BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan teknologi informasi dan komunikasi menjadi hal yang sangat penting dan harus ada dalam proses pengembangan institusi atau perusahaan. Dengan ketergantungan ini tanpa disadari akan meningkatkan resiko institusi atau perusahaan akan kejahatan di dunia teknologi informasi dan kominikasi.

Seiring dengan berjalannya waktu, pada tanggal 21 April 2008 telah ditetapkan UU No. 11 tahun 2008 tentang informasi dan transaksi elektronik [1], yang bertujuan untuk mengatur transfer informasi elektronik agar berjalan sesuai dengan etika bertransaksi informasi elektronik. Dengan adanya UU No. 11 tahun 2008 diharapkan tidak ada perorangan ataupun pihak lain yang merasa dirugikan karena transaksi informasi elektronik tersebut.

Hadirnya UU ini ternyata dirasa kurang memberikan kontribusi besar dalam proses penegakan kasus hukum di Indonesia, karena UU ini terkesan hanya mengatur perpindahan informasi elektronik secara umum, padahal terdapat hal-hal yang bersifat detail dalam persoalan kasus hukum dan penegakannya di Indonesia yang belum di atur dalam UU. Hal-hal yang bersifat mendetail inilah yang kemudian dijadikan acuan dalam keamanan teknologi informasi yang mengarah pada forensik digital.

Dalam sebuah sistem komputer terdapat *main memory* atau RAM (*Random Access Memory*) yang berperan sangat penting terhadap sebuah sistem. RAM juga merupakan salah satu media penyimpanan yang bersifat *volatile* atau data akan hilang saat tidak terdapat aliran listrik. Sedangkan data *volatile* yang terdapat pada RAM sangat berguna untuk proses forensik, karena RAM pada sistem komputer menggambarkan seluruh kegiatan yang telah terjadi pada sistem tersebut. Karena data *volatile* pada RAM sangat penting untuk proses forensik sehingga dikembangkan teknik forensik *memory.*

Forensik *memory* adalah proses investigator melakukan analisis terhadap data *volatile* pada RAM sebuah sistem komputer untuk mendapatkan bukti digital yang dapat dipertanggungjawabkan. Penanganan data *volatile* pada RAM ini harus hati-hati karena mengingat data dapat hilang jika sistem dimatikan. Oleh karena itu diperlukan teknik forensik *memory* yang dapat menjamin integritas data *volatile* tanpa menghilangkan data yang berpotensi menjadi barang bukti.

1.2 Rumusan Masalah

Rumusan masalah dalam penulisan proyek akhir ini adalah sebagai berikut:

1. Bagaimana proses kerja forensik *memory* pada data *volatile* sistem operasi komputer yang berpotensi sebagai barang bukti ?
2. Bagaimana keakuratan data hasil dari forensik *memory* dengan menggunakan beberapa variasi skenario kasus yang diujikan ?.

1.3 Tujuan

Tujuan pengambilan judul ini adalah sebagai berikut:

1. Melakukan analisis hasil sederhana dari bukti digital menggunakan metode *dumpmemory* yang ditemukan berdasarkan *IP Address attacker, backdoor* atau *payload* yang disisipkan, metode serangan yang digunakan.
2. Rekomendasi penggunaan proses forensik *memory* dengan menggunakan metode *dumpmemory* untuk keperluan investigasi dan memberikan solusi keamanan sesuai dengan skenario kasus yang tepat.

1.4 Batasan Masalah

Batasan masalah yang digunakan dalam penulisan proyek akhir ini adalah sebagai berikut:

1. Skenario kasus dilakukan pada sistem operasi Windows XP SP3 Professional yang berjalan pada mesin virtual.
2. Sistem yang diserang tidak menggunakan *firewall, proxy,* atau sistem keamanan lainnya.
3. Tidak membahas secara mendalam cara kerja *malware* dan *tools* penyerang.
4. Tidak membahas secara mendalam cara kerja dari *Random Access Memory*.
5. Tidak membahas mengenai algoritma pergantian pada *Random Access Memory.*
6. Tidak membahas secara mendalam mengenai sistem operasi dan *kernel.*
7. Kecurigaan investigator terhadap bukti yang dicurigai bersifat tidak alami, karena pihak yang berperan sebagai penyerang dan investigator adalah orang yang sama.
8. *Tools* yang digunakan bersifat *opensource*.

1.5 Definisi Operasional

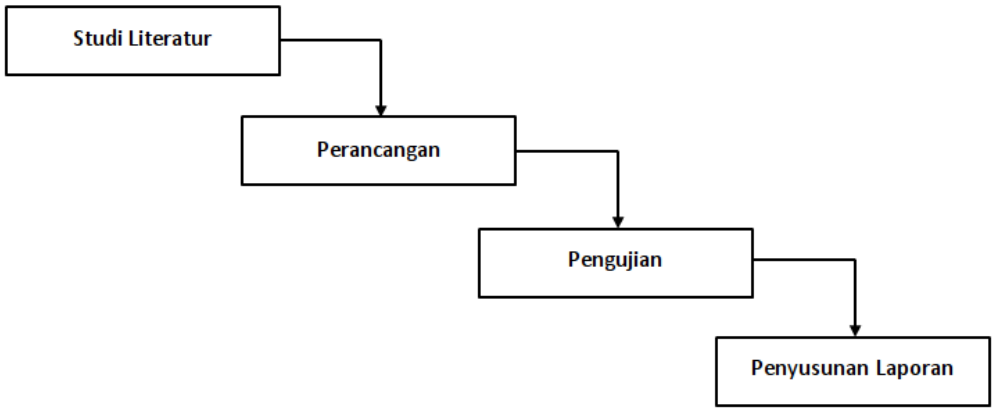
1. Forensik digital adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan meyimpan

bukti/informasi yang secara magnetis tersimpan/tersandikan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum.

2. *Random Access Memory* merupakan memori utama pada sebuah komputer yang bersifat *volatile* atau data akan hilang ketika daya komputer dimatikan, RAM terdiri atas cip-cip memori yang dapat dibaca dan ditulis oleh *processor* dan perangkat lainnya.
3. Sistem Operasi (*Operating System ; OS*) adalah sebuah program yang mengontrol eksekusi dari program aplikasi dan bertindak sebagai antarmuka pengguna komputer dan peranti keras komputer.
4. *Dumpmemory* merupakan sebuah metode atau cara untuk mendapatkan berkas digital yang berisikan *snapshot* (potret) statis *memory volatile* komputer.

1.6 Metode Pengerjaan

Metode pengerjaan yang dilakukan pada Proyek Akhir ini dengan metode Waterfall (air terjun) yang terdiri dari studi literatur, perancangan, pengujian, penyusunan laporan.



Gambar 1-1 Metode Waterfall

1. Studi Literatur

   Studi literatur di lakukan dengan mempelajari beberapa referensi yang mampu menunjang untuk melakukan penelitian, baik pengerjaan Proyek

Akhir. Referensi yang digunakan antara lain bersumber dari buku-buku, artikel, sumber dari internet, serta sumber-sumber lain yang berhubungan dengan pengerjaan Proyek Akhir yang dilakukan.

2. Perancangan

   Pada tahap ini dilakukan perancangan sistem yang akan dibangun pada mesin virtual, seperti desain topologi jaringan yang akan digunakan dan skenario kasus pengujian.

3. Pengujian

   melakukan pengujian forensik *memory* menggunakan metode *dumpmemory* dan menganalisis hasil yang diperoleh dari pengujian.

4. Penyusunan Laporan

   Penyusunan laporan secara keseluruhan atas kegiatan pembuatan Proyek Akhir dilakukan secara bertahap.

1.7 Jadwal Pengerjaan

Tabel 1-1 Jadwal Pengerjaan Proyek Akhir

Uraian	Tahun 2016																			
	Februari				Maret				April				Mei				Juni			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Studi Literatur																				
Perancangan																				
Pengujian																				
Penyusunan Laporan																				