

## BAB I PENDAHULUAN

### 1.1 Latar Belakang

Semakin berkembangnya dunia teknologi informasi saat ini memudahkan pengguna dalam memberikan dan memperoleh informasi. Dunia teknologi informasi tidak terlepas dari kemajuan dunia jaringan komputer, yang memberikan banyak kemudahan dalam mengakses dan mendapatkan informasi. Pengguna dibuat terhipnotis dengan banyak fasilitas yang diberikan, sehingga tidak menyadari bahwa banyak kejahatan yang dapat terjadi dalam dunia jaringan komputer.

*Cyber crime* merupakan aktivitas teknologi yang melakukan kejahatan, seperti menghapus informasi, meretas jaringan, mengambil data pengguna jaringan, dan menyembunyikan informasi, dalam suatu jaringan komputer. Beberapa kejahatan pada suatu data digital, seperti *file wiping*. *File wiping* merupakan tindakan menghapus segala file digital yang tersimpan pada suatu *device*. Hal ini tidak berbahaya apabila terjadi diimplementasikan untuk keperluan pribadi. Namun teknik anti forensic dengan file wiping menjadi teknik yang banyak digunakan oleh kejahatan digital untuk menghapus rekam jejak digital mereka.

Kejahatan-kejahatan yang terjadi dapat mengakibatkan pencurian data, rusaknya alat komunikasi, dan terputusnya konektivitas pada jaringan. Hal tersebut sangat merugikan pengguna jaringan, karena pelaku bisa saja mendapatkan informasi-informasi targetnya secara ilegal. Adapun informasi-informasi penting yang biasanya didapat oleh pelaku, seperti informasi kartu kredit, *username* dan *password*, baik email atau layanan perbankan, dan data-data penting lainnya [1].

Terdapat berbagai teknik *file wiping* yang ada saat ini antara lain memformat data, melakukan *overwrite* atau menimpa penyimpanan dengan file baru secara terus menerus, melakukan penghapusan partisi, dan berbagai teknik lainnya. Dalam proses menghapus / menghapus file sebenarnya file tidak berarti data dihapus secara permanen dari media penyimpanan [2]. Tapi itu hanya memberitahu komputer bahwa ruang yang ditempati oleh data tersedia untuk ditimpa / diisi / ditimpa oleh data lain [3]. Sehingga file dapat dikembalikan dengan mudah ke bentuk aslinya, asalkan tidak ada file lain yang telah ditimpa. Kapasitas media penyimpanan yang terus tumbuh memiliki kapasitas penyimpanan yang lebih besar juga. Ini memungkinkan pengguna untuk menggunakan semua ruang penyimpanan yang tersedia, sehingga proses menimpa cenderung hanya dilakukan dalam proses pemformatan [4].

Berdasarkan dari permasalahan tersebut maka penelitian ini bertujuan untuk menganalisis dan menginvestigasi serangan penghapusan data (anti forensic file wiping) dengan mempertimbangkan berbagai skenario dan perbandingan teknik analisa. Peneliti akan memaparkan bagaimana investigasi serangan tersebut dilakukan, dengan mengungkap file yang sudah terhapus.

## 1.2 Rumusan Masalah

Merujuk uraian latar belakang diatas, maka dibuat rumusan permasalahan antara lain yaitu :

- a. Bagaimana mekanisme akuisisi investigasi *disk forensic* untuk mendapatkan bukti digital dan mengungkap aktivitas *anti forensic* dengan mekanisme *file wiping*?
- b. Bagaimana hasil investigasi dari metode analisis *disk forensic* dalam mengungkap skenario serangan *anti forensic*?

## 1.3 Batasan Masalah

Agar penelitian lebih terarah dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya, maka peneliti membuat batasan masalah. Adapun batasan masalah yang ditetapkan adalah sebagai berikut :

- a. Barang bukti digital yang dijadikan topik analisa *disk forensic* terbatas pada *usb flashdisk*.
- b. *File system* yang digunakan pada skenario ini menggunakan NTFS.
- c. Penelitian menggunakan skenario *file wiping* untuk aktivitas *anti forensic* yang digunakan sebagai acuan investigasi dan terbatas pada pembuktian barang bukti yang sudah terhapus.
- d. Analisis pada penelitian ini Terbatas pada skenario sederhana dengan tujuan mengenalkan tahapan *disk forensic* yang bisa diterapkan pada aktivitas serangan *anti forensic*.
- e. Sistem operasi yang digunakan penelitian kali ini menggunakan Windows 7.

## 1.4 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya maka tujuan yang ingin dicapai dari penelitian adalah :

- a. Mengimplementasikan teknik *disk forensic* untuk melakukan investigasi skenario serangan anti forensic berupa penghapusan file dengan cara teknik *file wiping*.

Penelitian ini memperlihatkan secara rinci proses investigasi mulai dari akuisisi barang bukti.

- b. Mencari dan menemukan artefak yang bisa dijadikan bukti pada proses *recovery data*.
- c. Menguji berbagai tool *recovery* dan *file carving* dalam upaya memperoleh kembali bukti data digital yang sudah terhapus.

### 1.5 Manfaat Penelitian

Manfaat yang diharapkan pada penelitian ini berdasarkan latar belakang, rumusan masalah, batasan masalah dan tujuan adalah sebagai berikut :

- a. Memberikan gambaran bagaimana melakukan investigasi secara *disk forensic* pada studi kasus anti *forensic file wiping*.
- b. Menjadi referensi implementasi teknik *disk forensic* untuk investigasi skenario penghilangan jejak dengan teknik *file wiping*.
- c. Memberikan gambaran karakteristik bukti digital pada artefak hasil penerapan teknik-teknik analisa anti *forensic* untuk kegiatan *disk forensic*.
- d. Menjadi referensi akademisi dan melengkapi penelitian sebelumnya terkait proses *disk forensic* dan *anti forensic* investigation dengan tujuan mengembangkan penelitian forensika digital di Indonesia

### 1.6 Sistematika Penulisan

Tujuan sistematika penulisan berisikan garis besar atau gambaran secara umum laporan penelitian ini sehingga mempermudah pemahaman alur isi. Adapun garis besar isi laporan skripsi sebagai berikut :

**Bab I Pendahuluan**, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang masalah penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

**Bab II Landasan Teori**, bab ini menjelaskan tinjauan pustaka dari penelitian terkait dan membahas beberapa teori terkait forensika digital, standar operasional prosedur, bukti digital, dan tool yang digunakan dalam proses investigasi.

**Bab III Metodologi Penelitian**, bab ini berisikan gambaran umum tentang alur proses penelitian, prosedur dan mekanisme metode analisis yang diterapkan pada skenario kasus penelitian dan skenario kasus yang diterapkan pada penelitian.

**Bab IV Pembahasan**, pada tahapan ini membahas implementasi skenario kasus, implementasi investigasi dan hasil analisis berbagai artefak yang dapat ditemukan menggunakan beberapa metode analisis. Bab ini juga menyampaikan rangkuman pembahasan secara teknis dari hasil analisis.

**Bab V Penutup**, bab ini menjelaskan tahapan terakhir yang dilakukan peneliti dan memuat kesimpulan dari keseluruhan uraian dari bab-bab sebelumnya. Tahapan ini juga memaparkan kekurangan serta saran untuk pengembangan penelitian berikutnya.

**Daftar Pustaka**, berisi referensi terkait dengan penelitian ini, baik melalui ebook, publikasi jurnal, dan artikel situs yang dapat menunjang proses penelitian.

