinggi dan keandalan, seperti dalam lingkungan komputasi berat, server, dan perangkat mobile (Geier, 2015).

Namun, seperti halnya teknologi penyimpanan lainnya, SSD juga memiliki kelemahan, salah satunya terkait dengan masa pakai terbatas dari *chip* memori *flash* NAND yang digunakan. Proses penulisan ulang berulang pada *chip* memori *flash* dapat mengurangi umur SSD secara keseluruhan. Selain itu, SSD juga memiliki beberapa tantangan khusus dalam praktik forensik digital, terutama terkait dengan fitur TRIM yang secara permanen menghapus data yang tidak terpakai, sehingga mempengaruhi kemampuan *recovery* data yang telah dihapus dari SSD (Hepisuthar & Priyankasharma, 2021).

Meskipun demikian, keunggulan-keunggulan yang ditawarkan oleh SSD dalam hal kinerja dan keandalan telah menjadikannya sebagai salah satu pilihan utama dalam industri penyimpanan data modern. Dengan terus berkembangnya teknologi, SSD akan terus mengalami peningkatan dalam hal kapasitas, kecepatan, dan ketahanan, serta terus memainkan peran penting dalam mendukung aplikasi-aplikasi yang membutuhkan kinerja tinggi dan akses data yang cepat. Berdasarkan penelitian, meskipun SSD memiliki keunggulan dibanding HDD, namun ketika data dihapus secara permanen, integritas data sulit dipertahankan. Hal ini disebabkan oleh proses pembersihan menggunakan fitur TRIM pada SSD, sehingga menyulitkan penyelidikan forensik dalam beberapa kasus (Fatmah & Indrayani, 2022).

Pada SSD yang dilakukan frozen data dengan *shadow* defender memiliki pengaruh yang sama dengan fitur TRIM *enable* setelah dilakukan *recovery* dan perbandingan keberhasilan *recovery* dengan teknik statistik forensik ada sebagian file yang tidak berhasil di*recovery* (Riadi et al., 2018). SSD dengan konektor M.2 memiliki kecepatan dalam transfer data karena terhubung langsung dengan *motherboard* dengan teknik live forensik berhasil *recovery* sejumlah file saat fitur TRIM *enable* tetapi saat TRIM *disable* tidak terdapat data

yang berhasil di*recovery* (Pranoto et al., 2020a). Ini menunjukkan bahwa fitur TRIM membersihkan data yang telah dihapus permanen. Dalam penelitian terbaru terkait SSD forensik, diketahui bahwa SSD dengan file sistem berbeda memiliki pengaruh besar terhadap keberhasilan *recovery* data, ditunjukkan bahwa setiap file sistem pada sistem operasi yang berbeda saat *setting* TRIM *enable* tidak ada data yang berhasil di*recovery* sedangkan pada TRIM *disable* hanya file sistem NTFS yang menunjukkan tanda keberhasilan *recovery* yaitu dengan melakukan pencocokan nilai hash (Ramadhan & Mualfah, 2020). Selain itu terdapat beberapa tahapan yang dilakukan SSD memiliki efek yang negatif untuk proses forensik *recovery* salah satunya TRIM *Command*, pada gambar 2.1 menunjukkan peran file sistem dan tahapan yang terlibat pada proses penghapusan data di media penyimpanan.

Gambar 2.1 Tahapan Yang Terlibat Dalam Proses Penghapusan File Di SSD

1. *Marking Block* Data:

   Saat pengguna menghapus file, sistem operasi tidak langsung menghapus data fisik dari SSD. Sebaliknya, blok tersebut ditandai sebagai "tersedia" atau "dihapus" dalam metadata sistem file (Carrier, 2005; Nisbet & Jacob, 2019; Porter et al., 2021).

2. TRIM *Command*:

   Sistem Operasi mengambil data blok yang telah ditandai sistem file agar dapat mengirimkan perintah "TRIM" ke SSD untuk memberi tahu kontroler SSD tentang blok-blok yang sebenarnya sudah tidak digunakan lagi. TRIM *command* menandai blok-blok yang tidak diperlukan untuk membantu SSD secara proaktif mengidentifikasi file yang tidak valid untuk dibersihkan, kegiatan pembersihan file oleh TRIM akan menghasilkan *Garbage* pada blok-blok SSD (Nisbet & Jacob, 2019; Vieyra et al., 2019).

3. *Garbage Collection*:

   SSD menggunakan teknik yang disebut "*garbage collection*" untuk mengelola blok-blok yang sudah tidak terpakai. Proses ini melibatkan identifikasi yang telah dilakukan TRIM pada blok-blok sampah dan dikumpulkan menjadi satu kemudian dikosongkan untuk penggunaan lebih lanjut. Blok-blok sampah yang dikumpulkan kemudian dihapus secara fisik oleh kontroler SSD sebagai bagian dari operasi *garbage collection*. Untuk mengganti blok-blok sampah yang telah dikumpulkan akan mengenakan kapasitas penyimpanan yang tidak bisa dilihat oleh pengguna (Neyaz et al., 2019; Nisbet & Jacob, 2019).

4. *Over-Provisioning*:

   SSD umumnya memiliki kapasitas penyimpanan lebih besar daripada yang terlihat oleh pengguna. Bagian dari kapasitas ini disediakan untuk keperluan *over-provisioning*, yang digunakan oleh *kontroler* SSD untuk mengganti blok yang rusak atau dihapus. *Over-provisioning* membantu menjaga kinerja dan daya tahan SSD seiring waktu (Ahn & Lee, 2021; Jeremic et al., 2012).

5. *Wear Leveling*:

   SSD melakukan *wear leveling* untuk meratakan penggunaan sel penyimpanan secara merata. Ini menghindari pemakaian berlebihan pada blok tertentu, karena sel penyimpanan dalam SSD memiliki jumlah operasi tulis terbatas (Neyaz et al., 2018, 2019).

2.2.6 Konektor SATA

Konektor SATA atau *Seriel Advanced Technology Attachment* adalah standar internasional yang digunakan untuk menghubungkan perangkat di dalam komputer. Istilah ini mencakup kabel dan koneksi yang mematuhi standar internasional. konektor SATA umumnya digunakan untuk menghubungkan perangkat seperti CD-ROM, harddisk, SSD, dan berbagai perangkat lainnya ke *motherboard* komputer. (Pranoto et al., 2020a).

Konektor SATA lebih sering digunakan dibandingkan dengan konektor lainnya karena lebih umum dan sudah ada dalam sebagian besar *motherboard*. Kompatibel dengan berbagai perangkat penyimpanan, termasuk HDD dan SSD SATA lebih banyak media penyimpanan yang kompatibel. Konektor SATA tersedia dalam dua ukuran: 7-pin untuk transfer data dan 15-pin yang memberikan daya ke perangkat penyimpanan.

2.2.7 File sistem

Sistem file adalah cara di mana komputer menyimpan dan mengatur data di dalam penyimpanan, mirip dengan cara menyimpan dan mengatur file di lemari atau rak buku. Setiap jenis sistem file memiliki aturan khusus untuk menempatkan file dan memastikan bahwa data disimpan dengan rapi. Ini membantu komputer mengetahui di mana file-file itu berada dan bagaimana cara mengaksesnya saat membutuhkannya. Sistem file juga memungkinkan untuk menyimpan informasi tambahan tentang file, seperti kapan dibuat atau dimodifikasi. Dengan aturan dan struktur ini, komputer dapat mengelola semua informasi

dengan efisien dan membantu menemukan file yang dibutuhkan dengan cepat (Carrier, 2005).

File sistem NTFS (*New Technology File System*) dan ReFS (*Resilient File System*) adalah dua jenis sistem file yang digunakan oleh sistem operasi Windows. Meskipun keduanya digunakan untuk menyimpan dan mengatur data di *hard drive* atau media penyimpanan lainnya, ada perbedaan mendasar antara keduanya. NTFS merupakan sistem file yang telah ada sejak lama dan digunakan secara luas. Ini memiliki dukungan yang kuat untuk pengelolaan ruang *disk*, pengamanan file, dan *recovery* kesalahan. NTFS memungkinkan penggunaan berbagai fitur keamanan, termasuk pengaturan hak akses dan enkripsi file (Nordvik et al., 2019).

Sementara itu, ReFS adalah sistem file yang lebih baru dan dirancang dengan fokus pada ketahanan dan integritas data. ReFS memiliki kemampuan yang lebih baik untuk mendeteksi kesalahan dan memperbaiki diri sendiri, menjadikannya pilihan yang baik untuk lingkungan penyimpanan yang memerlukan ketahanan terhadap kerusakan. ReFS juga memungkinkan manajemen volume yang lebih efisien dan mendukung ukuran file dan volume yang lebih besar. Perbedaan utama antara NTFS dan ReFS adalah bahwa ReFS lebih terfokus pada ketahanan dan integritas data, sementara NTFS memiliki fitur yang lebih luas untuk pengelolaan ruang *disk* dan keamanan file. Pemilihan antara keduanya tergantung pada kebutuhan spesifik lingkungan dan persyaratan penyimpanan data (Lee et al., 2021).

Salah satu perbedaan utama antara NTFS dan ReFS adalah bahwa ReFS menggunakan teknologi pemeriksaan integritas data yang disebut "metadata integrity," yang memungkinkannya secara otomatis mengidentifikasi dan memperbaiki kesalahan dalam metadata sistem file. Hal ini berarti bahwa ReFS mampu melindungi data Anda dari kerusakan akibat masalah perangkat keras atau perangkat lunak. Selain itu, ReFS mendukung penyatuan penyimpanan (storage pooling), yang memungkinkan beberapa unit penyimpanan digabungkan menjadi sumber daya bersama, memudahkan pengelolaan data pada volume besar (Prade et al., 2020).

Oleh karena itu, baik NTFS maupun ReFS sebaiknya dianggap sebagai sistem file yang handal dan canggih, masing-masing dengan fitur-fitur khususnya. NTFS tetap menjadi sistem file default, menjamin kompatibilitas ke belakang yang lebih besar dengan versi Windows sebelumnya dan dengan semua perangkat yang perlu berinteraksi dengan sistem Microsoft. Sementara itu, ReFS dirancang secara cermat untuk memberikan ketahanan dan

integritas data yang lebih baik, terutama untuk lingkungan penyimpanan besar dan kebutuhan ketersediaan tinggi.

Performa dan skalabilitas adalah salah satu kelebihan utama dari ReFS, mampu mengelola jumlah data besar dengan sangat cepat dan optimal. Bahkan, ReFS memungkinkan volume hingga 1 Yottabyte atau 1000 miliar Terabyte. ReFS menggunakan mode *B+ Tree* untuk mengelola struktur file. *B+ Tree* sangat efisien dalam penyimpanan data karena memiliki jumlah simpul anak yang sangat tinggi dalam struktur tersebut. Dengan menggunakan penunjuk, *B+ Tree* dapat mengurangi jumlah operasi I/O untuk mengambil elemen dalam pohon tersebut .

2.2.8 B+ *tree*

B+ *tree* (B Plus Tree) adalah sebuah struktur data pohon terurut yang efisien digunakan dalam pengelolaan indeks pada basis data dan sistem penyimpanan file. Struktur pohon ini memiliki ciri khas di mana setiap simpul dapat memiliki beberapa anak, dan data sebenarnya hanya disimpan di simpul daun pohon. Pohon B+ memanfaatkan struktur terurut dengan mengurutkan kunci-kunci di setiap simpul, yang meningkatkan efisiensi operasi pencarian dan pengurutan data. Penyimpanan data di simpul daun dan penambahan penunjuk pada kunci memungkinkan pengurangan langkah-langkah yang diperlukan untuk mencapai data yang diinginkan, membuat pencarian data menjadi lebih efisien.

B+ *tree* sering digunakan dalam sistem manajemen basis data dan sistem penyimpanan file untuk indeksing dan pencarian data. Kemampuannya yang baik dalam menangani operasi pencarian, penyisipan, dan penghapusan dengan efisien membuatnya sangat cocok untuk meminimalkan jumlah operasi I/O yang diperlukan. Dengan struktur yang terurut dan penyimpanan data di simpul daun, B+ *tree* memberikan performa pencarian yang konsisten, bahkan untuk dataset yang besar, menjadikannya pilihan yang populer dalam implementasi indeks database (Nordvik et al., 2019).

Dalam file sistem ReFS (Resilient File System), penerapan B+ *tree* memainkan peran krusial dalam manajemen indeks, struktur metadata, dan efisiensi operasional. B+ *tree* digunakan untuk mengorganisir struktur metadata file sistem, mencakup atribut file, izin akses, dan lokasi fisik data dalam volume. Sebagai indeks, B+ *tree* mempercepat pencarian data dengan kunci yang diurutkan, memungkinkan navigasi efisien ke file atau direktori yang dibutuhkan.

Selain itu, B+ *tree* menyimpan indeks dan pointer yang mengarah ke lokasi data aktual, memfasilitasi sistem untuk dengan cepat menemukan dan mengakses informasi yang diperlukan. Struktur B+ *tree* juga digunakan untuk mengatur alamat blok data atau sektor pada disk fisik, memastikan pengelolaan yang efisien terhadap lokasi fisik data dalam volume ReFS.

Dalam mengelola file dan direktori, B+ *tree* berperan dalam menyusun dan menyimpan hierarki direktori serta hubungan antara file. Kemampuannya menangani volume besar dengan efisien membuatnya menjadi pilihan yang tepat untuk menyederhanakan operasi pada volume yang luas. Selain itu, B+ tree memainkan peran kunci dalam meningkatkan ketahanan terhadap kerusakan data, dengan kemampuannya mendeteksi dan memperbaiki kesalahan metadata secara otomatis (Wang et al., 2022).

2.2.9 Fitur TRIM

TRIM membantu mengatasi masalah yang dikenal sebagai "*garbage collection*" pada SSD. Tanpa TRIM, SSD cenderung menyimpan data yang sebenarnya sudah dihapus oleh sistem operasi, menyebabkan performa menurun seiring waktu. TRIM membantu memastikan bahwa blok penyimpanan yang tidak lagi diperlukan dapat dihapus dan dijaga kebersihannya Tidak semua sistem file mendukung TRIM karena implementasi TRIM memerlukan dukungan dan integrasi yang baik dari sistem operasi, perangkat keras penyimpanan (seperti SSD), dan sistem file itu sendiri (Hepisuthar & Priyankasharma, 2021).

Faktor-faktor yang mempengaruhi inklusi TRIM dalam suatu sistem file melibatkan desain dan struktur sistem file, kompatibilitas dengan perangkat keras (terutama SSD), prioritas pengembangan, dukungan sistem operasi, dan rancangan untuk jenis media penyimpanan tertentu. Sebagai hasilnya, beberapa sistem file mungkin memiliki arsitektur yang sulit untuk diintegrasikan dengan fitur TRIM, sementara yang lain mungkin memprioritaskan fitur atau kebutuhan lainnya. Selain itu, tidak semua SSD mendukung TRIM, dan perangkat penyimpanan yang berbeda mungkin memiliki implementasi TRIM yang beragam. Oleh karena itu, meskipun TRIM memberikan manfaat yang signifikan untuk performa dan keberlanjutan SSD, keberadaannya tidak dijamin dalam semua sistem file. Dalam beberapa kasus, fitur pengelolaan penyimpanan alternatif atau serupa mungkin digunakan untuk mencapai hasil yang serupa.(Ramadhan & Mualfah, 2020).

Ketika fitur TRIM dihidupkan, blok data yang dihapus secara permanen ditandai sebagai tidak digunakan oleh sistem operasi. Meskipun ada kemungkinan untuk *recovery*

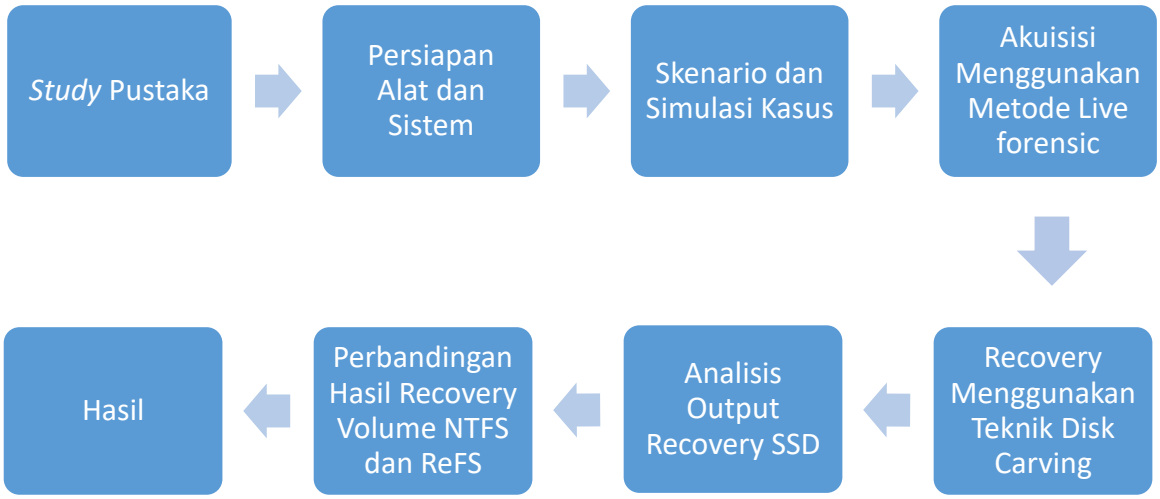
data dari SSD dengan TRIM diaktifkan, proses tersebut biasanya jauh lebih sulit atau bahkan tidak mungkin dilakukan karena saat proses TRIM selesai data akan terhapus pada tingkat fisik. Selain itu SSD dengan fitur TRIM aktif secara rutin membersihkan blok yang dihapus secara permanen untuk memastikan kinerja yang optimal. Oleh karena itu, data yang dihapus dengan fitur TRIM aktif mungkin telah dihapus secara permanen dan sulit dipulihkan Tetapi bukan tidak mungkin untuk *recovery* data yang telah dihapus permanen saat fitur TRIM hidup (Pranoto et al., 2020b). Berikut adalah urutan umum kerja fitur TRIM pada Solid State Drive (SSD) (Nisbet et al., 2013; Nisbet & Jacob, 2019; Zhou et al., 2021):

1. Penghapusan File
   Pengguna menghapus atau memindahkan file dari SSD menggunakan sistem operasi.
2. Penandaan Blok Data sebagai Usang (Stale)
   Sistem operasi menandai blok data yang mengandung file yang dihapus sebagai "usang" atau bebas untuk dihapus.
3. Permintaan TRIM dari Sistem Operasi.
   Sistem operasi menghasilkan permintaan TRM yang berisi informasi blok data yang seharusnya dihapus.
4. Pengiriman Perintah TRIM ke SSD
   Sistem operasi mengirim permintaan TRIM ke SSD.
5. Penerimaan Permintaan TRIM oleh SSD
   SSD menerima permintaan TRIM dan memproses informasi yang terkandung dalam permintaan tersebut.
6. Penghapusan Blok Data pada Tingkat Fisik
   SSD membersihkan blok data yang dihapus pada tingkat fisik, menghapus data yang seharusnya dihapus dari sel memori.
7. Penandaan Blok yang Telah Dihapus
   SSD menandai blok data yang telah dihapus sebagai kosong atau tersedia untuk penulisan data baru.

BAB 3
Metodologi

3.1 Tahapan Penelitian

Alur kerja dari awal hingga akhir akan dirangkum dalam metodologi yang diusulkan. Agar bisa mudah memahami langkah demi langkah dilengkapi dengan gambar dan yang disusun secara sistematis agar menjadi pedoman dalam menyelesaikan permasalahan yang ada. Berikut langkah – langkah atau tahapan pada penelitian ini dapat dilihat pada gambar 3.1.



Gambar 3.1 Metodologi Penelitian

3.2 Studi Pustaka

Penelitian ini dimulai dari mengumpulkan jurnal *review* dan makalah *conference* untuk menemukan topik pembahasan terkait masalah Fitur TRIM di *Solid State Drive* yang menghilangkan informasi penting untuk *recovery* file. Tahap selanjutnya mengumpulkan jurnal terkait dari topik masalah dan menganalisis secara mendalam kekurangan dan hal-hal yang belum berhasil dilakukan pada penelitian sebelumnya. Menggunakan buku, artikel, makalah, dan laporan penelitian untuk mempelajari teknik akuisisi *live forensic*.

3.3 Persiapan Alat dan Sistem

Pada penelitian ini akan menggunakan teknik *disk carving* untuk *recovery* SSD volume NTFS dan ReFS Persiapan Sistem dan Alat. Untuk menunjang penelitian ini dibutuhkan alat dan *tool* yang memadai agar penelitian bisa berjalan dengan lancar dan mendapatkan hasil akhir yang diinginkan. Sistem dan *tool* yang digunakan pada penelitian ini antara lain:

a. SSD SATA

   Akan di analisa pengaruhnya dengan sistem file ReFS dan NTFS. Sistem operasi windows 11 enterprise versi 21H2 sudah mendukung untuk melakukan *formating* ReFS dan NTFS.

b. Laptop acer aspire E1-471g.

