IMPLEMENTASI DAN ANALISIS FORENSIKA DIGITAL PADA FITUR TRIM SOLID STATE DRIVE

Rizdqi Akbar Ramadhan[(1)], Yudi Prayudi[(2)], Bambang Sugiantoro[(3)]

[1,2] Magister Teknik Informatika Fakultas Teknologi Industri
Universitas Islam Indonesia, Jl. Kaliurang Km 14.5 Sleman Yogyakarta
[3] Fakultas Sains dan Teknologi, UIN Sunan Kalijaga
Jl. Laksda Adisucipto Yogyakarta

rr6369791@gmail.com

Abstrak

Salah satu solusi perangkat keras yang digunakan untuk kebutuhan terkait kecepatan akses adalah memaksimalkan fungsi storage dengan mengembangkan teknologi storage konvensional atau yang kita kenal dengan Hardisk Drive (HDD) menjadi Solid State Drive (SSD). Berbeda dari arsitektur HDD konvensional dengan piringan magnetis, SSD memiliki arsitektur berupa flash storage dimana menjanjikan kecepatan read/write yang lebih baik secara signifikan. Selanjutnya, penelitian ini melakukan eksperimen menggunakan teknik forensika digital yaitu melakukan imaging, analisis dan examinasi terhadap SSD. Penelitian ini akan membahas perbandingan terkait tools Forensika digital yang digunakan terhadap analisis dan examinasi SSD. Output yang diharapkan berupa gambaran perbedaan fundamental antara HDD dan SSD, alur proses analisis SSD dengan implementasi TRIM serta mendapatkan gambaran terkait tools yang paling efektif dalam melakukan aktifitas Forensika digital dengan SSD. Metode analisis forensic dalam penelitian ini adalah metode Static Forensic dengan menggunakan tools Sleuth Kit Autopsy sebagai media untuk melakukan analisis.

Kata Kunci: *Storage, Solid State Drive (SSD), Tools* Forensika digital, *Hardware*

1. Pendahuluan

Pada saat ini, tingkat kejahatan digital semakin meningkat signifikan. Menurut Symantec, 2 dari 3 orang dewasa bisa menjadi korban kejahatan internet selama hidupnya. Bila dihitung secara global, total kerugian dan kerusakan dari cybercrime mencapai 110 milyar dollar (obengon.com, 2012). *Cybercrime* dapat melalui layanan jejaring social, maupun perangkat komunikasi seperti handphone, smartphone, laptop, tablet PC atau pengguna komputer lainnya. Pesatnya perkembangan *cybercrime*, ternyata beriringan dengan perkembangan teknologi komputer dalam hal ini adalah *hardware.* Sehingga, pada penelitian ini akan membahas implementasi forensika digital terhadap teknologi baru dalam media *storage.*

Teknologi 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. Sehingga ketika akan ditulis, tidak perlu melakukan proses penghapusan dulu. Fitur TRIM membantu menjaga agar performa *Write* di drive SSD terus terjaga baik (Sufehmi, 2015). Menurut Florian Geier (2015) 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"*. Penghapusan yang dilakukan tidak dijamin terangkat kembali karena sistem *controller* memori pada SSD telah memutuskan kapan dan berapa banyak blok ditandai untuk penghapusan. Sederhananya, TRIM yang telah ter-*enable* berfungsi untuk memusnahkan *garbage* data yang telah dihapus (Bednar, Katos, 2011).

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 fungi TRIM selalu menjadi tantangan dalam *recovery data.* Pada kasus *recovery data* menggunakan HDD konvensional, proses *recovery data* secara garis besar dapat mengangkat kembali Bukti Digital yang diperlukan guna kebutuhan investigasi. Pada penelitian ini, solusi terkait kebutuhan pengangkatan informasi atau *recovery data* yang diperlukan dalam proses SSD Forensik dengan implementasi fitur TRIM-nya yang menjadi kendala pada proses *recovery data* SSD yaitu dengan cara menggunakan 3 *tools* forensik yang berbeda dengan parameter yang diuji dalam penelitian ini dipersempit dalam bagaimana kemampuan masing-masing *tools* khususnya dalam melakukan *recovery data.*

2. Literatur Review

2.1 Forensika Digital

Forensika digital adalah rangkaian metode dari teknik dan prosedur untuk mendapatkan barang bukti dari peralatan computer, berbagai media penyimpanan dan media digital yang dapat direpresentasikan di pengadilan dengan format yang dapat dipahami dan memiliki arti (ECCouncil, 2008).

