BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era teknologi yang semakin berkembang pesat sekarang ini, komputer digunakan dalam memudahkan pekerjaan manusia, dalam pengoprasiannya ada *software* yang berjalan diatas sistem operasi, dan ini sangat berperan penting dalam melakukan tugas-tugas yang dikerjakan oleh pengguna karena melalui *software* inilah suatu komputer dapat menjalankan perintah sehingga membantu pengguna dalam menyelesaikan pekerjaannya. Namun tidak semua *software* dapat membantu dan memudahkan manusia dalam melakukan pekerjaannya, adapula jenis *software* yang diciptakan untuk melakukan perusakan atau tindak kejahatan yang dapat merugikan orang lain, software tersebut dikategorikan sebagai *Malicous Software*.

Malicous Software atau yang lebih dikenal sebagai *Malware* merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya seperti *Trojan, Virus, Spyware* dan *Exploit* (Kramer, S., dan Bradfield, J. C, 2009). *Malware* diciptakan dengan maksud tertentu yaitu melakukan aktifitas berbahaya yang berdampak sangat merugikan bagi para korbannya, antara lain seperti penyadapan serta pencurian informasi pribadi, hingga kasus perusakan sistem yang dilakukan oleh penyusup (*Intruder*) terhadap perangkat korban dengan berbagai alasan. Salah satu media yang digunakan oleh *intruder* untuk mengendalikan komputer pengguna secara diam-diam dari jarak jauh adalah *malware poison ivy*, dikenal sebagai "*trojan access remote*" karena dapat memberikan kontrol penuh kepada *intruder* melalui pintu belakang (*backdoor)*, kemampuan *malware poison ivy* mengadopsi dari software *Remote Administration Tool* (RAT), yaitu termasuk kategori software yang baik (legal) yang dapat melakukan monitoring & pengontrolan secara penuh, contoh penggunaan software RAT ini biasa digunakan oleh seorang pimpinan perusahaan untuk mengontrol perangkat kerja (komputer) karyawannya melalui jaringan jarak jauh, dengan fitur tersebut tidak jarang *malware poison ivy* dikatakan juga sebagai Software RAT yang ilegal (RAT *Malware*) dikarenakan tidak

memberikan informasi berupa *notifikasi* saat proses remote terhubung (terhubung secara diam-diam), dengan *malware* sebagai medianya maka dalam hal ini merupakan sebuah bukti tindak kejahatan digital yang dilakukan oleh seorang *intruder*.

Forensik Digital merupakan disiplin ilmu yang menerapkan investigasi dan identifikasi dalam menindak kejahatan digital (Wahanggara dan Prayudi, 2015). Salah satu tahapan utama dalam menginvestigasi tindak kejahatan yaitu mengumpulkan barang bukti digital. Untuk menemukan barang bukti digital pada *malware*, dibutuhkan analisis lebih mendetail agar dapat mendeteksi aktifitas sebuah *malware* serta mempelajari bagaimana sebuah *malware* menginfeksi dan berkembang dalam sebuah sistem. Ada dua tipe analisis dalam melakukan analisis pada *malware* yaitu dengan analisis statis (analisa kode) dan analisis dinamis (Distler, 2007). Meskipun dari kedua tipe analisis tersebut mempunyai tujuan yang sama yaitu menjelaskan tentang bagaimana sebuah *malware* bekerja namun peralatan, waktu dan kemampuan yang dibutuhkan dalam menganalisa sangatlah berbeda, Analisis Statis melakukan dengan pembongkaran terhadap *source code* dari *malware* lalu mempelajari dan memahami melalui kode tersebut atau dengan kata lain proses analisis tidak memerlukan eksekusi terhadap *malware*, berbeda dengan analisis dinamis yang pada proses analisisnya membutuhkan pengeksekusian terhadap contoh *malware* untuk kemudian dipelajari perilaku yang ditimbulkan oleh *malware* tersebut sehingga dapat diperoleh informasi tentang bagaimana sebuah *malware* tersebut bisa berkembang atau memanipulasi dirinya sendiri, dan pada komponen sistem apa saja *malware* tersebut berkomunikasi. Harapan setelah proses eksplorasi dilakukan semoga bisa memberikan pembelajaran tentang efek yang ditimbulkan oleh *malware* dan membantu praktisi dalam menemukan barang bukti digital.

1.2 Rumusan Masalah

Yang menjadi permasalahan dalam menyusun skripsi ini adalah

1. Bagaimana menganalisis program *Poison Ivy* sehingga dapat diuji, apakah program tersebut merupakan suatu *malware* atau bukan?
2. Bagaimana menyajikan laporan hasil pengujian dan analisis pada program *Poison Ivy*?

1.3 Batasan Masalah

Adapun batasan masalah untuk melakukan pengujian *malware* ini meliputi :

1. Metode analisis yang digunakan dalam penelitian ini adalah *malware* analisis dinamis dan *malware* analisis statis, yaitu mempelajari *malware* dari sisi perilakunya, baik dengan eksekusi langsung pada file *malware* dilingkungan *sandbox* maupun dengan mempelajari kode yang terkandung didalam file *malware* tersebut.
2. Sampel yang digunakan peneliti adalah *malware* dengan jenis *trojan access remote* (*Poison Ivy*).
3. *Environtment* yang digunakan dalam penelitian ini adalah sistem operasi *Windows XP Service Pack III*

1.4 Tujuan Penelitian

Tujuan dari skripsi ini adalah :

1. Menerapkan metode analisis dinamis dan metode analisis statis dalam mempelajari perilaku *malware*.
2. Mengidentifikasi program *Poison Ivy* sebagai suatu *malware* atau bukan.
3. Menyusun dokumentasi yang terkait dengan penemuan barang bukti *digital* pada program *Poison Ivy*.

1.5 Manfaat Penelitian

Manfaat dari skripsi ini adalah

1. Mengenalkan metode *malware analysis* dalam mempelajari perilaku sebuah *malware*.
2. Hasil perilaku *malware* yang telah dipelajari dapat diterapkan dalam pengembangan anti *malware*.
3. Membantu praktisi dalam menemukan barang bukti *digital*.
4. Sebagai referensi bagi peneliti lain yang ingin melakukan penelitian khususnya dalam bidang keamanan sistem komputer.