   Laptop ini akan digunakan oleh pelaku(*red team*) berfungsi untuk menjalankan sistem operasi untuk menghapus file secara permanen.

c. Laptop acer sift 3

   Perangkat ini digunakan oleh investigator untuk melakukan analisa file hasil *imaging*.

d. Windows 11 enterprise versi 21H2

   Windows ini digunakan karena sudah mendukung format partisi volume ke File sistem ReFS.

e. Hetman *Partition Recovery*

   Tool yang digunakan untuk melakukan penarikan data dari SSD volume ReFS dan NTFS yang sudah dihapus permanen(shift+delete). Hetman *Partition Recovery* adalah *tool* yang bisa melakukan *mounting disk* hasil *imaging* untuk melakukan teknik *disk carving* secara *automaticly.*

f. AccessData FTK Imager

   Digunakan untuk melakukan *imaging* SSD volume ReFS dan NTFS. FTKimager adalah alat yang digunakan untuk membuat gambaran *disk* (*imaging*), dengan cara di *imaging* pemeriksa forensik tidak perlu takut mengubah bukti asli karena hasil *imaging* FTKimager bisa digunakan untuk diperiksa dan sudah memenuhi standar untuk *live forensik.*

3.4 Skenario dan Simulasi Kasus

Pada bagian skenario data yang bersifat sensitif akan dimasukkan ke dalam SSD yang sudah di format dengan NTFS dan ReFS. Kasus yang terjadi adalah data tersebut dihapus dan dibutuhkan untuk menjadi bukti yang kuat di meja pengadilan. Untuk menganalisa data yang telah di hapus maka dibutuhkan bantuan ahli forensik dimana data yang dipulihkan akan memiliki nilai hash yang sama dengan data sebelumnya. Sementara itu data yang berhasil dipulihkan akan di analisa sesuai dengan format file sistem yang akan mempengaruhi waktu dari pembuatan file dan metadata itu sendiri.

3.5 Menggunakan Metode *live* forensik

Dengan metode *live* forensik data yang dihapus akan dipulihkan agar tidak ada data yang tertinggal saat proses pembuatan *imaging disk* metode ini dipilih. Metode *live* forensik ini dapat berisiko menyebabkan kerusakan data jika tidak dilakukan dengan benar. Cara peneliti melakukan *imaging* adalah dengan menutup perubahan yang akan dilakukan pada port USB HDD yang sudah di masukan *tool* FTK Imager *portable* jadi, jika USB HDD di masukan maka data dari komputer tidak berubah.

3.6 Menggunakan Teknik *Disk Carving*

Dengan teknik *disk carving tool* yang digunakan akan melakukan *scan* pada file data yang telah dihapus permanen kemudian akan di *recovery* secara *automatically*, teknik ini akan melakukan pencarian file data yang telah dihapus permanen dengan berdasarkan *header* dan *footer* (Kessler, 2023). Teknik *disk carving* digunakan dalam penelitian ini bertujuan untuk mengatasi adanya file sistem yang tidak mampu dibaca oleh alat yang mengandalkan master file tabel sebagai *database* tempat file sistem menyimpan semua perubahan yang terjadi pada suatu file.

3.7 Analisis Output SSD Volume ReFS dan NTFS

Pada tahapan ini dilakukan analisa hasil *imaging* dari *tool* FTK Imager *portable* dengan menggunakan hetman *partition recovery* untuk melihat file-file yang telah dihapus dari SSD. Untuk mengetahui bagaimana *header* dan *footer* file setelah dipulihkan menggunakan FTKImager membuat metadata file harus dianalisa dengan teliti. Setiap file sistem memiliki cara mengatur metadata file yang unik digunakan untuk menunjang kebutuhan-kebutuhan tertentu. Contohnya pendahulunya adalah FAT32 dirancang agar menjadi lebih *portable* dan bisa di deteksi oleh berbagai macam sistem operasi sementara file sistem NTFS tidak terlalu *portable* dan bisa terjadi kerusakan jika dicabut mendadak atau terjadi lonjakan daya.

Contoh tabel analisis status hasil *recovery* tabel 3.1

Tabel 3.1 Contoh tabel analisis metadata file hasil *recovery*

NAMA FILE	*Header* File	*Footer* file	*Date Modified*	*Size*

Tabel 3.2 Daftar File Asli NTFS TRIM *Disable*

Jenis data	Nama File NTFS TRIM *Disable*	Ekstensi File	Nilai HASH File Asli MD5
File Aplikasi	file exe 1, N2	.exe	e67e681e116f50d14a557cd83e83596a
	file exe 2, N2	.exe	e500b16147893a4b4aa6a71a0b494475
	file exe 3, N2	.exe	375276a153cfcd10b60141a1bf6d4126
File Dokumen	Doc, N2	.doc	202bed6dade8a6b45f315af6ed4fec01
	Docx, N2	.docx	2a2539f683f34f5dc3a31f125601d94e
	ODT, N2	.odt	b43a20b258af2db416d87368ea99e871
	pdf, N2	.pdf	de61ec3a4bfdba769b63b2817d65abca
	PowerPoint, N2	.pptx	16bc6e9ff52573c9a133117e469578c6
	teks, N2	.txt	9fdbfbd6b9f80a12a4aed69366b1598f
	XLSX, N2	.xlsx	168dbdd011eb3113403c205310911801
File Gambar	BMP, N2	.bmp	60575664b29c4747ec20bc298394a6db
	GIF, N2	.gif	cf69c943fa8eea1605295ead83242f7a
	JPG, N2	.jpg	a3333bb3df4b47dd6a3a6abf4bede7ad
	PNG, N2	.png	068f0a46761a2c77df687f402f263a86
File Audio	m4a, N2	.m4a	27d27b8eb61f5f9d19753d517de0554e
	mp3, N2	.mp3	180b9de2ce8454e8862a37e33e8a5ed1
	WAV, N2	.wav	8f775199f5bf8a7a030185af4257ca5d
	WMA, N2	.wma	5717ede6eda50aeb373b621312ffbc3d
File Video	3gp, N2	.3gp	1ecc9837edc86b3370be6e85a2a0c4af
	AVI, N2	.avi	611daaf923e0f755ce19b8f981ccc8bf
	FLV, N2	.flv	54a827a332666830c3404c817cc1d934
	MKV, N2	.mkv	c08dc5bdebe741ca10dee0142a34fd17
	MOV, N2	.mov	440fd3c73c4be0bc1f9fae3955dfcbbf
	MP4, N2	.mp4	8b6e8415ada32d939eba45f75388c2aa
	MPG, N2	.mpg	3af1c20309fb85e8de8092c30425a106
	OGG, N2	.Ogg	69a4ca496c2c4472db7e6edd8a1db388
	webm, N2	.webm	bf23511f8770f9d5c74edc33836b488a
	WMV, N2	.wmv	52289d287f8522b4973372fd8fe0a642
File winrar	RAR 1, N2	.rar	76a42cc2609e2cfe2784077248ecceb7
	RAR 2, N2	.rar	8251719177e9bd5d549963c04829c9d3
	RAR 3, N2	.rar	3ca2fbabcb23b6fc9a0763bc9297fe01
File Zip	zip 1, N2	.zip	5349d6809d2cf1e8d82931b880265a9d
	zip 2, N2	.zip	18271d308f0c4aaebbf72c0e76ebab66
	zip 3, N2	.zip	c4e514a94643a96243dd347972963ec5

Tabel 3.2 adalah daftar file asli dari file sistem NTFS dengan TRIM yang *disable* dengan label N2 pada setiap nama file.

Tabel 3.3 Daftar File Asli NTFS TRIM *Enable*

Jenis data	Nama File NTFS TRIM Enable	Ekstensi File	Nilai HASH File Asli MD5
File Aplikasi	file exe 1, N1	.exe	e67e681e116f50d14a557cd83e83596a
	file exe 2, N1	.exe	e500b16147893a4b4aa6a71a0b494475
	file exe 3, N1	.exe	375276a153cfcd10b60141a1bf6d4126
File Dokumen	Doc, N1	.doc	202bed6dade8a6b45f315af6ed4fec01
	Docx, N1	.docx	2a2539f683f34f5dc3a31f125601d94e
	ODT, N1	.odt	b43a20b258af2db416d87368ea99e871
	pdf, N1	.pdf	de61ec3a4bfdba769b63b2817d65abca
	PowerPoint, N1	.pptx	16bc6e9ff52573c9a133117e469578c6
	teks, N1	.txt	9fdbfbd6b9f80a12a4aed69366b1598f
	XLSX, N1	.xlsx	168dbdd011eb3113403c205310911801
File Gambar	BMP, N1	.bmp	60575664b29c4747ec20bc298394a6db
	GIF, N1	.gif	cf69c943fa8eea1605295ead83242f7a
	JPG, N1	.jpg	a3333bb3df4b47dd6a3a6abf4bede7ad
	PNG, N1	.png	068f0a46761a2c77df687f402f263a86
File Audio	m4a, N1	.m4a	27d27b8eb61f5f9d19753d517de0554e
	mp3, N1	.mp3	180b9de2ce8454e8862a37e33e8a5ed1
	WAV, N1	.wav	8f775199f5bf8a7a030185af4257ca5d
	WMA, N1	.wma	5717ede6eda50aeb373b621312ffbc3d
File Video	3gp, N1	.3gp	1ecc9837edc86b3370be6e85a2a0c4af
	AVI, N1	.avi	611daaf923e0f755ce19b8f981ccc8bf
	FLV, N1	.flv	54a827a332666830c3404c817cc1d934
	MKV, N1	.mkv	c08dc5bdebe741ca10dee0142a34fd17
	MOV, N1	.mov	440fd3c73c4be0bc1f9fae3955dfcbbf
	MP4, N1	.mp4	8b6e8415ada32d939eba45f75388c2aa
	MPG, N1	.mpg	3af1c20309fb85e8de8092c30425a106
	OGG, N1	.Ogg	69a4ca496c2c4472db7e6edd8a1db388
	webm, N1	.webm	bf23511f8770f9d5c74edc33836b488a
	WMV, N1	.wmv	52289d287f8522b4973372fd8fe0a642
File winrar	RAR 1, N1	.rar	76a42cc2609e2cfe2784077248ecceb7
	RAR 2, N1	.rar	8251719177e9bd5d549963c04829c9d3
	RAR 3, N1	.rar	3ca2fbabcb23b6fc9a0763bc9297fe01
File Zip	zip 1, N1	.zip	5349d6809d2cf1e8d82931b880265a9d
	zip 2, N1	.zip	18271d308f0c4aaebbf72c0e76ebab66
	zip 3, N1	.zip	c4e514a94643a96243dd347972963ec5

Tabel 3.3 adalah daftar file asli dari file sistem NTFS dengan TRIM yang *enable* dengan label N1 pada setiap nama file.

Tabel 3.4 Daftar File asli ReFS TRIM *Disable*

Jenis data	Nama File ReFS TRIM Disable	Ekstensi File	Nilai HASH File Asli MD5
File Aplikasi	file exe 1, R2	.exe	e67e681e116f50d14a557cd83e83596a
	file exe 2, R2	.exe	e500b16147893a4b4aa6a71a0b494475
	file exe 3, R2	.exe	375276a153cfcd10b60141a1bf6d4126
File Dokumen	Doc, R2	.doc	202bed6dade8a6b45f315af6ed4fec01
	Docx, R2	.docx	2a2539f683f34f5dc3a31f125601d94e
	ODT, R2	.odt	b43a20b258af2db416d87368ea99e871
	pdf, R2	.pdf	de61ec3a4bfdba769b63b2817d65abca
	PowerPoint, R2	.pptx	16bc6e9ff52573c9a133117e469578c6
	teks, R2	.txt	9fdbfbd6b9f80a12a4aed69366b1598f
	XLSX, R2	.xlsx	168dbdd011eb3113403c205310911801
File Gambar	BMP, R2	.bmp	60575664b29c4747ec20bc298394a6db
	GIF, R2	.gif	cf69c943fa8eea1605295ead83242f7a
	JPG, R2	.jpg	a3333bb3df4b47dd6a3a6abf4bede7ad
	PNG, R2	.png	068f0a46761a2c77df687f402f263a86
File Audio	m4a, R2	.m4a	27d27b8eb61f5f9d19753d517de0554e
	mp3, R2	.mp3	180b9de2ce8454e8862a37e33e8a5ed1
	WAV, R2	.wav	8f775199f5bf8a7a030185af4257ca5d
	WMA, R2	.wma	5717ede6eda50aeb373b621312ffbc3d
File Video	3gp, R2	.3gp	1ecc9837edc86b3370be6e85a2a0c4af
	AVI, R2	.avi	611daaf923e0f755ce19b8f981ccc8bf
	FLV, R2	.flv	54a827a332666830c3404c817cc1d934
	MKV, R2	.mkv	c08dc5bdebe741ca10dee0142a34fd17
	MOV, R2	.mov	440fd3c73c4be0bc1f9fae3955dfcbbf
	MP4, R2	.mp4	8b6e8415ada32d939eba45f75388c2aa
	MPG, R2	.mpg	3af1c20309fb85e8de8092c30425a106
	OGG, R2	.Ogg	69a4ca496c2c4472db7e6edd8a1db388
	webm, R2	.webm	bf23511f8770f9d5c74edc33836b488a
	WMV, R2	.wmv	52289d287f8522b4973372fd8fe0a642
File winrar	RAR 1, R2	.rar	76a42cc2609e2cfe2784077248ecceb7
	RAR 2, R2	.rar	8251719177e9bd5d549963c04829c9d3
	RAR 3, R2	.rar	3ca2fbabcb23b6fc9a0763bc9297fe01
File Zip	zip 1, R2	.zip	5349d6809d2cf1e8d82931b880265a9d
	zip 2, R2	.zip	18271d308f0c4aaebbf72c0e76ebab66
	zip 3, R2	.zip	c4e514a94643a96243dd347972963ec5

Tabel 3.4 adalah daftar file asli dari file sistem ReFS dengan TRIM yang *disable* dengan label R2 pada setiap nama file.

Tabel 3.5 Daftar File asli ReFS TRIM *Enable*

Jenis data	Nama File ReFS TRIM Enable	Ekstensi File	Nilai HASH File Asli MD5
File Aplikasi	file exe 1, R1	.exe	e67e681e116f50d14a557cd83e83596a
	file exe 2, R1	.exe	e500b16147893a4b4aa6a71a0b494475
	file exe 3, R1	.exe	375276a153cfcd10b60141a1bf6d4126
File Dokumen	Doc, R1	.doc	202bed6dade8a6b45f315af6ed4fec01
	Docx, R1	.docx	2a2539f683f34f5dc3a31f125601d94e
	ODT, R1	.odt	b43a20b258af2db416d87368ea99e871
	pdf, R1	.pdf	de61ec3a4bfdba769b63b2817d65abca
	PowerPoint, R1	.pptx	16bc6e9ff52573c9a133117e469578c6
	teks, R1	.txt	9fdbfbd6b9f80a12a4aed69366b1598f
	XLSX, R1	.xlsx	168dbdd011eb3113403c205310911801
File Gambar	BMP, R1	.bmp	60575664b29c4747ec20bc298394a6db
	GIF, R1	.gif	cf69c943fa8eea1605295ead83242f7a
	JPG, R1	.jpg	a3333bb3df4b47dd6a3a6abf4bede7ad
	PNG, R1	.png	068f0a46761a2c77df687f402f263a86
File Audio	m4a, R1	.m4a	27d27b8eb61f5f9d19753d517de0554e
	mp3, R1	.mp3	180b9de2ce8454e8862a37e33e8a5ed1
	WAV, R1	.wav	8f775199f5bf8a7a030185af4257ca5d
	WMA, R1	.wma	5717ede6eda50aeb373b621312ffbc3d
File Video	3gp, R1	.3gp	1ecc9837edc86b3370be6e85a2a0c4af
	AVI, R1	.avi	611daaf923e0f755ce19b8f981ccc8bf
	FLV, R1	.flv	54a827a332666830c3404c817cc1d934
	MKV, R1	.mkv	c08dc5bdebe741ca10dee0142a34fd17
	MOV, R1	.mov	440fd3c73c4be0bc1f9fae3955dfcbbf
	MP4, R1	.mp4	8b6e8415ada32d939eba45f75388c2aa
	MPG, R1	.mpg	3af1c20309fb85e8de8092c30425a106
	OGG, R1	.Ogg	69a4ca496c2c4472db7e6edd8a1db388
	webm, R1	.webm	bf23511f8770f9d5c74edc33836b488a
	WMV, R1	.wmv	52289d287f8522b4973372fd8fe0a642
File winrar	RAR 1, R1	.rar	76a42cc2609e2cfe2784077248ecceb7
	RAR 2, R1	.rar	8251719177e9bd5d549963c04829c9d3
	RAR 3, R1	.rar	3ca2fbabcb23b6fc9a0763bc9297fe01
File Zip	zip 1, R1	.zip	5349d6809d2cf1e8d82931b880265a9d
	zip 2, R1	.zip	18271d308f0c4aaebbf72c0e76ebab66
	zip 3, R1	.zip	c4e514a94643a96243dd347972963ec5

Tabel 3.5 adalah daftar file asli dari file sistem ReFS dengan TRIM yang *enable* dengan label R1 pada setiap nama file.

3.8 Perbandingan Hasil *Recovery* Volume NTFS dan ReFS

Penelitian ini menggunakan perhitungan angka indeks untuk menentukan pengaruh masing-masing file sistem sesuai dengan hasil akuisisi. Perbandingan angka Indeks tak tertimbang digunakan pada rumus perhitungan. Persamaan (1) merupakan penulisan persamaan untuk mengetahui hasil akuisisi secara forensik sesuai dengan file sistem yang digunakan (Riadi et al., 2020)

$$Pon = \frac{\sum \mathrm{Pn}}{\sum \mathrm{Po}}\ x\ 100\% \quad \text{.....(1)}$$

Keterangan:

Pon adalah hasil persentase yang diinginkan

∑ Pn adalah data asli dari SSD

∑ Po adalah hasil akuisisi data dengan *tool* forensik

Tabel 3.6 Contoh tabel status hasil *recovery*

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*

Tabel 3.6 akan digunakan untuk menempatkan perbandingan nilai HASH file pada setiap kondisi yang diuji yaitu format NTFS dengan TRIM *disable* dan *enable* serta format ReFS dengan TRIM *disable* dan *enable*.

3.9 Hasil

Hasil dan laporan akan dibuat setelah proses analisa *output* akan dibandingkan antara nilai hash file asli dan file yang telah di hapus, dan membandingkan berapa banyak file data yang bisa di *recovery* jika data dimasukkan ke dalam volume NTFS dan Volume ReFS. Metadata dari file akan ikut dilaporkan guna untuk mengetahui bagaimana data masih bisa dipulihkan setelah dihapus permanen pada file sistem NTFS dan ReFS. Hal yang akan menjadi penentu jika terjadi perbedaan waktu pembuatan dan modifikasi pada file yang telah di hapus.

BAB 4

Hasil dan Pembahasan

4.1 Studi Pustaka

SSD menggunakan memori flash semikonduktor untuk penyimpanan data, memungkinkan akses data secara elektronik tanpa adanya bagian mekanis yang bergerak. Di sisi lain, HDD menggunakan piringan magnetik berputar dan kepala pembaca-panjang yang bergerak secara mekanis untuk membaca dan menulis data. Keunggulan utama SSD terletak pada waktu akses yang lebih cepat, daya tahan terhadap guncangan, serta kinerja unggul dalam transfer data acak (Hepisuthar & Priyankasharma, 2021). Salah satu perbedaan mendasar dari SSD dengan HDD adalah fitur TRIM. Pada gambar 4.1 di tunjukan perbedaan besar antara komponen dari SSD dan HDD yang menyebabkan kebutuhan penggunaan TRIM.

Gambar 4.1 Komponen SSD dan HDD

TRIM merupakan sebuah perintah atau komando yang digunakan dalam teknologi penyimpanan Solid State Drive (SSD) dengan tujuan untuk meningkatkan efisiensi manajemen penyimpanan. Saat pengguna menghapus atau memindahkan data pada SSD, TRIM memberikan informasi ke *kontroler* SSD tentang sektor-sektor yang tidak lagi berisi data valid. Dengan adanya informasi ini, *kontroler* dapat secara proaktif membersihkan dan mengosongkan blok-blok yang tidak digunakan, memastikan ketersediaan ruang penyimpanan yang optimal. (Kumar, 2021). Selama proses TRIM, sistem operasi dan file sistem memainkan peran penting dalam menandai file yang masih valid dan tidak valid.

File sistem memiliki peran krusial dalam menjembatani perintah TRIM pada Solid State Drive (SSD). Perintah TRIM digunakan untuk memberikan informasi ke *kontroler* SSD mengenai sektor-sektor yang tidak lagi berisi data valid, sehingga dapat dihapus dan dikosongkan untuk penulisan data baru. Pengaruh file sistem pada perintah TRIM terutama

terlihat dalam bagaimana file sistem menyampaikan dan mengelola informasi mengenai blok-blok yang dapat dihapus.

struktur metadata file sistem menjadi kunci dalam pengenalan sektor-sektor yang telah dihapus. Metadata menyimpan informasi tentang bagaimana data disimpan dan diorganisir di dalam SSD. Oleh karena itu, file sistem yang efektif dalam menyimpan dan menyajikan metadata akan mendukung pelaksanaan perintah TRIM dengan akurat.