Menurut Prayudi (2014) dalam publikasi yang berjudull Problema dan Solusi Digital Chain of Custody Dalam Proses Investigasi Cybercrime*,* salah satu

faktor penting dalam proses investigasi adalah hal terkait dengan barang bukti. Dalam hal ini terdapat dua istilah yang hampir sama, yaitu barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah bersifat fisik dan dapat dikenali secara visual (komputer, *Handphone, Camera, CD, Hardisk,* dan lain-lain). Sementara barang bukti digital adalah barang bukti yang diekstrak atau di-*recover* dari barang elektronik (*file, email, sms, imafe, video, log, text).*

Berbeda dengan barang bukti lainnya, barang bukti digital sangat terpengaruh pada proses interpretasi terhadap kontennya. Oleh karena itu, integritas dari barang bukti serta kemampuan *expert* dalam menginterpretasikannya akan berpengaruh terhadap pemilihan dokumen-dokumen digital yang tersedia untuk dijadikan sebagai barang bukti (Schatz, 2007).

2.2 Akuisisi

Menurut dokumen SNI 27037:2014, akuisisi merupakan proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktifitas yang dilakukan. Petugas yang melakukan akuisisi harus memilih metode yang paling sesuai berdasarkan situasi, biaya dan waktu, dan mendokumentasikan keputusan yang dipilih untuk menggunakan metode tertentu dan tool yang sesuai. Metode yang dipilih juga harus dapat dipraktekkan, dapat diulang kembali prosesnya dengan hasil yang sama, dan dapat diverifikasi bahwa hasil salinan sama persis dengan barang bukti yang asli. Dalam keadaan dimana proses verifikasi tidak dapat dilakukan, sebagai contoh ketika proses akuisisi yang sedang berjalan, tiba-tiba salinan asli yang sedang dibuat mengalami *error sectors*, maka dalam kasus seperti ini petugas investigasi yang melakukan akuisisi harus memilih metode yang paling memungkinkan untuk melakukan proses akuisisi ulang dan mendokumentasikannya, lalu dapat menjelaskan kenapa dilakukan akuisisi ulang dan dapat mempertahankan argumennya. (Badan Standarisasi Nasional, 2014)

2.3 Static Forensic

Penelitian (Rafique & Khan, 2013) telah menjelaskan bahwa *Digital Forensic* dibagi menjadi dua metode, yaitu *Static Forensics* dan *Live Forensics. Static Forensics* menggunakan prosedur dan pendekatan konvensional di mana barang bukti elektronik di olah secara *bit-by-bit image* untuk melakukan proses forensik. Proses forensiknya sendri berjalan pada sistem yang tidak dalam keadaan menyala atau *running (off).*

Static Forensic difokuskan pada pemeriksaan hasil *imaging* untuk menganalisis isi dari bukti digital, seperti file yang dihapus, *history* web browsing, berkas fragmen, koneksi jaringan, file yang diakses, *history* login *user,* dll guna membuat *timeline* berupa ringkasan tentang kegiatan yang dilakukan pada bukti digital sewaktu digunakan. Dalam analisis *Static*, segala kebutuhan analisis forensik diperoleh dengan menggunakan berbagai jenis perangkat eksternal seperti USB. Kemudian data ini dibawa ke laboratorium forensik untuk investigator melakukan berbagai jenis operasi / langkah-langkah untuk analisa forensik.

2.3.1 Elaborasi *Static Forensic* dan *Live Forensic*

Analisis Forensik Digital dengan metode statik lebih menenkankan pendekatan tradisional untuk pengimplementasiannya. Pendekatan ini paling banyak digunakan, telah ditetapkan prosedur dan memiliki definisi validitas hukum dari bukti-bukti yang dikumpulkan. Dalam analisis *static forensic*, salinan forensik yang telah "sah" *(imaging)* dan semua media barang bukti ditetapkan untuk tidak terkena potensi kontaminasi, selanjutnya, dipersiapkan media atau alat untuk analisis mencari bukti-bukti digital. Alat ini digunakan dalam mencari *file* dan mencari konten mereka. Setalah melakukan analisis, dilanjutkan pembuatan berkas laporan. *File* yang dihapus biasanya dapat dipulihkan sampai batas tertentu *(recovery)*. Informasi lainnya seperti riwayat browsing, email catatan dan program yang diinstal juga ada potensi berhasil *recovery*. Analisis *static forensic* memiliki keterbatasan tertentu, salah satunya adalah bahwa hal itu tidak dapat memberikan gambaran yang lengkap dari peristiwa (B. Hay, M. Bishop, and K. Nance, 2009).

