

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kejahatan di dunia digital sudah banyak sekali baik yang bisa terpecahkan maupun tidak. Indonesia dengan komputer yang cukup banyak dan banyak orang yang menghabiskan waktunya menggunakan komputer.

Forensik komputer merupakan Teknik investigasi dan analisis komputer yang melibatkan tahapan dalam mengidentifikasi, menyiapkan, mengekstraksi, merekam, dan menginterpretasikan data yang terdapat pada komputer, tahapan tersebut digunakan sebagai adanya kejadian kejahatan di dunia maya cybercrime[1]. Dalam hal ini komputer forensic adalah salah satu bidang yang mendukung upaya penegakan hukum terhadap tindak kejahatan dengan bantuan komputer.

Memori volatile adalah memori yang bisa menyimpan data saat ada listrik dan akan menghilang Ketika tidak mendapatkan aliran listrik, memori volatile khususnya RAM atau memori fisik sebuah sistem menggambarkan seluruh kegiatan yang sedang terjadi di komputer tersebut [2]. Dengan melakukan penggalian barang bukti dari kejahatan digital. Penggalian barang bukti dengan memanfaatkan beberapa aplikasi seperti FTK Imager dan Volatility merupakan Langkah awal untuk melakukan analisis pada memori volatile yang akan dilakukan *dump* atau menduplikasi barang bukti agar tidak merusak barang bukti sesungguhnya.

1.2. Rumusan Masalah

Rumusan Masalah yang didapat bersarkan latar belakang di atas adalah

1. Bagaimana cara mendapatkan bukti digital aktivitas komputer dari memori volatile?
2. Bagaimana cara melakukan analisis aktivitas komputer berdasarkan hasil analisis forensic memori volatile?
3. Bagaimana mengimplementasikan priises analisis komputer berdasarkan hasil forensic memori volatile pada aplikasi?

4. Bagaimana mendapatkan akurasi dari hasil forensic memori volatile?

1.3. Tujuan dan Manfaat

Tujuan dari pembuatan tugas akhir adalah

1. Mendapatkan bukti digital aktivitas komputer dari memori volatile
2. Mendapatkan hasil analisis aktivitas dari komputer hasil analisis forensic volatile.
3. Mengimplementasikan proses analisis dari komputer berdasarkan hasil forensic volatile.
4. Mendapatkan akurasi hasil analisis forensic memori volatile.

1.4. Batasan Masalah

Berdasarkan rumusan masalah diatas maka penelitian ini membataskan masalah yaitu:

1. Pengujian menggunakan komputer dengan sistem operasi Windows.
2. Digital forensik yang dilakukan pada memori volatile dan *virtual machine*.
3. Tools yang digunakan analisis RAM adalah volatility.

1.5. Metode Penelitian

Metode penelitian yang dilakukan dengan cara:

1. Studi Litratur, yaitu dengan mengumpulkan referensi yang terkait dengan judul yang ingin diteliti.
2. Perancangan, yaitu dengan merancang bagaimana mengembangkan aplikasi analisis forensic dari memori volatile.

1.6. Jadwal Pelaksanaan

Jadwal pelaksanaan pengerjaan penelitian mengenai aplikasi analysis forensic dari memori volatile sebagai berikut.

Tabel 1.1 Jadwal dan *Milestone*.

No.	Deskripsi Tahapan	Durasi	Tanggal Selesai	<i>Milestone</i>
1	Studi literatur	2 Minggu	6 Maret 2022	Mencari referensi yang berkaitan dengan komputer forensik memori volatile
2	Perancangan dan pembuatan sistem	5 Minggu	10 April 2022	Membuat perancangan sistem dan implementasi
3	Simulasi	3 Minggu	1 Mei 2022	Melakukan pengujian dan evaluasi pada tools yang akan di gunakan
4	Akuisisi memori volatile	1 Bulan	1 Juni 2022	Melakukan akuisisi memori volatile dari komputer fisik
5	Membuat aplikasi tahap pertama	2 Minggu	15 Juni 2022	Aplikasi tahap pertama selesai
6	Extract file memori volatile	1 Bulan	15 Juli 2022	Hasil extract file pada memori volatile
7	Membuat data set hasil <i>extract</i> file pada memori volatile	1Bulan	15 Agustus 2022	Informasi file hasil <i>extract</i> memori volatile
8	Membuat perbandingan menggunakan <i>machine learning</i>	2 Minggu	29 Agustus	Akurasi perbandingan file
9	Penyusunan laporan/buku TA	2 Minggu	31 Agustus 2022	Buku TA selesai