ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM MENGGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS*

SKRIPSI

disusun oleh

Nabilla Fatmah

18.83.0193

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2022

ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM MENGGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS*

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Teknik Komputer

disusun oleh

Nabilla Fatmah

18.83.0193

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

PERSETUJUAN

SKRIPSI

ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM MENGGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS*

yang dipersiapkan dan disusun oleh

Nabilla Fatmah

18.83.0193

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 23 Maret 2022

Dosen Pembimbing,

Rini Indrayani, S.T., M.Eng.

NIK. 190302417

PENGESAHAN

SKRIPSI

ANALISIS FORENSIK DIGITAL PADA SSD FUNGSI TRIM MENGGUNAKAN TOOL *AUTOPSY* DAN *OSFORENSICS*

yang dipersiapkan dan disusun oleh

Nabilla Fatmah

18.83.0193

telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Maret 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, M.Kom. **NIK. 190302456**	
Muhammad Koprawi, S.Kom., M.Eng. **NIK. 190302454**	
Rini Indrayani, S.T., M.Eng. **NIK. 190302417**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Maret 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom.
NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 23 Maret 2022

Nabilla Fatmah

NIM. 18.83.0193

MOTTO

"Hatiku tenang karena mengetahui bahwa apa yang melewatkanku tidak akan pernah menjadi takdirku, dan apa yang ditakdirkan untukku tidak pernah melewatkanku"

(Umar bin Khattab)

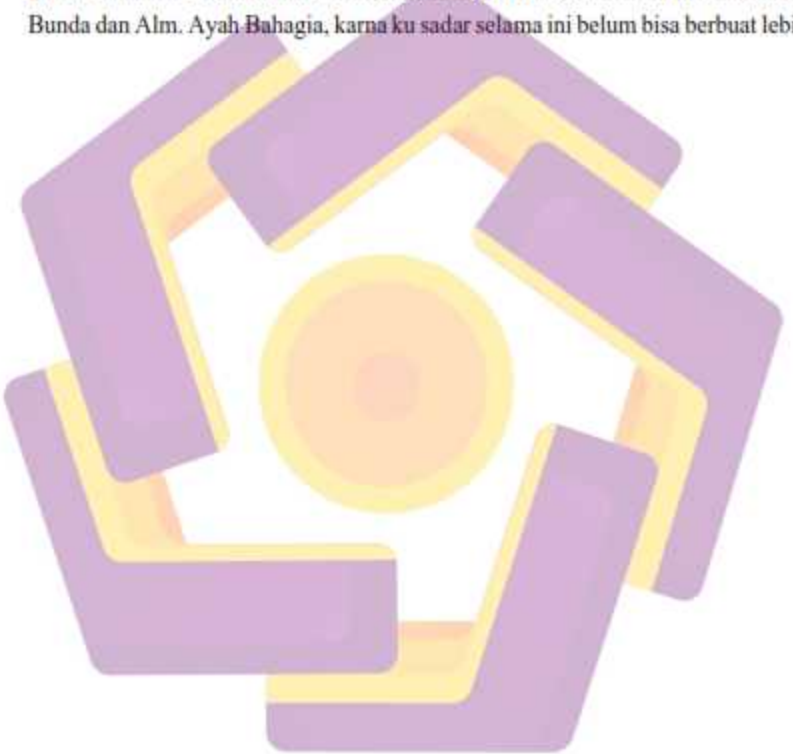
"Perbanyak bersyukur, kurangi mengeluh. Buka mata, jembarkan telinga, perluas hati. Sadari kamu ada pada sekarang, bukan kemarin atau besok, nikmati setiap momen dalam hidup, berpetualanglah"

(Ayu Estiningtyas)

PERSEMBAHAN

Ibunda dan Alm. Ayahanda tercinta,

Sebagai tanda bukti, hormat, dan rasa terimakasih yang tiada terhingga, kupersembahkan karya kecil ini kepada Bunda dan Alm. Ayah yang telah memberikan kasih sayang, dukungan dan cinta kasih yang tiada terhingga dan tidak mungkin dapat ku balas hanya dengan selembar kertas yang bertuliskan kata cinta dalam halaman persembahan. Semoga ini menjadi langkah awal untuk membuat Bunda dan Alm. Ayah Bahagia, karna ku sadar selama ini belum bisa berbuat lebih.



KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat ALLAH SWT atas segala nikmat, hidayah dan karunia-Nya. Penulis pada akhirnya dapat menyelesaikan skripsi ini. Penulis meyakini bahwa skripsi ini tidak akan berhasil diselesaikan tanpa pertolongan dan kebaikan Allah. Skripsi ini adalah tugas akhir untuk memenuhi persyaratan akademis guna memperoleh gelar Sarjana Strata Satu (S-1) Ilmu Komputer pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis merasakan kebaikan dan pertolongan Allah melalui banyak pihak yang dengan berbagai cara telah mendukung dan membantu penulis dalam penulisan skripsi ini. Oleh karena itu, penulis menyampaikan ungkapan terima kasih kepada:

1. **Bapak Prof. Dr. Suyanto, MM.** selaku Rektor Universitas Amikom Yogyakarta yang telah memberikan kesempatan kepada penulis untuk menempuh pendidikan di Universitas Amikom Yogyakarta.
2. **Ibu Rini Indrayani, S.T., M.Eng.** selaku dosen pembimbing yang telah memberikan dukungan, arahan dan bimbingan untuk penulis sehingga penulis dapat segera menyelesaikan skripsi ini.
3. **Bapak Hanif Al Fatta, S.Kom., M.Kom.** selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. **Bapak Dony Ariyus, M. Kom.** selaku Ketua Program Studi Teknik Komputer Universitas Yogyakarta yang telah mendukung penulis beserta para mahasiswa prodi Teknik Komputer lainnya selama belajar di Prodi ini.
5. **Para Dosen** di Fakultas Ilmu Komputer Universitas Amikom Yogyakarta, yang telah mengajari, mendidik dan membekali penulis dengan berbagai ilmu pengetahuan selama belajar di Fakultas ini.
6. **Orang tua, adik, sepupu, seluruh keluarga, pacar serta sahabat** yang senantiasa mendukung penulis melalui doa, nasihat dan perhatian.

Akhirnya, penulis menyadari bahwa skripsi ini belumlah sempurna. Oleh karena itu, penulis dengan rendah hati menerima segala koreksi, kritik dan saran yang membangun dari pembaca sekalian.

Yogyakarta, 23 Maret 2022

Penulis

Nabilla Fatmah

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Kegiatan kejahatan yang melibatkan sebuah perangkat komputer kemungkinan besar akan terekam pada media penyimpanan sistem komputer. Salah satu media penyimpanan utama komputer saat ini selain *harddisk* (HDD) adalah *Solid State Drive* (SSD). Belakangan ini banyak sekali perusahaan yang beralih ke SSD untuk mendapatkan kinerja yang lebih tinggi, ukuran fisik yang baik, dan efesiensi energi. Survei yang dipublikasikan oleh *statista.com* tentang perkembangan *Solid State Drive* diseluruh dunia menunjukkan bahwa penggunaan SSD semakin meningkat setiap tahunnya berbanding terbalik dengan penggunaan HDD yang terus menurun setiap tahunnya. SSD memiliki fungsi TRIM yang merupakan suatu fitur pada SSD yang berhubungan dengan sistem operasi. Fungsi TRIM tersebut memiliki efek negatif pada analisis forensik dan persistensi data setelah dilakukan penghapusan tidak dapat lagi dijamin karena pengontrol penyimpanan SSD memutuskan kapan dan berapa banyak blok yang ditandai untuk dihapus. Metode analisis yang digunakan pada penelitian ini adalah SNI *Acquisition* 27037:2014, yaitu salah satu tahapan dari SNI 27037:2014 yang memiliki beberapa proses yang perlu dilakukan seperti menyelidiki aspek keamanan barang bukti, menentukan model akuisisi, melakukan akuisisi dan meninjau hasil akuisisi.