4.2 Persiapan Alat dan Sistem

Rangka penelitian ini melibatkan persiapan sistem yang akan diterapkan selama proses akuisisi dan *recovery* data secara langsung. Tahap awal mencakup penyiapan spesifikasi komputer dan perangkat pendukung lainnya yang diperlukan untuk menjalankan penelitian ini. Beberapa peralatan yang harus dipersiapkan ditampilkan pada tabel 4.1.

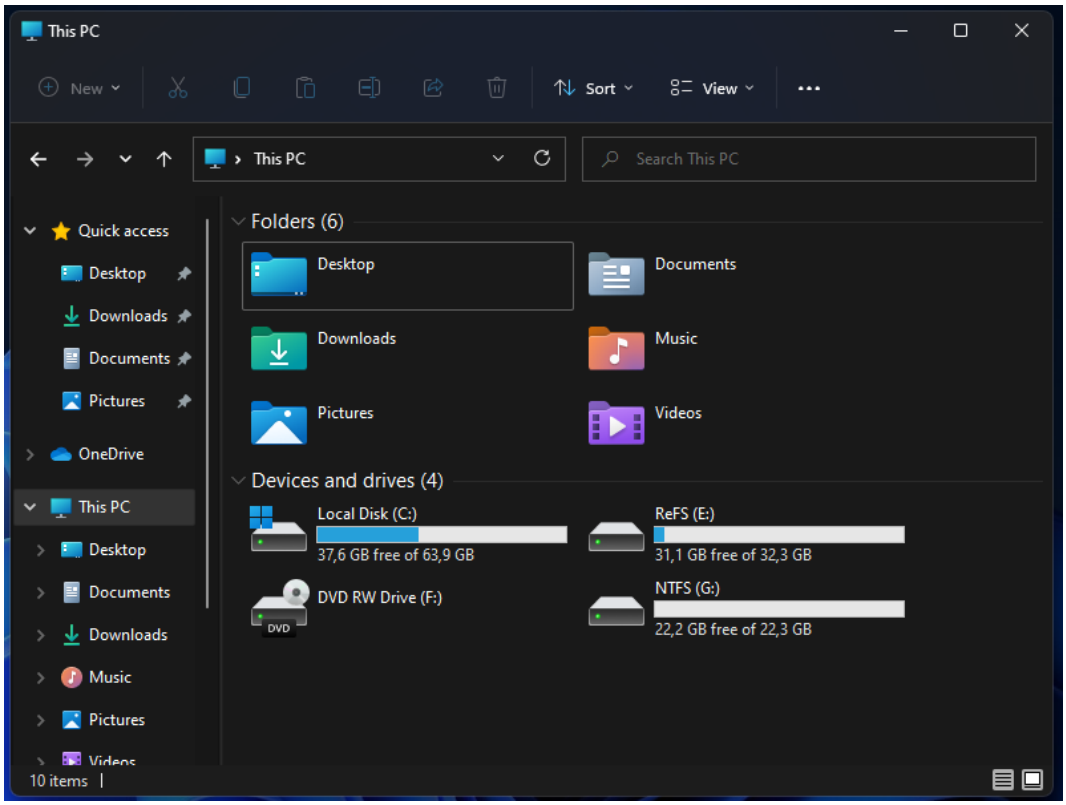
Tabel 4.1 Perincian Perangkat Keras dan Perangkat Lunak Yang Digunakan

No.	Perangkat Keras/ Perangkat Lunak	Keterangan
1	Laptop Acer Aspire E1-471G	Perangkat Keras
2	Laptop Acer Swift SF314-41	Perangkat Keras
3	*Solid State Driver* (SSD) SATA V-Gen Platinum kapasitas 128GB	Perangkat Keras
4	HDD *Ekstenal* Seagate kapasitas 1TB	Perangkat Keras
5	Converter SATA to USB	Perangkat Keras
6	USB 3.0 SATA	Perangkat Keras
7	Portable FTK Imager	*Tools* forensik
8	OS Windows 11 Enterprise Versi 21H2 arsitektur 64-bit	*operating system* Laptop pertama
9	OS Windows 11 Enterprise Versi 21H2 arsitektur 64-bit	*operating system* Laptop Kedua
10	Hetman *Partition Recovery*	*Tools* forensik
11	HxD	*Tools* forensik

FTK Imager Portable akan melakukan imaging SSD. HxD akan digunakan untuk melakukan pengecekan dari nilai heksadesimal file hasil *recovery tool hetman partition recovery.*

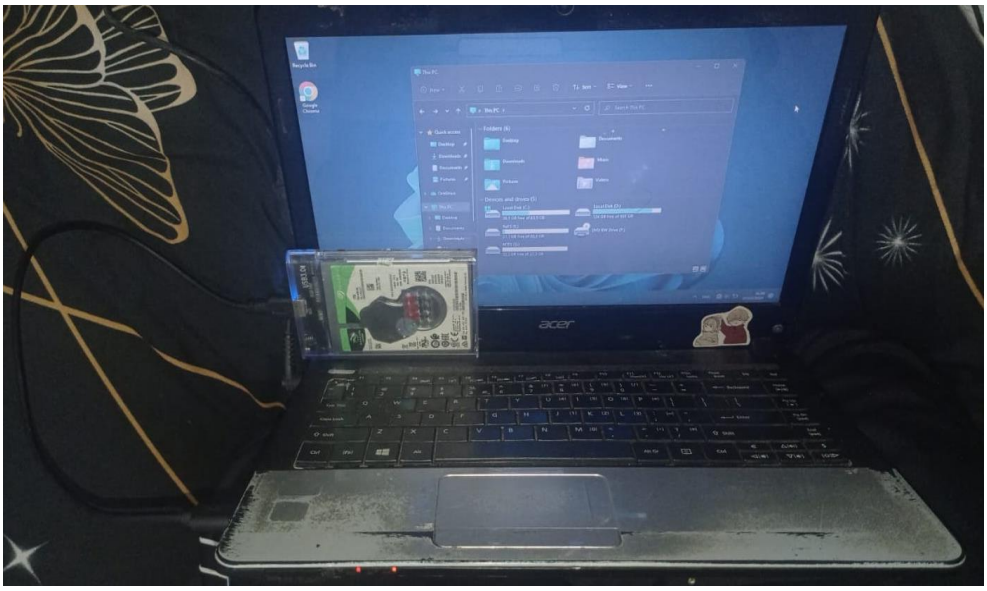
4.3 Skenario dan Simulasi Kasus

Dalam simulasi kasus media penyimpanan untuk memastikan pengaruh file sistem pada fitur TRIM dilakukan pembagian partisi pada komputer pertama yaitu C: tempat sistem operasi, partisi G: dan E:. penyalinan file ke dalam SSD dan penghapusan file dengan *shift+delete*. Saat komputer pertama ditemukan masih menunjukkan lampu menyala dan ditemukan partisi G: yang sudah diformat ke NTFS dan Partisi E: yang sudah diformat ke ReFS seperti pada pada gambar 4.2.



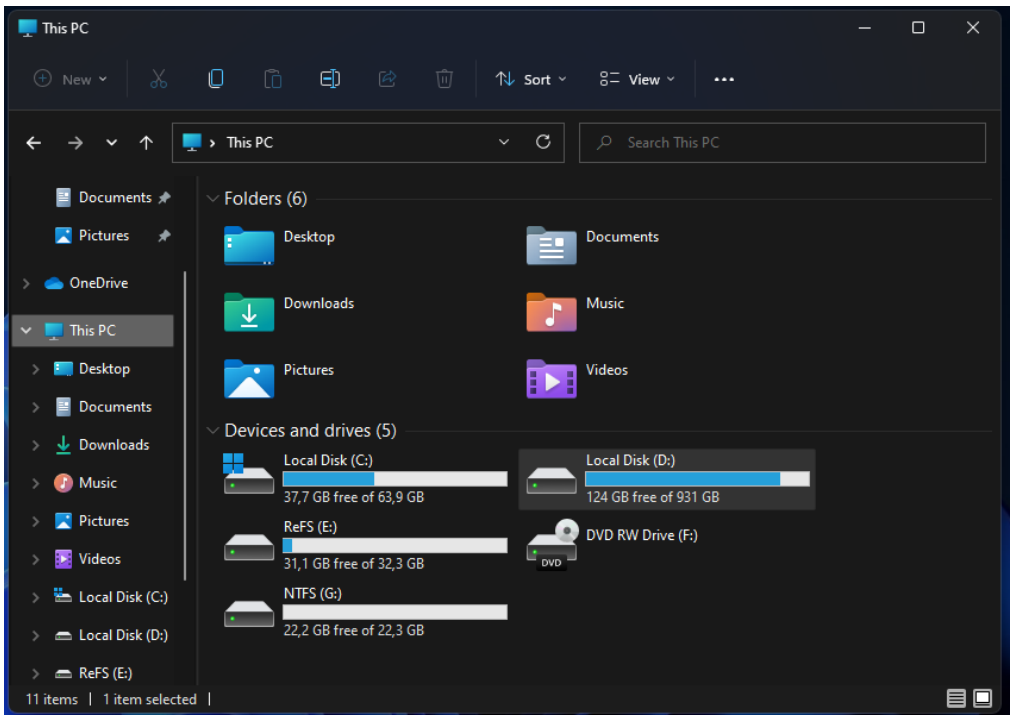
Gambar 4.2 Hasil Pembagian Partisi Disk SSD

Karena terdapat adanya partisi yang dianggap mencurigakan menyimpan bukti yang telah dihapus permanen oleh pelaku kejahatan karenanya pada kedua partisi proses live forensik dilakukan. Proses live forensik memungkinkan para penyelidik untuk melakukan analisis langsung pada sistem yang sedang berjalan, sehingga memungkinkan untuk mengumpulkan informasi yang masih tersedia secara dinamis, termasuk data yang disimpan dalam partisi-partisi yang dianggap mencurigakan tersebut. Dengan demikian, proses live forensik menjadi kunci dalam mengungkap bukti-bukti tersembunyi dan memperkuat kasus dalam investigasi kejahatan komputer. Dengan hal pertama yang dilakukan melakukan *copy* portable FTK Imager ke HDD eksternal Setelah HDD eksternal siap digunakan untuk menampung data hasil *imaging,* digunakan *coverter* USB to SATA untuk menghubungkan HDD eksternal ke komputer pertama seperti pada gambar 4.3



Gambar 4.3 Koneksi HDD Eksternal Untuk Menampung Data

Setelah melakukan koneksi melalu *port* USB kemudian dipastikan bahwa HDD eksternal telah dibaca oleh sistem operasi seperti pada gambar 4.4. HDD eksternal ditampilkan pada partisi D:, semua file hasil *imaging* akan disimpan pada *disk* ini.



Gambar 4.4 HDD Eksternal Telah Dibaca Sistem Operasi

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

1. Pembagian dan pemformatan partisi pada SSD

   Penjelasan: pembagian partisi dilakukan untuk mempermudah penempatan file-file yang telah disiapkan untuk dihapus permanen pada dua file sistem yaitu NTFS dan

ReFS. Dua volume disiapkan yaitu G:/ tempat format file sistem NTFS dan volume E:/ tempat format file sistem ReFS.

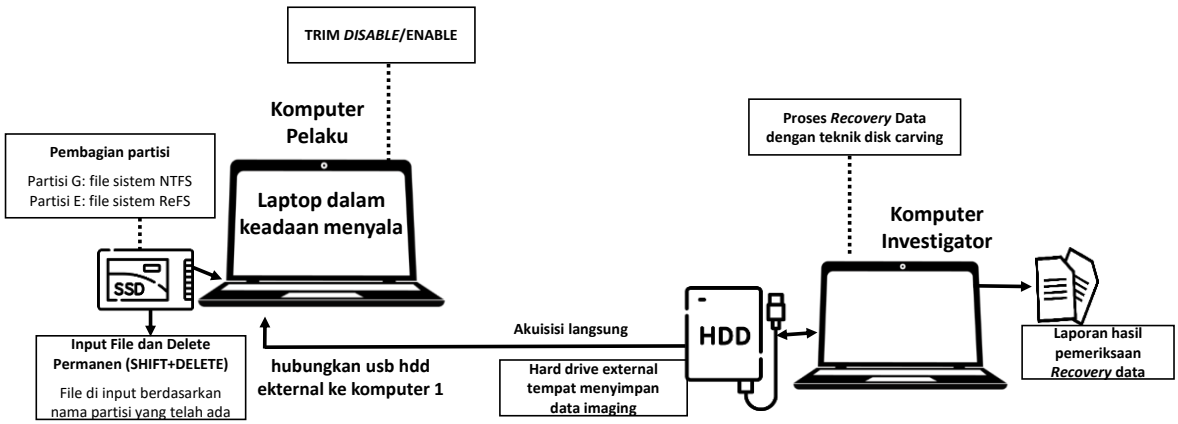
2. Mengaktifkan dan menonaktifkan fungsi TRIM

   Penjelasan: pada setiap file sistem fitur TRIM akan diaktifkan secara default, berbagai file dengan ekstensi yang berbeda akan di masukan ke dalam volume NTFS dan ReFS sesuai dengan nama file, file yang telah di masukan akan dihapus permanen dengan menekan *keyboard* (Shift+delete)

3. Melakukan live akuisisi terhadap SSD

   Penjelasan: FTK *Imager portable* disiapkan di dalam HDD eksternal akan digunakan untuk live akuisisi. Saat laptop masih dalam keadaan menyala live akuisisi akan dilakukan dengan cara menghubungkan HDD eksternal ke laptop yang telah di atur fitur TRIM.

Untuk penjelasan tahapan yang lebih rinci dari skenario dan simulasi kasus dijelaskan pada gambar 4.5:



Gambar 4.5 Gambaran Tahapan Skenario dan Simulasi Kasus Secara Menyeluruh

Berdasarkan gambar 4.5 dijelaskan tahapan yang akan dilakukan pelaku kejahatan dan penyidik.

Langkah-langkah bagi Pelaku:

1. Pelaku menggunakan SSD dengan sistem operasi Windows 11 Enterprise dan membagi partisi menjadi file sistem NTFS dan ReFS.
2. Pelaku membagi SSD menjadi tiga partisi, Drive C:\, Drive G:\ file sistem NTFS, dan Drive E:\ file sistem ReFS. File data asli disimpan di partisi Drive G:\ dan Drive E:\.
3. Pelaku meletakan file-file dengan label ganjil dan genap ke dalam masing-masing partisi.

4. Pelaku menerapkan fungsi TRIM yang dinonaktifkan dan yang diaktifkan.
5. Pelaku secara permanen menghapus (shift+delete) file berlabel ganjil genap pada SSD di partisi Drive G:\ dan Drive E:\..

Setelah langkah pelaku selesai dilakukan, penyidik menemukan laptop masih dalam keadaan menyala (power on) dan ditemukan bahwa laptop tersebut menggunakan SSD SATA seperti pada gambar 4.6, Selanjutnya langkah-langkah penyidik dilakukan untuk mendapatkan bukti.

Gambar 4.6 SSD SATA Yang Digunakan Pelaku Kejahatan

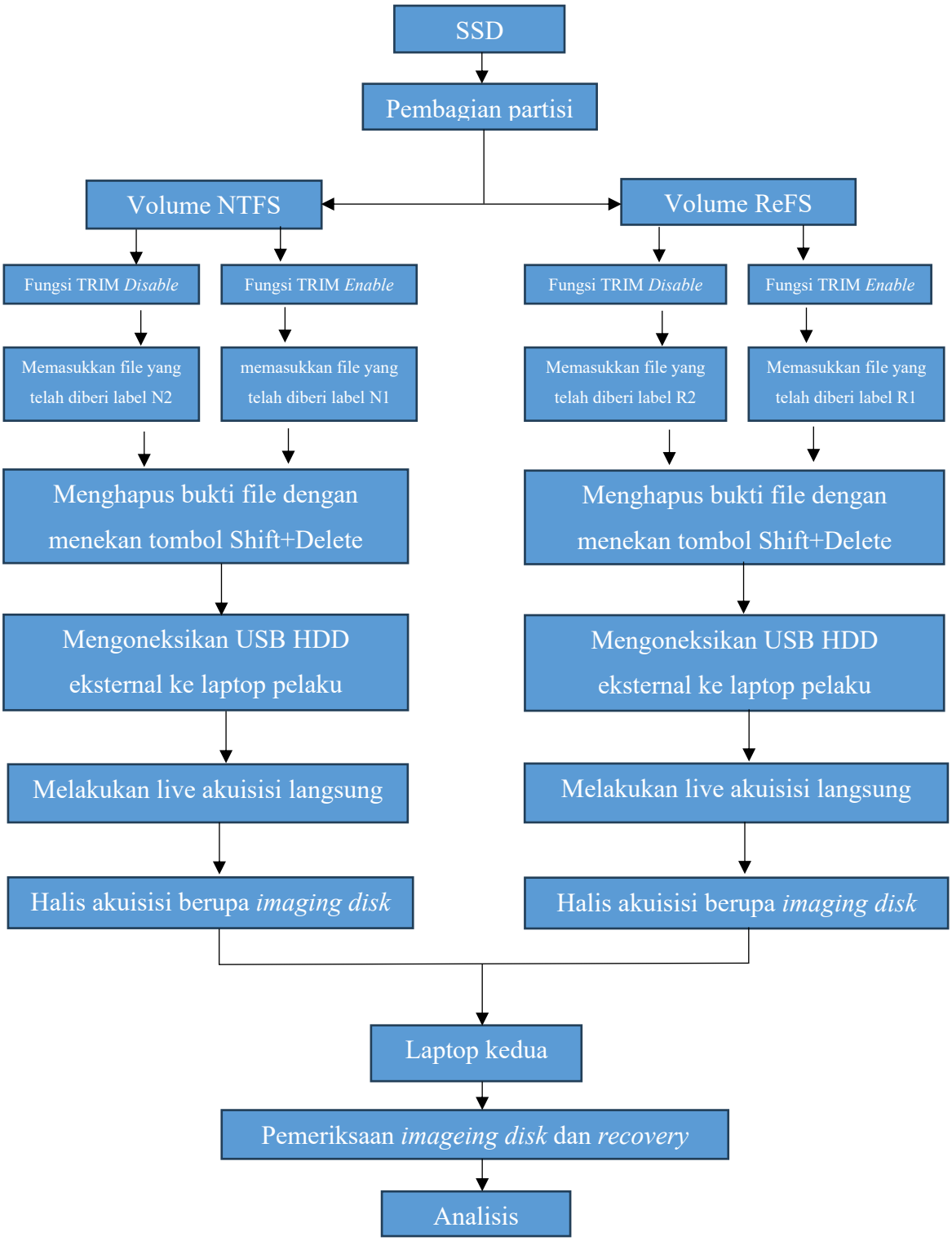
Langkah-langkah Penyidik:

1. Penyidik menghubungkan USB HDD SATA eksternal ke komputer Pelaku untuk menyimpan hasil perolehan *imaging disk.*
2. Penyidik melakukan akuisisi pada SSD langsung di komputer pelaku dengan USB HDD eksternal SATA dan *tool Portable FTK Imager.* Setelah *Imager.*
3. Setelah mendapatkan hasil *image disk* dari *tool Portable FTK Imager* penyidik akan menghubungkan HDD eksternal ke komputer penyidik untuk melakukan pemeriksaan dan analisis hasil *Imaging* dengan menggunakan teknik *disk carving*.

4.4 Akuisisi Menggunakan Metode Live forensik

Dalam penelitian ini, metode *live* forensik digunakan untuk melakukan akuisisi langsung dari SSD file sistem NTFS dan ReFS. USB HDD eksternal digunakan sebagai tempat penyimpanan data yang diakuisisi, dengan tujuan untuk menjaga keamanan bukti digital terkait fungsi SSD TRIM agar tidak mengalami kerusakan atau hilang. Peneliti melakukan ekstraksi data dari SSD dengan mengaktifkan dan menonaktifkan fungsi TRIM seperti pada penelitian sebelumnya (Pranoto et al., 2020a; Ramadhan & Mualfah, 2020). Penelitian Sebelumnya menggunakan *tool autopsy, belkasoft, dan testdisk,* pada penelitian kali ini akan mencoba teknik *disk carving* menggunakan *tool* Hetman *Partition Recovery* memiliki dukungan *scan* ReFS dan membandingkan akurasi *recovery* dari file sistem NTFS dan ReFS.

Dalam langkah ini, dilakukan akuisisi bukti digital yang terdapat dalam SSD menggunakan alat yang mendukung teknik forensik langsung, yaitu *Portable* FTK *Imager*.



