IT Journal Research and Development (ITJRD)
Vol.5, No.2, Maret 2021, E-ISSN : 2528-4053 | P-ISSN : 2528-4061
DOI : 10.25299/itjrd.2021.vol5(2).5750

Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh

Rizdqi Akbar Ramadhan[1], Desti Mualfah[2]
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Islam Riau[1]
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muhamadiyah Riau[2]
rizdqiramadhan@eng.uir.ac.id[1], destimualfah@umri.ac.id[2]

Article Info

History :

Dikirim 30 Oktober 2020
Direvisi 03 November 2020
Diterima 17 November 2020

Kata Kunci :

Solid State Drive
Digital Forensik
Investigation
Recovery Files
Operating System

Abstrak

Solid State Drive (SSD) merupakan solusi terkni untuk mempercepat pemrosesan data dari berbagai komputer desktop yang bersifat multiplatform. Fitur TRIM yang ada pada SSD berguna untuk menghilangkan garbage data yang dihapus permanen oleh user, dimana metode ini memiliki benefit untuk memperpanjang usia pakai dari perangkat SSD. Kontradiksi dari penggunaan metode ini adalah sulitnya bagi investigator forensik untuk melakukan recovery data yang telah terhapus apabila terjadi praktek cyber crime dalam kasus barang bukti berupa komputer dengan storage SSD. Objek eksperimen dalam penelitian ini berdasarkan perspektif sistem operasi mainstream yaitu Windows, Linux dan Macintosh yang terinstall pada SSD dimana pada masing-masing sistem operasi dilakukan simulasi penghapusan data yang tersimpan dengan perbandingan konfigurasi TRIM enable dan TRIM disable. Metode Digital Forensik yang diimplementasikan pada hal ini adalah National Intitute of Justice (NIJ) dimana metode ini berlaku sebagai acuan dalam praktek Digital Forensik pada penelitian ini. Perangkat lunak SLEUTH KIT Autopsy merupakan perangkat Digital Forensik yang digunakan dalam perspektif investigator dalam akusisi dan analisis barang bukti SSD pada simulasi kasus penelitian ini. Novelti yang didapatkan pada konten penelitian adalah sistem operasi yang menjadi objek eksperimen merupakan sistem operasi Windows, Linux, dan Macintosh rilis terkini yang tentunya memiliki potensi yang besar dalam hal eksplorasi, khususnya Digital Forensik. Windows memiliki peluang hasil *recovery* paling besar diantara 2 sistem operasi lainnya dalam penelitian ini.

© This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Koresponden:

Rizdqi Akbar Ramadhan
Program Studi Teknik Informatika, Fakultas Teknik
Universitas Islam Riau
Jalan Kaharudin Nasution, Pekanbaru, Indonesia, 28284
Email : rizdqiramadhan@eng.uir.ac.id

1. PENDAHULUAN

Teknologi komputer mengalami perkembangan yang pesat dalam dasawarsa terakhir. Komputer Forensic yang menjadi bidang ilmu khususnya mempelajari tentang anatomi komputer itu sendiri juga berbanding lurus dengan kemajuan teknologi tersebut [1]. Penelitian ini lebih menekankan kepada Investigasi Forensik secara praktikal dibandingkan teoritis namun dengan menggunakan kerangka kerja yang lazim digunakan, yaitu NIJ (National Institute of Justice). Dalam penelitian ini penulis lebih menekankan pendekatan teknis praktek investigasi Forensik Digital menggunakan *framewok* diluar aspek hukumnya. Komponen komputer secara esensial terdiri perangkat keras dan perangkat lunak [2] yang dalam ilmu komputer forensik perangkat keras menjadi objek penelitian secara anatomi. Perangkat lunak selain berperan sebagai objek penelitian secara anatomi dan logic disisi lainnya juga berperan sebagai perangkat pendukung *(tools). Tools* pendukung yang penulis gunakan dalam implementasi Digital Forensic dalam penelitian ini adalah Sleuth Kit Autopsy dan guna proses *imaging* akan menggunakan FTK Imager.

