BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah memberikan dampak positif yang signifikan untuk memudahkan aktivitas yang dilakukan baik dari individu maupun suatu kelompok. Terlepas dari manfaatnya, perkembangan teknologi juga membawa dampak negatif terutama dalam bentuk kejahatan *cybercrime*. Kejahatan *cybercrime* mengacu pada kegiatan kriminal yang dilakukan melalui atau terkait dengan penggunaan teknologi komputer dan internet.

Cybercrime biasanya meninggalkan jejak (histori) dari aktivitas kriminal, yang dapat digunakan sebagai barang bukti (Rosalina, Suhendarsah & Natsir, 2016). Dalam kasus *cybercrime*, barang bukti terbagi menjadi dua kategori yaitu barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah barang bukti fisik yang berasal dari perangkat elektronik atau perangkat penyimpanan. Barang bukti digital adalah barang bukti yang berupa *file* dokumen, *file histori*, atau *file log* yang berisi data yang terkait dengan pelanggaran *cybercrime* yang diekstraksi dari file pada barang bukti elektronik (Riadi, Umar & Nasrulloh, 2018).

Selain teknik penanganan bukti digital menggunakan alat yang tersedia berdasarkan konsep digital *chain of custody*, hal penting lainnya adalah adanya lembaga yang mengatur segala aktivitas investigasi kriminal dunia maya (*cybercrime*). Tugas lembaga ini adalah menganalisis ide, proyek, dan dukungan hukum terkait investigasi forensik digital dalam rangka merepresentasikan bukti

digital yang berintegritas sehingga dapat diterima dalam proses ligitasi (Granja & Rafael, 2015) .

Para pelaku *cybercrime* dalam melakukan suatu tindak kejahatan biasanya akan berusaha menghilangkan barang bukti apa pun. Menghapus, *memformat*, dan menghilangkan data dari media penyimpanan adalah langkah-langkah dalam proses menghilangkan barang bukti. Ini memastikan bahwa data atau informasi yang berkaitan dengan tindakan yang dilakukan tidak dapat ditemukan. Teknik ataupun cara yang biasanya digunakan oleh para *user* dalam melakukan penghapusan data ialah dengan menekan tombol *detele* dan mengosongkan folder *recycle bin* atau trash pada sistem (Al Anhar, Satrya, & Yulianto, 2014). Untuk itu proses forensik diperlukan untuk mendapatkan kembali data atau informasi sehingga penyidik dapat menentukan atau menyelesaikan kasus *cybercrime*. Pemindahan *file* data yang akurat dan dapat dipercaya sangat penting untuk memastikan integritas dan keandalan bukti digital dalam digital forensic. Salah satu aspek kritis dalam pemindahan *file* data adalah memastikan bahwa *metadatanya* tidak berubah atau dimanipulasi. *Metadata* ini memberikan informasi penting tentang asal-usul, integritas, dan keaslian *file* yang dapat digunakan sebagai bukti dalam proses analisis forensik. Menggunakan alat forensik yang tepat dan memahami secara mendalam bagaimana alat tersebut berinteraksi dengan *metadatanya* menjadi kunci dalam menjaga keaslian bukti digital. Penelitian ini dilakukan dua gambaran skenario data yang dihapus dan data yang tidak dihapus pada media penyimpanan SD Card dan flashdisk. Kemudian menggunakan dua *tools* yang berbeda dalam proses pengangkatan barang bukti. Hasil dalam penelitian ini nantinya akan

membandingkan barang bukti yang didapat dari dua proses data yang berbeda apakah *metadata file* berubah atau tidak dengan menggunakan parameter *checksum* yaitu MD5 (*Message Digest 5*), SHA-256 (*Secure Hash Algorithm 256*) dan *timestamp*.