Gambar 4.7 Tahapan Akuisisi

Seperti gambar 4.7 teknik *live* forensik diterapkan untuk *recovery* file yang telah dihapus secara permanen di SSD dengan file sistem NTFS dan ReFS, baik dengan TRIM

yang *disable* maupun *enable*. Dalam penelitian ini, alat *live* forensik yang digunakan adalah *Portable* FTK *Imager*, yang memiliki kemampuan untuk mengambil *image* dari *disk* , sehingga mendukung praktik forensik langsung. Gambar 4.8 (a) dan (b) menunjukkan dokumentasi hasil proses *imaging disk* langsung pada file sistem NTFS dengan TRIM *disable*, sementara Gambar 4.9 (a) dan (b) menunjukkan dokumentasi hasil proses pencitraan langsung pada file sistem NTFS dengan TRIM *enable*, menggunakan *Portable* FTK *Imager*. Tabel 4 berisi hasil dari proses imaging beserta nilai hash MD5. Tujuan dari proses imaging ini adalah untuk menjaga integritas bukti digital asli yang terdapat dalam SSD selama proses analisis, serta untuk mencegah terjadinya kerusakan pada bukti digital tersebut.

Hasil Verify Pencitraan	
Nama	NTFS TRIM DISABLE.001
Sector count	46864384
Nilai Hash MD5	
Computed Hash	f7cd3acd288ce72d70f3a693ab68afc6
Laporan Hash	f7cd3acd288ce72d70f3a693ab68afc6
Hasli verivikasi	Nilai Hash Sama

(a)

Hasil Verify Pencitraan	
Nama	NTFS TRIM ENABLE.001
Sector count	46864384
Nilai Hash MD5	
Computed Hash	d209a1a626d12b4c326f541c56915255
Laporan Hash	d209a1a626d12b4c326f541c56915255
Hasli verivikasi	Nilai Hash Sama

(b)

Gambar 4.8 (a) Pencitraan NTFS TRIM *Disable* (b) Pencitraan NTFS TRIM *Enable*

Hasil Verify Pencitraan	
Nama	ReFS TRIM DISABLE.001
Sector count	67833856
Nilai Hash MD5	
Computed Hash	018cd8000ca9a68104533c0823b280a1
Laporan Hash	018cd8000ca9a68104533c0823b280a1
Hasli verivikasi	Nilai Hash Sama

(a)

Hasil Verify Pencitraan	
Nama	REFS TRIM ENABLE.001
Sector count	67833856
Nilai Hash MD5	
Computed Hash	737b04c4ccb0c9e62ae5a51efa48ae1f
Laporan Hash	737b04c4ccb0c9e62ae5a51efa48ae1f
Hasli verivikasi	Nilai Hash Sama

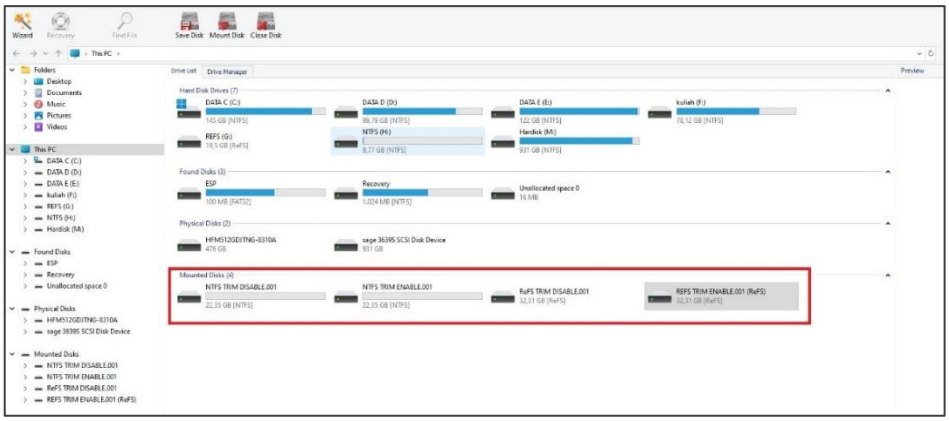
(b)

Gambar 4.9 (a) Pencitraan ReFS TRIM *disable* (b) Pencitraan ReFS TRIM *Enable*

4.5 *Recovery* Menggunakan Tool Hetman Partition Recovery

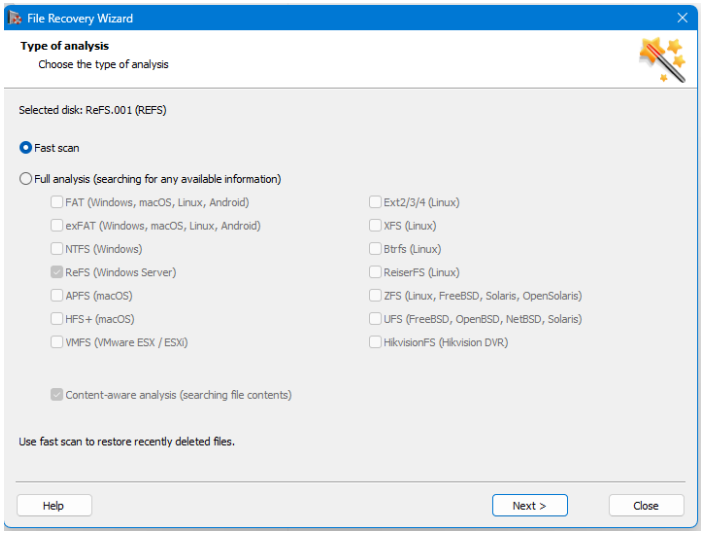
4.5.1 Reconstruction

Pada tahap ini sebelum mereka ulang *disk* hasil *imaging*, akan dilakukan duplikasi hasil *imaging*. Untuk menerapkan teknik *disk carving* dilakukan mounting *disk* hasil duplikasi file *imaging* FTK Imager portable agar aplikasi bisa membaca *disk* untuk melakukan scanning data yang telah dihapus di dalam partisi hasil mount *disk*, hasil mounting *disk* pada gambar 4.9 aplikasi tidak akan mengubah image yang telah di mount karena pada prosesnya hanya melakukan scanning data dengan teknik *disk carving* .



Gambar 4.10 Hasil Proses *Mounting Disk*

Setelah data di *mount* akan melakukan *scanning* dengan teknik *disk carving*, dengan pilihan *full scan* seperti gambar 4.10 maka aplikasi akan secara otomatis memeriksa data yang telah dihapus permanen. Teknik *disk carving* akan memeriksa *image* data yang telah di *mounting* berdasarkan *signature disk* file sistem untuk melakukan pemindaian mencari tempat potongan data yang telah dihapus permanen. Untuk menyatukan potongan data aplikasi akan menggunakan teknik file *carving*. Teknik file *carving* akan menyesuaikan *header* dan *footer* dari potongan file yang sama untuk disatukan. Proses *full scan* akan memakan waktu berdasarkan kecepatan transfer data dan pemrosesan dari komputer investigator.

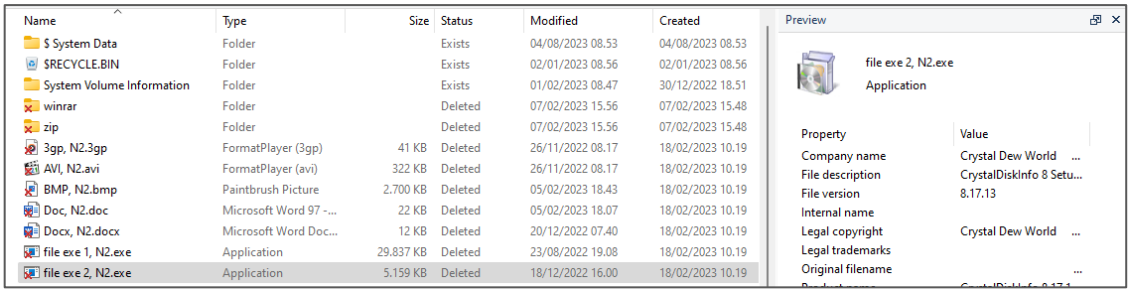


Gambar 4.11 Proses *Full Scan*

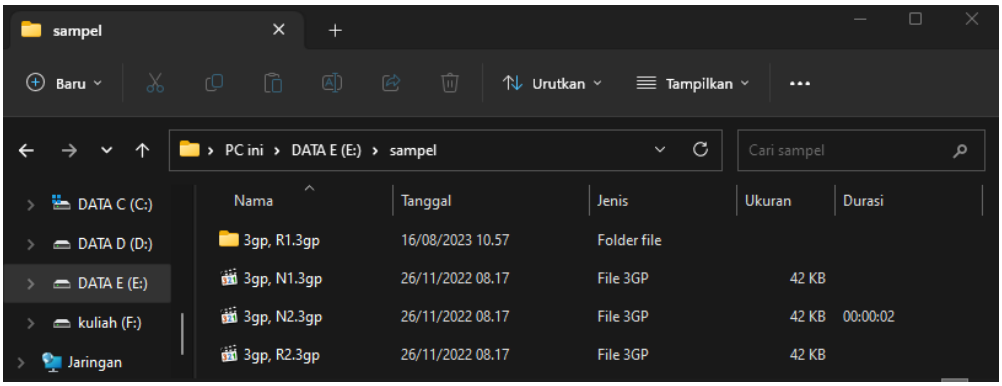
Proses *full scan* seperti gambar 4.11 akan memakan waktu bergantung pada kecepatan perangkat keras yang dimiliki dan banyak data yang akan diperiksa, dalam penelitian ini *scaning* memakan waktu lima sampai empat menit untuk setiap partisi hasil *imaging* yang diperiksa.

4.5.2 Extraction

Pada tahap ini, peneliti mengekstrak file pencitraan. Proses ini bertujuan untuk mendapatkan kembali file-file yang telah dihapus permanen oleh pelaku kejahatan. Untuk menjaga keutuhan dan keaslian barang bukti dilakukan duplikasi hasil *imaging* kemudian baru dilakukan ekstraksi bukti digital pada duplikat hasil *imaging*. Alat yang membantu proses ekstraksi pemeriksaan dan analisis pencitraan adalah hetman *partition recovery*. Gambar 4.12, adalah *scan* menggunakan alat hetman *partition recovery* yang menunjukkan bukti digital yang terhapus. Setelah di *scan* hasilnya akan di ekstrak ke komputer *investigator* seperti pada gambar 4.13.



Gambar 4.12 Hasil *Scan* NTFS TRIM *DISABLE*



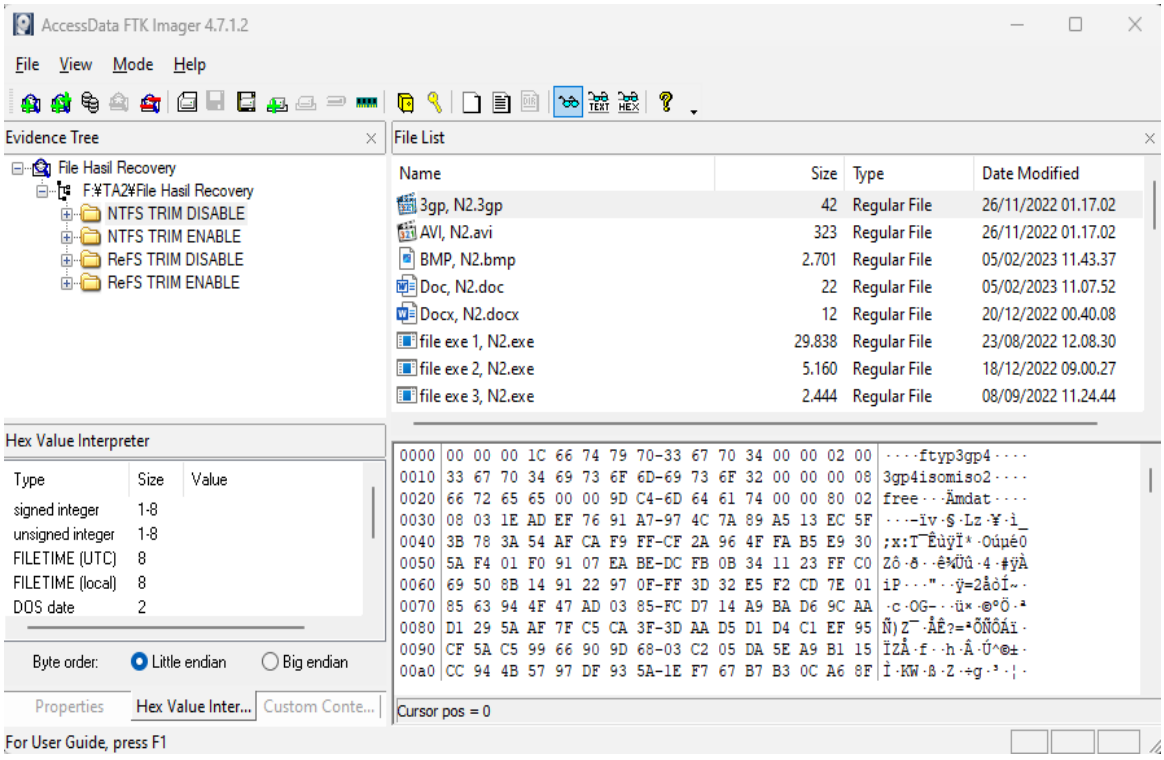
Gambar 4.13 Sampel Hasil Ekstraksi Data

Untuk menjaga integritas file setelah diekstraksi, peneliti mengunci file dengan nilai HASH md5 dari masing-masing file menggunakan FTK *imager*.

4.6 Analisis *Output Recovery* SSD

Proses analisis hasil akuisisi dilaksanakan menggunakan *Portable* FTK *Imager* dan HxD. Pada tahap ini, terlihat bahwa nilai file tanda tangan yang telah dihapus oleh fungsi TRIM, baik yang dinonaktifkan maupun diaktifkan. File tanda tangan ini berperan sebagai representasi informasi data yang digunakan untuk mengenali isi dari data tersebut (Jeong & Lee, 2019; Kessler, 2023). Gambar 4.14 menunjukkan, saat NTFS TRIM *disable*, *signature* masih utuh. Namun, Lain halnya dengan ReFS TRIM *disable* sebagian file mengalami

kerusakan karena telah terfragmentasi logis oleh file sistem. Sementara itu semua file pada ReFS TRIM *enable*, *signature* tidak bisa ditemukan karena data yang tersisa telah dibersihkan fitur TRIM saat *enable*, membuat data yang di*recovery* menjadi folder kosong.



Gambar 4.14 Tahap Analisis NTFS TRIM *Disable*

Dari hasil analisis menggunakan *tool* FTK *Imager* pada file sistem NTFS TRIM *disable* berdasarkan Gambar 4.14 file 3gp, N2.3gp ditunjukkan masih bisa diketahui ukuran dan waktu terakhir file tersebut dimodifikasi. Metadata file berada di bagian bawah seperti Gambar 4.14 diketahui bahwa masih utuh dengan awalan nilai hex 1C 66 74 79 70 33 67 70. Karena metadata file masih utuh maka dimungkinkan untuk dilakukan penguncian nilai dengan nilai HASH md5. Pada tahapan analisis NTFS TRIM *disable* semua file masih memiliki metadata yang utuh seperti contoh file AVI, N2.avi memiliki awalan nilai hex 52 49 46 46; file BMP, N2.bmp memiliki awalan 42 4D 36 30; file doc, N2.doc memiliki awalan nilai hex D0 CF 11 E0 A1 B1 1A E1, sementara file Docx, N2.

Docx memiliki awalan nilai hex 50 4B 03 04 14 00 06 00 semua analisis *footer* dan *header* file dari hasil *recovery* NTFS TRIM *disable* ditampilkan pada tabel 4.2. Metadata file akan memberikan informasi tambahan yang menyertai file dan memberikan konteks tentang file tersebut, Seperti ukuran, waktu pembuatan, waktu modifikasi, dan atribut lainnya sehingga memungkinkan identifikasi pemulihan data yang lebih baik, dan memfasilitasi penggunaan nilai hash untuk memastikan integritas file.

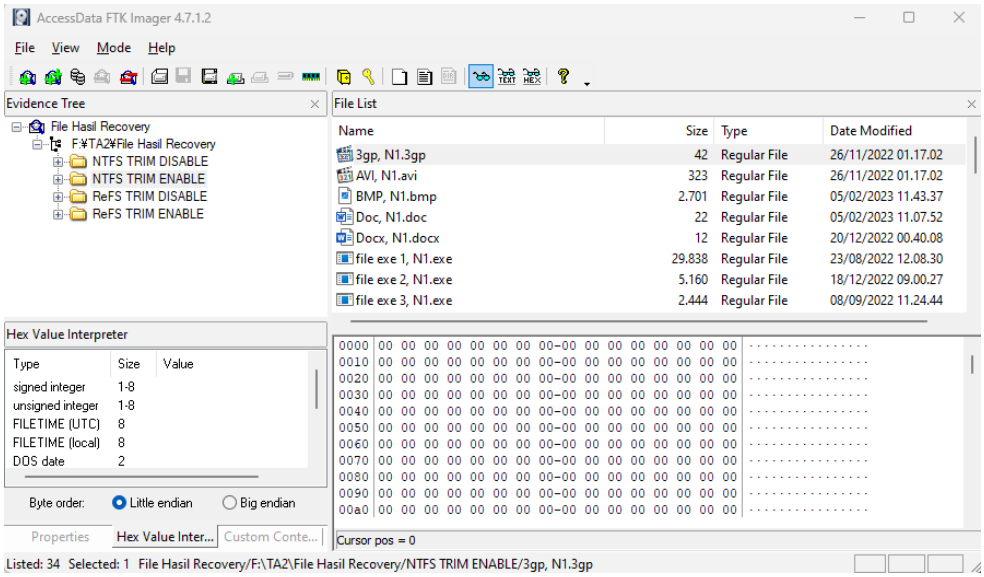
Tabel 4.2 Analisis *Output* Dari Hasil *Recovery* NTFS TRIM *Disable* SSD

NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
file exe 1, N2	.exe	4D 5A 90 00	F6 0B 29 96 1F 13 1C 43	23/08/2022 12.08.30	29.838 kb
file exe 2, N2	.exe	4D 5A 50 00	50 00 00 00 00 00 00 00	18/08/2022 12.08.30	5.160 kb
file exe 3, N2	.exe	4D 5A 90 00	41 94 C9 2F 58 E4 0C 00	08/09/2022 11.24.44	2.444 kb
Doc, N2	.doc	D0 CF 11 E0 A1 B1 1A E1	38 00 F4 39 B2 71 00 00	05/02/2023 11.07.52	22 kb
Docx, N2	.docx	50 4B 03 04 14 00 06 00	00 00 19 2C 00 00 00 00	20/12/2022 00.40.08	12 kb
ODT, N2	.odt	50 4B 03 04	00 0F 11 00 00 00 00	05/02/2023 11.08.39	5 kb
pdf, N2	.pdf	25 50 44 46	25 45 4F 46	05/02/2023 11.06.24	40 kb
PowerPoint, N2	.pptx	50 4B 03 04	00 00 DD 94 00 00 00 00	20/12/2022 00.41.00	41 kb
teks, N2	.txt	74 65 6B 6E 69 6B 20 66	75 61 74 2E	20/12/2022 00.39.33	134 bytes
XLSX, N2	.xlsx	50 4B 03 04	00 00 96 15 00 00 00 00	05/02/2023 11.04.13	7 kb
BMP, N2	.bmp	42 4D 36 30	1A 94 4B 19	05/02/2023 11.43.37	2.701 kb
GIF, N2	.gif	47 49 46 38	06 04 00 3B	05/02/2023 11.43.37	15 kb
JPG, N2	.jpg	FF D8 FF E0	FF D9	05/02/2023 11.43.37	163 kb
PNG, N2	.png	89 50 4E 47	60 82	05/02/2023 11.43.37	933 kb
m4a, N2	.m4a	00 00 00 1C 66 74 79 70	2E 31 30 31	02/05/2022 02.43.57	31.550 kb
mp3, N2	.mp3	49 44 33 04	33 2E 31 30 30 00 00 00	17/03/2023 01.56.01	6.101 kb
WAV, N2	.wav	52 49 46 46	FA FF 00 00 FF FF 00 00	02/05/2022 02.43.57	26.889 kb
WMA, N2	.wma	30 26 B2 75	4E 4E 4E 4E	02/05/2022 02.43.57	10.504 kb
3gp, N2	.3gp	1C 66 74 79 70 33 67 70	00 00 9D 68	26/11/2022 01.17.02	42 kb
AVI, N2	.avi	52 49 46 46	A0 D5 04 00 A2 01 00 00	26/11/2022 01.17.02	323 kb
FLV, N2	.flv	46 4C 56 01	00 00 00 10	26/11/2022 01.17.02	360 kb
MKV, N2	.mkv	1A 45 DF A3	79 F0 81 09	05/02/2023 11.37.54	78 kb
MOV, N2	.mov	00 00 00 14 66 74 79 70	2E 31 30 31	26/11/2022 01.17.02	359 kb
MP4, N2	.mp4	00 00 00 20 66 74 79 70	73 6D 68 64	26/11/2022 01.17.02	89 kb
MPG, N2	.mpg	00 00 01 BA 44 00 04 00	FF FF FF FF	26/11/2022 01.17.02	442 kb
OGG, N2	.Ogg	4F 67 67 53	50 35 00 0E	26/11/2022 01.17.02	352 kb
webm, N2	.webm	1A 45 DF A3 9F 42 86 81	EE F0 81 03	17/03/2023 01.56.01	64 kb

Tabel 4.3 Analisis *Output* Dari Hasil *Recovery* NTFS TRIM *Disable* SSD (Lanjutan)

NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
WMV, N2	.wmv	30 26 B2 75 8E 66 CF 11	4E 4E 4E 4E	02/05/2022 02.43.57	10.504 kb
RAR 1, N2	.rar	52 61 72 21	1D 77 56 51 03 05 04 00	20/12/2022 00.53.59	177 byte
RAR 2, N2	.rar	52 61 72 21	1D 77 56 51 03 05 04 00	05/02/2023 11.49.45	6 kb
RAR 3, N2	.rar	52 61 72 21	1D 77 56 51 03 05 04 00	05/02/2023 11.50.41	1.371 kb
zip 1, N2	.zip	50 4B 03 04	00 00 83 00 00 00 00 00	20/12/2022 00.54.14	243 byte
zip 2, N2	.zip	50 4B 03 04	00 00 BD 03 57 00 00 00	05/02/2023 11.51.48	5.570 kb
zip 3, N2	.zip	50 4B 03 04	00 00 64 C7 04 00 00 00	05/02/2023 11.52.48	306 kb

Tabel 4.2 – tabel 4.3 menjelaskan bahwa semua file yang telah dihapus permanen dengan file sistem NTFS dan perintah TRIM *disable* pada SSD berhasil di*recovery* dengan tidak ada perubahan metadata pada file yaitu Nama file, Ekstensi file, *header* file, *footer* file, *date modified/time modifed*, serta *size* yang sama dengan file asli.



