Teknik Disk Carving untuk Recovery Solid State Drive Volume ReFS dan NTFS dengan Fitur TRIM

Muhardinata[1], Ahmad Luthfi[2], Erika Ramadhani[3]
[1,2,3]Universitas Islam Indonesia
E-mail: 20917027@students.uii.ac.id, ahmad.luthfi@uii.ac.id, erika@uii.ac.id

Article Info
Article History
Received: 2023-09-17
Revised: 2023-10-23
Published: 2023-11-05

Keywords:
Forensika Langsung;
Teknik Disk Carving;
Solid Sate Drive;
New Technology File System;
Resilient File Sistem.

Abstract
The Resilient File System (ReFS) and New Technology File System (NTFS) have different metadata information, making the process of recovering permanently deleted data difficult. This is due to the fact that commonly used forensic analysis tools rely on the master file system table, which cannot be read on ReFS volumes. These differences in metadata also affect the TRIM feature on Solid State Drives (SSD). This research aims to examine the impact of Disk Carving Techniques on SSDs with ReFS and NTFS volumes. We employed a live forensic method following the Indonesian National Standard (SNI) 27037:2014. This method was chosen because it allows us to retrieve more data using tools like FTKImager. We collected 34 data samples from ReFS volumes and 34 data samples from NTFS volumes on SSDs with TRIM disabled and enabled. The research results show that the successfully recovered data on SSDs with active TRIM is approximately 9% for NTFS volumes, whereas for ReFS volumes, the successfully recovered data is 0%. However, on SSDs with TRIM disabled, all data was successfully recovered for NTFS volumes, while for ReFS volumes, around 74% of the data was successfully recovered. In conclusion, after this research, data on ReFS file systems with disabled TRIM can be retrieved using disk carving techniques. The file system also impacts SSDs with the TRIM feature enabled. After data recovery on ReFS volumes with active TRIM, the data will appear in the form of folders without HASH values, while on NTFS volumes with active TRIM, the data remains intact but largely has different HASH key values from the original files.

Artikel Info
Sejarah Artikel
Diterima: 2023-09-17
Direvisi: 2023-10-23
Dipublikasi: 2023-11-05

Kata kunci:
Forensika Langsung;
Teknik Disk Carving;
Solid Sate Drive;
New Technology File System;
Resilient File Sistem.

Abstrak
Resilient File Sistem (ReFS) dan New Technology File System (NTFS) memiliki informasi metadata yang berbeda, sehingga membuat proses pemulihan data yang telah dihapus secara permanen menjadi sulit. Ini disebabkan oleh fakta bahwa alat analisis forensik yang umum digunakan bergantung pada tabel master file sistem yang tidak dapat dibaca pada volume ReFS. Perbedaan dalam metadata ini juga memengaruhi fitur TRIM pada Solid State Drive (SSD). Penelitian ini bertujuan untuk menguji pengaruh Teknik Disk Carving pada SSD dengan volume ReFS dan NTFS. Kami menggunakan metode Forensika Langsung yang mengikuti Standar Nasional Indonesia (SNI) 27037:2014. Metode ini dipilih karena memungkinkan kami untuk mengambil lebih banyak data dengan menggunakan alat seperti FTKImager. Kami mengumpulkan 34 sampel data dari volume ReFS dan 34 sampel data dari volume NTFS pada SSD dengan TRIM dinonaktifkan dan diaktifkan. Hasil penelitian menunjukkan bahwa data yang berhasil dipulihkan pada SSD dengan TRIM aktif adalah sekitar 9% pada volume NTFS, sementara pada volume ReFS data yang berhasil dipulihkan adalah 0%. Namun, pada SSD dengan TRIM dinonaktifkan semua data berhasil dipulihkan pada volume NTFS, sementara pada volume ReFS sekitar 74% data berhasil dipulihkan. Kesimpulannya setelah penelitian ini, data pada sistem file ReFS dengan TRIM dinonaktifkan dapat dibaca kembali melalui teknik disk carving. Sistem file juga memengaruhi SSD dengan fitur TRIM yang diaktifkan. Setelah pemulihan data pada volume ReFS dengan TRIM aktif, data akan muncul dalam bentuk folder tanpa nilai HASH, sementara pada volume NTFS dengan TRIM aktif, data tetap utuh tetapi sebagian besar memiliki nilai kunci HASH yang berbeda dari file aslinya.

I. PENDAHULUAN

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 (Lv et al., 2020; Liu et al., 2022). SSD memiliki kelebihan dalam kecepatan transfer data, untuk menjaga kinerja dan perpanjangan masa pakai

dibuatlah fitur TRIM (Ramadhan and Mualfah, 2021).Tetapi fitur TRIM pada SSD akan menandai file pada blok yang telah using (dihapus permanen) kemudian memberikan informasi tersebut kepada sistem operasi agar dapat memerintah file sistem di SSD untuk membersihkan file pada blok-blok yang telah usang, membuat file yang telah dihapus permanen menjadi sulit untuk direcovery (Pranoto, RIadi and Prayudi, 2020). 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.

