BAB I

PENDAHULUAN

I.1. Latar Belakang

Dewasa ini, teknologi informasi berkembang dengan demikian pesatnya di seluruh dunia. Selain itu, teknologi informasi juga telah merasuk ke hampir setiap sudut kehidupan manusia. Singkat kata, teknologi informasi telah menjadi "barang canggih" yang berperan besar dalam kehidupan manusia.

Sebagaimana perkembangan teknologi pada umumnya, perkembangan teknologi informasi juga diikuti dengan "perkembangan" sisi negatifnya. Dalam kasus teknologi informasi, hal itu terjadi dalam bentuk "perkembangan" kejahatan teknologi informasi (*cybercrime*). Salah satu bentuk *cybercrime* adalah penciptaan dan peredaran *malware*.

Malware merupakan program komputer yang diciptakan dan diedarkan untuk tujuan kejahatan, seperti merusak sistem komputer (*cracking*, *denial of service*, dsb.), mencuri data dan informasi (*carding*, *identity theft*, dsb.), mengirimkan informasi yang tidak dikehendaki (pornografi, *spam*, dsb.), dan lain sebagainya (Microsoft Press, 2002).

Salah satu jenis *malware* yang cukup menjengkelkan adalah *malware-malware* "penyandera" dokumen. Karakteristik *malware-malware* semacam itu adalah "menyandera" *file* dokumen ("menyembunyikan" *file* dokumen dalam "tubuhnya") dan "menyamarkan" dirinya menjadi seperti *file* dokumen tersebut (misalnya, dengan mengubah

icon-nya). Apabila dirinya, yang telah "menyamar" menjadi seperti *file* dokumen, dijalankan, dirinya akan mengeluarkan (*extract*) dan membuka *file* dokumen tersebut, tentunya setelah menulari komputer tempat dirinya dijalankan dan mengakibatkan kerusakan-kerusakan lainnya. *Malware-malware* semacam itu dinilai menjengkelkan karena para pengguna komputer tidak dapat membuka dokumen-dokumen mereka tanpa membuat komputer mereka tertular *malware*. Apabila mereka mencoba melewati *malware* dengan membuka "dokumen" tersebut langsung dari programnya, "dokumen" tersebut tidak akan dapat dibuka karena sebenarnya "dokumen" tersebut adalah *malware* yang telah "menyamar" menjadi seperti dokumen.

Selama ini, para pengguna komputer mengatasi *malware-malware* semacam itu dengan aplikasi anti-*malware*. Dalam hal ini, aplikasi anti-*malware* berfungsi membersihkan *malware* dari dalam komputer dan menyelamatkan dokumen dari dalam tubuh *malware*.

Meskipun aplikasi-aplikasi anti-*malware* terus dikembangkan oleh para produsennya, aplikasi-aplikasi anti-*malware* masih memiliki beberapa keterbatasan utama, yaitu:

a. aplikasi-aplikasi anti-*malware* harus diperbarui (*update*) secara rutin agar dapat mendeteksi, membersihkan, dan menyelamatkan dokumen-dokumen yang "disandera" *malware-malware* terbaru (sayangnya, ukuran *file update* aplikasi-aplikasi anti-*malware* dapat mencapai puluhan megabyte, praktis menyebabkan orang-orang yang tidak memiliki sambungan Internet yang cepat untuk tidak terlindung dari *malware-malware* terbaru),
b. adanya waktu tunggu antara peredaran *malware* baru dengan ketersediaan pendeteksinya (dalam kasus

malware lokal, hal ini bahkan dapat mencapai beberapa minggu), dan

c. ketidakmampuan aplikasi-aplikasi anti-*malware* untuk mendeteksi *malware-malware* yang tidak pernah dilaporkan (seperti *malware* baru atau *malware* "*custom made*").

Melihat kenyataan tersebut, kemudian muncul pertanyaan dalam benak penulis: mungkinkah mengembangkan sistem yang dapat menyelamatkan dokumen yang "disandera" *malware* secara otomatis, yang sekaligus mudah diakses dan digunakan para pengguna komputer? Dengan sistem seperti itu, diharapkan para pengguna komputer dapat menyelamatkan dokumen-dokumen mereka yang "disandera" *malware* (termasuk *malware-malware* baru dan yang tidak pernah dilaporkan) tanpa perlu repot-repot memperbarui aplikasi-aplikasi anti-*malware* secara rutin.

Selain itu, kebutuhan akan sistem semacam itu semakin lama dirasakan semakin mendesak, mengingat semakin meluasnya penggunaan komputer untuk penyimpanan dokumen dan semakin parahnya masalah *malware* di seluruh dunia. Sebagai ilustrasi, sebuah laporan dari F-Secure Corporation (2007) menyatakan, selama tahun 2007, jumlah *malware* baru di seluruh dunia meningkat 100% (dengan kata lain, berlipat ganda) dibanding tahun sebelumnya, sama dengan jumlah semua *malware* baru selama 20 tahun sebelumnya.

Penelitian ini akan dilaksanakan dalam empat tahap. Pada tahap pertama, dilakukan studi pustaka untuk mempelajari karakteristik *malware-malware* "penyandera" dokumen sekaligus mencari cara menyelamatkan dokumen dari dalam tubuh *malware*. Setelah itu, pada tahap kedua, dilakukan analisis dan perancangan sistem dengan metode terstruktur untuk menentukan arsitektur sistem dan

teknologi yang cocok untuk memecahkan masalah. Selanjutnya, pada tahap ketiga, dilakukan implementasi sistem secara prosedural. Akhirnya, pada tahap keempat, dilakukan pengujian sistem.

Yang akan mendapatkan manfaat dari penelitian ini adalah para pengguna komputer pada umumnya. Sementara itu, keluaran yang akan dihasilkan penelitian ini adalah berupa perangkat lunak (terdiri atas program dan kode sumbernya) serta laporan tugas akhir.

Secara keseluruhan, penelitian ini bertujuan untuk mengembangkan sistem penyelamatan dokumen yang "disandera" *malware*. Penelitian ini dilakukan karena penulis ingin mengembangkan sistem yang dapat menyelamatkan dokumen yang "disandera" *malware* secara otomatis, yang sekaligus mudah diakses dan digunakan para pengguna komputer. Penelitian ini perlu dilakukan karena semakin meluasnya penggunaan komputer untuk penyimpanan dokumen dan semakin parahnya masalah *malware* di seluruh dunia. Penelitian ini akan dilaksanakan dalam empat tahap, yaitu tahap studi pustaka, tahap analisis dan perancangan sistem, tahap implementasi sistem, serta tahap pengujian sistem. Yang akan mendapatkan manfaat dari penelitian ini adalah para pengguna komputer pada umumnya. Keluaran yang akan dihasilkan penelitian ini adalah berupa perangkat lunak (terdiri atas program dan kode sumbernya) serta laporan tugas akhir.

I.2. Perumusan Masalah

Berdasarkan latar belakang masalah di atas, dapat dirumuskan masalah sebagai berikut:

> Bagaimana caranya mengembangkan sistem yang dapat menyelamatkan dokumen yang "disandera" *malware* secara otomatis, yang sekaligus mudah diakses dan digunakan para pengguna komputer?

I.3. Batasan Masalah

Dalam penelitian ini, masalah yang akan diteliti dibatasi sebagai berikut:

1. sistem yang akan dikembangkan merupakan sistem berbasis web yang dapat diakses melalui Internet,
2. sistem yang akan dikembangkan merupakan sistem *batch* yang dapat memproses sejumlah *malware* sekaligus secara otomatis dan terjadwal,
3. *malware* yang akan diproses sistem adalah *malware-malware* yang dapat berjalan di sistem operasi Windows XP,
4. *malware* yang akan diproses sistem adalah *malware-malware* yang hanya terdiri atas sebuah *file* EXE dan hanya "menyandera" sebuah *file* dokumen,
5. *malware* yang akan dianalisis sistem adalah *malware-malware* yang "kooperatif" dengan sistem, dan
6. metode penyelamatan dokumen yang digunakan sistem adalah *hooking* Windows API dalam *virtual machine*.

I.4. Tujuan

Penelitian ini bertujuan untuk mengembangkan sistem yang dapat menyelamatkan dokumen yang "disandera" *malware* secara otomatis, yang sekaligus mudah diakses dan digunakan para pengguna komputer.

I.5. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah:

1. **Metode Studi Pustaka**, yaitu mempelajari bahan-bahan dan materi-materi yang diperlukan dari berbagai literatur yang dapat dijadikan sebagai acuan pembuatan tugas akhir.
2. **Metode Pembangunan Perangkat Lunak**, yaitu melakukan implementasi dan desain sistem yang akan dibuat, dengan langkah-langkah sebagai berikut:
   a. **Analisis Sistem**, yaitu proses untuk mendefinisikan kebutuhan perangkat lunak yang akan dikembangkan, yang dituangkan dalam laporan Spesifikasi Kebutuhan Perangkat Lunak (SKPL),
   b. **Perancangan Sistem**, yaitu proses untuk mendefinisikan perancangan sistem yang akan dikembangkan, yang dituangkan dalam laporan Deskripsi Perancangan Perangkat Lunak (DPPL),
   c. **Pengkodean**, yaitu proses penulisan program yang merealisasikan rancangan sistem yang dikembangkan dengan menggunakan bahasa pemrograman, dengan mengikuti kaidah pemrograman yang berlaku, dan
   d. **Pengujian Perangkat Lunak**, yaitu proses pengujian fungsionalitas perangkat lunak, apakah sudah sesuai dengan dokumen Perencanaan, Deskripsi, dan Hasil Uji Perangkat Lunak (PDHUPL).

I.6. Sistematika Penulisan

Laporan penelitian ini disusun menjadi 5 bab, yaitu Pendahuluan, Landasan Teori, Analisis dan Perancangan Sistem, Implementasi dan Pengujian Sistem, serta Kesimpulan dan Saran.

BAB I PENDAHULUAN

Pada bab ini akan dijelaskan mengenai pendahuluan, latar belakang masalah, perumusan masalah, batasan

masalah, maksud dan tujuan penulisan, langkah-langkah penyusunan tugas akhir, dan sistematika penulisan laporan.

BAB II LANDASAN TEORI

Pada bab ini akan dijelaskan mengenai teori-teori, pendapat, prinsip, dan sumber-sumber lain yang dapat dipertanggungjawabkan secara ilmiah dan dapat dipergunakan sebagai pembanding atau acuan di dalam pembahasan masalah.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan mengenai analisis permasalahan yang ada, perancangan sistem, dan mencari alternatif pemecahan masalah beserta implementasinya.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini akan dijelaskan mengenai implementasi dari perancangan perangkat lunak yang akan dibuat dan pengujian fungsionalitas perangkat lunak.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan dijelaskan kesimpulan dari pembahasan laporan secara keseluruhan beserta saran-saran dari penulis.

DAFTAR PUSTAKA

LAMPIRAN