Secara organisasi dan arsitektur komputer, dalam hal ini adalah CPU *(central processing unit)* terdiri dari komponen inti berupa Processor, Random Access Memory (RAM), serta media penyimpanan *non volatile* berupa *storage* yang sering disebut Hardisk [3]. *Storage* sendiri [4] dewasa ini terbagi atas dua spesifikasi yaitu HDD *(Harddisk Drive)* dan SDD *(Solid State Drive).* Teknologi terbaru komputer dituntut akan kecepatan akses dalam pengoperasiannya, salah satunya dengan penggunaan Solid State Drive yang menggantikan posisi Hardisk Drive dalam media penyimpanan data. SSD memiliki fitur yang bernama fitur TRIM. Fitur TRIM memungkinkan OS (operating system) untuk mengintruksikan SSD terkait block mana saja yang sudah tidak digunakan [5]. Sehingga ketika akan ditulis, tidak perlu melakukan proses penghapusan terlebih dahulu. Fitur TRIM membantu menjaga agar performa Write di drive SSD terus terjaga baik. Fungsi TRIM menghapus blok yang telah ditandai untuk dihapus oleh sistem operasi. Menurut kacamata forensika digital, kontradiksi dari penggunaan SSD dengan fitur TRIM nya adalah ”fungsi TRIM memiliki efek negatif pada analisis forensik khususnya pada recovery data”[6]. Penghapusan yang dilakukan tidak dijamin terangkat kembali karena sistem controller memori pada SSD telah memutuskan kapan dan berapa banyak blok ditandai untuk penghapusan [7].

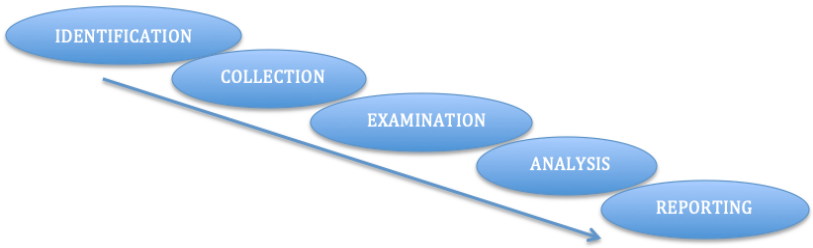
Sederhananya, TRIM yang telah ter-enable berfungsi untuk memusnahkan garbage data yang telah dihapus [8]. Berdasarkan studi literatur dari penelitian-penelitian terdahulu yang digunakan sebagai pendukung dari penelitian ini, selalu ditemukan eksperimen pada SSD Forensik dengan menggunakan tools yang lazim digunakan dalam melakukan recovery data. Sayangnya, dari eksperimen-eksperimen sebelumnya terlihat bahwa fungsi TRIM selalu menjadi tantangan dalam recovery data. Pada kasus recovery data menggunakan HDD konvensional, [9] proses recovery data secara garis besar dapat mengangkat kembali Bukti Digital yang diperlukan guna kebutuhan investigasi. Dalam penelitian ini SSD menjadi objek penelitian yang mewakili perangkat keras serta *Operating System* Windows, Linux dan Macintosh sebagai objek eksperimen yang mewakili perangkat lunak. Parameter yang diukur dalam penelitian ini berupa kemampuan Sleuth Kit Autopsy dalam recovery file serta durasi waktu yang dibutuhkannya dalam analisis dari masing-masing sistem operasi Windows, Linux, dan Macintosh beserta file didalamnya.

2. METODE PENELITIAN

Penelitian dilakukan dengan simulasi skenario berdasarkan 2 perspektif, yaitu perspektif investigator dan lainnya adalah perspektif pelaku kejahatan digital yang dikemas dalam satu garis waktu. Perspektif pelaku dalam skenario melakukan manipulasi jejak digital menggunakan SSD, selanjutnya perspektif investigator dalam mencari dan analisa bukti digital dari SSD skenario pelaku. Tahapan penelitian yang dilakukan adalah menggunakan pendekatan metodologi teknik statik forensik berdasarkan acuan NIJ (Natinal Institute of Justice) yang dapat dilihat pada gambar 1. Tahapan metode dari NIJ ini terbagi menjadi lima tahapan yakni identification, collection, examination, analysis, dan reporting [10], secara lengkap dipaparkan sebagai berikut: Tahap identification atau tahap identifikasi merupakan kegiatan pemilahan barang bukti tindak kejahatan

digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti. Tahap collection atau tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan [11]. Tahap examination atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik *hashing* [12]. *Hash* merupakan suatu kode dari hasil enkripsi yang umumnya terdiri dari huruf maupun angka yang acak. Fungsi Hash dalam digital forensik digunakan untuk kalkulasi serta analisa duplikasi di sebuah arsip komputer yang besar. Ekstensi hash yang digunakan dalam penelitian ini adalah MD5.

Tahap analysis atau tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggung jawabkan secara ilmiah dan secara hukum. Tahap reporting atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis [13]. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tools, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, tools, atau aspek pendukung lainnya pada proses tindakan digital forensik [14].