Fokus penelitian ini membahas bagaimana memperoleh, mengambil dan menampilkan data atau informasi tentang rekaman aktivitas *cybercrime* pada media penyimpanan memori *SD Card* dan *flashdisk* di mana *metadatanya* tidak boleh berubah dan bertujuan untuk menggunakan ilmu digital forensik untuk membantu proses penyelidikan pelaku tindak kejahatan. Penelitian ini menggunakan metode *National Institute of Justice* (NIJ) dan menggunakan *FTK Imager* sebagai *tool forensic* dan *Autopsy* sebagai tools analisis data. Tools forensic *FTK Imager* dapat digunakan dalam proses mekanisme pengambilan data atau file secara otomatis maupun manual dan dapat digunakan pada media penyimpanan termasuk *SD Card* dan *flashdisk*. Penelitian ini menggunakan metode *National Institute of Justice* (NIJ) karena metode ini menerapkan standar profesional yang ketat untuk praktik forensik digital, standar ini membantu memastikan bahwa penyelidikan forensik digital dilakukan secara konsisten dan objektif, serta mencakup metode yang teruji dan terbukti. Metode NIJ dapat dijadikan pedoman dalam menyelesaikan kasus forensic yang ada di mana metode ini dapat diketahui alur dan langkah-langkah penelitian secara sistematis (Riadi, et al 2018).

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah yang didapatkan adalah sebagai berikut:

a. Bagaimana cara mengetahui data yang sudah di akuisisi apakah *metadatanya* sesuai dengan *file* asli dengan parameter checksum pada portable storage (*sdcard dan flashdisk*)?
b. Bagaimana proses menerapkan metode *National Institute of Justice* (NIJ) dalam pengambilan data pada portable storage (*sdcard dan flashdisk*)?

1.3 Tujuan Penelitian

Tujuan dari penelitian adalah sebagai berikut:

a. Menganalisis cara mengetahui *metadata* dalam suatu *file* yang sudah di akuisisi sama dengan *file* asli dengan parameter *checksum* pada portable storage (*sdcard* dan *flashdisk*).
b. Menerapkan metode *National Institute of Justice* (NIJ) dalam pengambilan data pada *portable storage.*

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

a. Penelitian ini akan fokus pada pengambilan data pada portable storage (*sdcard*).
b. Penelitian akan memfokuskan pada analisis *metadata* dengan parameter *checksum* untuk memastikan bahwa tidak ada perubahan yang terjadi selama pengambilan data.
c. Metode yang digunakan dalam penelitian ini adalah *National Institute of Justice* (NIJ).
d. Penelitian ini menggunakan dua tools forensik yaitu *FTK Imager* dan *Autopsy* dalam proses pengambilan data.

e. Penelitian ini tidak akan membahas proses analisis lebih lanjut pada data yang telah diambil, fokus hanya pada pengambilan data dan validasi *metadata*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan kontribusi pada bidang ilmu forensik khususnya dalam pengambilan data pada portable storage (*sdcard* dan *flashdisk*) dan menjaga keutuhan *metadata file* menggunakan metode *National Institute of Justice* (NIJ) penelitian ini akan memberikan pemahaman yang lebih baik tentang perlunya validasi *metadata file* dalam pengambilan data forensik.

Penelitian ini diharapkan dapat membantu dalam pengembangan metode forensik yang lebih efektif dan akurat dalam memastikan keutuhan *metadata file* pada *portable storage* (*sdcard* dan *flashdisk*), dengan menggunakan *FTK Imager* dan *Autopsy* serta menerapkan metode *National Institute of Justice* (NIJ), penelitian ini diharapkan dapat memberikan landasan untuk pengembangan lebih lanjut dalam proses pengambilan data forensik.

1.6 Sistematika Penulisan

Laporan Tugas Akhir ini dibagi menjadi beberapa sub bab yang saling berhubungan untuk memberikan gambaran yang jelas mengenai pembahasan Tugas Akhir. Sistematika penulisan yang digunakan adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang permasalahan, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang uraian penelitian-penelitian terkait serta dasar teori yang menjadi rujukan dalam penelitian. Sumber referensi yang menjadi acuan adalah buku, jurnal, dan media elektronik. Dasar teori yang menjadi rujukan dalam penelitian ini adalah analisis, perbandingan, *digital forensic*, *portable storage.*

BAB III METODOLOGI PENELITIAN

Bab ini berisi metodologi dan langkah langkah yang digunakan untuk menyelesaikan permasalahan dalam penelitian ini, yang terdiri dari pembuatan skenario, melakukan simulasi, proses forensik, dan perbandingan bukti digital.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil analisa bukti digital dari portable storage berdasarkan skenario yang dilakukan. Pengambilan bukti digital tidak boleh berubah metadatanya dilakukan dalam bentuk tabel.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil analisa pengambilan data dari portable storage, serta membahas kekurangan dalam penelitian ini untuk disempurnakan di masa mendatang.