Fokus dari penelitian ini adalah untuk melakukan percobaan akusisi dan *recovery* dengan *tool Autopsy* dan *tool OSForensics* pada SSD NVme M.2 fungsi TRIM *enable* dan *disable*. Proses investigasi diawali dengan melakukan *imaging* menggunakan *tool AccessData FTK Imager* dengan fungsi TRIM *enable* dan *disable* yang diatur menggunakan *command promt* yang sudah tersedia pada sistem operasi *Windows 10 Pro*, kemudian dilakukan penghapusan permanen (*SHIFT+DELETE*) file target yang akan menjadi objek *recovery*, kemudian dilakukan akuisisi file *image* SSD dan dilanjutkan dengan *recovery* data menggunakan *tool Autopsy* dan *tool OSForensics*.

Hasil dari proses percobaan akuisisi dan *recovery* menunjukkan bahwa *tool OSForensics* memiliki durasi waktu proses akuisisi yang lebih cepat, yaitu 228 menit dengan TRIM *enable* dan 231 menit pada TRIM *disable* sedangkan pada *tool Autopsy* 323 menit pada TRIM *enable* dan 334 menit pada TRIM *disable*. Namun pada proses *recovery*, *tool Autopsy* menunjukkan fitur yang sangat memudahkan penggunanya yaitu bisa melakukan *recovery* file secara kolektif, sedangkan pada *tool OSForensics* versi Trial harus melakukan *recovery* file satu-persatu secara manual. Persentase tingkat keberhasilan *tool Autopsy* dalam melakukan *recovery* pada *Solid State Drive* (SSD) NVMe M.2 dengan fungsi TRIM *enable* sebesar 0% sedangkan dengan fungsi TRIM *disable* 100%. Hasil yang sama juga didapatkan oleh *tool OSForensics* dimana *recovery* yang dilakukan pada *Solid State Drive* (SSD) NVMe M.2 dengan fungsi TRIM *enable* sebesar 0% sedangkan dengan fungsi TRIM *disable* 100%.

Kata Kunci: *Autopsy*, *OSForensics*, SSD Fungsi TRIM, Akuisisi, *Recovery*

ABSTRACT

Crime activities involving a computer device are likely to be recorded on computer system storage media. One of the main storage media for computers today besides the hard disk (HDD) is the Solid State Drive (SSD). Recently, many companies are turning to SSD for higher performance, good physical size, and energy efficiency. A survey published by statista.com on the development of Solid State Drives around the world shows that the use of SSD is increasing every year, inversely proportional to the use of HDD which continues to decline every year. SSD have a TRIM function which is a feature on SSD related to the operating system. The TRIM function has a negative effect on forensic analysis and data persistence after deletion can no longer be guaranteed as the SSD storage controller decides when and how many blocks are marked for deletion. Live forensic is one of the forensic methods that is carried out while the system is running (active). The analytical method used in this study is SNI Acquisition 27037:2014, which is one of the stages of SNI 27037:2014 which has several processes that need to be carried out such as investigating the security aspects of evidence, determining the acquisition model, making acquisitions and reviewing the acquisition results.

The focus of this research is to conduct acquisition and recovery experiments with Autopsy tool and OSForensics tool on NVme M.2 SSDs enable and disable TRIM functions. The investigation process begins with imaging using the AccessData FTK Imager tool with the TRIM enable and disable functions which are set using the command prompt that is already available on the Windows 10 Pro operating system, then permanent deletion (SHIFT+DELETE) of the target file will be the object of recovery, then SSD image file acquisition was carried out and continued with data recovery using the Autopsy tool and the OSForensics tool.

The results of the acquisition and recovery processes show that the OSForensics tool has a faster acquisition process time duration The results of the acquisition and recovery experiment show that the OSForensics tool has a faster acquisition process time duration, which is 228 minutes with TRIM enabled and 231 minutes on TRIM disabled, while the Autopsy tool is 323 minutes on TRIM enabled and 334 minutes on TRIM disabled. However, in the recovery process, the Autopsy tool shows features that make it very easy for users, namely being able to collectively recover files, while the Trial version of the OSForensics tool has to manually recover files one by one. The percentage of the Autopsy tool's success rate in performing recovery on an NVMe M.2 Solid State Drive (SSD) with the TRIM function enabled is 0% while the TRIM function disabled is 100%. The same result is also obtained by the OSForensics tool where the recovery is performed on the NVMe M.2 Solid State Drive (SSD) with the TRIM function enabled at 0% while the TRIM function disabled is 100%.

Keyword: *Autopsy, OSForensics, TRIM Function SSD, Acquisition, Recovery*