BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring pesatnya kemajuan teknologi informasi khususnya di bidang teknologi komputer dan jaringan, keamanan dan isu yang kerap kali dibahas. Mulai dari ancaman langsung para *craker* atau *hacker* jahat hingga acaman yang dilakukan melalui program yang disebut malcode (*malicious code*). Suatu program atau script apapun yang bersifat merusak atau merugikan dapat katagorikan sebagai malcode termasuk virus komputer, worm atau trojan horse.

Selama lebih dari tiga dekade yang lalu, virus komputer telah berkembang dari sekedar riset akademis menjadi masalah yang umum bagi para pengguna komputer di dunia. Masalah terbesar dari virus ini berasal dari penanggulangan efek kerugian yang ditimbulkan oleh penyebarannya. Efek kerugian ini semakin menjadi dengan maraknya penggunaan internet sebagai jalur komunikasi global antara pengguna komputer di seluruh dunia. Berdasarkan hasil survei CSI/FB sejak tahun 1999-2006 pada sekitar 300-an responden dari berbagai organisasi di Amerika Serikat, tentang kejahatan komputer dan keamanan nya menyebutkan bahwa virus menempati urutan pertama sebagai kejahatan komputer yang paling merugikan. Masih dari hasil survei tersebut, dinyatakan kerugian rata-rata yang diderita organisasi-organisasi itu akibat virus komputer ditaksir mencapai sekitar 38 juta dolar amerika pertahun. Seiring dengan perkembangannya, virus komputer mengalami beberapa evolusi dalam bentuk, karakteristik serta media penyebarannya. bentuk evolusi tersebut dikenal dengan *Worms, Spyware, Trojan horse* dan program Malcode lain.

Perkembangan penyebaran malcode di Indonesia pada awalnya lebih banyak didominasi oleh *worms* dan *virus* yang berasal dari luar negeri. Namun pada bulan Oktober 2005, dominasi ini mulai runtuh dengan menyebarnya virus-virus lokal yang hampir ada disetiap komputer di seluruh Indonesia, virus menyebar dengan sangat cepat dan sangat membuat risih bagi pengguna komputer, dengan demikian dibuatlah anti virus sebagai salah satu solusi mencegah penyebaran.
Pada sekitar tahun 2007-2010 perkembangan virus lokal di Indonesia semakin marak dengan di buat nya virus - virus yang ber ekstensi .vbs sehingga para pembuat antivirus lokal membutuhkan contoh virus yang dikirimkan langsung oleh pengguna komputer.

Metode pencarian virus yang paling sering di pakai oleh anti virus yaitu metode CRC-32 (*Cyclic Redundancy Code*). Metode CRC-32 merupakan teknik yang semulanya digunakan untuk mengecek kerusakan pada file. Metode ini yang sering digunakan oleh anti virus lokal untuk mengecek *signature* dari virus, tetapi teknik ini tidak efesien apabila diterapkan pada malware yang sudah mengimplementasikan teknik polymorph.. Kasus virus lokal sudah ditemukan penggunaan teknik polymorph. Baik itu secara sederhana maupun kompleks. Cara yang biasa digunakan yaitu :

- Merubah atau mengenkripsi nama variabel dan string
- Menambah atau mengurangi byte-byte tertentu di virus
- menggunakan *engine polymorph* tertentu

Jika secara normal metode Crc-32 ini sangat gampang untuk dikelabui, hal ini dikarenakan perubahan 1 bit kode pada program maka akan menyebabkan perubahan hasil pengecekan CRC-32.
Hal ini yang melatarbelakangi mengapa “implementasi Anti Virus Dengan Metode Pencarian Header File Data Sizeofcode Dan Addresofentrypoint Sebagai Pattern Virus” diangkat sebagai judul

skripsi, karena berdasarkan pengamatan penulis walaupun virus sudah melakukan modifikasi terhadap dos header dengan tujuan untuk memperkecil ukuran virus, tetapi data optimal header dari virus yang berupa SizeOfCode dan AddressOfEntry, tidak akan berubah.

1.2 Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah, maka permasalahan dalam skripsi ini, adalah bagaimana teknik pembuatan anti virus dengan metode pencarian header file data sizeofcode dan addressofentrypoint .

1.3 Batasan Masalah

Penulis membatasi penelitian ini dengan membahas :

1. File yang akan di jadikan sampel virus yaitu berupa file yang berekstensi *.exe. dan sample virus sality
2. *Pattern virus* dalam bentuk hexadecimal yang merupakan data AddressOfEntryPoint dan SizeOfCode.
3. Menyimpan *pattern virus* pada suatu text file terpisah dimana 16 digit pertama adalah pola virus yang berupa bilangan hexa, dan diikuti oleh nama virus

1.4 Tujuan Penelitian

Dari hasi penelitian yang dilakukan, adapun tujuan yang ingin dicapai dalam merancang suatu sistem anti virus yaitu :

1. Untuk membuat sebuah anti virus dengan metode pencarian header file data SizeOfCode dan AddressOfEntrypoint sebagai *pattern virus*.
2. Menganalisa kinerja virus dan mengatasinya

3. Untuk melakukan pengujian terhadap anti virus yang menggunakan header file sizeofcode dan AddressOfEntryPoint sebagai *pattren virus* yang dirancang, untuk dibandingkan dengan sistem yang menggunakan metode *checksum* (CRC-32).

1.5 Metode Penelitian

Metode penelitian yang digunakan dalam tugas akhir ini adalah:

1. Studi Literatur

Studi literature dilakukan dengan cara membaca dan mempelajari sejumlah refrensi dan literature yang berhubungan dengan *Pembuatan antivirus*

2. Pengumpulan Data

Dilakukan dengan melakukan penelitian dari metode Pencarian Header File Data Sizeofcode Dan Addresofentrypoint Sebagai Pattern Virus, untuk mendapatkan data dan informasi yang dibutuhkan untuk laporan ini.

3. Analisa Data

Dilakukan dengan cara mengolah data yang telah didapatkan pada tahap pengumpulan data dan membandingkannya.

4. Wawancara

Metode yang digunakan dalam memperoleh data adalah dengan mengadakan tanya-jawab informal untuk mendapatkan keterangan langsung dari pihak-pihak yang dianggap dapat memberikan kontribusi dan informasi terhadap penulisan tugas akhir ini.

1.6 Sistematika Penulisan

Penulisan Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab Pendahuluan berisi latar belakang masalah, perumusan masalah, tujuan dan manfaat studi, ruang lingkup studi, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini memuat tentang hasil studi pustaka mengenai teori serta konsep. Menjelaskan materi yang tersedia yang berhubungan erat dengan topik laporan Tugas Akhir. Tinjauan pustaka berisi beberapa referensi dari hasil penelitian yang relevan dengan topik tugas akhir yang disajikan, yang diperoleh dari berbagai sumber.

BAB III METODE PENELITIAN

Bab ini memuat persiapan instalasi visual basic 6.0 baik dari hardware yang dibutuhkan untuk instalasi dan bagaimana cara menjalankan visual basic 6.0.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menguraikan pembahasan perancangan antivirus dan disertai dengan implementasi pada aplikasi tersebut.

BAB V KESIMPULAN DAN SARAN

Kesimpulan mengemukakan secara singkat hasil penting yang diperoleh dari penelitian sesuai dengan masalah dan tujuan penelitian. Saran merupakan masukan penulis berupa rekomendasi yang diambil dari hasil pembahasan serta kesimpulan.