Gambar 1. National Institue of Justice (NIJ) Methodology

2.1. Perangkat Keras dan Perangkat Lunak beserta *Environment* Lainnya

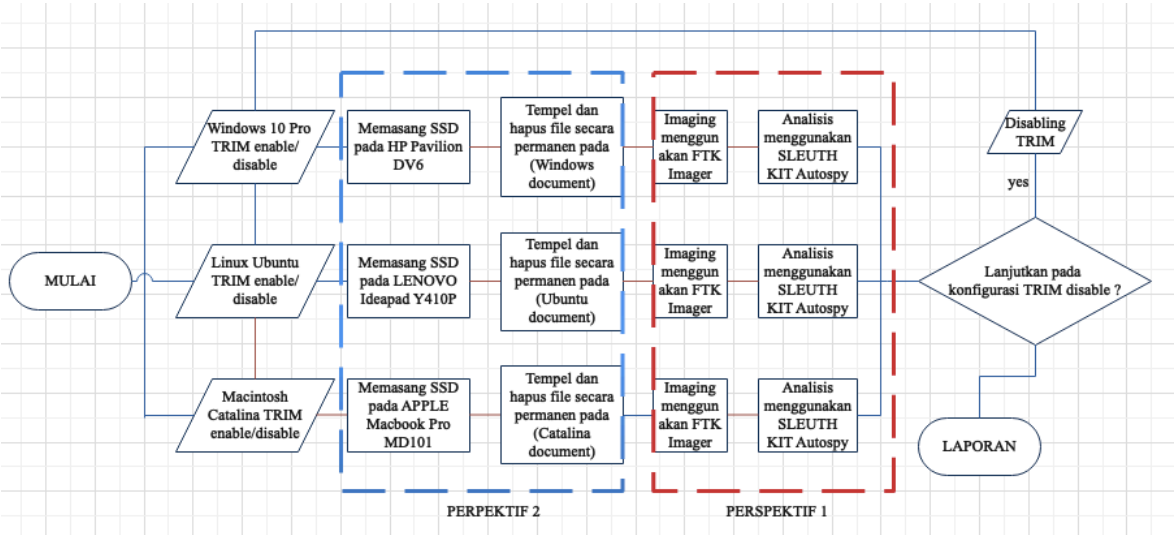
Pengumpulan yang meliputi hardware dan software dalam penelitian ini terbagi pada 2 perspektif. Perspektif yang pertama adalah perspektif investigator yang menggunakan perangkat keras berupa Asus TUF Gaming FX505DD yang dapat dilihat pada tabel 1, serta perangkat lunak penunjang implementasi digital forensik berupa FTK Imager, Hash Calculator dan SLEUTH KIT Autopsy. Selanjutnya untuk perspektif yang kedua adalah perspektif barang bukti yang akan diambil bukti digitalnya. Pada perspektif kedua, perangkat keras yang digunakan adalah Solid State Drive (SSD) Midasforce 120GB yang sudah mendukung fitur TRIM enable atau TRIM disable. Masing-masing SSD akan terinstall 3 sistem operasi yang berbeda; Windows 10 Profesional, Linux Ubuntu, dan Macintosh OSX Catalina. Ketiga sistem operasi yang dipilih merupakan sistem operasi yang umum digunakan dalam komputasi *desktop* pribadi maupun skala *workstation.* Hal lain terkait sistem operasi yang menjadi objek eksperimen penelitian ini telah diperbarui melalui pembaruan paling mutakhir dalam kuartal ke-3 tahun ini. Fakta ini bertujuan sebagai novelti dalam proses beserta luaran yang dapat disimpulkan setelah eksperimen berjalan.

Tabel 1. Perbandingan Antara Perspetif 1 dan Perspektif 2

Perspective	Hardware	Software
1	ASUS Tuf Gaming FX505DD	FTK Imager, Hash Calculator, SLEUTH KIT Autopsy.
2	3 units of SSD Midasforce 120GB	Windows 10 Pro x64, Linux Ubuntu amd64, Macintosh OSX Catalina 10.15.4 64bit.

2.2. Konsep Teori

Pada penelitian ini mengadaptasi dan mengimplementasikan metode analisa forensik dari National Institute of Justice (NIJ). Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada [15]. Simulasi dan skenario dilakukan secara eksplisit terhadap SSD dengan 2 konfigurasi yaitu; TRIM enable dan TRIM disable. Hasil yang diharapkan secara garis besar untuk mengetahui perbedaan karakteristik dari masing-masing konfigurasi terhadap masing-masing sistem operasi serta mengetahui jangka waktu SLEUTH KIT Autopsy dalam melakukan analisis sistem dengan ukuran storage 120GB pada Windows, Linux, dan Macintosh. Gambar 2 menjelaskan bagaimana simulasi akan dijalankan berdasarkan 2 perspektif:



Gambar 2. Riset Metodologi dan Analisa Simulasi

2.3. Pengumpulan Data

Dalam melakukan tahapan riset pada perspektif kedua, terdapat 14 sampel file yang umum digunakan dan bersifat kompatibilitas secara global. Masing-masing file di-klasifikasikan atas 7 ekstensi yang berbeda yang dapat dilihat pada Tabel 2. Parameter ukuran file serta nilai hash yang tertampil akan menjadi salah satu sudut pandang analisa karena sifatnya yang rentan terhadap perubahan volume.

