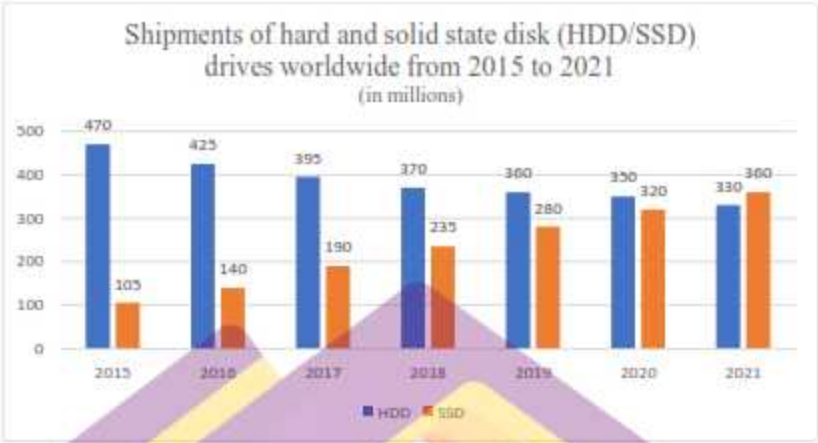
BAB I
PENDAHULUAN

1.1 Latar Belakang

Jejak dan bukti digital yang ditemukan pada kasus kejahatan komputer harus dianalisis menggunakan ilmu dan metode forensik. Analisis forensik terhadap jejak dan bukti digital di bidang teknologi dikenal sebagai forensik digital [1]. Forensik digital pada dasarnya adalah menemukan bukti digital yang dapat disimpan dalam penyimpanan sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan dan lainnya. Kemudian, digital forensik menjadi bagian penting dalam keamanan informasi [2].

Digital forensik Pada dasarnya memiliki dua metode analisis, yaitu *static forensic* dan *live forensic*. *Static forensic* menggunakan pendekatan secara konvensional yaitu, bukti digital diproses menjadi *bit-by-bit image* untuk melakukan proses forensik. Proses forensik sendiri berjalan pada sistem yang tidak berjalan *(shutdown)*. Sedangkan analisis *live forensic* adalah proses forensik yang dilakukan dengan cara untuk mengumpulkan data *volatile* atau yang mudah hilang dan menganalisis bukti tanpa harus mengganggu fungsional sistem selama proses analisis digital [3].

SSD merupakan singkatan dari *Solid State Drive* dan SSD memiliki fungsi yang sama dengan HDD yang digunakan sebagai tempat penyimpanan data. SSD merupakan wadah yang digunakan untuk menyimpan segala informasi pada *chip memory flash* [4]. SSD telah memperkenalkan produk perangkat penyimpanan barunya, SSD *Non-volatile Memory Express* (SSD NVMe). SSD NVMe menggunakan *interface* PCIe (*Peripheral Component Interconnect Express*) untuk transfer data yang lebih efisien [5]. Belakangan ini banyak sekali perusahaan yang beralih ke SSD untuk mendapatkan kinerja yang lebih tinggi, ukuran fisik yang baik, dan efesiensi energi [4]. Berikut survei yang dipublikasikan oleh statista.com tentang perkembangan *Solid State Drive* diseluruh dunia.



Gambar 1. 1 Statistik Penggunaan SSD (Sumber : statista.com)

Gambar 1.1 menunjukan statistik perbandingan penggunaan *harddisk* (HDD) dan SSD. Penggunaan SSD semakin meningkat tiap tahunnya berbanding terbalik dengan penggunaan HDD yang terus menurun setiap tahunnya. SSD saat ini memiliki fitur baru yaitu *Solid State Drive Non-Volatile Memory Express* (SSD NVMe), dan memiliki perbedaan *interface* dengan yang digunakan oleh SATA SSD yaitu *interface* PCIe (*Peripheral Component Interconnect Express*) yang dapat melakukan transfer data lebih cepat jika dibandingkan dengan *interface* yang digunakan oleh SATA SSD.

SSD juga memiliki fungsi TRIM. Fungsi TRIM merupakan suatu ftur pada SSD yang berhubungan dengan sistem operasi[6]. Cara kerjanya adalah TRIM akan menghapus secara internal *block* mana yang dianggap perlu dihapus. [7].

