

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi komunikasi dan informasi merupakan sarana paling krusial yang berdampak cukup besar terhadap pola kehidupan masyarakat, sehingga menjadikan teknologi dapat berkembang dengan pesat. Manfaat positif dari penggunaan teknologi yaitu dapat mempermudah setiap individu atau kelompok dalam melakukan aktivitasnya, sedangkan munculnya dampak negatif dipengaruhi oleh keegoisan manusia dengan tindakan mereka yang melakukan penyalahgunaan teknologi atau kejahatan dalam dunia maya (*cybercrime*) sehingga mengakibatkan orang lain merugi [1]. Kejahatan *cybercrime* berupa aktivitas yang menargetkan teknologi sebagai media perantara dalam melancarkan aksi kejahatan, seperti melakukan peretasan terhadap jaringan, pencurian data, menghapus dan merusak informasi pribadi orang lain. Bukti suatu kejahatan *cybercrime* biasanya berupa *file* digital atau program yang disembunyikan oleh pelaku pada media penyimpanan. Di mana *file* atau program tersebut dapat dibuka, diubah, dihapus, atau diformat dengan bantuan komputer atau laptop.

Maraknya kasus *cybercrime* menjadikan instansi hukum perlu melakukan tindakan yang mampu membawa pelaku ke pengadilan hukum, yaitu dengan melakukan digital forensik untuk memperoleh bukti. Proses digital forensik merupakan tindakan investigasi dan analisis barang bukti atau *file* yang disimpan dan diambil dari perangkat penyimpanan pelaku kejahatan, dengan beberapa tahapan seperti pengumpulan, pemeriksaan, analisis, dan pelaporan bukti *cybercrime*. Sehingga, apabila pelaku *cybercrime* menghapus, memformat, atau menyembunyikan semua data yang berpotensi sebagai bukti yang memberatkan pelaku di mata hukum, maka bukti tersebut dapat ditemukan atau diidentifikasi oleh pihak berwajib [2].

Secara umum kasus *cybercrime* akan meninggalkan jejak rekam dari aktivitas kejahatan yang dilakukan sehingga akan lebih mudah untuk menemukan barang bukti. Barang bukti yang didapatkan pada kasus *cybercrime* terbagi menjadi dua kategori, yaitu barang bukti elektronik dan digital. Barang bukti elektronik adalah rekam jejak suatu kejahatan yang memiliki bentuk nyata fisik berupa perangkat elektronik atau penyimpanan (*storage device*). Sedangkan bukti digital merupakan rekam jejak dari kasus kejahatan dalam bentuk *file* dokumen, *history*, atau *log* yang berisi data atau informasi mengenai *cybercrime* yang didapat melalui proses ekstraksi atau pengambilan data yang berada dalam bukti elektronik yang sebelumnya telah diidentifikasi [3].

Selain itu, barang bukti yang didapatkan dari kasus *cybercrime* berbeda dengan bukti yang didapat dari kasus kejahatan konvensional, dimana untuk memproses bukti elektronik maupun bukti digital perlu adanya penanganan khusus karena adanya resiko mengalami perubahan atau kebocoran data, sehingga bukti elektronik dan digital harus disimpan dan didokumentasikan dengan baik melalui proses forensik digital [4]. Di dalam Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjelaskan bahwa, “*informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.*”. Dapat diartikan jika terjadi kesalahan dalam penanganan barang bukti baik disengaja maupun tidak akan menyebabkan bukti menjadi tidak akurat atau rusak. Risiko tersebut dapat dihindari dengan menggunakan kerangka kerja dan aplikasi forensik digital sesuai standar yang berlaku.

Sehingga, adapun tujuan dilakukannya proses forensik digital terhadap kasus *cybercrime* yang terjadi di masyarakat, yaitu:

1. Sebagai proses dalam melakukan investigasi barang bukti pada kasus *cybercrime*
2. Mengembalikan dan memulihkan data yang sebelumnya telah dihapus maupun diformat oleh pelaku *cybercrime*
3. Mengurangi resiko terjadinya kerusakan atau kebocoran barang bukti

Tidak sedikit kasus kejahatan yang melibatkan jaringan internet sebagai alat untuk menyerang atau mencuri sistem informasi korban. Diantara berbagai macam kejahatan *cyber*, kejahatan *carding* yang akan menjadi fokus utama dalam penelitian ini. *Carding* merupakan tindakan kejahatan siber yang berkaitan dengan dunia perbankan, dimana pelaku melakukan pembobolan dan pencurian nomor maupun identitas kartu kredit milik orang lain secara *illegal*. Salah satu kasus *carding* yang pernah terjadi di Indonesia adalah pembobolan kartu kredit berkedok usaha travel yang berada di Jawa Timur, dimana pelaku mendapatkan nomor dan identitas kartu kredit korban dengan membeli dari jaringan *spammer* atau pencuri data. Tujuan utama pelaku nekat melakukan *carding* adalah untuk membeli *gift card* berbayar dan dijual kembali sehingga pelaku mendapatkan uang. Dari tindakan tersebut mengakibatkan korban dirugikan secara materi.