Gambar 4.15 Tahap Analisis NTFS TRIM *Enable*

Hasil analisa berdasarkan gambar 4.15 hasil dari *recovery* pada kasus NTFS TRIM *enable* file dengan format 3gp dan sebagian besar file tidak memiliki *signature* yang jelas dan masih memungkinkan untuk dikunci dengan nilai hash md5 karena masih memiliki format dan data *size* file. Sehingga pada file sistem NTFS TRIM *enable* bisa diketahui fitur TRIM hanya menghapus metadata dari file seperti pada gambar 4.15 di bagian bawah kanan, tetapi masih menyisakan ukuran dan kapan waktu terakhir file dimodifikasi sehingga adanya kemungkinan file yang telah dihapus bisa dipulihkan dan dikunci dengan nilai hash md5.

Pada tabel 4.4 – 4.5 di tunjukan *header* file dan *footer* file yang dimiliki teks, N1; rar 1, N1; zip 1, N1 memiliki size file di bawah 700 bytes sehingga memiliki kesempatan tinggi file akan berhasil dipulihkan. proses analisis *output* file yang bisa *direcovery* pada TRIM *enable* akan dilanjutkan pada perbandingan hasil *recovery.*

Tabel 4.4 Analisis Output Dari Hasil *Recovery* NTFS TRIM *Enable* SSD

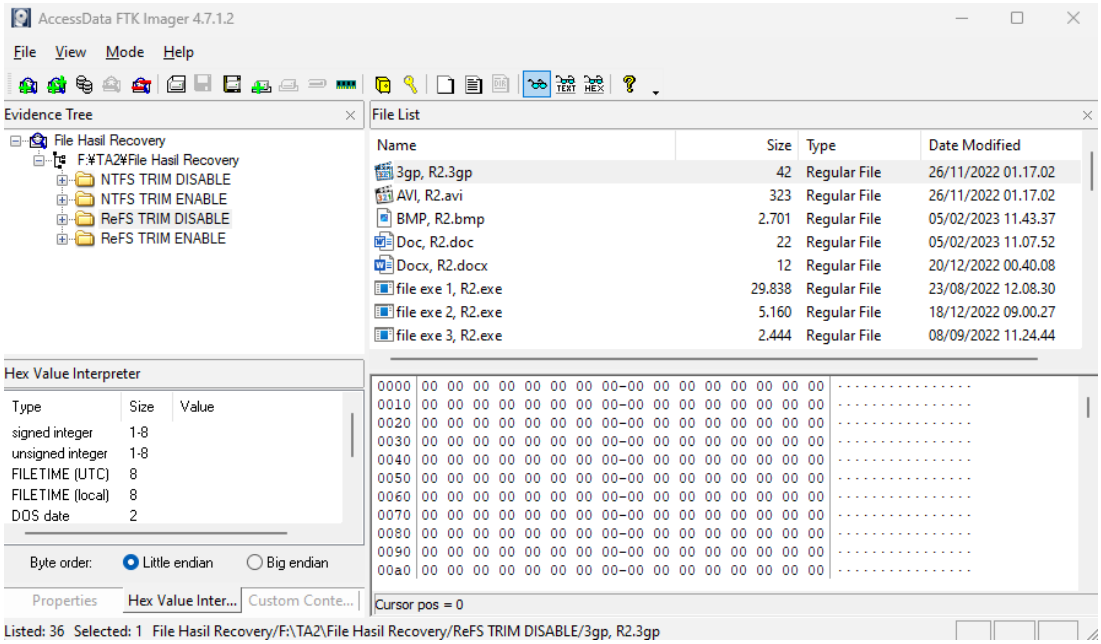
NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
file exe 1, N1	.exe	00 00 00 00	00 00 00 00	23/08/2022 12.08.30	29.838 kb
file exe 2, N1	.exe	00 00 00 00	00 00 00 00	18/12/2022 09.00.27	5.160 kb
file exe 3, N1	.exe	00 00 00 00	00 00 00 00	08/09/2022 11.24.44	2.444 kb
Doc, N1	.doc	00 00 00 00	00 00 00 00	05/02/2023 11.07.52	22 kb
Docx, N1	.docx	00 00 00 00	00 00 00 00	20/12/2022 00.40.08	12 kb
ODT, N1	.odt	00 00 00 00	00 00 00 00	05/02/2023 11.08.39	5 kb
pdf, N1	.pdf	00 00 00 00	00 00 00 00	05/02/2023 11.06.24	40 kb
PowerPoint, N1	.pptx	00 00 00 00	00 00 00 00	20/12/2022 00.41.00	41 kb
teks, N1	.txt	74 65 6B 6E 69 6B 20 66	75 61 74 2E	20/12/2022 00.39.33	134 byte
XLSX, N1	.xlsx	00 00 00 00	00 00 00 00	05/02/2023 11.04.13	7 kb
BMP, N1	.bmp	00 00 00 00	00 00 00 00	05/02/2023 11.43.37	2.701 kb
GIF, N1	.gif	00 00 00 00	00 00 00 00	05/02/2023 11.43.37	15 kb
JPG, N1	.jpg	00 00 00 00	00 00	05/02/2023 11.43.37	163 kb
PNG, N1	.png	00 00 00 00	00 00	05/02/2023 11.43.37	933 kb
m4a, N1	.m4a	00 00 00 00 00 00 00 00	00 00 00 00	02/05/2022 02.43.57	31.550 kb
mp3, N1	.mp3	00 00 00 00	00 00 00 00 00 00 00 00	17/03/2023 02.12.49	6.101 kb
WAV, N1	.wav	00 00 00 00	00 00 00 00 00 00 00 00	02/05/2022 02.43.57	26.889 kb
WMA, N1	.wma	00 00 00 00	00 00 00 00	02/05/2022 02.43.57	10.504 kb
3gp, N1	.3gp	00 00 00 00 00 00 00 00	00 00 00 00	26/11/2022 01.17.02	42 kb
AVI, N1	.avi	00 00 00 00	00 00 00 00 00 00 00 00	26/11/2022 01.17.02	323 kb
FLV, N1	.flv	00 00 00 00	00 00 00 00	26/11/2022 01.17.02	360 kb
MKV, N1	.mkv	00 00 00 00	00 00 00 00	05/02/2023 11.37.54	78 kb
MOV, N1	.mov	00 00 00 00 00 00 00 00	00 00 00 00	26/11/2022 01.17.02	359 kb
MP4, N1	.mp4	00 00 00 00 00 00 00 00	00 00 00 00	26/11/2022 01.17.02	89 kb

Tabel 4.5 Analisis Output Dari Hasil *Recovery* NTFS TRIM *Enable* SSD (Lanjutan)

NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
MPG, N1	.mpg	00 00 00 00 00 00 00 00	00 00 00 00	26/11/2022 01.17.02	442 kb
OGG, N1	.Ogg	00 00 00 00	00 00 00 00	26/11/2022 01.17.02	352 kb
webm, N1	.webm	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	17/03/2023 02.12.49	64 kb
WMV, N1	.wmv	00 00 00 00 00 00 00 00	00 00 00 00	02/05/2022 02.43.57	10.504 kb
RAR 1, N1	.rar	52 61 72 21	1D 77 56 51 03 05 04 00	20/12/2022 00.53.59	177 byte
RAR 2, N1	.rar	00 00 00 00	00 00 00 00 00 00 00 00	05/02/2023 11.49.45	6 kb
RAR 3, N1	.rar	00 00 00 00	00 00 00 00 00 00 00 00	05/02/2023 11.50.41	1.371 kb
zip 1, N1	.zip	50 4B 03 04	00 00 83 00 00 00 00 00	20/12/2022 00.54.14	243 byte
zip 2, N1	.zip	00 00 00 00	00 00 00 00 00 00 00 00	05/02/2023 11.51.48	5.570 kb
zip 3, N1	.zip	00 00 00 00	00 00 00 00 00 00 00 00	05/02/2023 11.52.48	306 kb

Selain itu file text, N1 masih memiliki nilai *signature* header dan footer yang utuh dengan *setting* TRIM *enable* saat menghapus file, hal yang sama terjadi dengan file RAR 1, N1 dan zip 1, N1 ini bisa terjadi karena file sistem NTFS menggunakan struktur metadata yang berbeda. Salah satu tugas struktur metadata file sistem adalah menandai lokasi file-file yang ada di dalam penyimpanan, jadi yang terjadi saat penghapusan file text, N1 oleh user, NTFS tidak menandai bahwa file tersebut bebas atau usang. Fitur TRIM menerima data file yang ditandai untuk dihapus tetapi tidak menemukan file dengan ekstensi .txt, file text, N1 yang telah dihapus oleh pengguna. Jadi hanya jalur untuk sampai ke file tersebut yang dihapus.

Selanjutnya berdasarkan analisis ReFS TRIM *disable* yang merujuk gambar 4.16 sebagian file mengalami kerusakan metadata file menunjukkan angka 0 karena data yang telah *terfragmentasi* logis. Pada analisa ReFS TRIM *disable* fitur TRIM tidak mempengaruhi file yang telah dihapus. Dalam partisi file sistem ReFS ditemukan file yang telah usang atau dihapus permanen dengan nilai hexadecimal menjadinya menjadi 0 seperti pada gambar 4.16 dibagikan kanan bawah, sehingga saat file baru dimasukkan ke ruang penyimpanan SSD maka file sistem akan mengatur file baru untuk bisa menempatkan file baru ke block yang sudah dibersihkan dengan hexadecimal 0.



Gambar 4.16 Tahap Analisis ReFS TRIM *Disable*

Dengan adanya fitur fragmentasi ini file sistem ReFS akan menysun ulang file yang telah dihapus permanen menjadi satu dalam file tmp. Sehingga ReFS memiliki keunggulan dalam kecepatan dalam proses transfer data pada saat fitur TRIM SSD *disable*. pada tabel 4.6 - 4.7 ditunjukkan file yang telah mengalami fragmentasi logis tidak berhasil dipulihkan melihat dari pengecekan isi metadata *header* dan *footer* yang kosong pada file yang telah di*recovery.*

Tabel 4.6 Analisis Output Dari Hasil *Recovery* ReFS TRIM *Disable* SSD

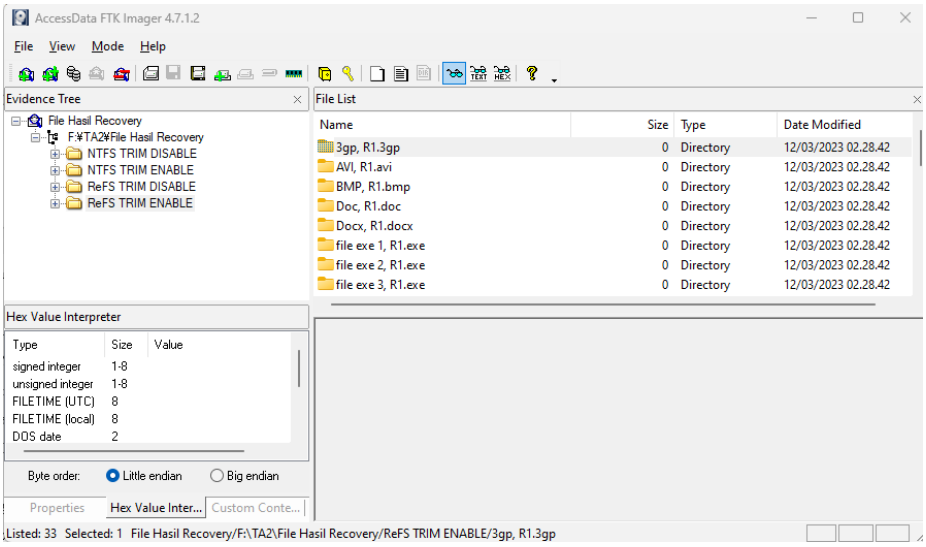
NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
file exe 1, R2	.exe	4D 5A 90 00	F6 0B 29 96 1F 13 1C 43	23/08/2022 12.08.30	29.838 kb
file exe 2, R2	.exe	4D 5A 50 00	50 00 00 00 00 00 00 00	18/12/2022 09.00.27	5.160 kb
file exe 3, R2	.exe	4D 5A 90 00	41 94 C9 2F 58 E4 0C 00	08/09/2022 11.24.44	2.444 kb
Doc, R2	.doc	D0 CF 11 E0 A1 B1 1A E1	38 00 F4 39 B2 71 00 00	05/02/2023 11.07.52	22 kb
Docx, R2	.docx	50 4B 03 04 14 00 06 00	00 00 19 2C 00 00 00 00	20/12/2022 00.40.08	12 kb
ODT, R2	.odt	50 4B 03 04	00 0F 11 00 00 00 00	05/02/2023 11.08.39	5 kb
pdf, R2	.pdf	25 50 44 46	25 45 4F 46	05/02/2023 11.06.24	40 kb
PowerPoint, R2	.pptx	50 4B 03 04	00 00 DD 94 00 00 00 00	20/12/2022 00.41.00	41 kb
teks, R2	.txt	74 65 6B 6E 69 6B 20 66	75 61 74 2E	20/12/2022 00.39.33	134 byte
XLSX, R2	.xlsx	00 00 00 00	00 00 00 00 00 00 00 00	05/02/2023 11.04.13	7 kb
BMP, R2	.bmp	42 4D 36 30	1A 94 4B 19	05/02/2023 11.43.37	2.701 kb

Tabel 4.7 Analisis Output Dari Hasil *Recovery* ReFS TRIM *Disable* SSD (Lanjutan)

NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
GIF, R2	.gif	47 49 46 38	06 04 00 3B	05/02/2023 11.43.37	15 kb
JPG, R2	.jpg	FF D8 FF E0	FF D9	05/02/2023 11.43.37	163 kb
PNG, R2	.png	89 50 4E 47	60 82	05/02/2023 11.43.37	933 kb
m4a, R2	.m4a	00 00 00 1C 66 74 79 70	2E 31 30 31	02/05/2022 02.43.57	31.550 kb
mp3, R2	.mp3	-	-	02/05/2022 02.43.57	0 kb
WAV, R2	.wav	52 49 46 46	02 00 04 00 02 00 04 00	02/05/2022 02.43.57	26.889 kb
WMA, R2	.wma	30 26 B2 75	4E 4E 4E 4E	02/05/2022 02.43.57	10.504 kb
3gp, R2	.3gp	00 00 00 00 00 00 00 00	00 00 00 00	26/11/2022 01.17.02	42 kb
AVI, R2	.avi	52 49 46 46	A0 D5 04 00 A2 01 00 00	26/11/2022 01.17.02	323 kb
FLV, R2	.flv	46 4C 56 01	00 00 00 10	26/11/2022 01.17.02	360 kb
MKV, R2	.mkv	1A 45 DF A3	79 F0 81 09	05/02/2023 11.37.54	78 kb
MOV, R2	.mov	00 00 00 14 66 74 79 70	2E 31 30 31	26/11/2022 01.17.02	359 kb
MP4, R2	.mp4	00 00 00 20 66 74 79 70	73 6D 68 64	26/11/2022 01.17.02	89 kb
MPG, R2	.mpg	00 00 01 BA 44 00 04 00	FF FF FF FF	26/11/2022 01.17.02	442 kb
OGG, R2	.Ogg	4F 67 67 53	50 35 00 0E	26/11/2022 01.17.02	352 kb
webm, R2	.webm	-	-	05/02/2023 11.35.48	0 kb
WMV, R2	.wmv	00 00 00 00 00 00 00 00	00 00 00 00	26/11/2022 01.17.02	361 kb
RAR 1, R2	.rar	52 61 72 21	1D 77 56 51 03 05 04 00	20/12/2022 00.53.59	177 byte
RAR 2, R2	.rar	52 61 72 21	1D 77 56 51 03 05 04 00	05/02/2023 11.49.45	6 kb
RAR 3, R2	.rar	52 61 72 21	1D 77 56 51 03 05 04 00	05/02/2023 11.50.41	1.371 kb
zip 1, R2	.zip	00 00 00 00	00 00 00 00 00 00 00 00	20/12/2022 00.54.14	243 byte
zip 2, R2	.zip	50 4B 03 04	14 12 FF 23 CF 8F 01 4A	05/02/2023 11.51.48	5.570 kb
zip 3, R2	.zip	50 4B 03 04	00 00 64 C7 04 00 00 00	05/02/2023 11.52.48	306 kb

Dari gambar 4.17 berhasil diketahui bahwa file sistem akan mempengaruhi TRIM dalam melakukan operasi pembersihan data yang telah dihapus permanen, Saat pengguna pada file sistem ReFS menghapus data permanen maka fitur TRIM akan mengubah data tersebut menjadi folder kosong dan tidak memiliki *size* sehingga semua file hasil *recovery*

tidak dimungkinkan untuk dikunci dengan nilai HASH. Hal ini menunjukkan bahwa file sistem ReFS memiliki ketangguhan dalam menangani kerusakan data dan eror yang berkemungkinan terjadi pada saat data dihapus permanen. Saat fitur TRIM mendeteksi file sistem yang digunakan adalah ReFS, sistem operasi akan membuat semua data yang telah dihapus permanen memerintahkan TRIM untuk menandai semua bagian file tidak hanya metadata file tetapi *file size* dan *date modified* yang tersimpan di *block* bagian pencatat file dalam file sistem untuk dibersihkan sepenuhnya. Saat semua file telah dihapus permanen, file tersebut tidak akan ditemukan lagi pada bagian database file sistem ataupun *block* penyimpanan sehingga hasil *recovery* hanya sebuah folder seperti gambar 4.17.



Gambar 4.17 Tahap Analisis ReFS TRIM *Enable*

Semua pemrosesan tersebut terjadi di latar belakang sistem operasi sehingga pengguna tidak bisa mendeteksi file tersebut telah dibersihkan atau belum. karena sebagian file dengan file *size* yang lebih besar membutuhkan waktu untuk terbersihkah sepenuhnya, maka sebaiknya jika komputer masih hidup saat data baru saja dihapus segera untuk melakukan live forensik agar data yang belum sempat dibersihkan TRIM bisa dipulihkan. Penanganan dan pendokumentasian barang bukti dengan tepat sangat krusial dalam melakukan live forensik, terutama jika hasilnya akan digunakan sebagai bukti dalam pengadilan.

Tabel 4.8 Analisis *Output* Dari Hasil *Recovery* ReFS TRIM *Enable* SSD

NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
file exe 1, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
file exe 2, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
file exe 3, R1	Folder	-	-	12/03/2023 02.28.42	0 kb

Tabel 4. 9 Analisis *Output* Dari Hasil *Recovery* ReFS TRIM *Enable* SSD (Lanjutan)

NAMA FILE	***Ekstensi File***	***Header* File**	***Footer* file**	***Date Modified/ Time Modified***	***Size***
Doc, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
Docx, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
ODT, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
pdf, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
PowerPoint, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
teks, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
XLSX, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
BMP, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
GIF, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
JPG, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
PNG, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
m4a, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
mp3, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
WAV, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
WMA, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
3gp, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
AVI, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
FLV, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
MKV, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
MOV, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
MP4, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
MPG, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
OGG, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
webm, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
WMV, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
RAR 1, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
RAR 2, R1	Folder	-	-	12/03/2023 02.28.42	0 kb

Tabel 4. 10 Analisis Output Dari Hasil Recovery ReFS TRIM Enable SSD (Lanjutan)

NAMA FILE	*Ekstensi File*	*Header* File	*Footer* file	*Date Modified/ Time Modified*	*Size*
RAR 3, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
zip 1, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
zip 2, R1	Folder	-	-	12/03/2023 02.28.42	0 kb
zip 3, R1	Folder	-	-	12/03/2023 02.28.42	0 kb

Pada tabel 4.8 – 4.10 ditunjukkan keadaan file yang telah dihapus saat *setting* TRIM di*enable* pada volume ReFS, semua file berbentuk folder dan tidak menyisakan metadata file yang berhasil diambil hanya nama file. Ini menunjukkan bahwa Volume ReFS melakukan pembersihan file lebih baik dari Volume NTFS.