Kamus Besar Bahasa Indonesia mendefinisikan penggelapan sebagai proses, cara dan perbuatan penggelapan (penyelewengan) dimana barang digunakan secara tidak sah [8]. Lebih lanjut dapat dijelaskan bahwa penggelapan adalah Tindakan merusak kepercayaan orang lain dengan meningkari janji tanpa perilaku yang baik.

Pasal 372 KUHP juga menyebutkan pengertian tentang Tindak Pidana Penggelapan yang berbunyi "Barang siapa dengan sengaja memiliki dengan melawan hak suatu benda yang sama sekali atau sebahagiannya termasuk kepunyaan orang lain dan benda itu ada dalam tangannya bukan karena kejahatan,

dihukum karena penggelapan, dengan hukuman penjara selama-lamanya empat tahun atau denda sebanyak Rp. 900." [9].

Penelitian ini akan dilakukan pada skenario kasus *dummy* tentang kasus penggelapan dana dengan menggunakan objek penelitian SSD NVMe M.2 fungsi TRIM di *Windows 10 Pro* menggunakan *tool Autopsy* dan *tool OSForensics* untuk pemulihan file atau *recovery* dengan fungsi TRIM dengan menerapkan metode SNI *Acquisition* 27037:2014 sebagai standar forensik digital yang dilakukan.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang maka dibuatlah perumusan suatu masalah penelitian sebagai berikut :

1. Bagaimana proses akuisisi dan *recovery* dilakukan pada SSD NVMe dengan fungsi TRIM menggunakan *tool Autopsy* dan *tool OSForensics*?
2. Bagaimana perbandingan persentase tingkat keberhasilan *tool Autopsy* dan *tool OSForensics* dalam melakukan *recovery* pada SSD NVMe dengan fungsi TRIM *enable* dan *disable*?

1.3 Batasan Masalah

Berdasarkan identifikasi masalah yang telah diuaraikan di atas, agar pembahasan tidak meluas dari pokok pembahasan, maka diperlukan batasan masalah penelitian sebagai berikut:

1. Sistem operasi yang digunakan pada penelitian ini adalah *Windows 10 Pro*.
2. *Tool* yang digunakan untuk kebutuhan akuisisi dan *file recovery* adalah *tool Autopsy* dan *tool OSForensics*.
3. Penelitian dilakukan pada skenario kasus *dummy* terkait penggelapan dana organisasi yang dibuat dan disimulasikan untuk membandingkan tingkat keberhasilan dan kinerja *tool Autopsy* dan *tool OSForensics* dalam melakukan akuisisi dan *recovery* terhadap SSD NVMe M.2 dengan fungsi TRIM *enable* & *disable*.

4. *Solid State Drive Non-volatile Memory Express* (SSD NVMe) M.2 kapasitas 256GB adalah objek yang digunakan dalam penelitian ini.
5. Penerapan fungsi TRIM dalam SSD NVMe M.2 menggunakan *service* yang sudah ada pada sistem operasi *Windows 10 Pro*.
6. Akuisisi dan *recovery* dilakukan setelah SSD NVMe M.2 di-*imaging* menggunakan *tool AccessData FTK Imager*.
7. Akuisisi dilakukan pada perangkat SSD NVMe M.2 dan hanya dilakukan pada data *non-volatile*.
8. Penelitian ini dilakukan dengan tujuan untuk membandingkan persentase tingkat keberhasilan dan kinerja *tool Autopsy* dan *tool OSForensics* dalam melakukan akuisisi dan *recovery* data pada SSD NVMe M.2 fungsi *enable* dan *disable*.
9. Penelitian hanya dilakukan untuk mendapatkan data persentase keberhasilan *tool Autopsy* dan *tool OSForensics* dalam melakukan *recovery* data pada SSD NVMe M.2 fungsi *enable* dan *disable*, sehingga hasil akhir yang didapatkan terbatas pada apakah data berhasil atau tidak berhasil di-*recovery* tanpa adanya tindakan tambahan, seperti melakukan percobaan lanjutan untuk memperbaiki data hasil *recovery* yang sudah rusak.
10. Persentase tingkat keberhasilan *tool Autopsy* dan *tool OSForensics* dalam melakukan *recovery* data pada SSD NVMe M.2 fungsi *enable* dan *disable* ditentukan dengan melakukan perhitungan dengan metode persamaan indeks tidak tertimbang sedangkan kinerja dilakukan dengan mengevaluasi proses yang sudah dilakukan dengan mempertimbangkan waktu proses percobaan.