Tabel 2. Sampel File Objek Simulasi Forensik

Materials	Extensions	Size	Hash Value
LAGU1	mp3	4,18MB	afbae4d76a5165f3f949eb45c3df9a82
LAGU2	mp3	3,48MB	6c7b092771ff94db8c57ff9cde3760e5

DOKUMEN1	docx	50,3KB	f93ccfee75e8c413094f178afce6d436
DOKUMEN2	docx	660KB	c9a998879b076f106803582ab5fa4d10
FILE1	pdf	203KB	c21d96078a7c5074fb1423987b77b7d7
FILE2	pdf	156KB	615e1a485939664dda4bf2e3bb91c220
FORM1	xlsx	329KB	621d21e4182b6f760519e12f970292ef
FORM2	xlsx	14,1KB	10477bc204af16dc6bff9d298fc2058e
GAMBAR1	jpg	769KB	33ac33365869548ce96c8b6fd90b25ab
GAMBAR2	jpg	49,0KB	a22d7b5b268df6476f06213c11ffd4a9
SLIDE1	pptx	228KB	fb9b95c3cb21ed4ca4edff74df351862
SLIDE2	pptx	402KB	d0fcfadf940310851e0e820aa6eafb60
FILM1	bluray	1,67GB	f81b311b93e1d8d20ea8462f230bb807
FILM2	bluray	1,81GB	e6d2084a9dee34d15efa804754b74ab6

Selanjutnya setelah menentukan sejumlah file yang telah ditetapkan, file-file tersebut akan disalin kepada 3 perangkat SSD yang masing-masing dibedakan atas sistem operasi yang terdapat pada Gambar 3. File sampel akan diletakkan pada direktori *documents* yang terdapat seragam pada 3 sistem operasi tersebut. Pada langkah pertama, konfigurasi TRIM diatur dalam posisi *enable* terlebih dahulu dan selanjutnya dilakukan penghapusan 14 file sampel secara permanen dengan perintah yang variatif dari masing-masing sistem operasi.

Tabel 3. Perbandingan Resource Memori A dan B

Operating System	Enabling TRIM	Disabling TRIM
Windows 10	fsutil behavior set DisableDeleteNotify 0	fsutil behavior set DisableDeleteNotify 1
Linux Ubuntu	sudo fstrim -v /	sudo rm /etc/cron.weekly/fstrim
MacOS Catalina	sudo trimforce enable	sudo trimforce disable

Pada Tabel 3 ditampilkan perintah-perintah konfigurasi *enabling* dan *disabling* TRIM yang terdapat pada masing-masing sistem operasi. Untuk setiap sistem operasi, perintah dijalankan pada CLI *(Command Line Interface)* [16]. Secara terminologi arsitektur komputer, perintah ini merupakan set instruksi sistem operasi kepada *controller* SSD. Metode seperti tidak berlaku pada media penyimpanan konvensional, yaitu Hardisk Drive [17].

(a) (b) (c)

Gambar 3. Sistem Operasi Objek Penelitian (a) Windows10 Pro (b) Linux Ubuntu (c) MacOS 10.15.4 Catalina

3. HASIL DAN PEMBAHASAN

Terdapat 3 perangkat lunak utama dalam metode riset sebagai perspektif 2 yaitu, Hash Calculator yang digunakan untuk menghitung nilai hash dari masing-masing file, hasil *imaging,*

serta hasil *autopsy*. Berikutnya adalah FTK Imager yang merupakan perangkat lunak untuk kontribusinya dalam melakukan *imaging* dari 3 SSD yang digunakan. Selanjutnya, SLEUTH KIT Autopsy yang berjalan pada sistem operasi Windows dengan spesifikasi perangkat keras Processor AMD RYZEN dengan jangkauan *clockspeed* di-angka 2.1-3.7Ghz serta RAM sebesar 8GB ddr4. Berdasarkan spesifikasi tersebut, durasi dalam parameter jam dan menit pada SLEUTH KIT Autopsy dalam melakukan eksaminasi dari awal eksekusi hingga tahapan optimalisasi dalam *recovery* 14 sampel file dalam masing-masing sistem operasi pada SSD sebesar 120GB dapat dilihat pada Tabel 4:

Tabel 4. Hasil Perbandingan Durasi Analisis Sistem Autopsy

Konfigurasi	Windows 10 x64	Linux Ubuntu amd64	Macintosh OSX Catalina
TRIM enable	18 jam 26 menit	11 jam 31 menit	77 jam 19 menit
TRIM disable	19 jam 45 menit	20 jam 10 menit	74 jam 32 menit

Selanjutnya dalam tahapan analisis yang didapatkan dari objek sistem operasi Windows 10 Professional dengan arsitektur 64bit dapat dilihat pada Tabel 5. Pada konfigurasi TRIM enable, keseluruhan dari 14 file dapat terdeteksi kembali namun dengan status *corrupt.* Status ini menyebabkan nilai hash yang berbeda antara pre-autopsy dengan post-autopsy. Dengan ini dapat disimpulkan bahwa file-file tersebut berubah bentuk dan menjadi *orphan files.* Dalam konfigurasi TRIM disable , 12 dari 14 file dapat *recovery* kembali dengan nilai hash yang sama. Sedangkan file DOKUMEN 1 yang berstatus corrupt terdapat perubahan nilai hash yang semulanya bernilai c9a998879b076f106803582ab5fa4d10 menjadi f46940555900b45a14bb633ee744cdb6 serta file bernama FILE1 berekstensi PDF yang awalnya bernilai c21d96078a7c5074fb1423987b77b7d7 berubah menjadi 19cbdc4f6e7e8bec2fbb0eb952046c9c.

Tabel 5. Hasil Analisis Sistem Operasi Windows 10

TRIM enable	Status	Hash Value (pre-autopsy)	Hash Value (post-autopsy)
LAGU1	corrupt	afbae4d76a516....c3df9a82	e126e1323ec1a039f....6aae1358e
LAGU2	corrupt	6c7b092771ff94.....760e5	3b0dd842213775cc6.....b4a8e46
DOKUMEN1	corrupt	f93ccfee75e8c.....e6d436	ab260777b35c17d3fca.....d528c
DOKUMEN2	corrupt	c9a998879b0.....b5fa4d10	73e37c54936f04fe96.....14d5
FILE1	corrupt	c21d96078.....77b7d7	77f270318d54c1c322e.....8af07
FILE2	corrupt	615e1a485939.....91c220	ba4942c353da3e0be6b6....b093b
FORM1	corrupt	621d21e418.....0292ef	c4a51baa1e387fc02272.....730e
FORM2	corrupt	10477bc204af1.....2058e	b182b927e3b6dee7c.....3931e
GAMBAR1	corrupt	33ac333658695.....b25ab	66f35d3e62996ed7ab.....dee6b
GAMBAR2	corrupt	a22d7b5b268df64.....fd4a9	66ff57ab16bbfa39f5a.....49751
SLIDE1	corrupt	fb9b95c3cb2.....1862	ed716fb3fe5f6d2163cd.....1e2e
SLIDE2	corrupt	d0fcfadf94031085....fb60	262c01ff1cc692018b7b.....22fe
FILM1	corrupt	f81b311b93e1.....b807	b2e7f69ba8560bfcf12.....692fa
FILM2	corrupt	e6d2084a9de.....4ab6	fdd74fba92b1d1438bc27.....493

TRIM disable	Status	Hash Value (pre-autopsy)	Hash Value (post-autopsy)
LAGU1	recovered	afbae4d7....df9a82	afbae4d7....df9a82
LAGU2	recovered	6c7b092771ff....3760e5	6c7b092771ff....3760e5
DOKUMEN1	recovered	f93ccfee.....e6d436	f93ccfee.....e6d436
DOKUMEN2	corrupt	c9a998879b0....5fa4d10	f46940555900b45a14b....44cdb6
FILE1	corrupt	c21d96078.....77b7d7	19cbdc4f6e7e8bec2fb.....046c9c

FILE2	recovered	615e1a485939.....91c220	615e1a485939.....91c220
FORM1	recovered	621d21e418.....0292ef	621d21e418.....0292ef
FORM2	recovered	10477bc204af1.....2058e	10477bc204af1.....2058e
GAMBAR1	recovered	33ac333658695.....b25ab	33ac333658695.....b25ab
GAMBAR2	recovered	a22d7b5b268df64.....fd4a9	a22d7b5b268df64.....fd4a9
SLIDE1	recovered	fb9b95c3cb2.....1862	fb9b95c3cb2.....1862
SLIDE2	recovered	d0fcfadf94031085....fb60	d0fcfadf94031085....fb60
FILM1	recovered	f81b311b93e1.....b807	f81b311b93e1.....b807
FILM2	recovered	e6d2084a9de.....4ab6	e6d2084a9de.....4ab6