4.7 Perbandingan Hasil *Recovery* Volume NTFS dan ReFS

Indikator yang menunjukkan keberhasilan atau kegagalan hasil *recovery* pada penelitian kali ini adalah pencocokan nilai HASH MD5 file asli dan nilai MD5 file hasil *recovery*, jika kedua nilai HASH sama maka bisa dikatakan file berhasil *direcovery* dan jika nilai HASH tidak sama maka file hasil *recovery* dapat dikatakan gagal. Untuk nilai HASH MD5 file asli didapatkan pada BAB 3 bagian analisis *output* SSD volume ReFS dan NTFS yang ditunjukkan pada tabel 3.2 sampai tabel 3.5. Data - data file penelitian ini yang berhasil dan gagal di*recovery* ditunjukkan pada tabel 4.11 sampai 4.14.

Tabel 4.11 Hasil *Recovery* SSD Trim *Disable* File Sistem NTFS

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
1	file exe 1, N2	.exe	MD5 File Asli: e67e681e116f50d14a557cd83e83596a MD5 File Hasil *Recovery:* e67e681e116f50d14a557cd83e83596a	Sukses
2	file exe 2, N2	.exe	MD5 File Asli: e500b16147893a4b4aa6a71a0b494475 MD5 File Hasil *Recovery:* e500b16147893a4b4aa6a71a0b494475	Sukses
3	file exe 3, N2	.exe	MD5 File Asli: 375276a153cfcd10b60141a1bf6d4126 MD5 File Hasil *Recovery:* 375276a153cfcd10b60141a1bf6d4126	Sukses
4	Doc, N2	.doc	MD5 File Asli: 202bed6dade8a6b45f315af6ed4fec01 MD5 File Hasil *Recovery:* 202bed6dade8a6b45f315af6ed4fec01	Sukses
5	Docx, N2	.docx	MD5 File Asli: 2a2539f683f34f5dc3a31f125601d94e MD5 File Hasil *Recovery:* 2a2539f683f34f5dc3a31f125601d94e	Sukses
6	ODT, N2	.odt	MD5 File Asli: b43a20b258af2db416d87368ea99e871 MD5 File Hasil *Recovery:* b43a20b258af2db416d87368ea99e871	Sukses

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
7	pdf, N2	.pdf	MD5 File Asli: de61ec3a4bfdba769b63b2817d65abca MD5 File Hasil *Recovery:* de61ec3a4bfdba769b63b2817d65abca	Sukses
8	PowerPoint, N2	.pptx	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* 16bc6e9ff52573c9a133117e469578c6	Sukses
9	teks, N2	.txt	MD5 File Asli: 9fdbfbd6b9f80a12a4aed69366b1598f MD5 File Hasil *Recovery:* 9fdbfbd6b9f80a12a4aed69366b1598f	Sukses
10	XLSX, N2	.xlsx	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* 16bc6e9ff52573c9a133117e469578c6	Sukses
11	BMP, N2	.bmp	MD5 File Asli: 60575664b29c4747ec20bc298394a6db MD5 File Hasil *Recovery:* 60575664b29c4747ec20bc298394a6db	Sukses
12	GIF, N2	.gif	MD5 File Asli: cf69c943fa8eea1605295ead83242f7a MD5 File Hasil *Recovery:* cf69c943fa8eea1605295ead83242f7a	Sukses
13	JPG, N2	.jpg	MD5 File Asli: a3333bb3df4b47dd6a3a6abf4bede7ad MD5 File Hasil *Recovery:* a3333bb3df4b47dd6a3a6abf4bede7ad	Sukses
14	PNG, N2	.png	MD5 File Asli: 068f0a46761a2c77df687f402f263a86 MD5 File Hasil *Recovery:* 068f0a46761a2c77df687f402f263a86	Sukses
15	m4a, N2	.m4a	MD5 File Asli: 27d27b8eb61f5f9d19753d517de0554e MD5 File Hasil *Recovery:* 27d27b8eb61f5f9d19753d517de0554e	Sukses
16	mp3, N2	.mp3	MD5 File Asli: 180b9de2ce8454e8862a37e33e8a5ed1 MD5 File Hasil *Recovery:* 180b9de2ce8454e8862a37e33e8a5ed1	Sukses
17	WAV, N2	.wav	MD5 File Asli: 8f775199f5bf8a7a030185af4257ca5d MD5 File Hasil *Recovery:* 8f775199f5bf8a7a030185af4257ca5d	Sukses
18	WMA, N2	.wma	MD5 File Asli: 5717ede6eda50aeb373b621312ffbc3d MD5 File Hasil *Recovery:* 5717ede6eda50aeb373b621312ffbc3d	Sukses
19	3gp, N2	.3gp	MD5 File Asli: 1ecc9837edc86b3370be6e85a2a0c4af MD5 File Hasil *Recovery:* 1ecc9837edc86b3370be6e85a2a0c4af	Sukses
20	AVI, N2	.avi	MD5 File Asli: 611daaf923e0f755ce19b8f981ccc8bf MD5 File Hasil *Recovery:* 611daaf923e0f755ce19b8f981ccc8bf	Sukses
21	FLV, N2	.flv	MD5 File Asli: 54a827a332666830c3404c817cc1d934 MD5 File Hasil *Recovery:* 54a827a332666830c3404c817cc1d934	Sukses
22	MKV, N2	.mkv	MD5 File Asli: c08dc5bdebe741ca10dee0142a34fd17 MD5 File Hasil *Recovery:* c08dc5bdebe741ca10dee0142a34fd17	Sukses
23	MOV, N2	.mov	MD5 File Asli: 440fd3c73c4be0bc1f9fae3955dfcbbf MD5 File Hasil *Recovery:* 440fd3c73c4be0bc1f9fae3955dfcbbf	Sukses
24	MP4, N2	.mp4	MD5 File Asli: 8b6e8415ada32d939eba45f75388c2aa MD5 File Hasil *Recovery:* 8b6e8415ada32d939eba45f75388c2aa	Sukses

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
25	MPG, N2	.mpg	MD5 File Asli: 3af1c20309fb85e8de8092c30425a106 MD5 File Hasil *Recovery:* 3af1c20309fb85e8de8092c30425a106	Sukses
26	OGG, N2	.Ogg	MD5 File Asli: 69a4ca496c2c4472db7e6edd8a1db388 MD5 File Hasil *Recovery:* 69a4ca496c2c4472db7e6edd8a1db388	Sukses
27	webm, N2	.webm	MD5 File Asli: bf23511f8770f9d5c74edc33836b488a MD5 File Hasil *Recovery:* bf23511f8770f9d5c74edc33836b488a	Sukses
28	WMV, N2	.wmv	MD5 File Asli: 52289d287f8522b4973372fd8fe0a642 MD5 File Hasil *Recovery:* 52289d287f8522b4973372fd8fe0a642	Sukses
29	RAR 1, N2	.rar	MD5 File Asli: 76a42cc2609e2cfe2784077248ecceb7 MD5 File Hasil *Recovery:* 76a42cc2609e2cfe2784077248ecceb7	Sukses
30	RAR 2, N2	.rar	MD5 File Asli: 8251719177e9bd5d549963c04829c9d3 MD5 File Hasil *Recovery:* 8251719177e9bd5d549963c04829c9d3	Sukses
31	RAR 3, N2	.rar	MD5 File Asli: 3ca2fbabcb23b6fc9a0763bc9297fe01 MD5 File Hasil *Recovery:* 3ca2fbabcb23b6fc9a0763bc9297fe01	Sukses
32	zip 1, N2	.zip	MD5 File Asli: 5349d6809d2cf1e8d82931b880265a9d MD5 File Hasil *Recovery:* 5349d6809d2cf1e8d82931b880265a9d	Sukses
33	zip 2, N2	.zip	MD5 File Asli: 18271d308f0c4aaebbf72c0e76ebab66 MD5 File Hasil *Recovery:* 18271d308f0c4aaebbf72c0e76ebab66	Sukses
34	zip 3, N2	.zip	MD5 File Asli: c4e514a94643a96243dd347972963ec5 MD5 File Hasil *Recovery:* c4e514a94643a96243dd347972963ec5	Sukses

Persentase keberhasilan *recovery* = $\frac{34}{34}$ x 100% = 100%

Dari tabel 4.11 ditunjukkan bahwa semua file yang telah dihapus permanen (Shift+delete) berhasil dipulihkan sepenuhnya karena setiap file memiliki nilai hash yang sama dengan file asli. Setting Fitur TRIM *disable* dilakukan sehingga SSD masih menyisakan data yang telah dihapus permanen menjadi bisa dipulihkan. Pada kasus ini file sistem hanya menghilangkan alamat file yang telah dihapus permanen sehingga menjadi tidak bisa ditemukan secara normal melalui *windows explorer*. Berdasarkan pengecekan nilai hash md5 yang telah dilakukan dengan menggunakan FTK *Imager* hasil menunjukkan bahwa semua file memiliki nilai hash yang sama dengan file asli. Teknik *carving* akan melakukan *scan header* dan *footer* serta mencari metadata file yang masih utuh di dalam volume NTFS dengan *setting* TRIM *disable* sehingga file yang telah dihapus permanen menjadi bisa untuk dipulihkan kembali dalam keadaan normal. Dari berbagai *extensi* file yang berbeda semua file berhasil dipulihkan.

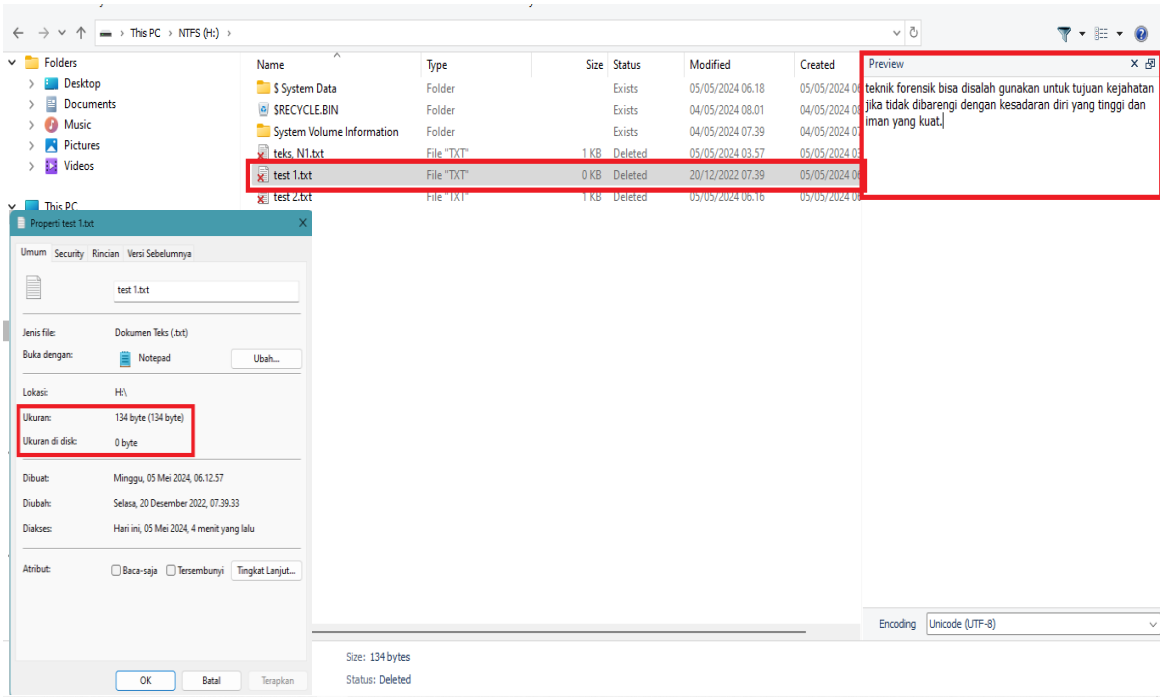
Tabel 4.12 Hasil *Recovery* SSD Trim *Enable* File System NTFS

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil Recovery
1	file exe 1, N1	.exe	MD5 File Asli: e67e681e116f50d14a557cd83e83596a MD5 File Hasil *Recovery:* 9169444a06f40661bfe7515f293f819f	Gagal
2	file exe 2, N1	.exe	MD5 File Asli: e500b16147893a4b4aa6a71a0b494475 MD5 File Hasil *Recovery:* c38dac66f18d00b30cf7dea733ea2a41	Gagal
3	file exe 3, N1	.exe	MD5 File Asli: 375276a153cfcd10b60141a1bf6d4126 MD5 File Hasil *Recovery:* ad5425ffc7c2068b12b605310274fe38	Gagal
4	Doc, N1	.doc	MD5 File Asli: 202bed6dade8a6b45f315af6ed4fec01 MD5 File Hasil *Recovery:* 0231a10415a008d131d2b5ecd0e794c8	Gagal
5	Docx, N1	.docx	MD5 File Asli: 2a2539f683f34f5dc3a31f125601d94e MD5 File Hasil *Recovery:* 3dfa7a695bc85ebc0405c7a44bc6be19	Gagal
6	ODT, N1	.odt	MD5 File Asli: b43a20b258af2db416d87368ea99e871 MD5 File Hasil *Recovery:* 52dabc872d3723b3f6ec82d0f509bee2	Gagal
7	pdf, N1	.pdf	MD5 File Asli: de61ec3a4bfdba769b63b2817d65abca MD5 File Hasil *Recovery:* c1da441e912c93ce03e6a8cbd0c09574	Gagal
8	PowerPoint, N1	.pptx	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* d8701e3fb748fc791c721969a6b9d2ef	Gagal
9	teks, N1	.txt	MD5 File Asli: 9fdbfbd6b9f80a12a4aed69366b1598f MD5 File Hasil *Recovery:* 9fdbfbd6b9f80a12a4aed69366b1598f	Sukses
10	XLSX, N1	.xlsx	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* dc8d5e956fb9ba57fd459ffd4da1c798	Gagal
11	BMP, N1	.bmp	MD5 File Asli: 60575664b29c4747ec20bc298394a6db MD5 File Hasil *Recovery:* 7f5da6c96e95568debf431e835eda5fc	Gagal
12	GIF, N1	.gif	MD5 File Asli: cf69c943fa8eea1605295ead83242f7a MD5 File Hasil *Recovery:* a28367241f1afa1dac4979457819e7f9	Gagal
13	JPG, N1	.jpg	MD5 File Asli: a3333bb3df4b47dd6a3a6abf4bede7ad MD5 File Hasil *Recovery:* 9e5d9eb9c90cbadfedda9e424199c135	Gagal
14	PNG, N1	.png	MD5 File Asli: 068f0a46761a2c77df687f402f263a86 MD5 File Hasil *Recovery:* ddd8bddce6268f905cdb9754952dbfc4	Gagal
15	m4a, N1	.m4a	MD5 File Asli: 27d27b8eb61f5f9d19753d517de0554e MD5 File Hasil *Recovery:* d0dfdcac3c3292772bd7da16f9341edb	Gagal
16	mp3, N1	.mp3	MD5 File Asli: 180b9de2ce8454e8862a37e33e8a5ed1 MD5 File Hasil *Recovery:* 235332b810b7c09f8aef5ca954f523a7	Gagal
17	WAV, N1	.wav	MD5 File Asli: 8f775199f5bf8a7a030185af4257ca5d MD5 File Hasil *Recovery:* 4f057099f7a5f65b26f045369f194362	Gagal

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil Recovery
18	WMA, N1	.wma	MD5 File Asli: 5717ede6eda50aeb373b621312ffbc3d MD5 File Hasil *Recovery:* 3abac356cbce09fa1779d22dead36d28	Gagal
19	3gp, N1	.3gp	MD5 File Asli: 1ecc9837edc86b3370be6e85a2a0c4af MD5 File Hasil *Recovery:* a1c3c3c26cbee786570ee6b2eb3df3fb	Gagal
20	AVI, N1	.avi	MD5 File Asli: 611daaf923e0f755ce19b8f981ccc8bf MD5 File Hasil *Recovery:* 83a6d597341af4102821c6bc2eff96f7	Gagal
21	FLV, N1	.flv	MD5 File Asli: 54a827a332666830c3404c817cc1d934 MD5 File Hasil *Recovery:* 432de84989f8f8948cfdc54f3d676737	Gagal
22	MKV, N1	.mkv	MD5 File Asli: c08dc5bdebe741ca10dee0142a34fd17 MD5 File Hasil *Recovery:* 1a9f14f7de17faadec899f9b3275d903	Gagal
23	MOV, N1	.mov	MD5 File Asli: 440fd3c73c4be0bc1f9fae3955dfcbbf MD5 File Hasil *Recovery:* bc464e6f945c9e654cd1d7bcab63a701	Gagal
24	MP4, N1	.mp4	MD5 File Asli: 8b6e8415ada32d939eba45f75388c2aa MD5 File Hasil *Recovery:* 06bf27971fd6915f41299605d668129e	Gagal
25	MPG, N1	.mpg	MD5 File Asli: 3af1c20309fb85e8de8092c30425a106 MD5 File Hasil *Recovery:* 36859069000eec24debd967f819b9915	Gagal
26	OGG, N1	.Ogg	MD5 File Asli: 69a4ca496c2c4472db7e6edd8a1db388 MD5 File Hasil *Recovery:* 83fa28afc521684fe11694494fd90564	Gagal
27	webm, N1	.webm	MD5 File Asli: bf23511f8770f9d5c74edc33836b488a MD5 File Hasil *Recovery:* 5bba319b01d88e99ed8b0d575271a194	Gagal
28	WMV, N1	.wmv	MD5 File Asli: 52289d287f8522b4973372fd8fe0a642 MD5 File Hasil *Recovery:* 87e3a7f011492bf6c27ebed0042033fb	Gagal
29	RAR 1, N1	.rar	MD5 File Asli: 76a42cc2609e2cfe2784077248ecceb7 MD5 File Hasil *Recovery:* 76a42cc2609e2cfe2784077248ecceb7	Sukses
30	RAR 2, N1	.rar	MD5 File Asli: 8251719177e9bd5d549963c04829c9d3 MD5 File Hasil *Recovery:* b82eecf8b33078201cfd1b25f4e74f0c	Gagal
31	RAR 3, N1	.rar	MD5 File Asli: 3ca2fbabcb23b6fc9a0763bc9297fe01 MD5 File Hasil *Recovery:* bc48758e738f0088aabb04ac1b67a15c	Gagal
32	zip 1, N1	.zip	MD5 File Asli: 5349d6809d2cf1e8d82931b880265a9d MD5 File Hasil *Recovery:* 5349d6809d2cf1e8d82931b880265a9d	Sukses
33	zip 2, N1	.zip	MD5 File Asli: 18271d308f0c4aaebbf72c0e76ebab66 MD5 File Hasil *Recovery:* ed10a316d74893eff8727337c5078817	Gagal
34	zip 3, N1	.zip	MD5 File Asli: c4e514a94643a96243dd347972963ec5 MD5 File Hasil *Recovery:* fc382e6b39d0595298967d2a78e59d25	Gagal

Persentase keberhasilan *recovery* = $\frac{3}{34}$ x 100% = 9%

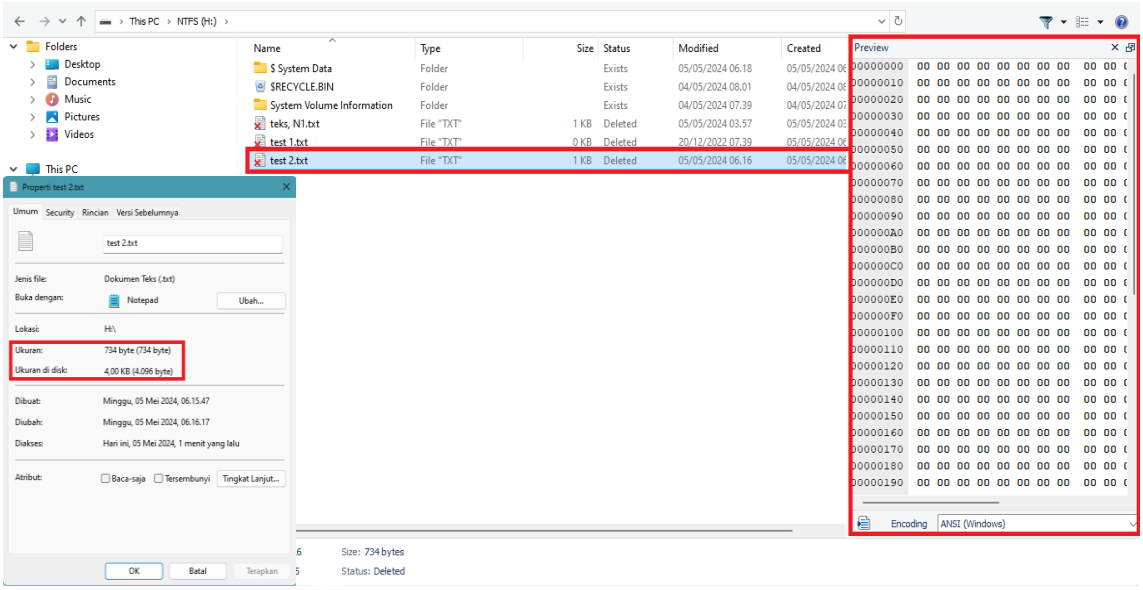
Dari penyesuaian nilai hash MD5 file asli dan file hasil *recovery* pada tabel 4.12 menunjukkan bahwa file dengan format .txt bisa di*recovery* setelah dihapus permanen dengan teknik *disk carving*. Tidak hanya itu file dengan format .txt yang dikompres di dalam file .rar dan .zip masih bisa di*recovery*. Dari kasus *recovery* pada tabel 4.12 file sistem NTFS masih menyisakan data yang bisa dibangkitkan kembali setelah dihapus permanen walaupun pada saat fitur TRIM pada SSD berstatus *enable*. Hasil yang berharga ini berbeda dari penelitian sebelumnya, penelitian sebelumnya menunjukkan bahwa tidak ada file yang bisa dipulihkan setelah dihapus permanen pada saat TRIM SSD *enable*. Perbedaan dari hasil *recovery* ini dikarenakan pada volume NTFS file data dengan *size* tidak melebihi 700 bytes dan *size on disk* 0 bytes sehingga tidak ditandai sebagai file yang memakan ruang di disk yang akan membuat fitur TRIM membiarkan file tersebut seperti contoh pada gambar 4.18.



Gambar 4.18 Hasil Analisa File Berhasil Di*recovery* Pada NTFS TRIM *Enable*

Dari gambar 4.18 bisa diketahui bahwa semua informasi tentang file melihat dari *preview* di bagian kanan. Dari kasus ini bisa diketahui melihat dari properti file percobaan yang diteliti berukuran hanya 134 byte dan ukuran di disk 0 byte melihat pada bagian kiri gambar 4.18.

Sedangkan pada file dengan ukuran lebih dari 700 bytes dan *size on disk* lebih dari 0 bytes akan gagal dipulihkan, karena *preview* metadata file di bagian kanan menunjukkan angka 0 yang berarti isi metadata file tersebut telah dihapus TRIM seperti pada gambar 4.19



Gambar 4. 19 Hasil Analisa File Gagal Di*recovery* Pada NTFS TRIM *Enable*

Seperti yang bisa dilihat pada gambar 4.18 dan 4.19 terdapat perbedaan size file yang memberikan dampak kepada fitur TRIM *enable* di file sistem NTFS sehingga file tidak dibersihkan jika file memiliki ukuran di *disk* adalah 0kb.

Tabel 4.13 Hasil *Recovery* SSD Trim *Disable* File Sistem ReFS

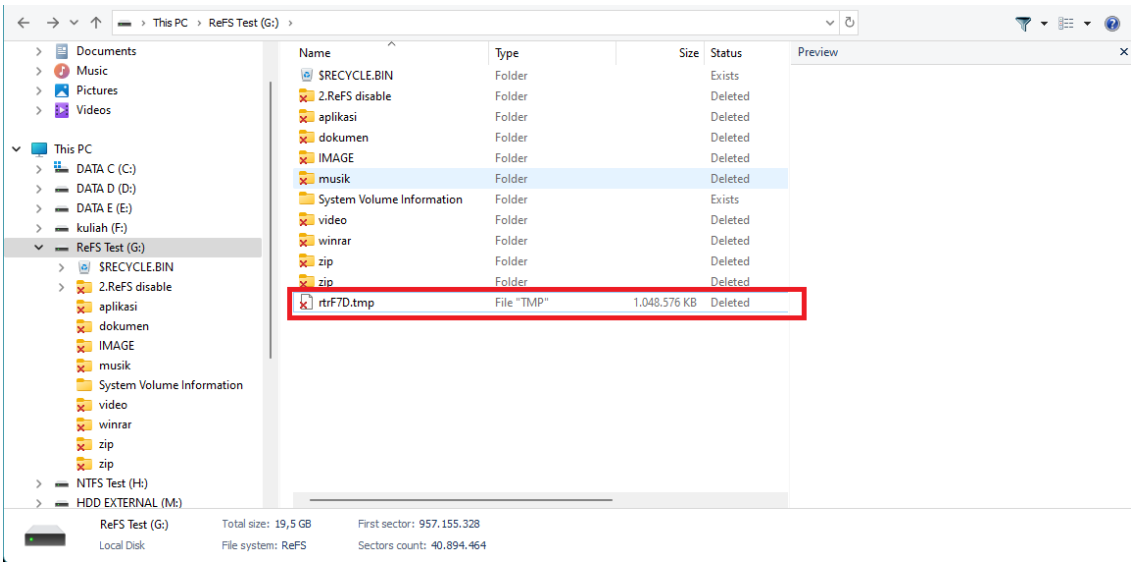
No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
1	file exe 1, R2	.exe	MD5 File Asli: e67e681e116f50d14a557cd83e83596a MD5 File Hasil *Recovery:* e67e681e116f50d14a557cd83e83596a	Sukses
2	file exe 2, R2	.exe	MD5 File Asli: e500b16147893a4b4aa6a71a0b494475 MD5 File Hasil *Recovery:* e500b16147893a4b4aa6a71a0b494475	Sukses
3	file exe 3, R2	.exe	MD5 File Asli: 375276a153cfcd10b60141a1bf6d4126 MD5 File Hasil *Recovery:* 375276a153cfcd10b60141a1bf6d4126	Sukses
4	Doc, R2	.doc	MD5 File Asli: 202bed6dade8a6b45f315af6ed4fec01 MD5 File Hasil *Recovery:* 202bed6dade8a6b45f315af6ed4fec01	Sukses
5	Docx, R2	.docx	MD5 File Asli: 2a2539f683f34f5dc3a31f125601d94e MD5 File Hasil *Recovery:* 2a2539f683f34f5dc3a31f125601d94e	Sukses
6	ODT, R2	.odt	MD5 File Asli: b43a20b258af2db416d87368ea99e871 MD5 File Hasil *Recovery:* b43a20b258af2db416d87368ea99e871	Sukses
7	pdf, R2	.pdf	MD5 File Asli: de61ec3a4bfdba769b63b2817d65abca MD5 File Hasil *Recovery:* de61ec3a4bfdba769b63b2817d65abca	Sukses
8	PowerPoint, R2	.pptx	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* 16bc6e9ff52573c9a133117e469578c6	Sukses

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
9	teks, R2	.txt	MD5 File Asli: 9fdbfbd6b9f80a12a4aed69366b1598f MD5 File Hasil *Recovery:* 9fdbfbd6b9f80a12a4aed69366b1598f	Sukses
10	XLSX, R2	.xlsx	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* 168dbdd011eb3113403c205310911801	Gagal
11	BMP, R2	.bmp	MD5 File Asli: 60575664b29c4747ec20bc298394a6db MD5 File Hasil *Recovery:* 60575664b29c4747ec20bc298394a6db	Sukses
12	GIF, R2	.gif	MD5 File Asli: cf69c943fa8eea1605295ead83242f7a MD5 File Hasil *Recovery:* cf69c943fa8eea1605295ead83242f7a	Sukses
13	JPG, R2	.jpg	MD5 File Asli: a3333bb3df4b47dd6a3a6abf4bede7ad MD5 File Hasil *Recovery:* a3333bb3df4b47dd6a3a6abf4bede7ad	Sukses
14	PNG, R2	.png	MD5 File Asli: 068f0a46761a2c77df687f402f263a86 MD5 File Hasil *Recovery:* 068f0a46761a2c77df687f402f263a86	Sukses
15	m4a, R2	.m4a	MD5 File Asli: 27d27b8eb61f5f9d19753d517de0554e MD5 File Hasil *Recovery:* 27d27b8eb61f5f9d19753d517de0554e	Sukses
16	mp3, R2	.mp3	MD5 File Asli: 180b9de2ce8454e8862a37e33e8a5ed1 MD5 File Hasil *Recovery:* d41d8cd98f00b204e9800998ecf8427e	Gagal
17	WAV, R2	.wav	MD5 File Asli: 8f775199f5bf8a7a030185af4257ca5d MD5 File Hasil *Recovery:* a937364668c318aa0d6b91eb89e1e513	Gagal
18	WMA, R2	.wma	MD5 File Asli: 5717ede6eda50aeb373b621312ffbc3d MD5 File Hasil *Recovery:* 91bdf25daf35289bf8d4355afcb3ed25	Gagal
19	3gp, R2	.3gp	MD5 File Asli: 1ecc9837edc86b3370be6e85a2a0c4af MD5 File Hasil *Recovery:* a1c3c3c26cbee786570ee6b2eb3df3fb	Gagal
20	AVI, R2	.avi	MD5 File Asli: 611daaf923e0f755ce19b8f981ccc8bf MD5 File Hasil *Recovery:* 611daaf923e0f755ce19b8f981ccc8bf	Sukses
21	FLV, R2	.flv	MD5 File Asli: 54a827a332666830c3404c817cc1d934 MD5 File Hasil *Recovery:* 54a827a332666830c3404c817cc1d934	Sukses
22	MKV, R2	.mkv	MD5 File Asli: c08dc5bdebe741ca10dee0142a34fd17 MD5 File Hasil *Recovery:* c08dc5bdebe741ca10dee0142a34fd17	Sukses
23	MOV, R2	.mov	MD5 File Asli: 440fd3c73c4be0bc1f9fae3955dfcbbf MD5 File Hasil *Recovery:* 440fd3c73c4be0bc1f9fae3955dfcbbf	Sukses
24	MP4, R2	.mp4	MD5 File Asli: 8b6e8415ada32d939eba45f75388c2aa MD5 File Hasil *Recovery:* 8b6e8415ada32d939eba45f75388c2aa	Sukses
25	MPG, R2	.mpg	MD5 File Asli: 3af1c20309fb85e8de8092c30425a106 MD5 File Hasil *Recovery:* 3af1c20309fb85e8de8092c30425a106	Sukses
26	OGG, R2	.Ogg	MD5 File Asli: 69a4ca496c2c4472db7e6edd8a1db388 MD5 File Hasil *Recovery:* 69a4ca496c2c4472db7e6edd8a1db388	Sukses

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
27	webm, R2	.webm	MD5 File Asli: bf23511f8770f9d5c74edc33836b488a MD5 File Hasil *Recovery:* d41d8cd98f00b204e9800998ecf8427e	Gagal
28	WMV, R2	.wmv	MD5 File Asli: 52289d287f8522b4973372fd8fe0a642 MD5 File Hasil *Recovery:* 87e3a7f011492bf6c27ebed0042033fb	Gagal
29	RAR 1, R2	.rar	MD5 File Asli: 76a42cc2609e2cfe2784077248ecceb7 MD5 File Hasil *Recovery:* 76a42cc2609e2cfe2784077248ecceb7	Sukses
30	RAR 2, R2	.rar	MD5 File Asli: 8251719177e9bd5d549963c04829c9d3 MD5 File Hasil *Recovery:* 8251719177e9bd5d549963c04829c9d3	Sukses
31	RAR 3, R2	.rar	MD5 File Asli: 3ca2fbabcb23b6fc9a0763bc9297fe01 MD5 File Hasil *Recovery:* 3ca2fbabcb23b6fc9a0763bc9297fe01	Sukses
32	zip 1, R2	.zip	MD5 File Asli: 5349d6809d2cf1e8d82931b880265a9d MD5 File Hasil *Recovery:* f76f0a335388e887c2b67433c8541115	Gagal
33	zip 2, R2	.zip	MD5 File Asli: 18271d308f0c4aaebbf72c0e76ebab66 MD5 File Hasil *Recovery:* 141fc9aa2a64d8335b15f8d3c6f41018	Gagal
34	zip 3, R2	.zip	MD5 File Asli: c4e514a94643a96243dd347972963ec5 MD5 File Hasil *Recovery:* c4e514a94643a96243dd347972963ec5	Sukses

Persentase keberhasilan *recovery* $= \frac{25}{34}\ x\ 100\% = 74\%$

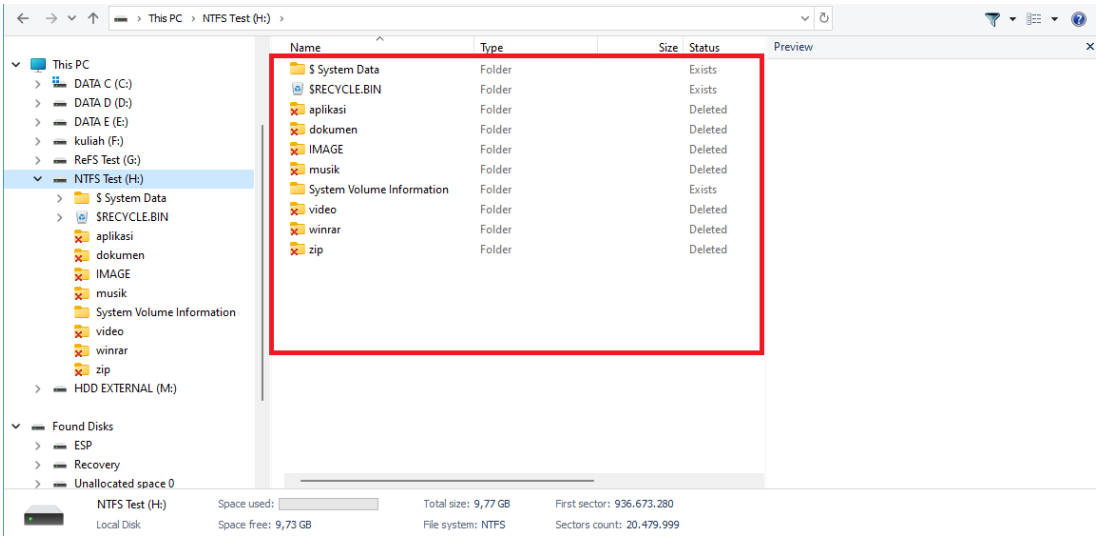
Menurut hasil *recovery* data pada tabel 4.13 menunjukkan 9 file dengan nilai hash yang telah berubah. Hasil analisis menunjukkan file sistem ReFS mempengaruhi file data yang mampu dipulihkan dengan teknik *disk carving*. Data yang tidak berhasil dipulihkan berstatus file *corrupt* karena file tidak bisa dibuka dengan normal dan memiliki nilai hash yang berbeda dengan file asli.



Gambar 4.20 Hasil Analisa Sebagian File Gagal *Direcovery* Pada ReFS TRIM *Disable*

Kemudian pada tabel 4.13 Fitur TRIM pada ReFS tidak di*enable* sehingga penyebab file yang tidak berhasil dipulihkan terletak pada file sistem yang digunakan. File sistem ReFS akan memfragmentasi logis file yang telah dianggap usang untuk tujuan mengosongkan penyimpanan dan memberikan ruang untuk file lain disimpan. Seperti pada gambar 4.20 file yang telah dihapus akan difragmentasi logis ke dalam file tmp. Proses fragmentasi logis akan membutuhkan waktu sehingga file yang belum terfragmen akan berhasil di*recovery.*

Sementara untuk file sistem NTFS tanda-tanda fragmentasi logis tidak ditemukan melihat dari tidak ada file tmp pada saat *recovery* seperti pada gambar 4.21



Gambar 4.21 Hasil Analisa File Berhasil *Direcovery* Pada NTFS TRIM *Disable*

Karena tidak ada file yang *terfragment* membuat semua file pada NTFS TRIM *disable* bisa dipulihkan sepenuhnya. dari gambar 4.20 dan 4.21 bisa diketahui bahwa *tool* yang digunakan belum mendukung untuk pemulihan file yang terfragmentasi.

Tabel 4.14 Hasil *Recovery* SSD Trim *Enable* File Sistem ReFS

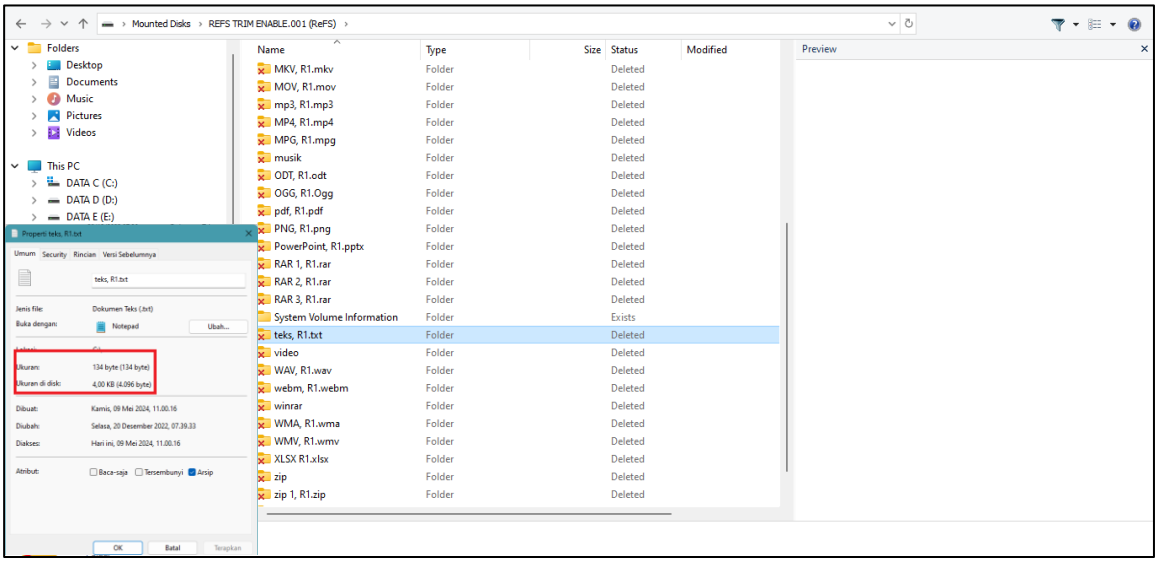
No	NAMA FILE	**Ekstensi**	**Pencocokan Nilai HASH**	**Hasil *Recovery***
1	file exe 1, R1.exe	.exe	MD5 File Asli: e67e681e116f50d14a557cd83e83596a MD5 File Hasil *Recovery:* e67e681e116f50d14a557cd83e83596a	Gagal
2	file exe 2, R1.exe	.exe	MD5 File Asli: e500b16147893a4b4aa6a71a0b494475 MD5 File Hasil *Recovery:* e500b16147893a4b4aa6a71a0b494475	Gagal
3	file exe 3, R1.exe	.exe	MD5 File Asli: 375276a153cfcd10b60141a1bf6d4126 MD5 File Hasil *Recovery:* 375276a153cfcd10b60141a1bf6d4126	Gagal
4	Doc, R1.doc	.doc	MD5 File Asli: 202bed6dade8a6b45f315af6ed4fec01 MD5 File Hasil *Recovery:* 202bed6dade8a6b45f315af6ed4fec01	Gagal

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
5	Docx, R1.docx	Folder	MD5 File Asli: 2a2539f683f34f5dc3a31f125601d94e MD5 File Hasil *Recovery:* -	Gagal
6	ODT, R1.odt	Folder	MD5 File Asli: b43a20b258af2db416d87368ea99e871 MD5 File Hasil *Recovery:* -	Gagal
7	pdf, R1.pdf	Folder	MD5 File Asli: de61ec3a4bfdba769b63b2817d65abca MD5 File Hasil *Recovery:* -	Gagal
8	PowerPoint, R1.pptx	Folder	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* -	Gagal
9	teks, R1.txt	Folder	MD5 File Asli: 9fdbfbd6b9f80a12a4aed69366b1598f MD5 File Hasil *Recovery:* -	Gagal
10	XLSX, R1.xlsx	Folder	MD5 File Asli: 16bc6e9ff52573c9a133117e469578c6 MD5 File Hasil *Recovery:* -	Gagal
11	BMP, R1.bmp	Folder	MD5 File Asli: 60575664b29c4747ec20bc298394a6db MD5 File Hasil *Recovery:* -	Gagal
12	GIF, R1.gif	Folder	MD5 File Asli: cf69c943fa8eea1605295ead83242f7a MD5 File Hasil *Recovery:* -	Gagal
13	JPG, R1.jpg	Folder	MD5 File Asli: a3333bb3df4b47dd6a3a6abf4bede7ad MD5 File Hasil *Recovery:* -	Gagal
14	PNG, R1.png	Folder	MD5 File Asli: 068f0a46761a2c77df687f402f263a86 MD5 File Hasil *Recovery:* -	Gagal
15	m4a, R1.m4a	Folder	MD5 File Asli: 27d27b8eb61f5f9d19753d517de0554e MD5 File Hasil *Recovery:* -	Gagal
16	mp3, R1.mp3	Folder	MD5 File Asli: 180b9de2ce8454e8862a37e33e8a5ed1 MD5 File Hasil *Recovery:* -	Gagal
17	WAV, R1.wav	Folder	MD5 File Asli: 8f775199f5bf8a7a030185af4257ca5d MD5 File Hasil *Recovery:* -	Gagal
18	WMA, R1.wma	Folder	MD5 File Asli: 5717ede6eda50aeb373b621312ffbc3d MD5 File Hasil *Recovery:* -	Gagal
19	3gp, R1.3gp	Folder	MD5 File Asli: 1ecc9837edc86b3370be6e85a2a0c4af MD5 File Hasil *Recovery:* -	Gagal
20	AVI, R1.avi	Folder	MD5 File Asli: 611daaf923e0f755ce19b8f981ccc8bf MD5 File Hasil *Recovery:* -	Gagal
21	FLV, R1.flv	Folder	MD5 File Asli: 54a827a332666830c3404c817cc1d934 MD5 File Hasil *Recovery:* -	Gagal
22	MKV, R1.mkv	Folder	MD5 File Asli: c08dc5bdebe741ca10dee0142a34fd17 MD5 File Hasil *Recovery:* -	Gagal