1.4 Maksud dan Tujuan Penelitian

Berdasarkan perumusan masalah yang telah dilakukan maka tujuan penelitian yang hendak dicapai adalah sebagai berikut:

1. Melakukan akuisisi dan *recovery* pada SSD NVMe dengan fungsi TRIM menggunakan *tool Autopsy* dan *tool OSForensics*.

2. Membandingkan persentase tingkat keberhasilan *tool Autopsy* dan *tool OSForensics* dalam melakukan *recovery* pada SSD NVMe dengan fungsi TRIM *enable* dan *disable*.

1.5 Manfaat Penelitian

Berdasarkan maksud dan tujuan penelitian yang telah diuraikan diats, maka diharapkan penelitian ini memberikan manfaat sebagai berikut:

1. Memberikan pemahaman tentang bagaimana proses akuisisi dan *recovery* dilakukan pada SSD NVMe M.2 fungsi TRIM menggunakan *tool Autopsy* dan *tool OSForensics*.
2. Mengetahui perbandingan kemampuan dan tingkat efektifitas dari *tool Autopsy* dan *tool OSForensics* yang digunakan untuk melakukan *recovery* pada SSD NVme M.2 dengan fungsi TRIM *enable* dan *disable*.

1.6 Metode Penelitian

Metode yang digunakan untuk mendukung jalannya penelitian ini sebagai berikut:

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan untuk mendukung proses penyusunan skripsi ini sebagai berikut:

1. Metode uji coba/eksperimen, yaitu melakukan akuisisi dan *recovery* terhadap SSD NVMe M.2 fungsi TRIM dengan menggunakan *tool Autopsy* dan *tool OSForensics* untuk memperoleh data faktual mengenai kemampuan dan tingkat efektifitas dari *tools* tersebut.
2. Metode studi pustaka, yaitu melakukan kajian pustaka pada sumber-sumber informasi terpercaya seperti buku, artikel jurnal, dan internet.

1.6.2 Metode Analisis

Metode analisis pada penelitian ini adalah SNI *Acquisition* 27037:2014. Tahapan-tahapan yang ada didalam metode SNI *Acquisition* 27037:2014 adalah sebagai berikut:

1. Persiapan

   Hal pertama yang perlu dipersiapkan adalah ruang untuk menyimpan *data imaging* hasil akuisisi yang juga akan menyimpan data hasil *recovery*. Akuisisi dan *recovery* dilakukan dengan menggunakan *tool Autopsy* dan *tool OSForensics*.

2. Ekstrasi

   Ekstraksi SSD NVMe dilakukan dengan mengindentifikasi dan memulihkan file yang sudah terhapus. Ekstrasi file juga mengungkapkan data yang dihapus termasuk nama file dan nilai *hash*.

3. Analisis

   Tahap ini melakukan analisis dari hasil proses ekstraksi yang dilakukan untuk mengukur tingkat keefektifitasan ekstraksi file yang telah dilakukan.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan meliputi :

1. BAB I PENDAHULUAN

   Bab ini memuat tentang latar belakang masalah, rumusan masalah, batasan penelitian, maksud dnn tujuan penelitian, metode penelitian dan sistematika penulisan.

2. BAB II LATAR BELAKANG

   Menguraikan teori-teori yang digunakan untuk membangun sistem informasi yang dapat mendukung pengolahan data serta laporan yang berhubungan langsung dengan ilmu yang dikaji.

3. BAB III METODOLOGI PENELITIAN

   Bab ini membahas tentang tahap-tahap penelitian yang akan dilakukan, alat dan bahan penelitian yang diperlukan, serta desain antarmuka *tool* yang digunakan.

4. BAB IV HASIL DAN PEMBAHASAN

   Bab ini mendokumentasikan langkah-langkah penelitian yang telah dilakukan beserta hasil akhir penelitian tersebut, yang akan digunakan untuk menentukan hasil analisis dan evaluasi.

5. BAB V PENUTUP

   Bab ini berisi kesimpulan yang ditarik dari hasil penelitian beserta saran yang harus diperhatikan selama penelitian karena keterbatasan dalam memperoleh bahan dan rekomendasi untuk pengembangan penelitian selanjutnya.