Sehubungan dengan kejahatan *carding*, perangkat penyimpanan seperti *harddisk* dan *flashdisk*, merupakan satu alat elektronik yang dapat digunakan sebagai bukti untuk membawa kasus *cyber* ke pengadilan, hal ini dikemukakan oleh Kepala Penyidik Unit Cyber Crime Barrerkrim Mabes Polri, AKBP Edi Hartono. *Harddisk* dan *flashdisk* merupakan media penyimpanan eksternal yang berbentuk *portable* dengan USB sebagai penghubung ke perangkat

komputer. Dalam beberapa kasus *carding*, pelaku menggunakan perangkat penyimpanan eksternal untuk menyimpan bukti kejahatannya, hal ini dikarenakan penyimpanan eksternal cenderung memiliki ukuran yang kecil dan mudah untuk dibawa kemanapun [5].

Oleh demikian, alat yang digunakan sebagai media penelitian ini adalah *harddisk* dan *flashdisk*, hal ini karena fleksibilitas dari perangkat tersebut yang mudah dibawa kemana saja serta umum digunakan para pelaku *cybercrime*. Alasan selanjutnya adalah media yang digunakan dalam penelitian ini dapat merepresentasikan media penyimpanan lainnya seperti *SD card*, *SSD*, *HDD* komputer dengan ruang penyimpanan yang lebih besar dan efisien.

Untuk melakukan digital forensik dibutuhkan suatu metode yang mampu membantu proses penemuan barang bukti. Dengan demikian, dalam penelitian ini menggunakan metode *National Institute of Standards and Technology (NIST) Special Publication 800-86* guna membantu proses digital forensik. Penggunaan metode NIST bertujuan membantu dan mempermudah pekerjaan penyidik dalam mengetahui langkah-langkah dan alur penelitian secara sistematis, dan menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat dijadikan pedoman dalam melakukan pendokumentasian dan mempertahankan barang bukti.

Metode *National Institute of Standards and Technology* merupakan metode yang membahas mengenai fase digital forensik yaitu *Collection*, *Examination*, *Analysis* dan *Reporting*. Metode ini masuk ke dalam standar yang direkomendasikan dan dijadikan sebagai pedoman dalam melakukan digital forensik. Hal ini karena NIST memiliki teknis yang lebih rinci dalam melakukan pengumpulan dan pemeriksaan terhadap *file* barang bukti, sistem operasi, dan sumber lainnya [6].

Berdasarkan latar belakang yang telah dipaparkan, pemilihan metode NIST SP 800-86 dikarenakan tahapan-tahapan yang dijabarkan mengenai penanganan forensik lebih terperinci mengenai penyimpanan dan pendokumentasian barang bukti agar tidak terjadi kerusakan atau kebocoran. Tahapan NIST SP 800-86 diantaranya proses pengumpulan, pemeriksaan, analisis, dan pelaporan. Dengan ini, penggunaan metode NIST dapat membantu proses forensik digital dalam investigasi kejahatan *carding* pada barang bukti *harddisk* dan *flashdisk*. Sehingga, peneliti mengambil judul “Penerapan Metode *National Institute of Standards Technology (NIST)* dalam Analisis Forensik Digital pada Pemulihan Barang Bukti yang dihapus”.

1.2 Rumusan Masalah

1.2.1 Permasalahan

Carding merupakan kejahatan yang ada di dunia maya, pelaku melakukan tindakan yang dapat merugikan korban seperti penipuan dan pencurian data kartu kredit korban. Biasanya, pelaku

menyimpan bukti pada media penyimpanan eksternal seperti *harddisk* dan *flashdisk*. Namun tidak bisa dipungkiri bahwa beberapa pelaku akan menghapus barang bukti dari kejahatan yang dilakukan untuk menghilangkan bukti. Dari kasus tersebut perlu adanya tindakan guna melakukan investigasi dan memulihkan barang bukti yang telah dihapus oleh pelaku.

