BAB 1

Pendahuluan

1.1 Latar Belakang Masalah

Berbagai macam jenis teknologi dalam bentuk digital menjadi populer dan diminati oleh masyarakat dunia, internet salah satunya. Dengan internet berbagai macam aplikasi yang dapat dimanfaatkan oleh pengguna komputer. Seiring meluasnya penggunaan komputer maka dimungkinkan peluang kejahatan yang melibatkan komputer juga semakin meningkat baik secara langsung maupun tidak langsung. Untuk menanggulangi peristiwa tersebut selain dibutuhkan manajemen keamanan yang bertujuan untuk mencegah, diperlukan pula prosedur penanggulangan apabila peristiwa sudah terlanjur terjadi, dimana salah satu prosedur yang dilakukan adalah komputer forensics. Komputer forensics adalah investigasi serta teknik analisis komputer yang melibatkan tahapan identifikasi, penyimpanan, analisa, dokumentasi dan presentasi dari data yang ada dikomputer yang nantinya dapat berguna sebagai bukti dari peristiwa *cyber crime*.

Menurut Danuri (2018) yang berjudul “*Trend Cyber Crime dan Teknologi Informasi Di Indonesia*” Kasus *cyber crime* yang terjadi sekarang ini sudah mengarah ke pencurian *user_id*, email dan password yang merupakan informasi pribadi bersifat sensitive bagi sebagian orang. Seperti pada account email, facebook, paypal, dan lain sebagainya.

Akibat dari pencurian *user_id*, email dan password ini, bisa saja terjadi pencemaran nama baik jika yang dicuri merupakan account social media. Sedangkan jika yang dicuri merupakan account paypal maka dimungkinkan terjadi tindak pidana pencurian uang melalui transfer paypal dengan cara pembebanan biaya kepada si pemilik sah account *user_id* dan password. Jika account tersebut digunakan untuk transaksi illegal dengan mengatasnamakan si pemilik sah account paypal tetapi alamat pengiriman ditujukan ke alamat si pencuri.

Informasi berupa *user_id*, email dan password selain tersimpan pada cookies browser yang digunakan untuk melakukan hak akses pada perangkat

laptop atau komputer, juga tersimpan didalam memory perangkat tersebut. Untuk itu diperlukan teknik atau metode yang tepat untuk menganalisis memory pada perangkat laptop. Hal ini dikarenakan data yang ada di memory perangkat bersifat volatile, data akan hilang jika komputer dimatikan atau mengalami restart. Akuisisi informasi digital yang ada di memory perangkat hanya bisa dilakukan ketika sistem sedang berjalan. Berbeda dengan harddisk drive karena perangkat bersifat non-volatile. Memory digital tidak kehilangan konten karena gangguan daya atau daya hilang. Ini juga disebut sebagai memory permanen karena sistem dapat mengambil kembali informasi yang tersimpan bahkan setelah power dimatikan dan kembali menyala.

Data volatile menggambarkan seluruh kegiatan yang sedang terjadi pada sistem komputer atau laptop yang digunakan. Oleh karena itu metode *live forensics* adalah metode yang tepat untuk menjamin integritas data volatile tanpa menghilangkan data yang berpotensi menjadi barang bukti. Jika dibandingkan dengan metode tradisional forensik atau *dead forensic*, metode live forensic adalah pilihan yang tepat untuk kasus tersebut karena keadaan media penyimpanan bersifat volatile atau sistem sedang berjalan sedangkan metode tradisional forensics atau *dead forensics* sistem dalam keadaan mati. Kekurangan dari metode tradisional forensics adalah tidak bisa mendapat data dan informasi ketika sistem berjalan, misalnya aktifitas memory, network process, swap file, running system process dan informasi dari file sistem.

Untuk memperoleh bagaimana mengenai kinerja metode tersebut, diperlukan penelitian yang bisa menggambarkan proses kinerja dari analisis metode *live forensics* memory untuk pencarian artefak digital yang berada di memory.

1.2 Rumusan Masalah

Dari latar belakang di atas dapat disimpulkan rumusan masalah sebagai berikut:

1. Bagaimana metode *live forensics* dapat digunakan untuk proses akuisisi data pada memory perangkat laptop ?
2. Bagaimana mencari artefak digital pada memory perangkat laptop ?

1.3 Batasan Masalah

Untuk batasan masalah dalam penelitian ini sebagai berikut :

1. Menganalisa memory dengan ukuran 2GB pada perangkat laptop Asus X453S berbasis linux .
2. Melakukan akuisisi data pada memory perangkat laptop menggunakan metode *live forensics*.
3. Tools menggunakan *Linux Memory Extractor* (LiME) dan *volatility*.
4. Fokus analisis bukti digital yang ingin dicari pada memory perangkat laptop yaitu informasi mengenai *user_id*, email dan password pada facebook, account gmail, paypal dan link url.

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini sebagai berikut :

1. Mencari dan menemukan artefak digital yang berguna bagi investigator yang tersimpan pada memory perangkat laptop.
2. Mengetahui tahapan dalam proses akuisisi bukti digital yang terdapat pada memory di perangkat laptop berbasis linux dengan menggunakan metode *live forensics*.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini sebagai berikut :

1. Menambah wawasan dan pengetahuan tentang metode *live forensics*.
2. Peneliti dan pembaca dapat mengerti tentang digital forensics pada memory dengan menggunakan metode *live forensics* pada perangkat laptop.
3. Mempermudah investigator dalam mencari artefak digital di memory pada perangkat laptop.