Pada tahapan analisis TRIM enable dengan objek sistem operasi Linux Ubuntu dengan arsitektur amd64 pada Tabel 6 ditampilkan bahwa seluruh sampel file simulasi tidak dapat *recovery* kembali. Metode yang diterapkan sama halnya dengan 2 sistem operasi lainnya dalam penelitian ini. Dapat dianalisa bahwa seluruh file yang hilang mengindikasikan bahwa fitur TRIM enable pada Linux Ubuntu efektif menghilangkan *garbage* file. Hal ini berdampak signifikan pada investigasi Digital Forensik apabila didapatkan barang bukti berupa SSD dengan sistem operasi Linux Ubuntu. Kemudian pada konfigurasi TRIM disable, terdapat 4 dari 14 sampel file yang dapat dianalisis dengan status *corrupt.* Pada file bernama DOKUMEN1 terdapat perubahan nilai hash yang pada awal mulanya tercatat bernilai f93ccfee75e8c413094f178afce6d436 menjadi bernilai 216a0bc703be344a431c1ebab06194a8 serta pada file DOKUMEN2, FORM1 dan FORM2 sama-sama mendapatkan nilai hash post-autopsy d41d8cd98f00b204e9800998ecf8427e meskipun pada pre-autopsy memiliki nilai hash yang berbeda-beda.

Tabel 6. Hasil Analisis Sistem Operasi Linux Ubuntu

TRIM enable	Status	Hash Value (pre-autopsy)	Hash Value (post-autopsy)
LAGU1	disappear	afbae4d76a516....c3df9a82	-
LAGU2	disappear	6c7b092771ff94.....760e5	-
DOKUMEN1	disappear	f93ccfee75e8c.....e6d436	-
DOKUMEN2	disappear	c9a998879b0.....b5fa4d10	-
FILE1	disappear	c21d96078.....77b7d7	-
FILE2	disappear	615e1a485939.....91c220	-
FORM1	disappear	621d21e418.....0292ef	-
FORM2	disappear	10477bc204af1.....2058e	-
GAMBAR1	disappear	33ac333658695.....b25ab	-
GAMBAR2	disappear	a22d7b5b268df64.....fd4a9	-
SLIDE1	disappear	fb9b95c3cb2.....1862	-
SLIDE2	disappear	d0fcfadf94031085....fb60	-
FILM1	disappear	f81b311b93e1.....b807	-
FILM2	disappear	e6d2084a9de.....4ab6	-

TRIM disable	Status	Hash Value (pre-autopsy)	Hash Value (post-autopsy)
LAGU1	disappear	afbae4d7....df9a82	-
LAGU2	disappear	6c7b092771ff....3760e5	-
DOKUMEN1	corrupt	f93ccfee.....e6d436	216a0bc703b....94a8
DOKUMEN2	corrupt	c9a998879b0....5fa4d10	d41d8cd9.....8427e
FILE1	disappear	c21d96078.....77b7d7	-
FILE2	disappear	615e1a485939.....91c220	-
FORM1	corrupt	621d21e418.....0292ef	d41d8cd9.....8427e
FORM2	corrupt	10477bc204af1.....2058e	d41d8cd9.....8427e
GAMBAR1	disappear	33ac333658695.....b25ab	-

GAMBAR2	disappear	a22d7b5b268df64.....fd4a9	-
SLIDE1	disappear	fb9b95c3cb2.....1862	-
SLIDE2	disappear	d0fcfadf94031085....fb60	-
FILM1	disappear	f81b311b93e1.....b807	-
FILM2	disappear	e6d2084a9de.....4ab6	-

Selanjutnya pada objek simulasi pada sistem operasi Macintosh OSX Catalina 10.15.4 dengan arsitektur 64bit dapat dilihat pada Tabel 7 bahwa pada konfigurasi TRIM enable maupun konfigurasi TRIM disable didapatkan hasil bahwa tidak ada file yang berhasil terdeteksi kembali maupun recovery. Fakta lainnya, durasi eksaminasi pada sistem operasi MacOS Catalina tercatat memiliki durasi yang lebih panjang secara signifikan.

Tabel 7. Hasil Analisis Sistem Operasi MacOS Catalina

TRIM enable	Status	Hash Value (pre-autopsy)	Hash Value (post-autopsy)
LAGU1	disappear	afbae4d76a516....c3df9a82	-
LAGU2	disappear	6c7b092771ff94.....760e5	-
DOKUMEN1	disappear	f93ccfee75e8c.....e6d436	-
DOKUMEN2	disappear	c9a998879b0.....b5fa4d10	-
FILE1	disappear	c21d96078.....77b7d7	-
FILE2	disappear	615e1a485939.....91c220	-
FORM1	disappear	621d21e418.....0292ef	-
FORM2	disappear	10477bc204af1.....2058e	-
GAMBAR1	disappear	33ac333658695.....b25ab	-
GAMBAR2	disappear	a22d7b5b268df64.....fd4a9	-
SLIDE1	disappear	fb9b95c3cb2.....1862	-
SLIDE2	disappear	d0fcfadf94031085....fb60	-
FILM1	disappear	f81b311b93e1.....b807	-
FILM2	disappear	e6d2084a9de.....4ab6	-

TRIM enable	Status	Hash Value (pre-autopsy)	Hash Value (post-autopsy)
LAGU1	disappear	afbae4d76a516....c3df9a82	-
LAGU2	disappear	6c7b092771ff94.....760e5	-
DOKUMEN1	disappear	f93ccfee75e8c.....e6d436	-
DOKUMEN2	disappear	c9a998879b0.....b5fa4d10	-
FILE1	disappear	c21d96078.....77b7d7	-
FILE2	disappear	615e1a485939.....91c220	-
FORM1	disappear	621d21e418.....0292ef	-
FORM2	disappear	10477bc204af1.....2058e	-
GAMBAR1	disappear	33ac333658695.....b25ab	-
GAMBAR2	disappear	a22d7b5b268df64.....fd4a9	-
SLIDE1	disappear	fb9b95c3cb2.....1862	-
SLIDE2	disappear	d0fcfadf94031085....fb60	-
FILM1	disappear	f81b311b93e1.....b807	-
FILM2	disappear	e6d2084a9de.....4ab6	-

Berdasarkan hasil skenario simulasi dan analisis menggunakan 3 sistem operasi yang berbeda, Windows memiliki peluang untuk recovery paling besar, diikuti oleh Linux dan Macintosh dibelakanganya. [18] Ini merupakan tantangan investigator forensik dalam mencari dan eksplorasi bukti digital yang terdapat pada SSD.

4. KESIMPULAN

Berdasarkan hasil penelitian dengan berbagai perangkat keras dan perangkat lunak dari 2 perspektif yang telah ditetapkan, didapatkan beberapa fakta. Linux Ubuntu mencatatkan rata-rata durasi waktu tersingkat dalam proses eksaminasi dan diteruskan oleh sistem operasi Windows 10. Sistem operasi MacOS Catalina secara signifikan memiliki durasi terpanjang dalam hal eksaminasi dengan rata-rata waktu tiga kali lipat lebih lama dibandingkan Linux Ubuntu dan Windows 10. Pada Windows 10 dalam persentase-nya pada konfigurasi TRIM enable, 0% dari 14 file tidak dapat *recovery* dan berstatus *corrupt.* Sedangkan pada TRIM disable, 85,7% file berhasil *recovery* dan 14,3% *corrupt.* Pada Linux Ubuntu presentase *recovery* pada TRIM enable adalah 0% dengan status *disappear* serta pada TRIM disable jumlah file *recovery* adalah 0% dengan catatan 28,5% *corrupt* dan 71,5% *disappear.* Selanjutnya pada Macintosh Catalina presentase *recovery* sebesar 0% dan presentase *disappear* sebesar 100%. Dalam hal *recovery deleted files* sistem operasi Windows 10 dengan file system NTFS memiliki potensi ditemukan artefak barang bukti digital lebih besar, baik dalam konfigurasi TRIM enable maupun TRIM disable, diikuti oleh sistem operasi Linux Ubuntu dengan file system ext4 dan secara signifikan pada sistem operasi MacOS Catalina dengan file system APFS tidak ditemukan sama sekali *recovery deleted files* yang mana hal ini akan menjadi *obstacle* kepada investigator forensik kedepannya. Secara sederhana terkait minimalnya *recovery files* diluar sistem operasi Windows 10 adalah SLEUTH KIT Autopsy yang bersifat *native.* Alternatif *tools* forensik digital yang bisa digunakan adalah ENCASE Forensic yang pada penelitian penulis sebelumnya memiliki kapabilitas lebih baik atas SLEUTH KIT Autopsy. OXYGEN Forensic termasuk alternatif lainnya, namun *tools* ini lebih idientik dengan investigasi *mobile forensic*. Bagi penelitian selanjutnya diharapkan untuk melakukan uji forensik SSD dengan konfigurasi menggunakan RAID 0 yang dimana konfigurasi ini menjadi tren yang akan berkembang dalam pengimplementasian arsitektur penyimpanan digital.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada LLDIKTI Wilayah Kopertis X dalam skema Simlitabmas Penelitian Dosen Pemula (PDP) sebagai penyedia dana untuk realisasi berjalannya penelitian ini.