Sebuah alternatif untuk analisis statis, atau lebih tepatnya pendekatan komplementer, adalah *Live Forensic Analisys*. Dalam hal ini, semua bukti digital dikumpulkan saat sistem sedang berjalan *(running)*. *Live Forensic* mampu menutupi beberapa kekurangan analisis static. Namun, di sisi lain ada beberapa isu untuk *live forensic*. Isu yang paling penting adalah bahwa dengan *live forensic* tindakan analis adalah melakukan eksekusi pada sistem yang menyebabkan perubahan pada bukti digital yang dalam dalam kasus ini "baru ditemukan sebagai barang yang tersinyalir" (F. Adelstein, 2006). Perubahan atau kontaminasi pada bukti digital bertentangan dengan prinsip forensika digital (M.M. Pollitt, 2008). Ada beberapa masalah lain dengan *live forensic*, salah

satunya yaitu peneliti mungkin tidak memiliki tingkat hak yang *verified* terkait akses ke sistem diselidiki.

2.4 Solid State Dive (SSD)

SSD, singkatan dari *solid-state drive*, adalah media penyimpanan data yang menggunakan memori mantap atau memori tak gabar (*nonvolatile memory*) sebagai media, dan tidak menggunakan disk magnetis seperti media penyimpanan eksternal konvensional. Berbeda dengan memori gabar (*volatile memory*) (misalnya RAM), data yang tersimpan pada SSD tidak akan hilang meskipun daya listrik tidak ada.

Menurut (Syah, et.al, 2014) SSD tidak memiliki komponen elektromekanis dan dengan demikian jauh lebih cepat daripada HDD tradisional. Sedangkan menurut (Rasyid, 2014) SSD singkatan dari *Solid State Drive* atau *Solid State Disk*, adalah perangkat penyimpan data yang menggunakan serangkaian IC sebagai memori yang digunakan untuk menyimpan data atau informasi. SSD bisa dianggap sebagai versi canggih dari *USB Flash drive* dengan kapasitas yang jauh lebih besar dan berfungsi sebagai pengganti *Hardisk* yang selama ini diguna kan pada perangkat komputer.

Selanjutnya, SSD memiliki fitur yang bernama TRIM, TRIM merupakan sebuah perintah yang langsung ditujukan kepada firmware dari SSD. Sebuah media penyimpanan akan selalu menulis dan membaca data. Saat menghapus sebuah data, hal tersebut sebenarnya juga merupakan sebuah kegiatan menulis data pula. Pada sebuah *hard disk*, kegiatan penghapusan data tidak sepenuhnya terhapus, namun sebuah pranala yang merujuk ke data tersebut di rentetan data yang disebut dengan *Table Of Content.* Saat ada data yang mau ditulis di tempat (*sector*) yang sama, data baru tersebut akan ditimpa langsung di tempat data (*sector*) yang lama. Hal ini disebut dengan *overwriting*. Dalam *hard disk* konvensional, kegiatan *overwrite* ini adalah biasa. Sayangnya, tidak untuk SSD. Kegiatan overwriting akan menimbulkan “sampah data” atau bahasa Inggrisnya adalah *garbage*. *Garbage* ini yang menyebabkan sebuah SSD akan melambat seiring dengan waktu karena data lama masih ada sehingga membuat SSD harus memilah antara data lama dengan yang baru. Hal ini membuat SSD lamban dalam membaca data.

Perintah TRIM sebenarnya adalah perintah SATA (*Serial Advanced Technology Attachment*) yang dibuat oleh *host* sistem operasi yang kemudian diakui oleh SSD controller. Oleh karena itu ketika file dihapus dalam suatu sistem

operasi, perintah TRIM dikirim ke disk controller dengan LBA (*Logical Block Addresses*) untuk pengahapusan file. SSD kemudian me-*reset* blok-blok yang menjadi ruang kosong tambahan (Shampi, 2009). Sederhananya, fungsi tak kasat mata dari TRIM adalah guna menghapus data secara permanen serta menambah usia pemakaian dari SSD tersebut. TRIM sudah tersedia dari *firmware* SSD.

