

**PEMBUATAN APLICATION TOOLS UNTUK MENGATASI  
MALWARE PADA VCD**

**SKRIPSI**



**YHONY AGUS SETYA MAHENDRA**

**NIM. 03.12.0498**

**JURUSAN SISTEM INFORMASI  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

**“AMIKOM”**

**YOGYAKARTA**

**2009**

**PEMBUATAN APLICATION TOOLS UNTUK MENGATASI  
MALWARE PADA VCD**

**SKRIPSI**

Disusun sebagai salah satu syarat untuk memperoleh  
derajat Sarjana S1 pada jurusan Sistem Informasi



**YHONY AGUS SETYA MAHENDRA**

**NIM. 03.12.0498**

**JURUSAN SISTEM INFORMASI**

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

**“AMIKOM”**

**YOGYAKARTA**

**2009**

**HALAMAN PERSETUJUAN**


**PEMBUATAN APLICATION TOOLS UNTUK MENGATASI  
MALWARE PADA VCD**

**SKRIPSI**

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh derajat Sarjana (S1) pada jurusan Sistem Informasi Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Disetujui oleh :

Dosen Pembimbing,



**( ARIEF SETYANTO, S.Si, MT )**

## HALAMAN PENGESAHAN

Skripsi dengan judul “PEMBUATAN APLICATION TOOLS UNTUK MENGATASI MALWARE PADA VCD” ini telah dipertahankan di depan Dewan Penguji Skripsi pada :

Hari : JUM'AT  
Tanggal : 16 OKTOBER 2009  
Tempat : RUANG SIDANG SKRIPSI / TA PIXEL

Dewan Penguji :

TTD:

Penguji I,

  
( **HERI SISMORO, M.Kom** )

Penguji II,

  
( **KUSRINI, M.Kom** )

Penguji III,

  
( **SUDARMAWAN, MT** )

Mengesahkan,



**KETUA STMIK AMIKOM  
YOGYAKARTA**

  
( **Prof. Dr. M. SUYANTO, MM** )

## KATA PENGANTAR

Pada Era Informasi seperti sekarang ini banyak bermunculan berbagai macam teknologi informasi yang dalam pemanfaatannya kadangkala dipersalahkan oleh pihak-pihak tertentu. Salah satu contohnya adalah VCD yang dijual di masyarakat pada akhir-akhir ini yang dapat merusak data dan Sistem Operasi pada komputer.

Maka dari itu, kami panjatkan puji syukur kepada Allah SWT. atas segala rahmat-Nya kami dapat menyusun skripsi dengan judul **“PEMBUATAN APLICATION TOOLS UNTUK MENGATASI MALWARE PADA VCD”** berikut ini sebagai salah satu syarat untuk memperoleh derajat Sarjana (S1) pada jurusan Sistem Informasi STMIK AMIKOM Yogyakarta.

Dan dalam kesempatan ini tidak lupa kami sampaikan terima kasih kepada beberapa pihak yang telah membantu dalam penyusunan skripsi ini, di antaranya adalah sebagai berikut :

1. M. Suyanto, Prof., Dr., MM, selaku Ketua STMIK AMIKOM Yogyakarta yang telah berkenan mengesahkan Skripsi ini.
2. Arief Setyanto, S.Si, MT, selaku Dosen Pembimbing dalam penyusunan Skripsi ini; dan
3. Semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat kami sebutkan seluruhnya.

Kami susun skripsi ini sedemikian rupa sesuai dengan pedoman pembuatan Skripsi yang kami ketahui. Kemudian apabila terdapat kekurangan kami harap tanggapan dan masukan yang bersifat positif dari semua pihak.

Demikian pengantar yang dapat kami sampaikan, semoga Skripsi ini dapat bermanfaat bagi kami dan pihak-pihak yang berkepentingan.

