BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Teknologi merupakan ilmu pengetahuan akan keterampilan dan inovasi suatu alat dengan tujuan memudahkan aktivitas manusia. Seiring berjalannya waktu diiringi perkembangan ilmu pengetahuan serta perkembangan teknologi yang sangat cepat terdapat suatu ancaman yang selalu mengikuti khususnya dalam perkembangan teknologi salah satunya adalah *malware*.

Malware merupakan kepanjangan dari *malicious software* yang berarti perangkat lunak berbahaya dan dibuat dengan tujuan untuk merusak sistem atau sekadar memasuki sistem komputer, laptop, jaringan hingga server secara sembunyi-sembunyi. Pada umumnya *malware* bekerja dengan cara menyusup pada RAM korban lalu menyebar ke dalam data atau *file* penting atau bekerja lewat jaringan internet dengan cara menumpang pada halaman *web* yang dibuka atau *file* yang telah kita unduh dari internet lalu jika telah berhasil digunakan nantinya akan menginfeksi perangkat pengguna.

Pada tahun 2019 perusahaan Microsoft memberitakan bahwa kasus *malware* di Indonesia masih jauh dari kata rendah dengan nilai rata-rata sebesar 10.68%, bahkan pihak Microsoft menyatakan bahwa tingkat rata-rata kasus *malware* di Indonesia lebih tinggi daari kasus *malware* di kawasan Asia Pasifik [1]

Dalam penelitian [2] telah dilakukan pengujian dan analisis pada program poison ivy yang merupakan salah satu jenis *malware*. Program poison ivy tersebut tergolong *malware* yang berbahaya dimana program ini dapat mengontrol langsung korban tanpa diketahui secara kasat mata. Dari hasil penelitian ini hasil yang didapatkan yaitu penggunaan metode dirasa masih sulit dan pengambilan sampelnya yang masih sangat luas.

Untuk itu pada tugas akhir ini membuat suatu aplikasi analisis forensik *malware* yang dapat membantu melakukan klasifikasi *malware* berdasarkan *file* yang terdapat pada memori agar pengguna tidak membuka *file* berbahaya tersebut sehingga perangkat komputer tetap aman. Adapun proses forensik *malware*

mengacu pada standar NIST (*National Institue of Standards and Technology*) dimana barang bukti berupa memori volatil dikumpulkan terlebih dahulu (*collection*), lalu dipastikan bahwa tidak ada perubahan terhadap barang bukti yang ada (*examination*), kemudian dilakukan proses analisis terhadap barang bukti (*Analysis*) dalam hal ini menggunakan dua (2) metode analisis, metode yang pertama menggunakan yarascan dan metode kedua menggunakan virustotal, untuk metode analisisnya sendiri bekerja secara paralel sehingga setelah dilakukan analisis tiap metode maka hasil analisis akan langsung diberikan (*Reporting*). Cara ini dinilai efisien karena pengambilan sampel yang skalanya tidak terlalu luas, kemudian untuk prosesnya sendiri tidak memerlukan banyak aplikasi sehingga meminimalisir terjadinya *multitasking* saat aplikasi berjalan serta penggunaan ruang memori komputer yang lebih rendah.

1.2. Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana membangun sebuah aplikasi analisis forensik *malware* dari memori volatil dengan metode yarascan dan virustotal?
2. Bagaimana performansi yang diberikan dari aplikasi analisis forensik *malware* dari memori volatil dengan metode yarascan dan virustotal saat melakukan analisis pada memori volatil?
3. Bagaimana tingkat akurasi yang diberikan dari metode yang ada pada aplikasi analisis forensik *malware* dari memori volatil dengan metode yarascan dan virustotal?

1.3. Tujuan dan Manfaat

Tujuan dari penelitian ini yaitu:

1. Membangun aplikasi yang dapat melakukan analisis forensik *malware* pada memori volatil.
2. Mengimplementasikan 2 metode berbeda pada aplikasi analisis forensik *malware* dari memori volatil dengan metode yarascan dan virustotal untuk mengetahui tingkat performansi masing masing metode.
3. Mengetahui tingkat akurasi setiap metode yang digunakan.

Manfaat yang diharapkan tercapai setelah melakukan penelitian ini adalah:

1. Mengurangi serangan *malware* pada komputer.
2. Mengetahui *file process* yang terdapat *malware*.
3. Berkontribusi dalam penelitian dan pengembangan ilmu forensik.

1.4. Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1. Analisis *malware* menggunakan *vmware workstation*.
2. Tools yang digunakan untuk analisis forensik RAM adalah volatility 3 dan analisis *malware* menggunakan yarascan dan virustotal CLI.
3. Sampel yang digunakan dalam penelitian ini *file* memori volatil dengan ekstensi *file* .vmem dan juga *file* hasil *dump* proses memori volatil menggunakan volatility dengan ekstensi *file* .dmp
4. Sistem operasi dalam penilitian ini menggunakan windows 10.
5. Tugas akhir ini tidak membahas proses *dump process ID* (PID) memori dan analisis lebih lanjut terkait analisis memori volatil.

1.5. Metode Penelitian

Metode penelitian yang digunakan yaitu:

1. Studi Literatur

Studi literatur dilakukan untuk memperoleh informasi lebih dalam terkait permasalahan yang ditemui dalam penelitian.

2. Bimbingan

Bimbingan dilakukan dengan melaporkan *progress* pengerjaan dengan pembimbing baik secara *online* maupun bimbingan secara *onsite*

3. Penyusunan Buku Tugas Akhir

Penyusunan buku tugas akhir ini merupakan gambaran dari kegiatan yang dilakukan penulis selama melakukan penelitian dan penyusunan buku ini diharapkan memudahkan orang lain dalam membantu pengembangan aplikasi ini.

1.6. Ringkasan Sistematika Penulisan

Ringkasan sistematika penulisan buku yaitu:

BAB I Pendahuluan

BAB I berisi informasi tentang latar belakang masalah, rumusan masalah, tujuan dan manfaat, batasan masalah, metode penelitian dan ringkasan sistematika penulisan.

BAB II Tinjauan Pustaka

BAB II berisi informasi tentang teori-teori yang digunakan dalam menalukan penelitian tugas akhir.

BAB III Perancangan Sistem

BAB III berisi informasi tentang penjalasan mengenai sistem yang dibuat.

BAB IV Hasil dan Analisis

BAB IV berisi informasi tentang hasil pengujian dan analisis pengujian aplikasi.

BAB V Simpulan dan Saran

BAB V berisi tentang informasi kesimpulan penelitian tugas akhir dan saran untuk peneliti selanjutnya.