3. Metodologi Penelitian

Tahapan penelitian yang dilakukan adalah menggunakan pendekatan metodologi teknik *static* forensik yang akan digambarkan pada gambar 1 dibawah ini :

Gambar 1: Metodologi Penelitian

Metodologi ini dikaji serta dijabarkan untuk menjelaskan bagaimana tahapan penelitian dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan solusi dari permasalahan yang ada pada penelitian ini.

3.1 Persiapan Sistem

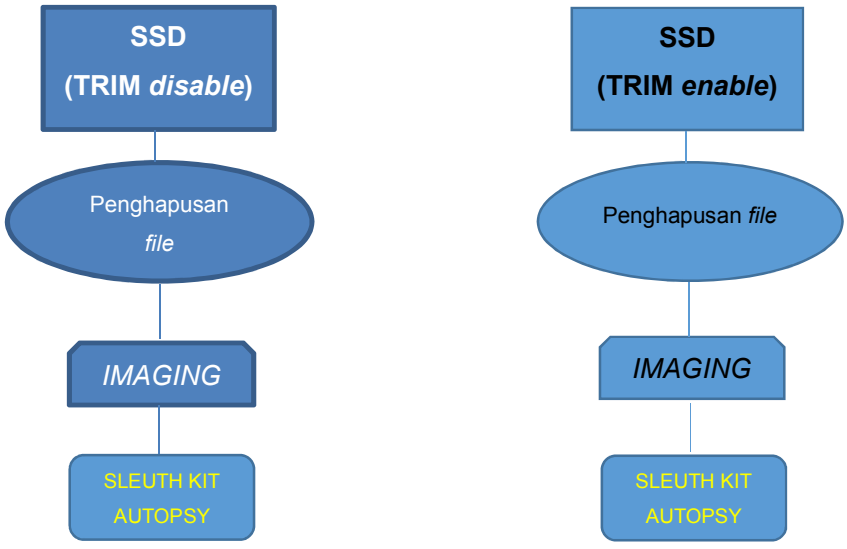
Merupakan tahap dalam melakukan eksperimen dan implementasi Analisis *Solid State Drive (SSD)*. Langkah pertama yang harus dilakukan dalam penelitian ini adalah mempersiapakan perangkat hardware dan software, merancang skenario, serta pengimplementasian Forensika digital. Persiapan *Hardware* dan *Software* yang menjadi kebutuhan penelitian ini antara lain:

1. Laptop Acer Aspire seri 4741 sebagai komputer simulasi dengan spesifikasi:
   a) Processor Intel Core i3 m350 (Arrandale) dengan kecepatan frekuensi 2.26 Ghz
   b) RAM 3GB ddr3 *Dual Channel.*
2. Laptop Dell Vostro seri 5459 sebagai komputer examinasi dan analisis dengan spesifikasi:
   a) Processor Intel Core i5 6200u (Skylake) dengan kecepatan frekuensi 2.3 Ghz dengan *turbo boost* hingga 2.9 Ghz.
   b) RAM 4GB ddr3 *Single Channel.*

3. *Hardisk* Toshiba 320GB 5400rpm.
4. Solid State Drive (SSD) Adata SP900 dengan kapasitas 64GB.
5. Sistem Operasi Windows 7 Professional dengan arsitektur 64-bit.
6. Sistem Operasi Windows 10 Enterprise dengan arsitektur 64-bit.
7. FTK Imager for Windows.
8. Sleuth Kit Autopsy Forensics for Windows.
9. *Docking* SATA Interface 2 slots.

3.2 Skenario Kasus

Melakukan praktek fungsi TRIM pada SSD, yaitu penonaktifan TRIM (TRIM *disable*) dan pengaktifan TRIM (TRIM *enable*). Implementasi yang dilakukan terhadap fungsi TRIM yaitu penghapusan beragam ekstensi *file* secara konvensional dengan perintah SHIFT+Delete. Tahapan berikutnya adalah melakukan Akuisisi terhadap SSD yang diimplementasikan dengan fungsi TRIM-nya guna menganalisis *file-file* apa saja yang dapat *recovery* setelah praktek penghapusan beragam *file* pada SSD. *Tools* yang digunakan dalam praktek akuisisi dan analisis adalah SLEUTH KIT AUTOPSY guna kebutuhan analisis serta FTK Imager guna membuat *image* dari SSD. Tahapan pada skenario kasus yang dijabarkan diatas, akan dijelaskan pada *gambar 3.1* berikut:



Gambar 2: Tahapan Skenario Solid State Drive (SSD) Forensik

Gambar 2 menjelaskan tahapan teknik akuisisi dan analisis yang digunakan yang melalui beberapa tahapan utama yaitu : Pertama, melakukan penonaktifkan fungsi TRIM pada SSD yang dioperasikan melalui *Command Line*

pada sistem operasi Windows. Perintah yang digunakan dapat dilihat pada gambar 3 berikut:

Gambar 3: Perintah Penonaktifan TRIM

Selanjutnya, setelah melakukan penonaktifan fungsi TRIM pada SSD maka akan dilakukan penghapusan terhadap *file* yang di skenario untuk selanjutnya akan dilakukan *Imaging*. SSD yang telah dilakukan *Imaging* menggunakan FTK Imager, selanjutnya akan dilkakukan analisis menggunakan Sleuth Kit Autopsy.

Tahapan Kedua, setelah melakukan akuisisi dan analisis pada SSD dengan TRIM *disable,* pada tahap ini akan dilakukan akuisisi dan analisis SSD pada posisi fitur TRIM *enable* dengan skenario yang sama pada penerapan sebelumnya, yaitu dengan penghapusan *file* yang ada untuk selanjutnya dilakukan *Imaging* kembali guna kebutuhan analisis. Pada gambar 4 berikut, adalah perintah untuk melakukan pengaktifan TRIM (TRIM *enable*).

Gambar 4: Perintah Pengaktifan TRIM

Pada tahapan kedua ini yang merupakan skenario analisis Forensik Digital pada SSD dalam posisi TRIM *disable*, akan kembali dilakukan analisis dengan menggunakan Sleuth Kit Autopsy guna mengetahui apakah *file-file* yang telah dihapus dapat di-*recovery* kembali.

4. Hasil dan Pembahasan

Bagian ini akan menjelaskan *knowledge* beserta hasil dari penelitian terhadap analisis Forensik Digital terhadap Solid State Drive (SSD). Pengimplementasian fitur TRIM *disable* dan TRIM *enable* pada SSD selanjutnya akan dilakukan analisis menggunakan *tools* Forensik Digital yaitu Sleuth Kit Autopsy menggunakan metode *Static* Forensik.

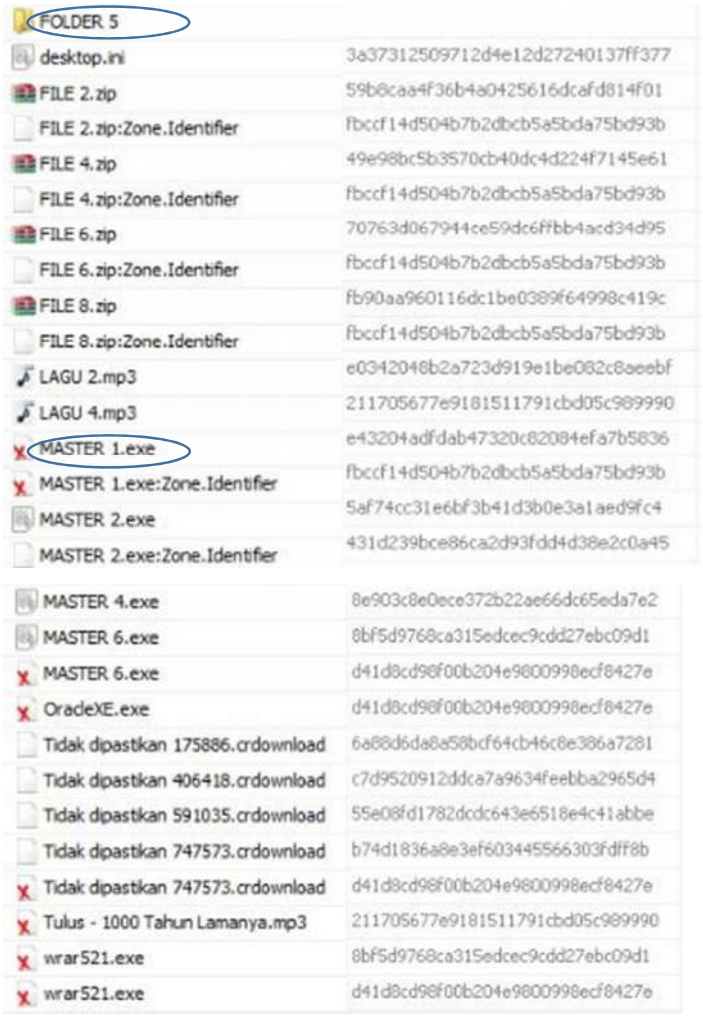
4.1 Hasil Analisis

Setelah berhasil melakukan akuisisi, tahapan selanjutnya adalah melakukan ekstraksi dan menganalisis data pada hasil akuisisi menggunakan Sleuth Kit Autopsy.

