

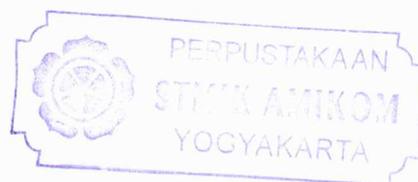
# BAB I

## PENDAHULUAN

### A. LATAR BELAKANG MASALAH

Pada Era Informasi seperti sekarang ini banyak bermunculan berbagai macam teknologi informasi yang dalam pemanfaatannya kadangkala dipersalahgunakan oleh pihak-pihak tertentu. Salah satu contohnya adalah VCD yang dijual secara umum di kios-kios penjualan VCD khususnya yang kami temui di salah satu kota di Jawa Timur. VCD tersebut secara fisik, harga jual, dan operasional sama seperti VCD yang lain. Ketika diputar (*Play*) di *VCD Player Conventional* sama seperti VCD yang lain yaitu memutar video yang ada dalam VCD tersebut dengan normal. Tetapi masalah akan timbul ketika VCD tersebut diputar (*Play*) menggunakan komputer melalui CD-ROM atau *Optical Drive* sejenis, seperti salah satu kasus yang terdapat dalam kejadian di bawah ini.

Pada pusat pelayanan komputer tempat kami bekerja ada seorang pelanggan datang dengan membawa CPU (*Central Processing Unit*) komputernya yang bermasalah. Setelah kami menanyakan masalah apa yang membuat pelanggan tersebut datang ke tempat kami, kemudian pelanggan tersebut menjelaskan bahwa ada kejadian yang sangat fatal menimpa komputernya sekaligus membuatnya sangat panik. Kemudian pelanggan tersebut menceritakan detailnya kepada kami bahwa ketika pelanggan tersebut memasukkan VCD yang baru saja ia beli ke dalam CD-ROM di komputernya,



komputernya pun merespon secara *default* seperti komputer pada umumnya apabila ada *drive* baru yang aktif maka komputer akan berusaha membaca isi *drive* yang baru tersebut secara otomatis. Tapi setelah itu muncul suatu respon yang tidak seperti biasanya, yaitu muncul tampilan *Command Prompt* dengan beberapa informasi yang muncul di dalamnya. Dan lebih parah lagi setelah *Command Prompt* tersebut menutup dengan sendirinya kemudian komputer *Shutdown* secara otomatis, setelah komputer dihidupkan kembali waktu *booting* tidak dapat masuk ke dalam Sistem Operasi (*Microsoft® Windows® XP*) dan muncul informasi yang menyatakan ada beberapa *system file* yang hilang. Sampai langkah ini kemudian proses *booting* berhenti dan komputer tidak dapat digunakan secara normal.

Dengan kejadian tersebut maka kami tertarik untuk menjadikannya sebagai bahan penelitian yang kami gunakan sebagai materi pembahasan dalam Skripsi yang berjudul “PEMBUATAN *APPLICATION TOOLS* UNTUK MENGATASI *MALWARE* PADA VCD”.

## B. RUMUSAN MASALAH

Berdasarkan kasus di atas, masalah yang timbul adalah komputer tidak dapat dioperasikan setelah pengguna (*user*) memasukkan VCD ke dalam CD-ROM. Hal tersebut perlu diperjelas sumber, akibat dan penyelsaiannya. Maka perlu dirumuskan beberapa hal berdasarkan dari kasus di atas, sebagai berikut:

1. Perlu diketahui dan diperjelas sumber masalah yang mengakibatkan komputer tidak dapat digunakan secara normal setelah memasukkan VCD

ke dalam CD-ROM. Apakah masalah timbul dari komputer atau VCD tersebut sebagai sumber masalahnya?

