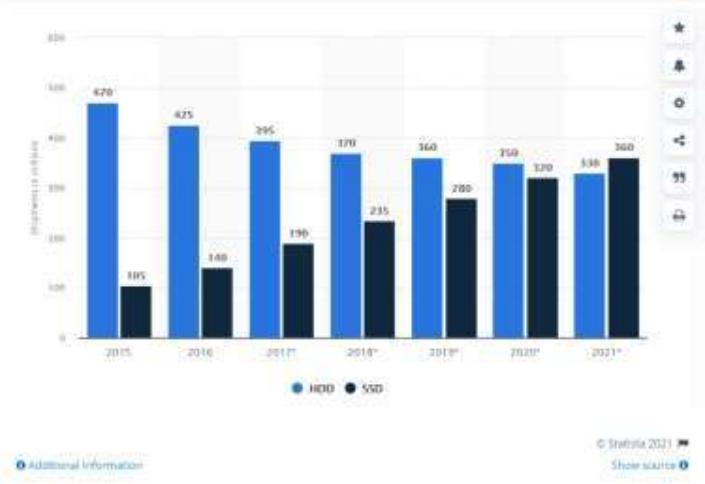
BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi semakin berkembang setiap harinya terutama dalam kurun waktu satu dasawarsa terakhir tak terkecuali pada media penyimpanan. *Hard Disk Drive* (HDD) sebagai media penyimpanan yang sudah lama digunakan di berbagai perangkat elektronik (khususnya komputer dan laptop) perlahan-lahan mulai tergantikan oleh media penyimpanan non-mekanik yang disebut *Solid State Drive* (SSD) [1]. Dilansir dari Statista.com, sejak tahun 2016-2021, pengiriman *Hard Disk Drive* (HDD) ke seluruh dunia mengalami penurunan sedangkan *Solid State Drive* (SSD) berlaku sebaliknya. Berikut data tersebut penulis sajikan dalam bentuk grafik.



Gambar 1. 1 Data Pengiriman HDD & SSD Tahun 2015-2021

Selain itu laptop-laptop keluaran terbaru biasanya sudah dilengkapi dengan *Solid State Drive* (SSD). Hal ini semakin memperkuat kenyataan bahwa tidak akan lama lagi posisi *Hard Disk Drive* (HDD) sebagai media penyimpanan selama beberapa dekade akan tergeser oleh SSD.

Solid State Drive (SSD) merupakan media penyimpanan baru dengan ketahanan lebih kuat dan cenderung tahan terhadap guncangan serta lebih hemat daya karena tidak seperti *Hard Disk Drive* (HDD) yang memiliki komponen

bergerak [2]. Salah satu fungsi yang terdapat pada SSD adalah fungsi TRIM. TRIM adalah istilah yang digunakan untuk mengidentifikasi perintah ATA *(Advanced Technology Attachment)* tertentu yang memungkinkan sistem operasi untuk memberi tahu *controller Solid State Drive* (SSD) bahwa data tersebut tidak dibutuhkan lagi. Arti kata TRIM berasal dari kenyataan bahwa area media penyimpanan dikurangi atau dipangkas (dibuat lebih kecil). Fungsi TRIM menjadi perlu untuk memungkinkan sistem operasi memberi tahu kepada SSD bahwa suatu area sudah tidak dibutuhkan lagi [3].

Perkembangan teknologi yang kian pesat diiringi juga dengan kejahatan komputer yang meningkat. Kejahatan komputer merupakan tindakan ilegal yang melibatkan teknologi dengan modus pencurian, manipulasi data digital, dan lain sebagainya [4]. Dilansir dari Kepolisian Republik Indonesia, dalam rentang waktu April 2020 hingga Juli 2021 instansi tersebut mendapat laporan sebanyak 937 kasus. Dari jumlah tersebut kasus *provocative,* konten kebencian, dan ujaran kebencian mendapat laporan paling banyak dengan jumlah kasus sebanyak 437 kasus. Penipuan secara daring dengan laporan sebanyak 259 kasus dan konten dewasa dengan 82 kasus. Tentunya dengan keadaan seperti ini dibutuhkan payung hukum yang menjadi landasan dalam menangani kasus kejahatan komputer. Dalam hal ini UU ITE Nomor 11 Tahun 2008 pasal 5 yang berbunyi "Informasi Elektronik dan Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah" menjadi dasar hukum yang mengatur tentang Forensika Digital.