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-125042687)	2	2048	125040640	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 125042688-125045423)	3	125042688	2736	Unallocated	Unallocated

Gambar 5: Examinasi Pada SLEUTH KIT AUTOPSY

Pada gambar 5 dapat dilihat bahwa hasil Imaging dari SSD Adata SP900 memiliki ukuran 64023257088 bytes dengan file system NTFS (*New Technology File System*). Berdasarkan pengamatan pada eksperimen ini, waktu yang dibutuhkan guna examinasi Image SSD Adata SP900 64GB pada Sleuth Kit Autopsy Forensic adalah 12 jam lebih 24 menit.



FOLDER 5	
desktop.ini	3a37312509712d4e12d27240137ff377
FILE 2.zip	59b8caa4f36b4a0425616dcafd814f01
FILE 2.zip:Zone.Identifier	fbccf14d504b7b2dbcb5a5bda75bd93b
FILE 4.zip	49e98bc5b3570cb40dc4d224f7145e61
FILE 4.zip:Zone.Identifier	fbccf14d504b7b2dbcb5a5bda75bd93b
FILE 6.zip	70763d067944ce59dc6ffbb4acd34d95
FILE 6.zip:Zone.Identifier	fbccf14d504b7b2dbcb5a5bda75bd93b
FILE 8.zip	fb90aa960116dc1be0389f64998c419c
FILE 8.zip:Zone.Identifier	fbccf14d504b7b2dbcb5a5bda75bd93b
LAGU 2.mp3	e0342048b2a723d919e1be082c8aeebf
LAGU 4.mp3	211705677e9181511791cbd05c989990
MASTER 1.exe	e43204adfdab47320c82084efa7b5836
MASTER 1.exe:Zone.Identifier	fbccf14d504b7b2dbcb5a5bda75bd93b
MASTER 2.exe	5af74cc31e6bf3b41d3b0e3a1aed9fc4
MASTER 2.exe:Zone.Identifier	431d239bce86ca2d93fdd4d38e2c0a45
MASTER 4.exe	8e903c8e0ece372b22ae66dc65eda7e2
MASTER 6.exe	8bf5d9768ca315edcec9cdd27ebc09d1
MASTER 6.exe	d41d8cd98f00b204e9800998ecf8427e
OracleXE.exe	d41d8cd98f00b204e9800998ecf8427e
Tidak dipastkan 175886.crdownload	6a88d6da8a58bcf64cb46c8e386a7281
Tidak dipastkan 406418.crdownload	c7d9520912ddca7a9634feebba2965d4
Tidak dipastkan 591035.crdownload	55e08fd1782dcdc643e6518e4c41abbe
Tidak dipastkan 747573.crdownload	b74d1836a8e3ef603445566303fdff8b
Tidak dipastkan 747573.crdownload	d41d8cd98f00b204e9800998ecf8427e
Tulus - 1000 Tahun Lamanya.mp3	211705677e9181511791cbd05c989990
wrar521.exe	8bf5d9768ca315edcec9cdd27ebc09d1
wrar521.exe	d41d8cd98f00b204e9800998ecf8427e

Gambar 6: Daftar *recovered file*

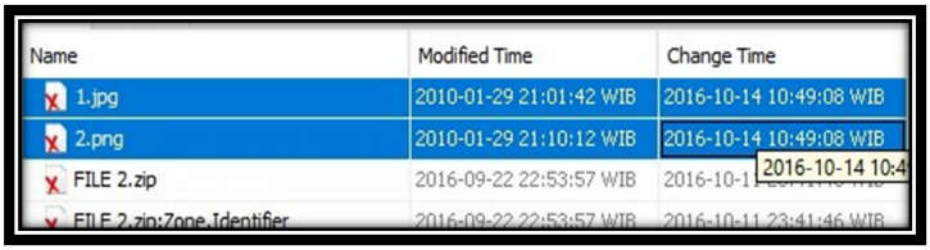
Dari hasil examinasi dan analisis pada SSD dengan fitur TRIM *disable, file-file* yang telah dihapus sebagian besar dapat di-*recovery* kembali. Berikut penjelasan dan rinciannya dapat dilihat pada tabel 1 dibawah:

Tabel 1: Daftar Deleted Files Yang Berhasil Recovery Pada Stattus TRIM Disabled

TRIM STATUS	*Disabled*
TOOLS	*SLEUTH KIT AUTOPSY FORENSIC*
DELETED FILES	***RECOVERED FILES (y/n)***
FOLDER 1 a.**MKV** MD5 : af7bd6f611b55381295c7d5f9716db74	**Yes**
FOLDER 3 Forrest Gump (1994).**MKV** MD5 :b4f259fd9d386b073684a7e294bbfc31	**Yes**
FOLDER 5 The Shawshank Redemption.**MKV** MD5 :d674d7434d48957e148ebd7958ea0171	**Yes**
FILE 1.**zip** MD5 :2d79486b677fbb06908efb5b365d6add	**Yes**
FILE 3.**zip** MD5 :9b4da0d765ffb175769ea281668aa30c	**Yes**
FILE 5.**zip** MD5 :e0922b990e2866369c746e4270ccd981	**Yes**
FILE 7.**zip** MD5 :06868d8728f3fac8f9a549320c957a0b	**Yes**
LAGU 1.**mp3** MD5 :ce1d6f742eed308b72ab857832c5bfb8	**Yes**
LAGU 3.**mp3** MD5 :83dae2eb02ab6e553a55641d140b22f6	**Yes**
MASTER 1.**exe** MD5 :e43204adfdab47320c82084efa7b5836	**Yes**
MASTER 3.**exe** MD5 :32bfaf8e91f26a820ccbb448e8e0347e	**Yes**
MASTER 5.**exe** / OracleXE MD5 :7b7c7a277ef84e100add514d780f9002	**No**

MASTER 7.**exe** MD5 :e61bdfebd1c11ae419ece2b220b585c2	**Yes**

Selanjutnya pada tahapan examinasi dan analisis pada SSD dengan posisi TRIM *enable*. Berdasarkan pengamatan pada eksperimen ini, waktu yang dibutuhkan guna examinasi *Image* SSD Adata SP900 64GB pada Sleuth Kit Autopsy Forensic adalah 13 jam lebih 25 menit.



Gambar 7: Daftar recovered file

Pada gambar 7 dapat disimpulkan bahwa beberapa *file* yang dihapus sebelumnya dengan perintah "SHIFT+DELETE" pada SSD dengan fitur TRIM di posisi *enable* tidak bisa di *recovery* seluruhnya dengan baik oleh Sleuth Kit Autopsy Forensic for Windows. Tercatat hanya ada beberapa file yang dapat *recovery*, yaitu *file* dalam **FOLDER 2** yaitu **Barfi! (2012) Hindi - 720p BluRay - 1GB – Zaeem** selanjutya adalah **FOLDER 4** yang berisi *file* **720p Bluray**. Kemudian *file* yang berhasil di *recovery* lainnya adalah *file* **1.jpg** dan *file* **2.png**. Dapat disimpulkan, *file-file* yang dapat di *recovery* Sleuth Kit Autopsy Forensic pada posisi TRIM *enable* adalah *file* berbasis Multimedia.

Tabel 2: Daftar Deleted Files Yang Berhasil Recovery Pada Stattus TRIM Enabled

TRIM STATUS	*Enabled*
TOOLS	*SLEUTH KIT AUTOPSY FORENSIC*
DELETED FILES	***RECOVERED FILES (y/n)***
FOLDER 2 Barfi! (2012) Hindi - 720p BluRay - 1GB - Zaeem.**MKV** MD5 : 6c951746e3dee75688a17b5205b70460	**Yes**
FOLDER 4 720p Bluray.**MKV**	**Yes**