2. Perlu diidentifikasi sumber masalah yang ditemukan dari komputer dan atau dari VCD. Sumber masalah termasuk ketidaksengajaan (*human error*, *physical error*, *operational error*) atau faktor kesengajaan dari pihak luar (*virus thread*, *harmful script*, *program infiltration*) dan sejenisnya?
3. Perlu dipelajari proses bagaimana masalah tersebut dapat timbul. Bagaimanakah proses mulai dari munculnya *Command Prompt* secara tiba-tiba hingga *booting* yang gagal dikarenakan beberapa *system file* yang tidak teridentifikasi oleh *system*?
4. Perlu diidentifikasi akibat-akibat yang timbul dari masalah tersebut. Akibat apa saja yang timbul dari permasalahan tersebut, terhadap media (komputer), terhadap pengguna (*user*), dan terhadap lingkungan sekitar (*environment*) serta termasuk akibat positif atau negatifkah yang timbul?
5. Setelah ditentukan akibat yang timbul dari permasalahan yang dimaksud, maka selanjutnya adalah mengelompokkan akibat-akibat yang timbul berdasarkan efek positif atau negatif yang ditimbulkan. Kemudian ditentukan apakah solusi yang tepat untuk memperbaiki/merekondisi akibat yang berefek negatif tersebut?
6. Setelah kerusakan diperbaiki dan komputer secara operasional bisa digunakan, maka langkah berikutnya adalah menentukan cara/solusi yang tepat untuk mencegah masalah tersebut timbul lagi. Bagaimana solusi

yang tepat untuk mengantisipasi sumber masalah tersebut agar tidak terjadi di kemudian waktu?

### C. BATASAN MASALAH

Dari beberapa hal yang telah dirumuskan di atas dapat ditarik beberapa masalah pokok yang akan kami bahas, yaitu :

1. Identifikasi dan analisa sebab-akibat masalah kerusakan sistem operasi Windows XP yang disebabkan oleh VCD yang didalamnya terdapat *malware* dalam bentuk *batch program* yang cara kerjanya memanfaatkan fasilitas *autorun* pada Windows XP.
2. Penanganan *malware* berupa *batch program* dalam bentuk file berekstensi *\*.cmd* yang memanfaatkan fasilitas *autorun* pada Windows XP menggunakan aplikasi yang kami buat.
3. Aplikasi recovery dan pencegahan terhadap *malware autorun* menggunakan bahasa pemrograman Visual Basic yang cara kerjanya memanfaatkan fungsi dan kemampuan *system registry* pada Windows XP.

### D. TUJUAN PENELITIAN

Penelitian dalam rangka penyusunan Skripsi ini memiliki Tujuan Primer sebagai tujuan utama jangka pendek dan Tujuan Sekunder sebagai tujuan tambahan jangka panjang.

#### D.1. TUJUAN PRIMER

Adapun tujuan primer dalam rangka penyusunan skripsi ini adalah sebagai berikut:

1. Memperoleh derajat Sarjana (S1) pada jurusan Sistem Informasi di STMIK AMIKOM Yogyakarta.
2. Menyelesaikan mata kuliah wajib Skripsi dengan kredit sebanyak 6 (enam) SKS untuk dapat menyelesaikan kuliah sehingga dapat mengikuti Wisuda kelulusan pendidikan Sarjana.

Membuktikan hipotesis bahwa ada sesuatu (*program, script, virus, dsb.*) dalam VCD yang kami jadikan sebagai objek penelitian yang dapat menghilangkan file dan merusak sistem operasi pada komputer.

#### D.2. TUJUAN SEKUNDER

Adapun tujuan sekunder penyusunan skripsi ini adalah sebagai berikut:

1. Membantu masyarakat untuk mencari dan menyajikan solusi yang efektif dan efisien untuk permasalahan pada komputer mereka.
2. Mencari solusi suatu masalah (komputer) yang belum pernah dibahas orang lain dan atau sudah pernah dibahas tetapi belum disajikan secara tuntas.
3. Berlatih menentukan solusi dari suatu masalah (komputer) dengan cara merunut suatu kejadian mulai dari sumber permasalahan, proses terjadinya masalah, akibat yang ditimbulkan, penanganan akibat, dan menentukan tindakan antisipatif untuk mencegah terjadinya masalah serupa di lain waktu.

#### E. MANFAAT PENELITIAN

Ada beberapa manfaat yang dapat diambil dari penelitian ini, antara lain sebagai berikut :

1. Diketahui salah satu media perusak sistem operasi komputer melalui beberapa *script* sederhana yang dapat mengakibatkan kerusakan sistem

komputer secara integral (merusak konfigurasi sistem operasi sekaligus menghilangkan file sistem dan file-file pada direktori tertentu).

2. Teratasinya masalah pada sistem operasi Windows XP yang ditimbulkan *malware* yang proses kerjanya memanfaatkan fasilitas *autorun* (pada sistem operasi Windows) dalam bentuk *batch* program khususnya yang kami jadikan sebagai objek penelitian.
3. Dapat dicegahnya masuknya *malware* lain yang cara kerjanya memanfaatkan *autorun* pada sistem operasi Windows XP dengan membatasi fasilitas *autorun* melalui pengaturan registry sistem pada Windows XP.