No	NAMA FILE	Ekstensi	Pencocokan Nilai HASH	Hasil *Recovery*
23	MOV, R1.mov	Folder	MD5 File Asli: 440fd3c73c4be0bc1f9fae3955dfcbbf MD5 File Hasil *Recovery:* -	Gagal
24	MP4, R1.mp4	Folder	MD5 File Asli: 8b6e8415ada32d939eba45f75388c2aa MD5 File Hasil *Recovery:* -	Gagal
25	MPG, R1.mpg	Folder	MD5 File Asli: 3af1c20309fb85e8de8092c30425a106 MD5 File Hasil *Recovery:* -	Gagal
26	OGG, R1.Ogg	Folder	MD5 File Asli: 69a4ca496c2c4472db7e6edd8a1db388 MD5 File Hasil *Recovery:* -	Gagal
27	webm, R1.webm	Folder	MD5 File Asli: bf23511f8770f9d5c74edc33836b488a MD5 File Hasil *Recovery:* -	Gagal
28	WMV, R1.wmv	Folder	MD5 File Asli: 52289d287f8522b4973372fd8fe0a642 MD5 File Hasil *Recovery:* -	Gagal
29	RAR 1, R1.rar	Folder	MD5 File Asli: 76a42cc2609e2cfe2784077248ecceb7 MD5 File Hasil *Recovery:* -	Gagal
30	RAR 2, R1.rar	Folder	MD5 File Asli: 8251719177e9bd5d549963c04829c9d3 MD5 File Hasil *Recovery:* -	Gagal
31	RAR 3, R1.rar	Folder	MD5 File Asli: 3ca2fbabcb23b6fc9a0763bc9297fe01 MD5 File Hasil *Recovery:* -	Gagal
32	zip 1, R1.zip	Folder	MD5 File Asli: 5349d6809d2cf1e8d82931b880265a9d MD5 File Hasil *Recovery:* -	Gagal
33	zip 2, R1.zip	Folder	MD5 File Asli: 18271d308f0c4aaebbf72c0e76ebab66 MD5 File Hasil *Recovery:* -	Gagal
34	zip 3, R1.zip	Folder	MD5 File Asli: c4e514a94643a96243dd347972963ec5 MD5 File Hasil *Recovery:* -	Gagal

Persentase keberhasilan *recovery* = $\frac{0}{34}\ x\ 100\% = 0\%$

Dari tabel 4.14 diketahui bahwa fitur TRIM SSD akan sangat mempengaruhi file sistem ReFS. Semua file yang telah dihapus permanen pada SSD yang diterapkan file sistem ReFS dengan fitur TRIM *enable* tidak berhasil dipulihkan kembali. Pada kasus tabel 4.14 file sistem dan fitur TRIM akan mengubah file yang telah dihapus permanen (Shift+delete) menjadi sebuah folder. Folder – folder yang berhasil dipulihkan memiliki nama yang sama dengan file asli sehingga dapat diketahui file sistem ReFS membentuk sebuah catatan dari nama-nama yang dimiliki file sebelum dihapus permanen ke dalam sebuah folder. File dengan ekstensi asli tidak berhasil ditemukan pada *recovery* file di file sistem ReFS TRIM *enable*.



Gambar 4.22 Hasil Analisa File Gagal *Direcovery* Pada ReFS TRIM *Enable*

Berdasarkan analisis dan observasi yang dilakukan terhadap ReFS TRIM *enable*, terlihat bahwa saat memeriksa properti suatu file dengan ukuran 134 byte sebelum dihapus secara permanen, ukuran di *disk* menunjukkan 4KB seperti yang terlihat pada gambar 4.22. Hal ini mengindikasikan bahwa dalam sistem file ReFS, file-file dengan ukuran di bawah 700 byte dikategorikan sebagai 4KB ukuran di disk, hal ini akan membuat TRIM dapat mendeteksinya. Temuan ini menunjukkan bahwa ReFS memiliki dukungan yang lebih baik untuk pembersihan file usang melalui TRIM *enable*.

4.8 Hasil

Indikator keberhasilan hasil dari penelitian ini dapat diidentifikasi dari akurasi *recovery* data pada setiap kondisi yang diuji, baik itu kondisi TRIM *enable/disable* maupun jenis sistem file NTFS atau ReFS. Berikut adalah indikator keberhasilan dari penelitian ini:

1. Berhasil me*recovery* file yang dihapus permanen saat TRIM *enable*: Indikator ini menunjukkan bahwa penelitian berhasil jika dapat me*recovery* file yang dihapus secara permanen saat TRIM *enable*. Ini mengukur efektivitas teknik atau metode *recovery* data yang digunakan.
2. Perbedaan akurasi *recovery* saat TRIM *disable* pada NTFS dan ReFS: Indikator ini menunjukkan bahwa penelitian berhasil jika dapat menemukan perbedaan akurasi *recovery* data saat TRIM *disable* pada file sistem NTFS dan ReFS. Ini menunjukkan bahwa penelitian ini mempertimbangkan variabel yang relevan dan menghasilkan temuan yang berharga terkait dengan kinerja *recovery* data.

Tabel 4.15 Hasil Jumlah Ekstraksi Data Sesuai Dengan Nama *Disk*

Nama *disk*	Berhasil di*recovery*	Gagal di*recovery*
SSD TRIM *disable* NTFS	34 file	0 file
SSD TRIM *disable* ReFS	25 file	9 file
SSD TRIM *enable* NTFS	3 file	31 file
SSD TRIM *enable* ReFS	0 file	34 file

Berdasarkan tabel 4.15 SSD TRIM *disable* NTFS 34 file berhasil *direcovery* dan pada SSD TRIM *disable* ReFS ada 25 file. SSD TRIM *enable* NTFS berhasil *direcovery* 3 file, dan pada SSD TRIM *enable* ReFS tidak ada data yang berhasil *direcovery*. Untuk mendapatkan hasil jumlah ekstraksi data seperti pada tabel 4.14 dibutuhkan empat tahapan utama yaitu persiapan mulai dari alat dan sistem yang akan dan digunakan untuk simulasi kasus serta penanganan live akuisisi, dilanjutkan dengan rekonstruksi *disk*, ekstraksi bukti, dan analisis *output* hasil *recovery*.

Tabel 4. 16 Hasil Persentase Jumlah Ekstraksi Data Sesuai Dengan Nama *Disk*

Nama *disk*	Berhasil di*recovery*	Gagal di*recovery*
SSD TRIM *disable* NTFS	100%	0%
SSD TRIM *disable* ReFS	74%	26%
SSD TRIM *enable* NTFS	9%	91%
SSD TRIM *enable* ReFS	0%	100%

Berdasarkan persentase tabel 4.16 menunjukkan bahwa saat TRIM *enable* NTFS terdapat file yang berhasil dipulihkan, ini bisa terjadi karena pada volume NTFS file berukuran kurang dari 700 byte ditandai dengan *size di disk* 0kb sehingga TRIM tidak mendeteksi dan membersihkan file tersebut. Pada penelitian kali ini file yang berhasil dipulihkan saat TRIM *enable* NTFS adalah “teks, N1.txt” , ”RAR 1, N1.rar” , “zip 1, N1.zip” yang semua ukuran file tersebut tidak melebihi 700 byte, penelitian sebelumnya gagal me*recovery* semua file saat TRIM *enable* karena tidak menggunakan file dengan *size* kurang dari 700 byte sebagai data pengujian. Sedangkan pada TRIM *enable* ReFS semua data tidak berhasil di*recovery* karena file-file dengan *size* kecil ditandai oleh file sistem dengan size di disk 4kb sehingga TRIM dapat mendeteksi file *size* kecil tersebut dan membersihkannya.

Selanjutnya saat SSD TRIM *disable ReFS 74%* data berhasil *direcovery* sedangkan SSD TRIM *disable* NTFS 100% data bisa *direcovery,* dari yang telah diteliti perbedaan keberhasilan *recovery* ini didasari oleh adanya fragmentasi logis data yang tidak bisa digabungkan oleh *tool* yang digunakan pada penelitian ini saat TRIM *disable* ReFS, sementara untuk TRIM *disable* NTFS tidak ditemukan adanya data yang terfragmentasi logis sehingga semua file berhasil dipulihkan.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan data penelitian ini bisa ditarik kesimpulan:

1. Dari data yang didapatkan, TRIM *enable* akan berpengaruh besar pada keberhasilan data untuk di*recovery* baik di file sistem NTFS atau ReFS. Ditemukan perbedaan tingkat keberhasilan *recovery* yaitu 9% pada TRIM *enable* file sistem NTFS, adanya data yang bisa di*recovery* disebabkan karena NTFS tidak menandai file dengan ukuran kurang dari 700 *Bytes* untuk dibersihkan oleh TRIM. Sedangkan pada TRIM *enable* file sistem ReFS 0% keberhasilan *recovery* karena file sistem ReFS menangani file-file ber*size* kecil lebih baik dengan cara menandai semua file yang telah dihapus permanen.
2. Hasil *imaging disk* SSD ReFS dan NTFS dari *tool* FTK *Imager* kemudian bisa dibaca oleh *tool* forensik hetman partition *recovery* yang sudah mendukung untuk *scan* file sistem ReFS serta penerapan teknik *disk carving* sehingga mampu me*recovery* data yang telah dihapus permanen dengan persentase *recovery* pada ReFS TRIM *disable* 74% data bisa di*recovery*, adanya file yang tidak berhasil di*recovery* disebabkan karena *tool* yang digunakan belum bisa menggabungkan fragmentasi logis dengan baik pada file sistem ReFS. pada NTFS TRIM *disable* 100% data yang berhasil di*recovery*, karena tidak ditemukan file terfragmentasi pada file sistem NTFS.

5.2 Saran

Penelitian kali ini berfokus pada perbedaan pengaruh TRIM di volume NTFS dan ReFS dengan analisa *recovery tool carving*, untuk penelitian selanjutnya disarankan membandingkan tingkat akurasi *recovery* data yang telah dihapus permanen pada file sistem berbeda dengan raid 0 yaitu seting penggabungan dua penyimpanan, mengeksplorasi dan membandingkan tingkat efektivitas *tool recovery* yang bisa digunakan pada fitur TRIM SSD Volume ReFS.

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

Ahn, N. Y., & Lee, D. H. (2021). Forensic Issues and Techniques to Improve Security in SSD with Flex Capacity Feature. *IEEE Access*, *9*, 167067–167075. https://doi.org/10.1109/ACCESS.2021.3136483

Alghafli, K., & Martin, T. (2016). Identification and Recovery of Video Fragments for Forensics File Carving. *The 11th International Conference for Internet Technology and Secured Transactions*, 267–272.

Alshumrani, A., Clarke, N., & Ghita, B. (2023). A Unified Forensics Analysis Approach to Digital Investigation. *International Conference on Cyber Warfare and Security*, *18*(1), 466–475. https://doi.org/10.34190/iccws.18.1.972

Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley Professional.

Daghmehchi Firoozjaei, M., Habibi Lashkari, A., & Ghorbani, A. A. (2022). Memory forensics tools: a comparative analysis. *Journal of Cyber Security Technology*, *6*(3), 149–173. https://doi.org/10.1080/23742917.2022.2100036

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. https://ojs.trigunadharma.ac.id/index.php/jsk/index

Freiling, F., Groß, T., Latzo, T., Müller, T., & Palutke, R. (2018). Advances in forensic data acquisition. *IEEE Design & Test*, *35*(5), 63–74. https://ieeexplore.ieee.org/abstract/document/8424163/

Geier, F. (2015). *The differences between SSD and HDD technology regarding forensic investigations*. https://www.diva-portal.org/smash/get/diva2:824922/FULLTEXT01.pdf

Hepisuthar, M., & Priyankasharma, D. (2021). Comparative Analysis Study on SSD, HDD, and SSHD. *Turkish Journal of Computer and Mathematics Education*, *12*(3), 3635–3641. https://turcomat.org/index.php/turkbilmat/article/view/1644

Jeong, D., & Lee, S. (2019). Forensic signature for tracking storage devices: Analysis of UEFI firmware image, disk signature and windows artifacts. *Digital Investigation*, *29*, 21–27. https://doi.org/10.1016/j.diin.2019.02.004

Kessler, G. C. (2023, August 6). *GCK'S FILE SIGNATURES TABLE*. Www.Garykessler.Net/Library/File_sigs.Html. https://www.garykessler.net/library/file_sigs.html

Khairunnisak, K., & Widodo, W. (2023). Digital Forensic Tools And Techniques For Handling Digital Evidence. *Jurnal RESISTOR Rekayasa Sistem Komputer*, *6*(1), 1–11. https://doi.org/https://doi.org/10.31598

Kumar, M. (2021). Solid state drive forensics analysis—Challenges and recommendations. *Concurrency and Computation: Practice and Experience*, *33*(24), e6442. https://doi.org/10.1002/cpe.6442

Lee, S., Park, J., Hwang, H., Lee, S., Lee, S., & Jeong, D. (2021). Forensic analysis of ReFS journaling. *Forensic Science International: Digital Investigation*, *38*, 301136. https://doi.org/10.1016/j.fsidi.2021.301136

Liu, R., Liu, D., Chen, X., Tan, Y., Zhang, R., & Liang, L. (2022a). Self-Adapting Channel Allocation for Multiple Tenants Sharing SSD Devices. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *41*(2), 294–305. https://doi.org/10.1109/TCAD.2021.3056374

Liu, R., Liu, D., Chen, X., Tan, Y., Zhang, R., & Liang, L. (2022b). Self-Adapting Channel Allocation for Multiple Tenants Sharing SSD Devices. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *41*(2), 294–305. https://doi.org/10.1109/TCAD.2021.3056374

Lv, Y., Shi, L., Li, Q., Xue, C. J., & Sha, E. H.-M. (2020). Access Characteristic Guided Partition for Read Performance Improvement on Solid State Drives. *2020 57th ACM/IEEE Design Automation Conference (DAC)*, 1–6. https://doi.org/10.1109/DAC18072.2020.9218540

Lv, Y., Shi, W., Zhang, W., Lu, H., & Tian, Z. (2023). Don't trust the Clouds easily: The Insecurity of Content Security Policy based on Object Storage. *IEEE Internet of Things Journal*, *10*(12), 10462–10470. https://doi.org/10.1109/JIOT.2023.3238658

Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of Cyber Security*, *2023*, 57–63. https://doi.org/10.58496/mjcs/2023/010

Munegowda, K., Sachs, G., Raju, G. T., & Raju, V. M. (2014). Evaluation of File Systems for Solid State Drives. *Proceeding of the Second International Conference on "Emerging Research in Computer, Information, Communication, and Application" ERICA2014*, 342–348. https://doi.org/10.13140/2.1.1213.0082

Neyaz, A., Shashidhar, N., & Karabiyik, U. (2018). Forensic Analysis of Wear Leveling on Solid-State Media. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 1706–1710. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00256

Neyaz, A., Zhou, B., & Karpoor, N. (2019). Comparative Study of Wear-leveling in Solid-State Drive with NTFS File System. *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019*, 4294–4298. https://doi.org/10.1109/BigData47090.2019.9006067

Nisbet, A., & Jacob, R. (2019). TRIM, wear levelling and garbage collection on solid state drives: A prediction model for forensic investigators. *Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019*, 419–426. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00063

Nisbet, A., Lawrence, S., & Ruff, M. (2013). A Forensic Analysis And Comparison Of Solid State Drive Data Retention With Trim Enabled File Systems. *Australia ECU Edith Cowan University*, 103–111. https://doi.org/10.4225/75/57b3d766fb873

Nordvik, R., Georges, H., Toolan, F., & Axelsson, S. (2019). Reverse engineering of ReFS. *Digital Investigation*, *30*, 127–147. https://doi.org/10.1016/j.diin.2019.07.004

Porter, K., Nordvik, R., Toolan, F., & Axelsson, S. (2021). Timestamp prefix carving for filesystem metadata extraction. *Forensic Science International: Digital Investigation*, *38*, 1–13. https://doi.org/10.1016/j.fsidi.2021.301266

Povar, D., & Bhadran, V. K. (2011). Forensic Data Carving. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *53*, 137–148. https://doi.org/https://doi.org/10.1007/978-3-642-19513-6_12

Prade, P., Groβ, T., & Dewald, A. (2020). Forensic Analysis of the Resilient File System (ReFS) Version 3.4. *Forensic Science International: Digital Investigation*, *32*, 51–59. https://doi.org/10.1016/j.fsidi.2020.300915

Pradhana, I., Riadi, I., & Prayudi, Y. (2021). Forensik Router untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic. *JRST (Jurnal Riset Sains Dan Teknologi)*, *5*(1), 31–38. https://doi.org/10.30595/jrst.v5i1.7662

Pranoto, W., Riadi, I., & Prayudi, Y. (2020a). Live Forensics Method for Acquisition on the Solid State Drive (SSD) NVMe TRIM Function. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *5*(2), 129–138. https://doi.org/10.22219/kinetik.v5i2.1032

Pranoto, W., Riadi, I., & Prayudi, Y. (2020b). Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics. *IT Journal Research and Development*, *4*(2), 135–148. https://doi.org/10.25299/itjrd.2020.vol4(2).4615

Rahman, S., & Khan, M. N. A. (2015). Review of Live Forensic Analysis Techniques. *International Journal of Hybrid Information Technology*, *8*(2), 379–388. https://doi.org/10.14257/ijhit.2015.8.2.35

Ramadhan, R. A., & Mualfah, D. (2020). Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh. *IT Journal Research and Development*, *5*(2), 183–192. https://doi.org/10.25299/itjrd.2021.vol5(2).5750

Riadi, I., Sunardi, & Sahiruddin. (2020). *PERBANDINGAN TOOL FORENSIK DATA RECOVERY BERBASIS ANDROID MENGGUNAKAN METODE NIST*. *7*(1), 197–204. https://doi.org/10.25126/jtiik.202071921

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ). *Elinvo (Electronics, Informatics, and Vocational Education)*, *3*(1), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Sadikin, N., & Sari, M. (2020). REPLIKASI VIRTUAL MACHINE ANTARA DUA LOKASI TERPISAH UNTUK BACKUP DAN DISASTER RECOVERY. *Jurnal Maklumatika*, *6*(2), 81–88.

Salih, K. M. M., & Ibrahim, N. B. (2023). Digital Forensic Tools: A Literature Review. *Journal of Education and Science*, *32*(1), 109–124. https://doi.org/10.33899/edusj.2023.137420.1304

Sari, S. A., & Mohamad, K. M. (2020). A Review of Graph Theoretic and Weightage Techniques in File Carving. *Journal of Physics: Conference Series*, *1529*(5), 1–16. https://doi.org/10.1088/1742-6596/1529/5/052011

Soni, Prayudi, Y., Sugiantoro, B., Sudyana, D., & Mukhtar, H. (2019). Server Virtualization Acquisition Using Live Forensics Method. *Proceedings of the International Conference of CELSciTech 2019 - Science and Technology Track (ICCELST-ST 2019)*, 18–23. https://doi.org/10.2991/iccelst-st-19.2019.4

Sudyana, D., Hadi, I., & Yudha, F. (2023). Analisis Investigasi Forensik Digital pada Layanan Private Cloud Computing Menggunakan SNI 27037:2014. *Buletin Profesi Insinyur*, *6*(1). https://doi.org/10.20527/bpi.v6i1.176

Vieyra, J., Scanlon, M., & Le-Khac, N. A. (2019). Solid State Drive Forensics: Where Do We Stand? *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *259*, 149–164. https://doi.org/10.1007/978-3-030-05487-8_8

Wang, C., Brihadiswarn, G., Jiang, X., & Chattopadhyay, S. (2022). Circ-Tree: A B+-Tree Variant with Circular Design for Persistent Memory. *IEEE Transactions on Computers*, *71*(2), 296–308. https://doi.org/10.1109/TC.2020.3047972

Yuwono, D. T., Fadlil, A., & Sunardi, S. (2019). Performance Comparison of Forensic Software for Carving Files using NIST Method. *Jurnal Teknologi Dan Sistem Komputer*, *7*(3), 89–92. https://doi.org/10.14710/jtsiskom.7.3.2019.89-92

Zhou, Y., Wang, K., Wu, F., Xie, C., & Lv, H. (2021). Seer-SSD: Bridging Semantic Gap between Log-Structured File Systems and SSDs to Reduce SSD Write Amplification. *Proceedings - IEEE International Conference on Computer Design: VLSI in Computers and Processors*, *2021-October*, 49–56. https://doi.org/10.1109/ICCD53106.2021.00020