BAB I
PENDAHULUAN

1.1 Latar Belakang

Penggunaan perangkat digital meningkat secara signifikan di era digital seperti saat ini. Mayoritas pengguna perangkat digital, sangat familiar dengan perangkat penyimpanan USB yang memiliki beragam variasi seperti *USB Flash Drive*, *Micro Memory Card*, *Hard Drive*, *Solid State Drive* , dsb. Peningkatan penggunaan perangkat penyimpanan USB cenderung massif & eksponensial disebabkan berbagai aspek, salah satunya ukuran dan harga perangkat penyimpanan USB yang terjangkau [1].

Forensik digital memiliki tujuan untuk membantu menemukan dan menganalisis fakta-fakta, serta membantu menganalisis bukti digital yang berkaitan tentang suatu insiden. Timeline sebuah peristiwa disekitar suatu insiden yang sedang diselidiki merupakan salah satu aspek paling krusial dalam penyelidikan forensic [2]. Dengan demikian, penting untuk mengetahui kapan perangkat penyimpanan USB yang dicurigai telah terhubung atau terputus dari sebuah sistem komputer. *Static Forensics* merupakan salah satu jenis metode dari forensik digital yang memperoleh bukti digital dengan melakukan ekstraksi serta analis setelah insiden terjadi, ataupun setelah sistem komputer dimatikan (*post incident*). Berbagai implementasi teknologi pada static forensics antara lain disk imaging, data recovery serta filtering information [3]. Walaupun diklaim sebagai sebuah metode yang tradisional namun, metode ini menawarkan perbandingan yang signifikan pada aspek ekstraksi bukti digital, analisis, penilaian serta kesesuaian terhadap prosedur hukum dibandingkan metode Live Forensics. Hal

ini dikarenakan live forensics melakukan analisis saat sebuah sistem masih berjalan, aspek tersebut dapat menyebabkan integritas sebuah bukti digital berubah. Dan tentu saja hal ini membuat bukti digital tersebut tidak valid lagi [4].

Berbagai topik yang muncul di media terkait *cybercrime*, serta proses pengambilan barang bukti elektronik meliputi perangkat komputasi yang berupa *storage devices* oleh penegak hukum terkait kian menjadi sorotan. Saat ini kualitas penanganan *cybercrime* di Indonesia masih minim, dimulai dengan masalah pengumpulan barang bukti cenderung tidak lengkap, kesalahan saat proses akuisisi barang bukti hingga yang paling parah hilang serta rusaknya barang bukti tersebut. Telah menjadi tugas investigator serta penegak hukum terkait untuk terus memperbaiki kinerja dalam bidang keilmuan ini dan tentu saja menemukan modus, motif serta siapa pelaku kejahatan dalam kasus tersebut [5]. Penelitian ini menghasilkan sebuah report untuk melakukan analisis bukti digital, serta penilaian akurasi bukti digital yang dapat di recovery di berbagai perangkat penyimpanan USB. Penelitian ini akan menguji 3 buah device yaitu USB Flash Drive, USB Hard Disk Drive serta Micro Memory Card menggunakan sebuah high-level digital forensic framework hasil pengembangan dari *National Institute of Standards and Technology* (NIST), yang dijalankan pada sistem operasi Windows dengan dibantu oleh Forensics Toolkit Imager.

1.2 Rumusan Masalah

Dari latar belakang tersebut, maka pokok permasalahan yang akan di teliti adalah cukup banyaknya varian dari USB Mass Storage oleh karena itu diperlukan komparasi akurasi bukti digital yang dapat di recovery pada berbagai

varian perangkat USB Mass Storage seperti USB Flash Drive, USB External Hard Disk Drive serta Micro Memory Card dilengkapi dengan ekstensi USB Card Reader.

1.3 Batasan Masalah

Penulis membatasi masalah yang akan dibahas pada penelitian ini. Lingkup pembahasan pada penelitian ini meliputi analisis metode static forensics di beberapa varian USB Mass Storage, akurasi recovery bukti digital dengan berbagai ekstensi file yang berbeda pada varian USB Mass Storage, serta penggunaan NIST Framework sebagai pengolahan bukti digital yang diharapkan dapat membantu para investigator dalam pemecahan kasus.

1.4 Tujuan Penelitian

Tujuan penulis dalam penelitian ini, antara lain mengetahui tingkat akurasi recovery bukti digital di berbagai varian USB Mass Storage dengan metode Static Forensics serta framework NIST.

1.5 Manfaat Penelitian

Sebelumnya telah dijabarkan tujuan penelitian, semestinya terdapat manfaat pada penelitian ini. Manfaat penelitian yang dilakukan antara lain, sebagai berikut :

1. Menghasilkan sebuah akurasi performa recovery dari masing-masing USB Mass Storage, yang diharapkan bisa menjadi acuan untuk penelitian linear selanjutnya.

2. Memberikan sebuah gambaran secara komprehensif kepada investigator digital forensic maupun pihak berwenang lain yang berkaitan tentang bidang keilmuan tersebut.
3. Sebagai bahan evaluasi penulis sebagai seorang mahasiswa untuk dapat membantu meningkatkan kualitas diri melalui pendekatan ilmiah akademis.

1.6 Metode Penelitian

Pada penelitian ini metode yang digunakan adalah Static Forensics untuk proses akuisisi pengambilan bukti digital dari devices terkait, serta dipadukan dengan Framework dari NIST yang berisikan beberapa tahap seperti Collection, Examination, Analyze dan Reporting. Framework tersebut akan digunakan untuk mengolah bukti digital yang telah ditemukan (recovery) dari devices terkait. Sebelum masuk ke proses pertama (collection), peneliti akan melakukan scenario uji coba yang bertujuan untuk menyiapkan beberapa USB Mass Storage devices yang akan digunakan. Untuk lebih jelasnya akan dijabarkan sebagai berikut :

1.6.1 Tahap Skenario

Pada tahap ini peneliti menyiapkan beberapa USB Mass Storage yang telah diisi beberapa bukti digital berupa berbagai file yang memiliki ekstensi berbeda di dalamnya untuk dilanjutkan proses ekstraksi pada tahap selanjutnya.

1.6.2 Tahap Koleksi

Tahap ini dibantu dengan tools Forensics Toolkit Imager untuk melakukan imaging bukti digital, melakukan labeling pada devices terkait

serta proses ekstraksi sekaligus menggunakan USB Write Blocker untuk menjaga integritas bukti digital tetap valid dan tidak berubah ketika proses imaging berlangsung.

1.6.3 Tahap Eksaminasi

Setelah melewati tahap collection, berikutnya hasil imaging akan diperiksa secara menyeluruh dengan melakukan pengecekan hash pada masing masing bukti digital tersebut.

1.6.4 Tahap Analisis

Tahap ini merupakan tahap validasi bukti digital dari proses sebelumnya. Setelah bukti digital ditemukan, perlu adanya pengecekan pada nilai hash, ekstensi file, serta kapan file tersebut terakhir dimodifikasi (timestamp). Tahap ini sangat krusial karena akan mempengaruhi *chain of custody* pada bukti digital saat ada di pengadilan.

1.6.5 Tahap Pelaporan

Tahap terakhir menjabarkan tentang proses pembuatan report dari hasil analisis yang telah dilakukan beberapa tahap sebelumnya. Penjelasan tools serta teknik metode yang digunakan pada saat melakukan penelitian (investigasi). Dalam konteks penelitian ini, report akan berupa diperoleh tabel persentase akurasi dan laporan tertulis.

1.7 Sistematika Penulisan

Pada bagian ini dituliskan urut-urutan dan sistematika penulisan yang dilakukan. Berikan ringkasan mengenai isi masing-masing bab.

BAB I **PENDAHULUAN**

Membahas tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan, manfaat serta pembuka dari metode penelitian.

BAB II TINJAUAN PUSTAKA

Membahas mengenai bagian teoritis yang berkaitan dengan penelitian yang dilakukan.

BAB III METODE PENELITIAN

Bagian ini menampilkan metode penelitian secara komprehensif, alat serta bahan yang digunakan dalam penelitian serta alur penelitian yang dilakukan oleh peneliti tersebut.

BAB IV HASIL DAN PEMBAHASAN

Ditampilkan analisis dari hasil penelitian serta pembahasan yang terkait dalam penelitian tersebut.

BAB V PENUTUP

Berisi karya tulis berupa kesimpulan dan saran dari penelitian yang telah dilakukan.