#### **F. METODE PENELITIAN**

Metode yang digunakan untuk mengumpulkan berbagai materi baik itu data maupun fakta dalam penelitian ini adalah sebagai berikut :

##### **1. Metode Pengamatan Langsung**

Mengamati obyek penelitian yaitu VCD (yang diduga dapat merusak integrasi sistem komputer) secara langsung beserta pengamatan isi/materi yang terdapat di dalamnya (yang terlihat maupun yang tidak terlihat/*hidden*) dan unit komputer terkait.

##### **2. Metode Wawancara**

Mengadakan percakapan dan identifikasi permasalahan dengan menggali informasi dari nara sumber yang dalam hal ini adalah seorang pelanggan Pusat Pelayanan Komputer (dimana tempat kami bekerja) dengan masalah VCD-nya.

### 3. Metode Referensi

Mencari referensi (arsip, dokumen, literatur, dsb.) yang dapat mendukung pengetahuan untuk membantu proses penelitian dalam bentuk media cetak maupun elektronik.

### 4. Metode Dokumentasi

Mencatat/mendokumentasikan setiap perkembangan penelitian sehingga pengumpulan data hasil penelitian dapat tersusun secara sistematis.

## G. SISTEMATIKA PENULISAN

Secara garis besar isi Skripsi ini dibagi menjadi bab-bab berikut :

### 1. Pendahuluan

Dalam bab ini dibahas tentang latar belakang masalah yang kami gunakan sebagai bahan penelitian dalam Skripsi ini, sekaligus rumusan beberapa masalah yang akhirnya dibatasi pada lingkup pembahasan beberapa masalah pokok yaitu sumber masalah, identifikasi proses, akibat yang ditimbulkan, solusi serta pencegahan agar masalah VCD rusak ini tidak terjadi lagi di lain waktu. Dibahas pula tujuan, manfaat, metode penelitian dan sistematika penulisan/garis besar uraian materi dalam setiap bab yang disajikan.

### 2. Dasar Teori

Diuraikan beberapa materi pokok yang berkaitan dengan permasalahan yang dimaksud yaitu tentang VCD sebagai media penyimpanan beserta materi yang ada di dalamnya, Sistem Operasi *Microsoft Windows XP* mulai cara kerja terhadap media penyimpanan khususnya VCD hingga

celah keamanan yang menyebabkan terjadinya permasalahan tersebut di atas. Serta materi dasar yang digunakan untuk membuat aplikasi untuk menangani masalah yang dimaksud dalam Bab 1, mulai dari bahasa pemrograman yang dipakai sampai *software* yang digunakan untuk membuat aplikasi.

### 3. Analisis dan Perancangan Aplikasi

Identifikasi obyek penelitian (VCD beserta isi di dalamnya dan unit komputer terkait) serta analisis sebab-akibat dari sudut pandang VCD dan atau sistem komputer sehingga dapat dipergunakan untuk memecahkan masalah dengan didukung referensi dari luar obyek penelitian sehingga hipotesis bahwa ada sesuatu (*software, malware, virus, dsb.*) dalam VCD yang dapat menghilangkan data dan merusak sistem operasi pada komputer dapat terbukti.

Perancangan aplikasi menggunakan bahasa pemrograman yang telah dikemukakan pada Bab 2, mulai penanganan sampai pencegahan masalah yang dimaksud dalam Bab 1.

### 4. Pembahasan

Pemaparan hasil identifikasi dari tahapan penelitian, mulai dari sumber masalah yaitu *malware* dalam bentuk *Windows NT Command Script* yang sengaja disusupkan di dalam VCD, identifikasi *malware* tersebut dari cara kerja sampai proses direspon oleh komputer yang bersangkutan, hasil analisis sebab-akibat yang ditimbulkan oleh proses perusakan yang disebabkan oleh *malware* tersebut hingga penentuan solusi

penanganan/perbaikan dan tindakan antisipatif terhadap *malware* sejenis dalam bentuk *application tools*.

#### 5. Penutup

Kesimpulan yang didasarkan pada pembuktian hipotesis bahwa ada sesuatu (*software, malware, virus, dsb.*) dalam VCD yang dapat menghilangkan data dan merusak sistem operasi pada komputer, dengan analisis yang obyektif dan diperkuat dengan bukti-bukti hasil penelitian.

Beberapa saran terhadap pengguna komputer dan pembaca yang berkaitan dengan keamanan sistem komputer.