MD5 : 122be59cf991250c03f0f6b0c0ff6300	
1.**jpg**	
MD5 : 47aba2e271ecc0f655c971abc0c9ab27	**Yes**
2.**png**	
MD5 : 8597eaa4b0a2c8416a6c17b9092bcc88	**Yes**
3.**jpg**	
MD5 : d674d7434d48957e148ebd7958ea0171	**No**
FILE 2.**zip**	
MD5 : 2f4869fb92cc5ad9dd71e7bb9d3f2bd6	**No**
FILE 4.**zip**	
MD5 : 50fa54f9ca6c5205f2c94dbe223b4e96	**No**
FILE 6.**zip**	
MD5 : 30f05286ee08e613e3e137d077cf6b90	**No**
FILE 8.**zip**	
MD5 : 6e4303d8c8fac838bcc9976ae1ee827d	**No**
LAGU 2.**mp3**	
MD5 : e5e7293d5b80bebdced17b4747f6bfa2	**No**
LAGU 4.**mp3**	
MD5 : c7f700cda22a341d6e012fa244821a18	**No**
MASTER 2.**exe**	
MD5 : 1c0195bbe14ed9459ff1540aa1290278	**No**
MASTER 4.**exe**	
MD5 : dc037d1260a716bbd93a0f21fca228a1	**No**
MASTER 6.**exe**	
MD5 : 606f6c9788ca39fe26a72981103b81aa	**No**

Tercatat hanya ada 4 file yang dapat *recovery*, yaitu *file* dalam **FOLDER 2** yaitu **Barfi! (2012) Hindi - 720p BluRay - 1GB – Zaeem** selanjutya adalah **FOLDER 4** yang berisi *file* **720p Bluray**. Kemudian *file* yang berhasil di *recovery* lainnya adalah *file* **1.jpg** dan *file* **2.png**. Dapat disimpulkan, *file-file* yang dapat di *recovery* Sleuth Kit Autopsy pada posisi TRIM *enable* adalah *file* berbasis Multimedia. Berdasarkan pengamatan pada eksperimen ini, waktu yang dibutuhkan guna examinasi *Image* SSD Adata SP900 64GB pada Sleuth Kit Autopsy adalah 13 jam lebih 25 menit.

Berdasarkan informasi yang dikumpulkan dan diurutkan dari literature-literatur dan eksperimen yang diimplementasikan pada penelitian ini, membuktikan bahwa mekanisme TRIM menimbulkan dalam penyelidikan forensik digital. Efektivitas mekanisme TRIM memiliki pengaruh ketika diaktifkan pada operating sistem (Fulton, 2014). Teknologi pada perangkat SSD memiliki

dampak penting pada kemampuan analis forensik dan penyelidik untuk mencari dan memahami data yang tersimpan pada perangkat SSD, ini adalah fakta bahwa SSD menjadi tantangan untuk analisis forensik (Belkasoft, 2014).

5. Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan, Implementasi fitur TRIM yang ada pada SSD terbukti berpengaruh terhadap praktek examinasi dan analisis Forensika digital. Pada SSD dalam posisi fitur TRIM dalam keadaan *disable,* sebagian besar data yang terhapus data di-*recovery* kembali seperti hal nya melakukan *recovery* data pada HDD konvensional. Namun, berbeda dengan SSD dalam posisi fitur TRIM dalam keadaan *enable,* sebagian besar data yang terhapus tidak dapat di-*recovery* kembali. Dapat disimpulkan, bahwa fitur TRIM yang ada pada SSD dapat menjadi hambatan dalam melakukan forensika digital.

Daftar Pustaka

ACPO. (2011). ACPO Good Practice Guide for Digital Evidence, (March), 41.

Agarwal, A., Gupta, M., & Gupta, S. (2011). Systematic Digital forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS), 5*(1), 118-134

B. Hay, M. Bishop, and K. Nance, “Live Analysis: Progress and Challenges,” IEEE Security and Privacy, vol. 7, Mar. 2009, pp. 30- 37. [4]

Bednar, P.M., & Katos, Vasilos. (2011). SSD: New Challenges for Digital Forensic.

F. Adelstein, “Live forensics: diagnosing your system without killing it first,” Commun. ACM, vol. 49, 2006, pp. 63-66.

Freeman, M., Woodward, A. (2009). Secure State Deletion: *Testing the efficacy and integrity of secure deletion tools onSolid State Drives.*

Karayanni, S., and Katos, V. (2011). „Practical password harvesting from volatile memory?. 7th International Conference in Global Security Safety and Sustainability.

M. Pollitt, “Applying traditional forensic taxonomy to digital forensics” in Advances in Digital Forensics IV (pp. 17-26), New York: Springer, 2008.

Rafique, M., Khan, M.N.A (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools