BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Forensik digital dapat didefinisikan sebagai suatu pendekatan untuk mengungkap fakta kejahatan menggunakan metode ilmiah untuk menegakkan hukum yang berlaku [1]. Forensik digital memudahkan *investigator* untuk mengumpulkan dan menganalisis data dengan tujuan menentukan dan melaporkan tindakan apa pun yang dilakukan pada perangkat digital yang mungkin relevan dengan kejahatan atau aktivitas ilegal [2]. Dalam penerapan forensik digital, salah satu turunan praktiknya adalah penanganan barang bukti digital [3]. Bukti ini dapat berbentuk file dokumen, histori, atau log aktivitas yang berisi data atau informasi. Bukti digital berada di dalam bukti elektronik yang sebelumnya telah diidentifikasi. Barang bukti elektronik memiliki bentuk fisik dan umumnya berupa perangkat elektronik atau penyimpanan (*storage device*) [4].

Dalam kebanyakan kasus *cybercrime* yang berhubungan dengan pemulihan data, bukti sering kali ditemukan pada SSD dan HDD [5][6]. SSD memiliki latensi yang lebih rendah daripada HDD. Selain itu, lebih banyaknya kemungkinan kegagalan komponen mekanis pada HDD menjadikan SSD sebagai perangkat penyimpanan yang lebih dapat diandalkan saat ini [7]. HDD dan SSD tersedia dalam dua bentuk, bentuk internal terletak di dalam perangkat komputasi, sedangkan bentuk eksternal dapat dihubungkan melalui kabel USB atau eSATA. SSD eksternal secara signifikan lebih kecil dan lebih portabel dibandingkan HDD eksternal [8][9].

Investigasi forensik tidak terlalu efektif karena semakin banyaknya penggunaan teknik anti-forensik dalam penerapan *cybercrime* [10]. Pelaku *cybercrime* biasanya akan melakukan berbagai cara untuk menghilangkan barang bukti yang berhubungan dengan tindak kejahatan yang mereka lakukan [4]. Seperti menghapus, menyembunyikan, dan memformat semua data yang dikumpulkan untuk menghilangkan jejak bukti digital [11]. Dengan demikian, para *investigator*

forensik hanya memiliki sedikit atau tidak ada bukti sama sekali untuk melakukan investigasi digital [10].

Dalam proses investigasi, integritas data adalah aspek krusial untuk menjamin bahwa data yang diperoleh akurat, dapat direplikasi, dan dapat digunakan sebagai alat bukti di pengadilan [12]. Jika data dalam suatu bukti elektronik telah dihapus atau disembunyikan, masalah ini dapat diselesaikan dengan salah satu teknik forensik digital, yaitu *file carving* [11]. Pendekatan *file carving* digunakan untuk merekonstruksi file dalam kasus di mana metadata file telah rusak atau hilang. Berbeda dengan teknik pemulihan konvensional yang hanya melibatkan proses pembacaan sistem file, *file carving* sebagian besar digunakan untuk memulihkan file yang terdapat pada ruang yang tidak teralokasi (*unallocated space files)* [13].

Penelitian ini bertujuan untuk menganalisis pengaruh teknik anti-forensik *disk wiping*, yang mencakup penghapusan, fragmentasi, *formatting*, dan *data overwriting*, terhadap hasil pemulihan data pada SSD dan HDD eksternal. Analisis dilaktukan dengan mengacu pada framework NIST SP 800-86, yang mencakup empat tahap utama: *collection*, *examination*, *analysis*, dan *reporting*. Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi perbedaan hasil antara metode pemulihan konvensional dan metode *file carving*. Dengan demikian, penelitian ini diharapkan dapat memberikan pemahaman lebih mendalam terkait tantangan dan peluang dalam pemulihan data pada SSD dan HDD eksternal.

1.2 Rumusan Masalah

1. Bagaimana penerapan teknik anti-forensik *disk wiping* yang mencakup penghapusan, *formatting*, *overwriting*, dan fragmentasi data pada SSD dan HDD eksternal?
2. Bagaimana penerapan framework NIST SP 800-86 untuk melakukan forensik digital pada SSD dan HDD eksternal setelah penerapan teknik anti-forensik *disk wiping*?

1.3 Batasan Masalah

1. Penelitian ini hanya menganalisis pemulihan data dari perangkat penyimpanan eksternal, yaitu SSD eksternal dan HDD eksternal.
2. Penelitian hanya akan menggunakan file standar seperti dokumen (TXT, DOCX, PDF), gambar (JPEG, PNG), video (MP4), dan ISO dalam skenario penghapusan dan pemulihan data.
3. Penelitian ini hanya menggunakan *tools* yang mencakup FTK Imager untuk imaging, Defraggler untuk menganalisis fragmentation pada disk, *utility* dd untuk *overwrite*, Autopsy untuk pemulihan konvensional dan analisis bukti digital, serta PhotoRec untuk file carving.
4. Penelitian ini menggunakan algoritma *hash* yang terbatas pada MD5 dan SHA-256 untuk verifikasi integritas data pada seluruh skenario.
5. Semua tahapan forensik digital dalam penelitian ini akan mengacu pada standar NIST SP 800-86 sebagai pedoman untuk proses pengamanan dan analisis bukti digital.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk menganalisis framework NIST SP 800-86 dalam proses forensik digital pada SSD dan HDD eksternal setelah penerapan teknik anti-forensik *disk wiping* untuk menganalisis dampaknya terhadap integritas data yang dipulihkan. Selain itu, penelitian ini akan membandingkan hasil pemulihan data menggunakan metode *file carving* dan metode pemulihan konvensional. Dengan menganalisis aspek-aspek tersebut, penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai tantangan dan peluang dalam pemulihan data pada perangkat penyimpanan berbasis SSD dan HDD.

1.5 Manfaat Penelitian

1. Bagi Peneliti Selanjutnya: Memberikan referensi untuk pengembangan penelitian lebih lanjut terkait teknik anti-forensik dan pemulihan data pada perangkat penyimpanan modern.
2. Bagi Pengembangan Ilmu Pengetahuan: Menyediakan referensi ilmiah terkait penerapan framework NIST SP 800-86 dalam investigasi digital

pada perangkat penyimpanan SSD dan HDD eksternal.

3. Bagi Organisasi atau Institusi Keamanan Siber: Mendukung pengembangan kebijakan keamanan data yang lebih efektif untuk mencegah dan menangani tindakan *cybercrime* yang melibatkan penghapusan bukti digital.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN, berisi Latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi studi literatur dan dasar-dasar teori yang digunakan.

BAB III METODE PENELITIAN, berisi objek penelitian, alur penelitian, alat dan bahan.

BAB IV HASIL DAN PEMBAHASAN, bab ini merupakan tahapan yang penulis lakukan dalam penerapan teknik anti-forensik, teknik pemulihan data dan metode yang digunakan pada objek penelitian.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.