Karena metadata dari ReFS sangat berbeda dengan NTFS membuat tool konvensional seperti autopsy yang mengandalkan tabel file sistem untuk proses recovery dibutuhkan pengembangan untuk membaca file sistem gabungan seperti ReFS (Hilgert, Lambertz and Plohmann, 2017; Daghmehchi Firoozjaei, Habibi Lashkari and Ghorbani, 2022). Teknik disk carving atau file carving bisa digunakan untuk proses recovery data yang telah dihapus permanen. Disc carving dan file caring adalah kemampuan untuk mendapatkan kembali file yang telah dihapus atau disembunyikan pada sebuah medium penyimpanan dengan atau tanpa file sistem (Raad Ali et al., 2018; Sari and Mohamad, 2020; Porter et al., 2021). Pada penelitian ini akan menggunakan tool hetman partition recovery yang sudah mendukung recovory dengan teknik disk carving.

Penelitian sebelumnya pernah membahas teknik file carving menggunakan tool scalpel yang tersedia di linux dengan media penyimpanan Flashdisk dan File sistem FAT32 telah membuktikan bahwa data dapat direcovery dengan tingkat keberhasilan 100% untuk 20 file dokumen dan 90% untuk file gambar (Yuwono, Fadlil and Sunardi, 2019). Tetapi pada penelitian tentang kasus recovey disebutkan bahwa metode lama yang digunakan untuk memulihkan data dengan aman pada Flashdisk atau HDD konfensional tidak selalu berfungsi pada SSD, hal ini disebabkan adanya fitur TRIM yang digunakan untuk menjaga penurunan kinerja SSD (Winter, 2013), (Hepisuthar, 2021).

Penelitian yang menggunakan tabel file sistem 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 shadowdefender terbukti berpengaruh tidak semua file bisa diperbaiki sepenuhnya dari 85 file yang bisa diperbaiki sepenuhnya hanya 25 file (Riadi, Umar and Nasrulloh, 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 testdisk 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 testdisk data 100% tetapi pada tool Belkasoft 3% berhasil dipulihkan sedangkan TRIM enable tidak ada satu pun data dapat dipulihkan, tool yang digunakan pada penelitian ini mengandalakan tabel file sistem untuk recovery (Pranoto, RIadi and Prayudi, 2020).

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 prespektif sistem operasi juga pernah dilakukan menunjukkan hasil penelitian yaitu pada konfigurasi TRIM enable di windows 11 volume NTFS, Linux Ubuntu volume ext4, dan MacOS Catalina volume

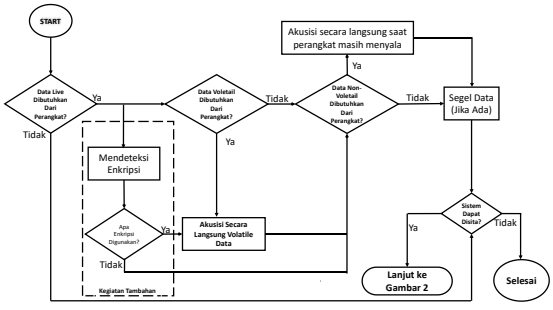
APFS tidak ada satupun file yang bisa direcovery. Pada konfigurasi TRIM disable di windows 11 volume NTFS 85,7% file berhasil direcovery, sedangkan pada Linux Ubuntu volume ext4 dan MacOS Catalina volume APFS tidak ada file yang berhasil di recovery (Ramadhan and Mualfah, 2021).

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 dienable, 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. Penelitian ini akan 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.

II. METODE PENELITIAN

A. Tahapan Penelitian

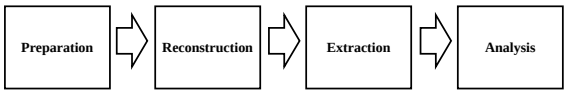
kriteria standar dalam Standar Nasional Indonesia (SNI) 27037:2014 menunjukkan metode akuisisi yang digunakan dalam penelitian live forensik yang diterapkan pada data non-volatile (Pranoto, Riadi and Prayudi, 2020). Menurut Standar Nasional Indonesia (SNI) 27037:2014 menjelaskan serangkaian tahapan yang harus diikuti dalam proses akuisisi data. Tahapan metode live forensik menurut SNI ditunjukan gambar 1.



Gambar 1. Tahapan metode akuisisi live forensik SNI 27037:2014

Menurut Standar Nasional Indonesia (SNI) 27037:2014 menjelaskan serangkaian tahapan yang harus diikuti dalam proses akuisisi data. Langkah pertama adalah menentukan metode akuisisi yang akan digunakan, mengidentifikasi jenis data yang ingin diperoleh, melaksanakan prosedur akuisisi, melakukan penyegelan terhadap data yang diperoleh dengan cara menerapkan prosedur hashing menggunakan algoritma MD5, dan terakhir memverifikasi integritas dan keaslian file akuisisi. Untuk mengukur tingkat keberhasilan recovery pada penelitian kali ini menggunakan angka indeks tidak tertimbang. Perhitungan perbandingan angka indeks, dengan rumus indeks tidak tertimbang bisa digunakan untuk membandingakan tingat keberhasilan recovery dari berbagai tool (Riadi, Sunardi and Sahiruddin, 2020).

