1 PENDAHULUAN

1.1 Latar Belakang

Bertajamnya perkembangan dunia teknologi saat ini, mengakibatkan banyaknya tindakan kejahatan yang dilakukan melalui teknologi itu sendiri. Berbagai kemudahan yang ditawarkan oleh para pengembang *malware* membuat orang dengan bebas dan mudah untuk berbuat kejahatannya secara tersembunyi. *Malware* merupakan singkatan dari *malicious software* yang berarti software yang tidak diinginkan. Beragam tujuan yang dimiliki oleh para pelaku, beberapa diantaranya adalah untuk mencari kesenangan semata, keuntungan dengan cara memanipulasi transaksi keuangan perbankan, dan ada juga untuk kepentingan *spy* (mata-mata) antar beberapa negara, seperti yang dilakukan oleh salah satu negara adidaya Amerika dan Israel yang menggunakan menggunakan *malware* Stuxnet. Dengan memanfaatkan kelemahan sistem jaringan komputer yang ada, pelaku menyusupkan program botnet sebagai media untuk memata-matai bahkan mencuri informasi dari suatu sistem komputer, dan program ini yang dinamakan dengan *malware*.

Malware merupakan program yang sangat berbahaya karena dalam aktivitasnya itu sendiri *malware* tidak dapat terdeteksi oleh sistem yang sedang bekerja, sehingga cara pencegahan yang sangat memungkinkan untuk dilakukan adalah menganalisis terkait aktivitas dari *malware* tersebut. *Malware* pernah menjadi sangat fenomenal karena menyebabkan kerugian besar serta melibatkan banyak negara sebagai korbannya, jenis *malware* ini bernama *Citadel*. *Citadel malware* ditemukan pertama kali pada tahun 2012 dan tersebar luas pada tahun 2013. *Citadel* merupakan *malware* yang termasuk ke dalam jenis Trojan. Pada tahun 2013 FBI dan Microsoft berhasil mengungkapkan informasi tentang kerugian yang diakibatkan oleh *malware* ini, aktivitas *cyber crime* mampu mencuri total uang sekitar $500 juta (£323 juta) dari kegiatan ilegalnya di 80 negara yang berbeda, dan berhasil mencuri data hingga mencapai 5 juta perangkat dan hanya berhasil dihentikan sejumlah 1,400 *network* yang berjalan di dalamnya. Sampai saat ini *Citadel malware* masih menjadi ancaman yang serius secara global karena perkembangannya yang semakin hari semakin canggih [1]. *Citadel malware* melakukan serangkaian tindak kejahatan *monitoring* pada komputer korban menggunakan bot yang berjalan pada sistem korban melalui jaringan komputer.

Untuk saat ini beberapa penanganan telah dilakukan, seperti penelitian yang dilakukan oleh Aan Kurniawan dan Yudi Prayudi dalam melakukan investigasi *Zeus malware* dengan menerapkan teknik *live forensics* yang digunakan untuk menginvestigasi bukti digital dari aktivitas *Citadel malware*. Teknik *live forensics* ini dilakukan dengan menggunakan cara pendekatan terhadap sistem komputer yang sedang bekerja dan terhubung pada jaringan komputer [2]. Teknik *live forensics* ini memiliki kelebihan dari teknik-teknik lainnya, karena dalam pengimplementasiannya, investigator dapat dengan mudah mengetahui informasi tentang sistem yang sedang berjalan, antara lain adalah aktivitas memori, *network*, *swap file*, *running system process*, dan informasi dari file sistem. Hanya saja dalam melakukan teknik ini, investigator harus

memiliki akses penuh terhadap sistem tersebut.

Penelitian ini dilakukan dengan cara menerapkan hasil penelitian yang disesuaikan dengan skenario kasus dan kerangka investigasi berbeda. Dari hasil analisis nanti dilakukan perbandingan kerangka investigasi dengan menggunakan beberapa evaluasi tertentu dalam perbandingannya, Penelitian yang akan digunakan sebagai pembanding yaitu penelitian yang dilakukan oleh Philip dalam analisisnya terhadap *Zeus malware*. Perbandingan ini dilakukan untuk mengetahui kerangka investigasi yang terstruktur dan benar dalam implementasi teknik *malware forensics*.

1.2 Perumusan Masalah

Berdasar latar belakang yang diuraikan di atas, maka dapat dirumuskan beberapa permasalahan sebagai berikut :

1. Bagaimana cara pengimplementasian teknik *live forensics* untuk investigasi bukti digital dari aktivitas *malware*.
2. Bagaimana proses analisis teknik *live forensics* untuk mendukung kerangka investigasi yang baik dan benar dalam *malware forensics*.
3. Bagaimana proses evaluasi dalam menyusun suatu kerangka investigasi *malware* yang baik dan benar.

1.3 Batasan Masalah

Adapun batasan masalah Tugas Akhir ini adalah sebagai berikut :

1. Penelitian ini menggunakan skema yang bersifat virtual dengan jaringan lokal, menggunakan mesin virtual VMware sebagai host, Korban menggunakan sistem operasi Windows Vista Home Premium dan penyerang menggunakan sistem operasi Windows 7 Ultimate.
2. Investigator menggunakan sistem operasi Kali Linux.
3. Analisis menggunakan perangkat lunak *volatility* pada Kali linux dan menggunakan parameter : proses yang disembunyikan, proses yang digunakan untuk menyerang, proses yang terinfeksi, IP address penyerang, alamat apihooks penyerang, dan registry dalam menentukan tingkat akurasi *tools.*
4. Penelitian menggunakan analisis *scanning* virus dari website virus total.
5. Teknik *Live Forensics* dilakukan secara eksternal.

1.4 Tujuan

Tujuan yang ingin dicapai dalam pengerjaan Tugas Akhir ini adalah sebagai berikut :

1. Mengimplementasikan teknik *live forensics* untuk investigasi *malware forensics* dengan studi kasus *Citadel Malware*.
2. Membandingkan serta mengevaluasi kerangka investigasi yang terstruktur untuk teknik *malware forensics* menggunakan hasil analisis *live forensics* yang telah didapat.

1.5 Hipotesis

Pengambilan hipotesis mengacu pada penelitian sebelumnya [2], yaitu cara terbaik untuk mengidentifikasi karakteristik serta bukti digital dari sebuah aktivitas *malware* adalah dengan menggunakan teknik *live forensics*, hal ini terkait dengan analisa bahwa *Zeus malware* melakukan serangan melalui jaringan komputer dan aktivitasnya berjalan ketika sistem dalam keadaan menyala maka teknik *live forensics* diperlukan sebagai solusi untuk mendapatkan bukti digital dari sebuah aktivitas *malware* yang berupa *image memory* dari sebuah sistem.

1.6 Metodologi Penelitian

Metodologi penelitian yang dilakukan dalam menyelesaikan Tugas Akhir ini adalah sebagai berikut :

1. Studi Literatur

   Peneliti melakukan review dari beberapa literatur sebagai referensi untuk melakukan tahapan-tahapan penelitian. Beberapa penelitian tersebut antara lain adalah penelitian dari Aan Kurniawan dan Yudi Prayudi, yang melakukan analisis terhadap aktivitas Zeus *malware* pada suatu sistem komputer yang terhubung dengan menggunakan teknik *live forensics* [2], penelitian dari Anders Orsten Flaglien, yang melakukan analisis terhadap aktivitas *malware* pada suatu sistem komputer yang terhubung dengan menggunakan metode korelasi [3]. Kemudian penelitian dilakukan oleh Murray Brand yang mengangkat tema analisis forensics terhadap *malware* dengan menggunakan teknologi *anti-analysis* [4], dan yang terakhir adalah paper yang diangkat Gursirman Kaur dan Bharti Nagpal dengan tema tentang gambaran umum suatu langkah-langkah melakukan analisis *malware* dalam suatu investigasi [5].
2. Perancangan

   Perancangan sistem dilakukan dengan membuat skema yang bersifat virtual dengan jaringan lokal menggunakan VMware sebagai host. Korban dan penyerang menggunakan sistem operasi Windows, sedangkan investigator menggunakan sistem operasi Kali linux. Inetsim dijalankan sebagai alat untuk memanipulasi jaringan lokal menjadi seolah-olah berjalan pada jaringan internet. WAMP digunakan pada komputer penyerang sebagai *web server* dan *database server* sebagai alat untuk memonitoring *Citadel malware* dan menggunakan perangkat lunak berbasi GUI yaitu Belkasoft Live RAM capturer sebagai *tools* akusisi *memory*, website virus total dan *volatility* sebagai *tools* analisis.
3. Implementasi

   Malware dijalankan pada komputer korban, setelah komputer penyerang melakukan *bot executable* dengan menggunakan program *citadel.exe* pada *Citadel malware*. Investigator melakukan konfigurasi inetsim yang digunakan untuk proses analisis pada komputer korban.

4. Pengujian

   Pengujian dilakukan pada komputer investigator yang berjalan pada sistem operasi Kali linux menggunakan *tools volatility*. Sedangkan dalam melakukan *scanning* menggunakan *live scanning* pada website virus total.

5. Analisis

   Analisis yang dilakukan setelah hasil pengujian didapatkan yaitu, analisis *process, network, apihooks, registry, dump process,* dan *file dump*.

6. Penulisan Laporan

   Peneliti mengumpulkan hasil dari seluruh tahapan, lalu menyimpulkan hasil akhir dari penelitian.