Yogyakarta, Agustus 2008

Penyusun,

**YHONY AGUS SETYA MAHENDRA**  
NIM. 03.12.0498

## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN .....	ii
HALAMAN PENGESAHAN .....	iii
KATA PENGANTAR .....	iv
DAFTAR ISI .....	vi
DAFTAR TABEL .....	xi
DAFTAR GAMBAR .....	xiii
INTISARI .....	xiv
ABSTRACT .....	xv
<b>BAB I    PENDAHULUAN</b>	
A. Latar Belakang Masalah .....	1
B. Rumusan Masalah .....	2
C. Batasan Masalah .....	4
D. Tujuan Penelitian .....	4
D.1. Tujuan Primer .....	4
D.2. Tujuan Skunder .....	5
E. Manfaat Penelitian .....	5
F. Metode Penelitian .....	6
G. Sistematika Penulisan .....	7
<b>BAB II    LANDASAN TEORI</b>	
A. Perangkat Keras .....	10

A.1. Personal Komputer .....	10
A.2. Media Penyimpanan .....	13
A.2.a. Hardisk .....	13
A.2.b. Compact Disk .....	15
B. Perangkat Lunak .....	18
B.1. Sistem Operasi .....	19
B.1.a. Microsoft Windows XP .....	20
B.1.b. MS-DOS .....	23
B.1.c. Booting .....	24
B.1.d. Sistem File .....	28
B.1.e. Sistem Registry .....	36
B.2. Malware .....	40
B.2.a. Bacteria .....	41
B.2.b. Logic Bomb .....	42
B.2.c. Trapdoor .....	42
B.2.d. Trojan Horse .....	43
B.2.e. Virus .....	44
B.2.f. Worm .....	45
B.3. Bahasa Pemrograman .....	46
B.3.a. Microsoft Visual Basic 6.0 .....	46
B.3.b. Dasar Pemrograman Visual Basic 6.0 .....	50
B.3.c. MS-DOS Based Program .....	68

### BAB III ANALISIS OBJEK PENELITIAN

A. Deskripsi Permasalahan .....	70
---------------------------------	----



A.1.	Identifikasi Objek Penelitian .....	70
A.1.a.	Identifikasi Sumber Masalah pada VCD .....	70
A.1.b.	Identifikasi Sumber Masalah pada PC .....	81
A.2.	Proses Interaksi Malware dan Komputer .....	83
A.2.a.	Interaksi Malware dengan Komputer PC .....	83
A.2.b.	Akibat-akibat yang ditimbulkan Malware .....	87
B.	Rancangan Solusi .....	88
B.1.	Langkah-langkah Recovery Ketika Terjadi .....	88
B.1.a.	Solusi Manual .....	89
B.1.b.	Rancangan Recovery Tools .....	94
B.2.	Langkah-langkah Pencegahan Sebelum Terjadi .....	97
B.2.a.	Pencegahan Manual .....	98
B.2.b.	Rancangan Protection Tools .....	100
<b>BAB IV</b>	<b>HASIL DAN PEMBAHASAN</b>	
A.	Struktur Aplikasi .....	103
A.1.	Recovery Tools .....	103
A.1.a.	Export Registry .....	104
A.1.b.	Delete Registry .....	104
A.1.c.	Add Registry .....	104
A.1.d.	Laporan Perbaikan .....	104
A.1.e.	Konfirmasi dan Instruksi Keluar Program .....	105
A.2.	Protection Tools .....	105
A.2.a.	Aktivasi Disable Autorun .....	105
A.2.b.	Aktivasi Disable Command Prompt .....	107