Tahapan analisis dan pemeriksaan yang digunakan dalam penelitian ini ditunjukkan dalam Gambar 2. Pertama, dilakukan pemeriksaan dan ekstraksi barang bukti digital yang telah diperoleh untuk mendapatkan petunjuk terkait skenario kasus. Pemeriksaan dilakukan pada komputer pelaku, sedangkan analisis dilakukan menggunakan komputer penyidik. Sebelum memeriksa hasil perolehan, penting untuk mempublikasikan hasil perolehan asli dan membandingkan nilai hash antara berkas asli dan berkas yang dipublikasikan, sebagai langkah untuk memastikan keaslian barang bukti. Selanjutnya, untuk dapat memastikan integritas barang bukti, dilakukan pemeriksaan terhadap salinan berkas perolehan.



Gambar 2. Tahap analisis dan pemeriksaan

1. Preparation

   Pada tahap persiapan akan dibutuhkan FTK Imager portable yang telah disimpan didalam hardisk eksternal dan dibutuhkan ruang kosong tempat menampung hasil pencitraan seluruh SSD (imaging). FTK Imager memberikan dukungan untuk investigator melakukan live forensik.
2. Reconstruction

   Tahap kedua reconstruction dilakukan mounting disk hasil pencitraan FTK Imager pada komputer investigator, dilakaukan juga pengecekan nilai HASH imaging

sebelum dan sesudah mounting disk untuk menghindari komputer investigator mengubah data hasil pencitraan disk.

3. Extraction

   Pata tahap ketiga extraction, file yang telah dihapus permanen di dalam imaging disk akan diekstaksi dan dilakukan pengecekan nilai HASH pada setiap file menggunakan FTK Imager.

4. Analysis

   Pada langkah keempat akan meng-analisa file yang telah dihapus, melakukan pencocokan file hasil recovery dengan file asli berdasarkan nilai hash dan mengukur tingkat keberhasilan recovery.

B. Skenario Kasus

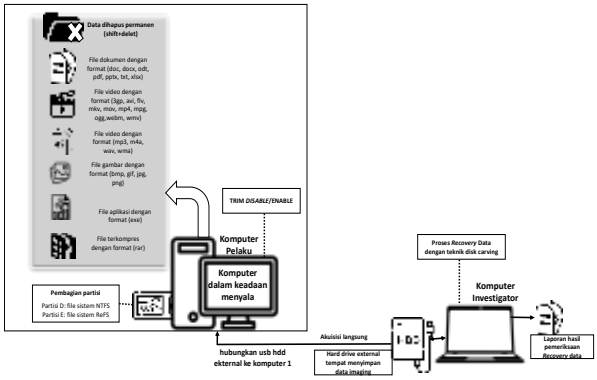
Untuk mengumpulkan bukti digital penelitian ini, diperlukan sebuah skenario. Skenario dibuat untuk mencakup semua operasi terkait SSD TRIM. Dengan skenario SSD dibuat dua partisi volume NTFS dan ReFS sebagai tempat untuk sejumlah file yang akan dilakukan penghapusan permanen (shift + delete), setelahnya masing-masing volume akan diakusisi dengan metode live forensik. Hasil dari akuisisi akan diperiksa untuk dilakukan recovery file yang telah dihapus, jika hasil file recovery menunjukkan nilai hash yang sama dengan file asli maka recovery bisa dinyatakan berhasil, tetapi jika nilai hash file hasil recovery tidak sesuai dengan nilai hash file asli maka recovery dinyatakan gagal.

Untuk mempermudah mengidentifikasi banyak file yang berhasil direcovery, file diidentifikasi dengan memasukan label pada setiap pemberian nama file, seperti R1 untuk ReFS TRIM enable, R2 untuk ReFS TRIM disable, N1 untuk NTFS TRIM enable, N2 untuk NTFS TRIM disable sehingga mem-permudah proses penghapusan dimana file lama tidak akan tertimpa dengan file baru. Untuk file dengan nama ganjil TRIM dinonaktifkan, dan untuk file dengan nama genap TRIM diaktifkan. Masing-masing file dengan label N1,N2 dimasukan pada partisi volume drive D:\ file sistem NTFS dan file dengan label R1,R2 drive E:\ file sistem ReFS.

