BAB I
PENDAHULUAN

1.1 Latar Belakang

Dewasa ini teknologi digital forensik semakin banyak diaplikasikan, antara lain sebagai cara untuk menemukan barang bukti yang berbentuk digital pada kasus kejahatan kriminal yang menggunakan perangkat elektronik sebagai cara untuk berkomunikasi atau saling bertransaksi dan juga bisa digunakan untuk menyimpan file-file yang bersifat ilegal.

Meluasnya layanan internet yang membuat pengguna dapat melakukan berbagai macam aktifitas walaupun dalam jarak yang saling berjauhan, hal ini menyebabkan munculnya kasus-kasus kejahatan siber di Indonesia, seperti yang sering terjadi yaitu kejahatan *hacking*, penipuan, pencurian dan penjualan data pribadi, pornografi, transaksi barang ilegal hingga penyadapan. Di Indonesia sendiri angka kejahatan dan serangan siber tergolong tinggi, diungkapkan oleh Ketua Lembaga Riset Keamanan Siber yaitu *Communication & Information System Security Research Center* (CISSReC) Pratama Pershada bahwa percobaan serangan yang ditujukan ke Indonesia menyentuh angka 1,3 miliar percobaan[1].

Dalam penelitian digital forensik ini, penelitian dilakukan menggunakan metode NIST (*National Institute of Standards and Technology*) yang bertujuan untuk menganalisis proses investigasi kejahatan siber pada forensik digital hingga memunculkan barang bukti digital. Bukti digital tersebut dapat diperoleh menggunakan berbagai *tools* forensik yang akan digunakan pada penelitian ini. Tahapan analisis menggunakan metode NIST berupa tahap *Collection, Examination, Analysis dan Reporting*.

Salah satu bagian dari *Deep web* adalah *Dark web*, bagian internet yang satu ini tidak dapat ditemukan menggunakan *search engine* seperti Google, Yahoo atau sejenisnya. Dikarenakan hal tersebut maka kejahatan siber seringkali terjadi pada bagian internet ini, situs-situs yang melakukan transaksi ilegal bisa ditemukan jika memiliki alamat url dari situsnya yang berbeda dari url pada *Surface web* dikarenakan situs-situs *Dark web* menggunakan domain *dot onion*. Sifat *Dark web*

yang terancang sebagai bagian internet yang tidak mudah untuk dilacak ini membuat penggunanya menjadikan *Dark web* sebagai tempat mereka berkomunikasi dan *software* yang paling umum digunakan adalah PGP (*Pretty Good Privacy*) sebagai layanan enkripsi.

Dalam investigasi forensik digital ini ada 2 ranah dunia maya yang akan dikaji, yang pertama yaitu *World Wide Web* atau *Surface Web* yang dimana akses yang diperlukan tergolong relatif mudah bagi siapapun dengan menggunakan *browser* seperti Chrome dan menggunakan mesin pencarian Google. Lalu kemudian ranah dunia maya yang lainnya dikenal dengan *Deep Web*, disini konten internet yang tidak terindeks dan sengaja untuk disembunyikan dan memerlukan akses yang lebih sehingga tidak bisa menggunakan *browser* standar seperti Chrome.

Penelitian ini akan difokuskan pada masalah bagaimana digital forensik bisa mendapatkan bukti digital pada kedua ranah dunia maya tersebut dan menampilkan informasi mengenai hasil jika digital forensik dilakukan pada halaman *Deep web* yang sifatnya lebih terenkripsi dan aman dibandingkan *Surface web*.

1.2 Perumusan masalah

Berdasarkan latar belakang yang telah disampaikan, diperoleh rumusan masalah yaitu "Bagaimana menemukan bukti digital kegiatan kejahatan siber di *surface web* dan *deep web* menggunakan Metode NIST"

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mendapatkan bukti digital terkait kegiatan kejahatan siber pada dua halaman *web* yang berbeda yaitu *surface web* dan *deep web* dan mengetahui informasi seperti tingkat kejahatan yang terjadi antara kedua halaman *web* tersebut.

1.4 Batasan Masalah

Mengingat luasnya pembahasan, maka permasalahan perlu dibatasi pada:

1. Bukti digital yang diolah adalah bukti hasil dari proses *capturing* halaman-halaman web.

2. Sampel yang diambil pada *surface web* adalah pada layanan forum dan sosial media.
3. Sampel yang diambil pada *Deep Web* adalah layanan pada domain .onion seperti forum, *darknet market*.

1.5 Manfaat Penelitian

Adapun manfaat penelitian dan pembuatan skripsi ini adalah sebagai berikut :

1. Memberikan gambaran mengenai dua jenis halaman *web* yang di analisis dan diharapkan memberikan pengetahuan dalam melakukan analisis halaman *surface web* dan *deep web* dalam mendukung investigasi kejahatan.
2. Sebagai bentuk referensi kebijakan atau tindakan kepada pihak-pihak yang memiliki wewenang untuk mengatur bagaimana akses dan penggunaan layanan internet di masyarakat sehingga dapat mengatur filterisasi akses layanan internet.
3. Sebagai sarana referensi bagi setiap analis digital forensik yang apabila menghadapi situasi dimana harus melakukan investigasi pada dua halaman web atau layanan internet yang berbeda.