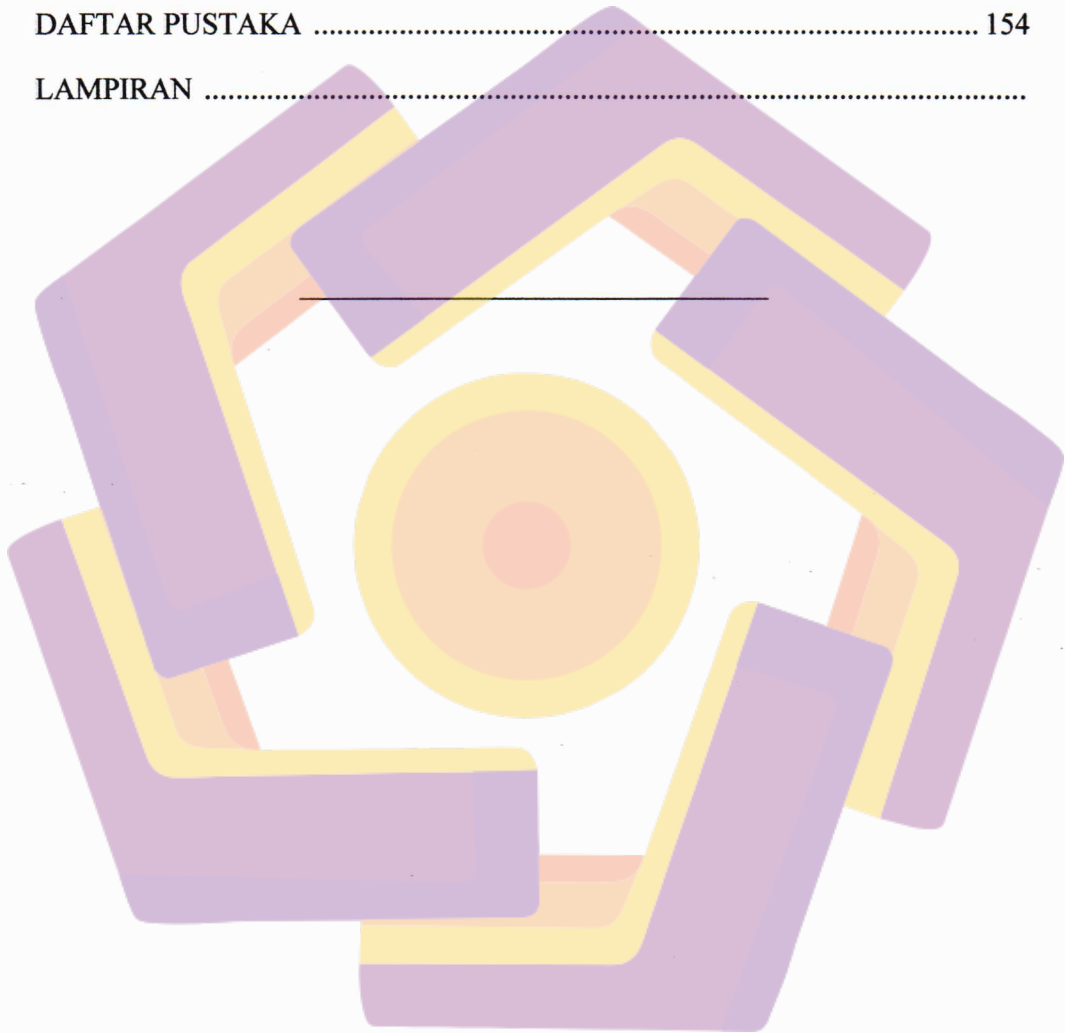
A.2.c. Daftar Pilihan Tipe Drive dan Pembatasan Command Prompt .....	108
A.2.d. Tombol Perintah Execute .....	109
A.2.e. Tombol Perintah Restore .....	115
A.2.f. Tombol Select All, Clear All, dan About .....	117
B. Pengujian Tools .....	122
B.1. Recovery Tools .....	122
B.1.a. Export Registry .....	122
B.1.b. Delete Registry .....	123
B.1.c. Add Registry .....	123
B.1.d. Laporan Perbaikan .....	124
B.1.e. Konfirmasi dan Instruksi Keluar Program .....	124
B.2. Protection Tools .....	126
B.2.a. Aktivasi Disable Autorun .....	126
B.2.b. Aktivasi Disable Command Prompt .....	127
B.2.c. Daftar Pilihan Tipe Drive dan Pembatasan Command Prompt .....	127
B.2.d. Perintah Execute .....	129
B.2.e. Perintah Restore .....	130
B.2.f. Perintah Select All, Clear All, dan About .....	131
C. Pembahasan Program .....	132
C.1. Recovery Tools .....	133
C.2. Protection Tools .....	136
D. Petunjuk Penggunaan .....	142
D.1. Recovery Tools .....	142
D.2. Protection Tools .....	144

**BAB V PENUTUP**

A. Kesimpulan ..... 150  
B. Saran ..... 151

DAFTAR PUSTAKA ..... 154

LAMPIRAN .....