Banyak nilai hash file ganjil-genap pada penelitian kali ini ada 136 dengan beberapa memiliki nilai hash yang sama tetapi dengan label nama file yang berbeda ditunjukan tabel 1. Gambar 3 menunjukan skenario yang akan digunakan pada penelitian ini, tim merah bertindak sebagai pelaku dan tim biru bertindak sebagai investigatior. Untuk meng-aktifkan dan menonaktifkan perintah TRIM pada SSD bisa dilakukan melalui command port pada windows kemudian mengetikan perintah "behavior set disableDeleteNotify ReFS 0" untuk mengaktifkan perintah TRIM pada volume dengan file sistem ReFS dan "behavior set disableDeleteNotify ReFS 1" untuk menonaktifkan perintah TRIM pada volume dengan file sistem ReFS, sementara itu untuk file sistem NTFS menggunakan perintah "behavior set disableDeleteNotify NTFS 0" untuk mengaktifkan perintah TRIM dan "behavior set disableDeleteNotify NTFS 1" untuk menonaktifkan perintah TRIM.

Tabel 1. Sampel Sebagian file Data

Nilai HASH MD5 File Asli	Nama File ReFS TRIM Enable	Nama File ReFS TRIM Disable	Nama File NTFS TRIM Enable	Nama File NTFS TRIM Disable
e67e68.....e81596a	file exe 1, R1.exe	file exe 1, R2.exe	file exe 1, N1.exe	file exe 1, N2.exe
e506b1.....0b494475	file exe 2, R1.exe	file exe 2, R2.exe	file exe 2, N1.exe	file exe 2, N2.exe
37527da.....1bf8d4126	file exe 3, R1.exe	file exe 3, R2.exe	file exe 3, N1.exe	file exe 3, N2.exe
202bed6d.....ed4fec01	Doc, R1.doc	Doc, R2.doc	Doc, N1.doc	Doc, N2.doc
2a2539f6.....601d94e	Docx, R1.docx	Docx, R2.docx	Docx, N1.docx	Docx, N2.docx
b43a20.....ea99e871	ODT, R1.odt	ODT, R2.odt	ODT, N1.odt	ODT, N2.odt
da61ec3a4b.....d65abca	pdf, R1.pdf	pdf, R2.pdf	pdf, N1.pdf	pdf, N2.pdf
16bc6e9ff.....0957bc6	PowerPoint, R1.pptx	PowerPoint, R2.pptx	PowerPoint, N1.pptx	PowerPoint, N2.pptx
9fdbfbd.....366b1598f	teks, R1.txt	teks, R2.txt	teks, N1.txt	teks, N2.txt
168dbd.....5310911801	XLSX, R1.xlsx	XLSX, R2.xlsx	XLSX, N1.xlsx	XLSX, N2.xlsx
605756.....98394a6db	BMP, R1.bmp	BMP, R2.bmp	BMP, N1.bmp	BMP, N2.bmp
cf69c943fa.....d83242f7a	GIF, R1.gif	GIF, R2.gif	GIF, N1.gif	GIF, N2.gif
a3333bb3.....bede7ad	JPG, R1.jpg	JPG, R2.jpg	JPG, N1.jpg	JPG, N2.jpg
068f0a467.....2f263a86	PNG, R1.png	PNG, R2.png	PNG, N1.png	PNG, N2.png
27d27b8eb.....de0554e	m4a, R1.m4a	m4a, R2.m4a	m4a, N1.m4a	m4a, N2.m4a
180b9de2.....3e8a5ed1	mp3, R1.mp3	mp3, R2.mp3	mp3, N1.mp3	mp3, N2.mp3
8f775190f5.....257ca5d	WAV, R1.wav	WAV, R2.wav	WAV, N1.wav	WAV, N2.wav
5717ede6e.....12fbc3d	WMA, R1.wma	WMA, R2.wma	WMA, N1.wma	WMA, N2.wma
1ecc983.....a2a0c4af	3gp, R1.3gp	3gp, R2.3gp	3gp, N1.3gp	3gp, N2.3gp
611daaf.....1ccc8bf	AVI, R1.avi	AVI, R2.avi	AVI, N1.avi	AVI, N2.avi
54a827.....ce1d934	FLV, R1.flv	FLV, R2.flv	FLV, N1.flv	FLV, N2.flv
c08dc5bdeb.....a34fd17	MKV, R1.mkv	MKV, R2.mkv	MKV, N1.mkv	MKV, N2.mkv
440fd3c73e.....5dfebbf	MOV, R1.mov	MOV, R2.mov	MOV, N1.mov	MOV, N2.mov
0b6e8415.....888c2aa	MP4, R1.mp4	MP4, R2.mp4	MP4, N1.mp4	MP4, N2.mp4
3af1e2030.....425a106	MPG, R1.mpg	MPG, R2.mpg	MPG, N1.mpg	MPG, N2.mpg
60a4ca406.....1db388	OGG, R1.Ogg	OGG, R2.Ogg	OGG, N1.Ogg	OGG, N2.Ogg
bf23511.....836b488a	webm, R1.webm	webm, R2.webm	webm, N1.webm	webm, N2.webm
5228d2.....86e0a642	WMV, R1.wmv	WMV, R2.wmv	WMV, N1.wmv	WMV, N2.wmv
70a42cc.....248ecceb7	RAR 1, R1.rar	RAR 1, R2.rar	RAR 1, N1.rar	RAR 1, N2.rar
82517191.....4820c9d3	RAR 2, R1.rar	RAR 2, R2.rar	RAR 2, N1.rar	RAR 2, N2.rar
3ca2fbabcb.....297fe01	RAR 3, R1.rar	RAR 3, R2.rar	RAR 3, N1.rar	RAR 3, N2.rar
5340d6809d.....65a9d	zip 1, R1.zip	zip 1, R2.zip	zip 1, N1.zip	zip 1, N2.zip
18271d30.....76eba6b6	zip 2, R1.zip	zip 2, R2.zip	zip 2, N1.zip	zip 2, N2.zip
c4e514a94.....7963ec5	zip 3, R1.zip	zip 3, R2.zip	zip 3, N1.zip	zip 3, N2.zip



Gambar 3. Skenario recovery SSD volume NTFS dan ReFS

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 D:\ file sistem NTFS, dan Drive E:\ file sistem ReFS. File yang dimanipulasi disimpan di partisi Drive D:\ dan Drive E:\.
3. Pelaku meletakan file-file dengan label ganjil dan genap kedalam 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 D:\ dan Drive E:\..

Langkah-langkah Penyidik:

1. Penyidik menghubungkan USB SSD SATA eksternal ke komputer Pelaku untuk menyimpan hasil perolehan dan recovery file.
2. Penyidik melakukan akuisisi pada SSD langsung di komputer pelaku dengan USB SSD eksternal SATA dan alat Portable Imager FTK.

a. Komputer penyidik digunakan untuk melakukan pemeriksaan dan analisis hasil pencitraan dengan menggunakan teknik disk

III. HASIL DAN PEMBAHASAN

A. Hasil

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 mengguna-kan alat Hetman Partition Recovery, sesuai dengan skenario yang telah ditetapkan.

Tabel 2. Hasil jumlah ekstraksi data sesuai dengan nama disk

Nama Disk	Berhasil Direcovery	Gagal Direcovery
SSD TRIM enable NTFS	34 file	0 file
SSD TRIM enable NTFS	3 file	31 file
SSD TRIM disable ReFS	25 file	9 file
SSD TRIM enable ReFS	0 file	34 file

Berdasarkan tabel 2 SSD TRIM disable NTFS berhasil dipulihkan sepenuhnya sedangkan pada SSD TRIM enable NTFS ada 3 file berhasil dipulihkan yaitu: teks, N1.txt; RAR 1, N1.rar; zip 1, N1.zip. SSD TRIM disable ReFS berhasil dipulihkan 25 file dan 9 file gagal dipulihkan, sedangkan pada SSD TRIM enable ReFS tidak ada data yang berhasil dipulihkan. Dari tabel 3 bisa diketahui bahwa file sistem akan berpengaruh pada fitur TRIM SSD karena pada TRIM enable NTFS adanya data yang bisa dipulihkan sedangkan TRIM enable ReFS tidak ada data yang bisa dipulihkan. Untuk mendapatkan hasil jumlah estraksi data seperti pada tabel 2 dubutuhkan empat tahapan yaitu persiapan, rekonstruksi, estraksi bukti, dan analisis.

B. Pembahasan

Hasil dari penelitian ini didapatkan dengan empat tahapan yaitu persiapan, rekonstruksi, estraksi bukti, dan analisis.

1. Persiapan

Dalam langkah ini, dilakukan akuisisi bukti digital yang terdapat dalam SSD menggunakan alat yang mendukung teknik forensik langsung, yaitu Portable FTK Imager. Teknik live forensik diterapkan untuk memulihkan file yang telah dihapus secara permanen di SSD dengan file sistem NTFS dan ReFS, baik dengan TRIM yang dinonaktifkan maupun diaktifkan. Dalam penelitian ini, alat live forensik yang digunakan adalah Portable FTK Imager, yang memiliki kemampuan untuk mengambil data dan file yang telah dihapus, sehingga mendukung praktik forensik langsung. Gambar 4 (a) dan Gambar 4 (b) menunjukkan dokumentasi hasil proses pencitraan langsung pada file sistem NTFS dengan TRIM dinonaktifkan, sementara Gambar 5 (a) dan Gambar 5 (b) menunjukkan dokumentasi hasil proses pencitraan langsung pada file sistem NTFS dengan TRIM diaktifkan, menggunakan Portable FTK Imager. Tabel 4 berisi hasil dari proses pencitraan beserta nilai hash MD5. Tujuan dari proses pencitraan 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	f7ed5aed288ce72d70f3a693ab68afc6
Laporan Hash	f7ed5aed288ce72d70f3a693ab68afc6
Hasil verivikasi	Nilai Hash Sama

(a)

Hasil Verify Pencitraan	
Nama	NTFS TRIM ENABLE.001
Sector count	46864384
Nilai Hash MD5	
Computed Hash	d2f9a1a626d12b4c326f541e56915255
Laporan Hash	d2f9a1a626d12b4c326f541e56915255
Hasil verivikasi	Nilai Hash Sama

(b)

Gambar 4. (a) Hasil proses pencitraan NTFS TRIM disable (b) Hasil proses pencitraan NTFS TRIM enable

Hasil Verify Pencitraan	
Nama	ReFS TRIM DISABLE.001
Sector count	67833856
Nilai Hash MD5	
Computed Hash	018cd8000ea9a6810453 3a08236f80e1
Laporan Hash	018cd8000ea9a6810453 3a08236f80e1
Hasil verivikasi	Nilai Hash Sama

(a)

Hasil Verify Pencitraan	
Nama	REFS TRIM ENABLE.001
Sector count	67833856
Nilai Hash MD5	
Computed Hash	737b64c4cc6b9e62ac5a51efa49ac1f
Laporan Hash	737b64c4cc6b9e62ac5a51efa49ac1f
Hasil verivikasi	Nilai Hash Sama

(b)

Gambar 5. (a) hasil proses pencitraan ReFS TRIM disable (b) Hasil proses pencitraan ReFS TRIM enable

2. Rekonstruksi

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 dilakukan scaning data yang telah dihapus didalam partisi hasil mount disk, hasil mounting disk pada gambar 6.

Gambar 6. Hasil proses mounting disk

Aplikasi tidak akan mengubah image yang telah dimount karena pada prosesnya hanya melakukan scaning data dengan teknik disk carving. Setelah data dimount akan dilakukan scaning dengan teknik disk carving, dengan pilihan full scan seperti gambar 7 maka aplikasi akan secara otomatis memeriksa data yang telah dihapus permanen. Teknik disk carving akan memeriksa *image* data yang telah dimounting 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 cariving akan menyesuaikan header dan foter dari potongan file yang sama untuk disatukan. Proses full scan akan memakan waktu berdasarkan kecepatan transfer data dan pemrosesan dari komputer pemeriksa.

Gambar 7. Proses full scan

Proses full scan akan memakan waktu bergantung pada kecepatan perangkat keras yang dimiliki pemeriksa dan banyak data yang akan diperiksa dalam penelitian ini kecepatan scan hanya memakan waktu lima sampai empat menit untuk setiap partisi yang diperiksa.

3. Estraksi bukti

Pada tahap ini, peneliti mengekstrak file pencitraan. Proses ini bertujuan untuk mengekstraksi hasil pencitraan. Untuk menjaga keutuhan dan keaslian barang bukti, dilakukan ekstraksi pada duplikat hasil pencitraan. Alat yang membantu proses ekstraksi pemeriksaan dan analisis pencitraan adalah hetman partition recovery. Gambar 8, adalah scan menggunakan alat hetman partition recovery yang menunjukkan bukti digital yang terhapus. Setelah di scan hasil dari scan akan di ekstrak ke komputer investigator seperti pada gambar 9.

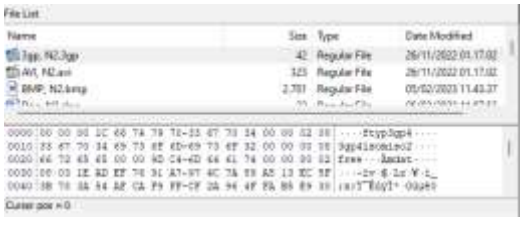
Gambar 8. Hasil scan NTFS TRIM DISABLE

Gambar 9. Sampel hasil ekstraksi data

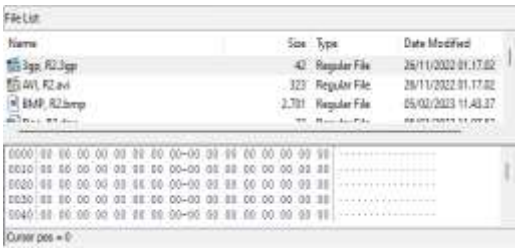
Untuk menjaga integritas file setelah diekstraksi, peneliti mengunci file dengan nilai HASH md5 dari masing-masing file dengan FTK imager.

4. Analisis

Pada langkah ini, proses analisis hasil akuisisi dilaksanakan menggunakan Portable FTK Imager. Pada tahap ini, ditemukan nilai file *signature* yang telah tidak berhasil *direcovery* karena telah dibersihkan oleh fungsi TRIM atau file sistem. File tanda tangan ini berperan sebagai representasi informasi data yang digunakan untuk mengenali isi dari data tersebut (Jeong and Lee, 2019; Kessler, 2023). Gambar 10 menunjukan, saat file hasil *recovery* pada NTFS TRIM *disable*, *signature* masih utuh. Namun, Lain halnya dengan ReFS TRIM *disable* pada gambar 11, sebagian file mengalami kerusakan karena telah dibersihkan oleh file sistem. Sementara itu semua file pada ReFS TRIM *enable, signature* tidak bisa ditemukan karena kemungkinan telah dihapus fitur TRIM membuat data yang dipulihkan menjadi folder kosong. Tetapi pada NTFS TRIM *enable* ditemukan file yang masih memiliki nilai hash yang sama dengan hash file asli.



Gambar 10. Analisis salah satu file hasil *recovery* NTFS TRIM disable



Gambar 11. Analisis salah satu file hasil *recovery* ReFS TRIM disable

Semua file data penelitian ini yang berhasil dan gagal *direcovery* pada tabel 3, ditunjukan adanya perbedaan hasil dari *recovery* dari file sistem NTFS TRIM disable dan ReFS TRIM disable.

Pada NTFS TRIM disable semua file berhasil dipulihkan tetapi tidak pada ReFS TRIM enable ada beberapa file yang gagal dipulihkan karena memiliki nilai kunci hash yang berbeda dengan file asli salah satunya XLSX, R2.xlsx; mp3, R2.mp3; WAV, R2.wav; 3gp, R2.3gp. Pada NTFS TRIM enable berhasil diketahui file teks, N1.txt; RAR 1, N1.rar; zip 1, N1.zip dari sini kita bisa mengetahui bahwa file yang telah dihapus permanen pada SSD dengan TRIM enable ada kemungkinan masih bisa dipulihkan, tetapi pada file sistem ReFS TRIM enable semua file tidak berhasil dipulihkan karena seluruh file telah menjadi folder kosong dengan labal nama R1 yang tidak memiliki nilai kunci hash.

Tabel 3. Hasil daftar file yang berhasil dan gagal dipulihkan

File yang berhasil direcovery	File yang gagal direcovery
file exe 1, N2.exe; file exe 1, R2.exe	file exe 1, N1.exe; file exe 1, R1.exe
file exe 2, N2.exe; file exe 2, R2.exe	file exe 2, N1.exe; file exe 2, R1.exe
file exe 3, N2.exe; file exe 3, R2.exe	file exe 3, N1.exe; file exe 3, R1.exe
Doc, N2.doc; Doc, R2.doc	Doc, N1.doc; Doc, R1.doc
Docx, N2.docx; Docx, R2.docx	Docx, N1.docx; Docx, R1.docx
ODT, N2.odt; ODT, R2.odt	ODT, N1.odt; ODT, R1.odt
pdf, N2.pdf; pdf, R2.pdf	pdf, N1.pdf; pdf, R1.pdf
PowerPoint, N2.pptx; PowerPoint, R2.pptx	PowerPoint, N1.pptx; PowerPoint, R1.pptx
teks, N1.txt; teks, N2.txt; teks, R2.txt	teks, R1.txt
XLSX, N2.xlsx	XLSX, N1.xlsx; XLSX, R2.xlsx; XLSX, R1.xlsx
BMP, N2.bmp; BMP, R2.bmp	BMP, N1.bmp; BMP, R1.bmp
GIF, N2.gif; GIF, R2.gif	GIF, N1.gif; GIF, R1.gif
JPG, N2.jpg; JPG, R2.jpg	JPG, N1.jpg; JPG, R1.jpg
PNG, N2.png; PNG, R2.png	PNG, N1.png; PNG, R1.png
m4a, N2.m4a; m4a, R2.m4a	m4a, N1.m4a; m4a, R1.m4a
mp3, N2.mp3	mp3, N1.mp3; mp3, R2.mp3; mp3, R1.mp3
WAV, N2.wav	WAV, N1.wav; WAV, R2.wav; WAV, R1.wav
WMA, N2.wma	WMA, N1.wma; WMA, R2.wma; WMA, R1.wma
3gp, N2.3gp	3gp, N1.3gp; 3gp, R2.3gp; 3gp, R1.3gp
AVI, N2.avi; AVI, R2.avi	AVI, N1.avi; AVI, R1.avi
FLV, N2.flv; FLV, R2.flv	FLV, N1.flv; FLV, R1.flv
MKV, N2.mkv; MKV, R2.mkv	MKV, N1.mkv; MKV, R1.mkv
MOV, N2.mov; MOV, R2.mov	MOV, N1.mov; MOV, R1.mov
MP4, N2.mp4; MP4, R2.mp4	MP4, N1.mp4; MP4, R1.mp4
MPG, N2.mpg; MPG, R2.mpg	MPG, N1.mpg; MPG, R1.mpg
OGG, N2.Ogg; OGG, R2.Ogg	OGG, N1.Ogg; OGG, R1.Ogg
webm, N2.webm	webm, N1.webm; webm, R2.webm; webm, R1.webm
WMV, N2.wmv	WMV, N1.wmv; WMV, R2.wmv; WMV, R1.wmv
RAR 1, N1.rar; RAR 1, R2.rar; zip 1, N2.zip	RAR 1, R1.rar
RAR 2, N2.rar; RAR 2, R2.rar	RAR 2, N1.rar; RAR 2, R1.rar
RAR 3, N2.rar; RAR 3, R2.rar	RAR 3, N1.rar; RAR 3, R1.rar
zip 1, N1.zip; zip 1, N2.zip	zip 1, R2.zip; zip 1, R1.zip
zip 2, N2.zip	zip 2, N1.zip; zip 2, R2.zip; zip 2, R1.zip
zip 3, N2.zip; zip 3, R2.zip	zip 3, N1.zip; zip 3, R1.zip

IV. SIMPULAN DAN SARAN

A. Simpulan

Dalam penelitian ini, kami berhasil menunjukkan bahwa teknik disk carving dapat digunakan untuk memulihkan data dari file sistem yang rusak, khususnya dalam konteks penggunaan file sistem ReFS yang tidak dapat dibaca oleh perangkat lunak komersial. Hasil pengujian menunjukkan bahwa dengan menggunakan teknik disk carving, kami dapat memulihkan lebih banyak data. Pada file sistem NTFS dengan TRIM diaktifkan, kami berhasil memulihkan sekitar 9% data, sedangkan pada TRIM dinonaktifkan, kami berhasil memulihkan 100% data. Tetapi, pada file sistem ReFS dengan TRIM diaktifkan, kami tidak berhasil memulihkan data sama sekali (0%), karena data yang diekstraksi hanya berbentuk folder. Namun, ketika TRIM dinonaktifkan pada file sistem ReFS, kami berhasil memulihkan sekitar 74% data. Selain itu, penelitian ini juga berhasil memulihkan data yang telah dihapus secara permanen dari SSD dengan TRIM diaktifkan pada file sistem NTFS, yang menjadi masalah penelitian sebelumnya.

B. Saran

Karena adanya keterbatasan penelitian ini, file yang berhasil dipulihkan dalam penelitian ini saat TRIM hidup hanya file dalam format txt, zip yang berisi file txt, dan rar yang juga berisi file txt. Oleh karena itu penelitian selanjutnya, disarankan untuk melakukan teknik disk carving secara manual pada fitur TRIM SSD untuk memahami penyebab data dalam format (.txt) dapat dipulihkan pada file sistem NTFS. Selain itu, pengujian *recovery* data pada file sistem dengan format yang berbeda dan data yang dihapus secara konvensional juga bisa menjadi fokus penelitian selanjutnya. Hasil penelitian ini juga menunjukkan bahwa jenis file sistem memiliki pengaruh pada fitur TRIM SSD dan dapat memengaruhi hasil *recovery* data. Oleh karena itu, penelitian lebih lanjut akan membantu memahami lebih dalam tentang kaitan antara jenis file sistem, fitur TRIM, dan *recovery* data.

DAFTAR RUJUKAN

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

Hepisuthar, M., 2021. Comparative Analysis Study on SSD, HDD, and SSHD. *Turkish Journal of Computer and Mathematics ….* [online] Available at: https://turcomat.org/index.php/turkbilmat/article/view/1644

Hilgert, J.N., Lambertz, M. and Plohmann, D., 2017. Extending the Sleuth Kit and its underlying model for pooled storage file system forensic analysis. In: *DFRWS 2017 USA - Proceedings of the 17th Annual DFRWS USA*. Digital Forensic Research Workshop. pp.S76–S85. https://doi.org/10.1016/j.diin.2017.06.003.

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

Kessler, G.C., 2023. *GCK'S FILE SIGNATURES TABLE*. [online] www.garykessler.net/library/file_sigs.html . Available at: https://www.garykessler.net/library/file_sigs.html [Accessed 30 June 2023].

Lee, S., Park, J., Hwang, H., Lee, S., Lee, S. and Jeong, D., 2021. Forensic analysis of ReFS journaling. *Forensic Science International: Digital Investigation*, 38, pp.1–10. https://doi.org/10.1016/j.fsidi.2021.301136.

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

Lv, Y., Shi, L., Li, Q., Xue, C.J. and Sha, E.H.-M., 2020. Access Characteristic Guided Partition for Read. IEEE.

Lv, Y., Shi, W., Zhang, W., Lu, H. and Tian, Z., 2023. Don't trust the Clouds easily: The Insecurity of Content Security Policy based on Object Storage. *IEEE Internet of Things Journal*, pp.1–1. https://doi.org/10.1109/JIOT.2023.3238658.

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

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

Pranoto, W., RIadi, I. and Prayudi, Y., 2020. 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), pp.129–138. https://doi.org/10.22219/kinetik.v5i2.1032.

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

Raad Ali, R., Malik Mohamad, K., Jamel, S. and Kamal Ahmad Khalid, S., 2018. A REVIEW OF DIGITAL FORENSICS METHODS FOR JPEG FILE CARVING. *Journal of Theoretical and Applied Information Technology*, [online] 15, p.17. Available at: <www.jatit.org>.

Ramadhan, R.A. and Mualfah, D., 2021. 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), pp.183–192. https://doi.org/10.25299/itjrd.2021.vol5(2).5750.

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

Riadi, I., Umar, R. and 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), pp.70–82. https://doi.org/10.21831/elinvo.v3i1.19308.

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

Winter, R., 2013. SSD vs HDD - Data recovery and destruction. *Network Security*, 2013(3), pp.12–14. https://doi.org/10.1016/S1353-4858(13)70041-2.

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