DAFTAR PUSTAKA

[1] Y. Prayudi and A. SN, "Digital Chain of Custody: State of The Art," *Int. J. Comput. Appl.*, vol. 114, no. 5, pp. 1–9, 2015.

[2] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD)," *Teknomatika*, vol. 9, no. 2, pp. 1–13, 2017.

[3] A. Aljaedi, D. Lindskog, P. Zavarsky, R. Ruhl, and F. Almari, "Comparative Analysis of Volatile Memory Forensics," *IEEE Int. Conf. Privacy, Secur. Risk Trust IEEE Int. Conf. Soc. Comput.*, pp. 1253–1258, 2011.

[4] R. Hubbard, "Forensics Analysis of Solid State Drive (SSD)," pp. 1–11, 2016.

[5] J. Wiebe, "Forensic Insight into Solid State Drives."

[6] F. F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and F. Daryabar, "Digital Forensic Trends and Future," *Int. J. Cyber-Security Digit. Forensics*, vol. 2, no. 2, pp. 48–76, 2013.

[7] N. Memon, "Challenges of SSD forensic analysis."

[8] P. M. Bednar and V. Katos, "SSD: New Challenges for Digital Forensics."

[9] M. Alazab and P. Watters, "Digital forensic techniques for static analysis of NTFS images," *4th Int. Conf. Inf. Technol. ICIT*, 2009.

[10] M. N. Faiz, R. Umar, and A. Yudhana, "Live Forensics Implementation for Browser Comparison on Email Security," *JISKa*, vol. 1, no. 3, pp. 108–114, 2017.

[11] S. Garfinkel, D. Malan, K. Dubec, C. Stevens, and C. Pham, "Disk Imaging with the Advanced Forensics Format, Library and Tools," *Proc. IFIP WG 11.9 Int. Conf. Digit. Forensics*, pp. 1–19, 2006.
[12] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," *Int. J. Sci. Eng. Res.*, vol. 4, no. 10, pp. 1048–1056, 2013.
[13] Z. Shah, A. N. Mahmood, and J. Slay, "Forensic Potentials of Solid State Drives."
[14] S. Mrdovic, A. Huseinovic, and E. Zajko, "Combining static and live digital forensic analysis in virtual environment," *2009 XXII Int. Symp. Information, Commun. Autom. Technol.*, no. August 2016, pp. 1–6, 2009.
[15] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018.
[16] N. Rahim, W. Wahab, Y. Idris, and L. Kiah, "Digital Forensics: An Overview of the Current Trends," *Researchgate.Net*, no. August 2016, 2014.
[17] N. Dwi and W. Cahyani, "FORENSICS ARISING CHALLENGES WHEN SSD IS HEADING FORWARDS REPLACING HDD," pp. 227–232.
[18] Belkasoft, "Recovering Evidence from SSD Drives in 2014: Understanding TRIM, Garbage Collection and Exclusions | Forensic Focus - Articles," *Forensic Focus*, pp. 1–8, 2014.

BIOGRAFI PENULIS

Rizdqi Akbar Ramadhan meraih gelar Sarjana S1 di Universitas Islam Indonesia pada tahun 2013 dengan jurusan Teknik Informatika. Melanjutkan pendidikan S2 dan meraih gelar Master pada tahun 2016 di Universitas Islam Indonesia. Konsentrasi yang dipelajari dan menjadi objek tri dharma pengajaran, pengabdian, penelitian hingga kini adalah cabang ilmu Digital Forensik dan memiliki Certified Hacking and Forensic Investigator (CHFI). Lahir di Pekanbaru dan mengabdi sebagai pengajar di Universitas Islam Riau.

Desti Mualfah lahir di Jawa Tengah dan meraih gelar Sarjana S1 di Universitas Muhamadiyah Magelang pada 2014 serta gelar Master S2 pada 2017 di Universitas Islam Indonesia. Memiliki sertifikasi internasional dalam Certified Ethical Hacking (CEH) dan Certified Hacking and Forensic Investigator (CHFI). Sejak tahun 2018 mengabdi sebagai pengajar di Universitas Muhamadiyah Riau dan aktif melakukan penelitian terhadap cabang ilmu Jaringan Komputer dan Digital Forensik.