## DAFTAR TABEL

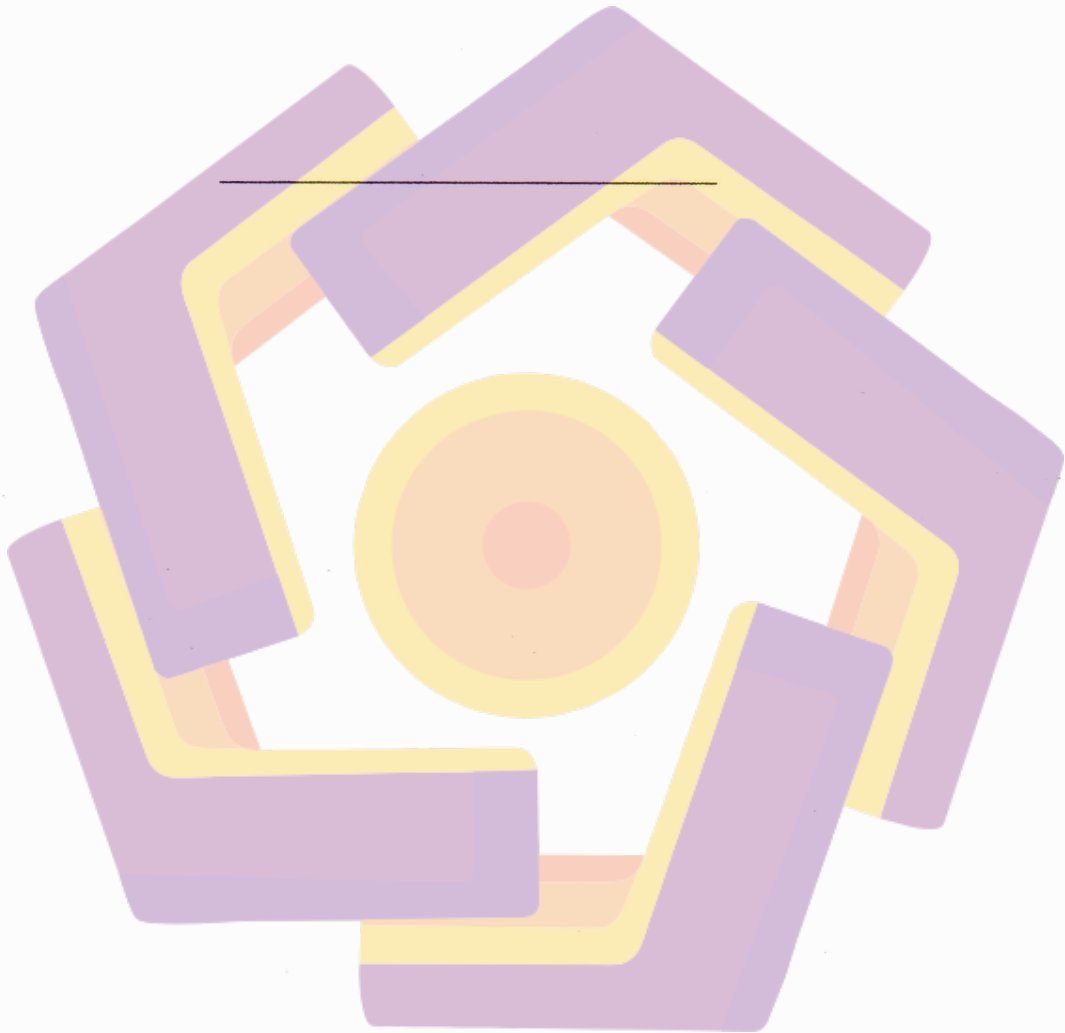
Tabel 2.1. Contoh Tipe File dan Ekstensinya .....	33
Tabel 2.2. Perbandingan Windows Explorer dengan Regedit .....	37
Tabel 2.3. Operator Aritmatika .....	58
Tabel 2.4. Operator Pembanding .....	59
Tabel 2.5. Operator Logika .....	59
Tabel 2.6. Tabel Kebenaran (Logika).....	59
Tabel 4.1. Daftar Pilihan pada Combo Box Berdasarkan Daftar Index .....	109
Tabel 4.2. Data Registry yang Dimasukkan Berdasarkan Pilihan Fitur pada Program .....	115
Tabel 4.3. Data Registry yang Dimasukkan pada Proses Tombol Perintah Restore .....	117
Tabel 4.4. Daftar Variabel Program Beserta Deskripsi dan Isi dari Masing-masing Variabel .....	121
Tabel 4.5. Daftar Pengujian Fasilitas Export Registry pada Recovery Tools ..	122
Tabel 4.6. Daftar Pengujian Fasilitas Delete Registry pada Recovery Tools ...	123
Tabel 4.7. Daftar Pengujian Fasilitas Add Registry pada Recovery Tools .....	123
Tabel 4.8. Daftar Pengujian Fasilitas Laporan Perbaikan pada Recovery Tools .....	124
Tabel 4.9. Daftar Pengujian Fasilitas Konfirmasi dan Instruksi Keluar Program pada Recovery Tools .....	124
Tabel 4.10. Daftar Pengujian Fasilitas Aktivasi Disable Autorun pada Protection Tools .....	126
Tabel 4.11. