BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Sampai saat ini, peningkatan kasus *cybercrime* begitu masif dan tidak terkendali. Berbagai teknik dan taktik para pelaku *cybercrime* ketika melancarkan aksinya sangat sulit dihindari. Banyaknya data breach yang terjadi pada individu, organisasi, perusahaan dan negara tentu sangat merugikan. [1]. Untuk itu ilmu digital forensik sangat diperlukan untuk mengumpulkan bukti valid dalam mengungkapkan suatu kasus. Upaya untuk mendapatkan bukti digital terkait kasus kejahatan yang terjadi dikenal sebagai forensik digital [2].

Teknik analisis digital forensik terdapat 2 cara, *static forensic* dan *live forensic*. Pada *static forensic* akuisisi data dilakukan pada media penyimpanan *non-volatile* atau permanen seperti *harddisk, ssd, usb flashdisk dan sd card*. Sedangkan pada live forensic target yang diakuisisi adalah data yang tersimpan pada *volatile memory RAM, hiberfile* dan *pagefile*. Sehingga proses investigasi menggunakan *live forensic* dilakukan saat sistem dalam keadaan hidup, karena keseluruhan service yang berjalan tersimpan pada RAM [3] [4]. Proses analisis menggunakan metode *live forensics* akan begitu efektif untuk temuan bukti *real time system* [2] [5]. Dengan banyaknya peningkatan jumlah kejahatan pada *cybercrime case*, analisis *live forensic* sangat dapat diandalkan untuk menganalisa kasus yang sedang ingin selesaikan.

Beberapa bukti penting digital forensik bisa terlewatkan jika tidak menerapkan metode *live forensic*. Komponen komputer tentu memiliki kegunaan, terutama *RAM (Random Access Memory)*, yang merupakan artefak menarik dari berbagai sumber bukti forensik tempat menyimpan informasi tentang data waktu nyata pada suatu sistem, seperti *running service, listening connection*, log aktivitas pengguna, *event log, dan private key [6]*.

Pada akhir-akhir ini, penerapan memori forensik pada penanganan investigasi kasus kejahatan *cybercrime* juga begitu banyak. Berbagai penelitian membahas berbagai studi kasus, tantangan dan solusi mengenai memori forensik [7] [8] [9] [6]. Dukungan komunitas dan investigator professional melalui tool

open source live forensic sangat membantu penyidik dalam menganalisis *volatile memory* [8].

Hasil sebuah studi sebelumnya yang relevan dengan penelitian ini [10] berjudul *Live Forensics Analysis Method For Random Access Memory On Laptop Devices* memperoleh informasi penting yang ada pada RAM, beberapa artefak penting yang bisa didapat seperti kata sandi user_id pada situs web seperti Facebook, PayPal, internet banking, dan bitcoin. *Tools* yang digunakan untuk melakukan akuisisi data, yakni *Linux Memory Extractor (LiME)* dan FTK Imager. Dalam penelitian lainnya [11] proses analisis sebuah memori secara langsung menggunakan tool Redline dapat memberikan beberapa bukti cukup banyak mengenai *Malware Risk Index (MRI)* suatu service yang sedang berjalan.

Dalam penelitian Digital forensics *random access memory using live technique based on network attacked* yang dilakukan oleh Periyadi, G. A. Mutiara dan R. Wijaya [12] melakukan investigasi dan analisis data akuisisi ram untuk membuktikan serangan pada jaringan yang terjadi pada suatu sistem seperti FTP attack dan session hijacking. Menurut penelitian yang dilakukan oleh Tri Rochmadi, Imam Riadi dan Yudi Prayudi [13] menerapkan metode *live forensic* dalam proses investigasi browser dalam *mode incognito mode (private mode).* Dimana hal ini biasa menjadi tantangan dalam proses investigasi karena termasuk dalam bentuk *anti-forensics.*

Berdasarkan permasalahan dan latar belakang di atas, penelitian ini berfokus pada analisis bukti digital yang terdapat pada RAM menggunakan metode *National Institute of Standards Technology (NIST),* dengan tujuan dapat membandingkan kinerja dari tiap-tiap tool live forensik dalam kemampuan menemukan artefak. Tool yang digunakan dalam penelitian kami menggunakan volatility, rekall dan redline dengan studi kasus skenario pada sistem operasi Windows 7.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah di kemukakan di atas, maka dapat dirumuskan sebuah permasalahan sebagai berikut :

a. Apakah permasalahan *data breach* di kalangan pengguna *desktop* dapat dianggap serius bagi masyarakat umum khususnya informasi pribadi mereka?
b. Bagaimana teknik yang digunakan untuk melakukan pengcapturean pada RAM yang berada di sistem operasi Windows?
c. Apakah semua artefak yang terdapat pada skenario dapat dibuktikan?
d. Apakah bisa dengan mengkombinasikan sistem operasi Windows dan Linux untuk proses investigasi pada *Digital Forensic?*

1.3 Batasan Masalah

Dalam investigasi analisis mengkakuisisi RAM pada Sistem Operasi Windows, dapat diberikan beberapa Batasan masalah dengan tujuan agar pembahasan tidak melebar dan lebih terperinci. Adapun beberapa ruang lingkup permasalahan sebagai berikut :

a. Yang akan dibahas dalam penelitian ini adalah bagaimana proses mengakuisisi pada RAM di sistem operasi Windows 7.
b. Analisis pada penelitian ini tidak mendalam, hanya terbatas pada skenario yang sederhana dengan tujuan mengenalkan beberapa tahapan yang ada di forensik.
c. Tools yang akan digunakan oleh penulis bersifat *open-source.*
d. Proses pengakuisisian akan dilakukan pada software *Virtual Machine* yakni Virtual Box.
e. Proses pengoleksian data atau artefak yang ada pada RAM dibantu dengan menggunakan tools tersebut.
f. Perbandingan performa masing-masing tools yang digunakan, mulai dari Volatility, Rekall dan Redline.
g. Proses mengakuisisi memori RAM menggunakan teknik Live Forensic dan dilakukan secara langsung dengan menggunakan bantuan Virtual Machine.

1.4 Tujuan Penelitian

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

a. Menemukan berbagai data informasi penting yang sekiranya perlu masyarakat umum ketahui jika, segala aktivitasnya dapat direkam pada RAM.
b. Untuk mengetahui bagaimana cara teknik mengakuisisi RAM pada sistem operasi Windows dengan menggunakan FTK Imager.
c. Dengan menjalankan skenario yang ada, maka dapat diketahui bahwa apakah seluruh data informasi yang terdapat pada RAM dapat di deteksi atau tidak dan dengan dijalankannya proses akuisisi pada RAM dapat diketahui pula bagaimana bentuk dari data tersebut.
d. Mengkombinasikan lingkungan kerja dari sistem operasi Windows dengan Linux untuk melakukan proses investigasi digital forensic.

1.5 Manfaat Penelitian

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

a. Agar masyarakat umum khususnya para pengguna *desktop user* bisa lebih peduli mengenai betapa pentingnya informasi pribadi mereka, agar tidak lupa untuk menghapus atau mengamankan data informasi tersebut.
b. Dapat menjadi referensi bagi masyarakat umum khususnya bagi mereka yang ingin belajar lebih dalam mengenai *digital forensic*, dengan belajar bagaimana caranya mengakuisisi RAM pada sistem operasi Windows.
c. Dapat menjadi patokan bagi masyarakat umum jika data informasi mereka juga tersimpan pada RAM khususnya pada sistem operasi Windows.
d. Agar masyakarat atau akademisi dapat mengetahui jika lingkungan kerja sistem operasi Windows dan Linux dapat digunakan untuk menginvestigasi ruang lingkup digital forensic.

1.6 Sistematika Penulisan

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

Bab I Pendahuluan, bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan.

Bab II Landasan Teori, bab ini menjelaskan mengenai forensic, dan akan menjelaskan mengenai live forensic serta penjelasan tentang beberapa tools yang digunakan.

Bab III Metodologi Penelitian, bab ini membahas mengenai proses pengcapturean data atau artefak, mulai dari persiapan, pencarian dan metode yang digunakan baik dari proses pembuatan skenario, pengumpulan serta pengolahan hasil dari data/artefak yang terkait.

Bab IV Pembahasan, bab ini membahas mengenai hasil proses mengakuisisi RAM itu sendiri, serta pengumpulan data/artefak yang telah didapatkan sebelumnya.

Bab V Penutup, bab ini menjelaskan mengenai kesimpulan dan hasil penelitian dan sebagai bahan peninjauan selanjutnya

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