1.2.2 Usulan Solusi

Berdasarkan permasalahan yang ada, maka perlu dilakukan proses digital forensik terhadap *file* digital pada media penyimpanan *harddisk* dan *flashdisk* menggunakan metode *National Institute of Standards Technology (NIST) Special Publication 800-86*.

1.2.3 Pertanyaan Penelitian

Bagaimana penerapan metode NIST SP 800-86 dalam melakukan investigasi barang bukti digital pada media penyimpanan *harddisk* dan *flashdisk*.

1.3 Tujuan

Tujuan yang diharapkan dapat tercapai dalam penelitian ini adalah menerapkan metode NIST SP 800-86 dalam melakukan investigasi barang bukti digital pada media penyimpanan eksternal.

1.4 Manfaat

1.4.1 Manfaat Teoritis

- 1) Dapat memberikan wawasan pengetahuan bagi peneliti dalam melakukan analisis dan menemukan barang bukti digital pada kejahatan di dunia maya
- 2) Mampu membuat perbandingan antara teori yang didapat dalam perkuliahan maupun dari buku atau jurnal dengan cara mengimplementasikan terhadap permasalahan secara nyata.

1.4.2 Manfaat Praktis

- 1) Sebagai pengalaman bagi peneliti dalam menemukan barang bukti digital dari kasus kejahatan pada dunia maya
- 2) Dapat dijadikan sebagai acuan pada ilmu digital forensik dalam menemukan barang bukti
- 3) Bagi pembaca dapat dijadikan sebagai referensi dalam menghadapi permasalahan kejahatan di dunia maya.

1.5 Batasan Masalah

Batasan masalah diharapkan mampu membuat penelitian yang dilakukan lebih fokus, tidak melebar secara luas, dan sebagai pembatas pada pembahasan yang dilakukan.

- 1) Analisis dan pencarian barang bukti didapatkan sesuai dengan skenario kasus kejahatan

- 2) Media penyimpanan yang disimulasikan sebagai barang bukti adalah *harddisk* dan *flashdisk*
- 3) Barang bukti dalam kondisi kosong akibat proses penghapusan seluruh data dengan metode “Shift+Delete” dan “Format”
- 4) Metode yang digunakan dalam penelitian ini adalah NIST SP 800-86
- 5) Aplikasi yang digunakan pada penelitian ini adalah FTK Imager dan Autopsy

1.6 Sistematika Penulisan

Susunan sistematika penulisan memuat beberapa Bab. Adapun susunan sistematika tersebut yaitu:

BAB I Pendahuluan

Pada bab ini berisikan latar belakang yang menjelaskan alasan pemilihan digital forensik sebagai topik penelitian dengan memperhatikan realita dan kesesuaian permasalahan yang sedang terjadi. Rumusan masalah menjelaskan permasalahan dan solusi yang dibutuhkan dalam penelitian ini. Tujuan dan manfaat menyajikan capaian dan kontribusi yang diharapkan. Batasan masalah berisi lingkup, metode, dan alat yang digunakan dalam penelitian ini. Sistematika penulisan berisi poin-poin yang akan dijelaskan dalam penelitian ini.

BAB II Tinjauan Pustaka

Pada bab ini berisi mengenai pijakan atau referensi bagi peneliti, yakni landasan teori dan penelitian terkait. Landasan teori menjelaskan mengenai teori dan konsep yang berhubungan dengan digital forensik. Pada penelitian terkait membahas penelitian sebelumnya yang relevan dengan penelitian terbaru, dan membahas perbedaan penelitian terdahulu dan sekarang.

BAB III Metode Penelitian

Pada bab ini memuat kerangka penelitian yang menjelaskan tahapan metode NIST SP 800-86 yang diaplikasikan pada digital forensik. Dalam skenario kasus dan perlakuan perangkat menjelaskan mengenai rancangan skenario kasus kejahatan *carding* yang dilakukan pelaku.

BAB IV Hasil Penelitian

Bab ini memuat hasil yang didapatkan dari pengujian digital forensik pada *harddisk* dan *flashdisk*. Hasil penelitian memaparkan bagaimana melakukan forensik menggunakan FTK Imager dan Autopsy, serta menganalisis mekanisme suatu data yang dihapus dapat dipulihkan kembali.

BAB V Penutup

Bab ini berisi kesimpulan yang didapatkan dari hasil penelitian yang telah dilakukan sebelumnya, dan saran peneliti mengenai metode atau alat yang lebih baik untuk penelitian selanjutnya