Digital Forensics atau Forensika Digital adalah cabang ilmu sains yang menginvestigasi barang bukti digital untuk kemudian mengumpulkan, memulihkan, dan menganalisa barang bukti tersebut. Barang bukti digital pada kejahatan komputer tersebut dapat diambil/dicari pada perangkat komunikasi seperti gawai, laptop, maupun komputer [5]. Teknik/analisis yang digunakan untuk mengungkap kejahatan komputer tersebut salah satunya adalah *Live Forensics.* Melakukan pemulihan data dalam penanganan kasus kejahatan komputer ketika sistem komputer dalam keadaan hidup adalah penerapan metode *Live Forensics* [6].

Penelitian ini menggunakan metode yang sering digunakan yaitu metode *National Institute of Justice* (NIJ). *National Institute of Justice* (NIJ) merupakan

metode yang digunakan untuk menjelaskan bagaimana tahapan penelitian yang dilakukan sehingga alur penelitian bisa selesai secara sistematis dan dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada [7]. Tahapan metode dari *National Institute of Justice* (NIJ) terbagi menjadi lima tahapan yakni *identification, collection, examination, analysis,* dan *reporting* [8].

Terlepas dari segala manfaat maupun keuntungan yang terdapat pada *Solid State Drive* (SSD) tentu saja SSD ini memiliki keterbatasan. Salah satunya seperti yang sudah penulis singgung pada paragraf sebelumnya yaitu mengenai fungsi TRIM yang akan melakukan penghapusan data secara periodik atau berkala.

Berlandaskan latar belakang yang sudah dijelaskan, penulis terdorong untuk melakukan penelitian dengan judul "**ANALISIS *LIVE FORENSICS* PADA SSD SATA FUNGSI TRIM MENGGUNAKAN METODE *NATIONAL INSTITUTE OF JUSTICE* (NIJ)**"

1.2 Rumusan Masalah

Berlandaskan latar belakang yang sudah dijelaskan, didapat rumusan masalah sebagai berikut:

1. Bagaimana cara menganalisis *live forensics* untuk mengakuisisi SSD SATA yang memiliki fungsi TRIM?
2. Apakah akuisisi *image* partisi dapat dibaca oleh perangkat lunak forensik?
3. Bagaimana proses pemulihan terhadap *file* yang sudah dihapus?

1.3 Tujuan Penelitian

Berangkat dari rumusan masalah yang sudah ditetapkan di atas, tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menerapkan analisis *live forensics* untuk mengakuisisi dan memulihkan *file* pada SSD SATA.
2. Memeriksa *image* partisi dari fungsi TRIM yang terdapat pada SSD SATA yang kemudian dibaca oleh perangkat lunak forensik untuk memulihkan *file* yang dihapus.

1.4 Batasan Masalah

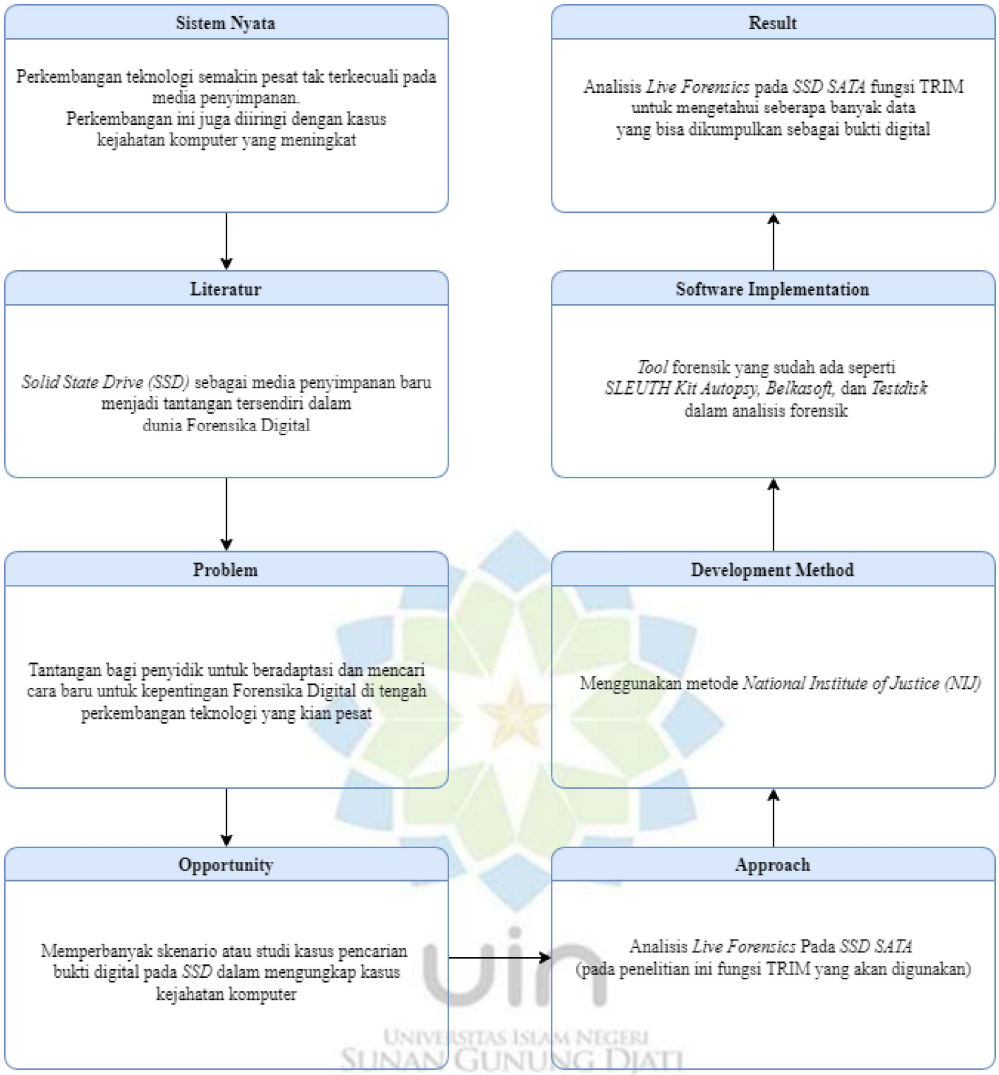
Dalam penelitian ini, batasan masalahnya meliputi beberapa hal yaitu:

1. Sistem operasi yang digunakan adalah Windows 11 Professional di mana sistem operasi tersebut sudah mendukung fungsi TRIM.
2. *Solid State Drive* (SSD) SATA yang digunakan dalam penelitian ini berkapasitas 128GB.
3. Menerapkan fungsi TRIM terhadap SSD sesuai skenario yang telah dibuat.
4. Untuk keperluan analisis menggunakan perangkat lunak forensik berlisensi *open source* yaitu Autopsy dan Testdisk serta perangkat lunak forensik berlisensi *trial* yaitu Belkasoft Evidence Center X.
5. Tahapan akuisisi langsung untuk pemulihan *file* dilakukan menggunakan SSD SATA eksternal.
6. Data *non-volatile* adalah bentuk data yang akan diakuisisi.

1.5 Manfaat Penelitian

Harapannya penelitian ini menghasilkan manfaat sebagai berikut:

1. Mengetahui pengaruh fungsi TRIM pada SSD dalam hal penghapusan *file*.
2. Mengetahui kemampuan perangkat lunak forensik dalam proses forensika digital untuk memulihkan *file* dari SSD.
3. Dapat menjadi referensi penelitian selanjutnya di bidang *Digital Forensics*.



Gambar 1. 2 Kerangka Pemikiran

1.6 Kerangka Pemikiran

Kerangka pemikiran di atas berisi mengenai skenario yang akan dilakukan. Didasari kenyataan bahwasanya perkembangan teknologi media penyimpanan berkembang begitu pesat seiring dengan tuntutan untuk melakukan segalanya dengan lebih cepat, namun di sisi lain perkembangan ini membawa dampak negatif salah satunya dalam kasus kejahatan komputer. Media penyimpanan (dalam hal ini SSD) memberikan tantangan tersendiri bagi para penyidik. Tantangan ini menggiring para penyidik untuk mencari cara baru dalam ranah kepentingan

forensika digital. SSD dengan segala kelebihan dan kekurangannya perlu diteliti lebih jauh lagi agar memudahkan para penyidik dalam mengungkap kasus kejahatan komputer utamanya dalam forensika digital. Agar data dan referensi yang dihasilkan bisa cukup baik untuk nantinya digunakan maka dari itu perlu untuk membuat skenario kasus yang kemungkinan terjadi agar nantinya ketika skenario tersebut terjadi di dunia nyata maka penyidik tidak kebingungan dalam mengambil tindakan. Metode *National Institute of Justice* (NIJ) dipilih untuk pembuatan skenario yang kemudian diimplementasikan menggunakan perangkat lunak forensik seperti Autopsy, Belkasoft, dan Testdisk. Perangkat lunak Autopsy dan Testdisk dipilih karena berlisensi *open source* sedangkan Belkasoft berlisensi *trial.* Harapannya data yang nantinya didapat dari skenario ini bisa menjadi panduan bagi penanganan kasus forensika digital di kemudian hari.

1.7 Metodologi Penelitian

1.7.1 Metodologi Penelitian

Penelitian ini menggunakan metodologi sebagai berikut:

a. Tahap Skenario

Pada penelitian ini bukti digital yang digunakan tidak didapatkan pada lingkungan yang sebenarnya atau dengan kata lain barang bukti tidak didapatkan dari hasil tindak kejahatan komputer yang sebenarnya. Bukti digital dibuat dan diperoleh dari hasil desain skenario dengan tujuan untuk mendapatkan bukti digital seperti pada kasus kejahatan komputer yang sebenarnya.

b. Studi Literatur

Pengambilan data dan informasi penunjang dilakukan dengan cara mengumpulkan beberapa bahan acuan terkait penelitian ini yang didapat dari beberapa sumber seperti *paper,* jurnal ilmiah, buku, Internet, maupun referensi lain yang memiliki topik serupa.

1.7.2 Metodologi Pengembangan

Penelitian ini menggunakan metode dari *National Institute of Justice* (NIJ) yang dijelaskan di bawah ini:

Gambar 1. 3 Metode NIJ

a. Identification

Tahap *Identification* adalah tahap pemilahan barang bukti dan data-data yang berkaitan dalam proses penyidikan dengan tujuan mencari barang bukti digital. Barang bukti yang ditemukan lalu diidentifikasi, diberi label atau didokumentasikan agar barang bukti tidak rusak.

b. Collection

Tahap ini berisi kegiatan untuk mengumpulkan data-data demi kepentingan proses penyelidikan dalam pencarian barang bukti. Dalam tahap ini dilakukan pengambilan data dari sumber yang berkaitan serta menjaga keaslian barang bukti dari kontaminasi.

c. Examination

Pada tahap ini data dikumpulkan lalu diperiksa secara forensik untuk memastikan data tersebut terjaga keasliannya sesuai dengan temuan yang didapat di TKP. Agar hal tersebut bisa dilaksanakan dengan baik maka data diidentifikasi dan divalidasi menggunakan teknik *hashing.*

d. Analysis

Teknik Analisis dilakukan setelah data atau *file* digital didapatkan dari proses eksaminasi. Analisis data dilakukan secara detail dan menyeluruh menggunakan panduan yang sudah ditentukan baik dalam hal teknis maupun hukum agar data tersebut dapat dibuktikan. Kemudian hasil analisis tersebut dapat digunakan sebagai barang bukti digital dan temuan tersebut dapat dibuktikan baik secara hukum maupun ilmiah.

e. Reporting

Setelah barang bukti digital diperoleh dari proses pemeriksaan lalu kemudian dianalisis, maka dibuatlah laporannya. Isi dari laporan tersebut antara lain tindakan

yang dilakukan, penggunaan serta penjelasan metode dan perangkat lunak yang digunakan, tindakan penunjang lain yang diambil, serta merekomendasikan aspek-aspek lainnya dalam proses tindakan *digital forensics*.

1.8 Sistematika Penulisan

Bagian ini berisi informasi maupun data yang didapatkan berdasarkan metode yang sudah dijelaskan pada metodologi penelitian. Sistematika penulisan terdiri dari lima bab dengan penjelasan berikut:

BAB I PENDAHULUAN

Bagian ini membahas tentang latar belakang masalah, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metodologi penelitian, kerangka pemikiran, dan sistematika penulisan.

BAB II KAJIAN LITERATUR

Bagian ini membahas konsep dan teori-teori terkait dengan penelitian yang akan dilakukan untuk mendukung pencarian solusi. Selain itu pada bagian ini berisi penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini membahas perancangan skenario dan analisis yang akan dibuat menyesuaikan dengan metode penelitian yang diambil.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bagian ini membahas data hasil pengujian dari skenario yang sudah dilakukan.

BAB V PENUTUP

Bagian ini berisi kesimpulan dan saran dari penelitian.

DAFTAR PUSTAKA

Bagian ini berisi sumber-sumber yang terdapat pada laporan penulisan yang digunakan dalam penelitian.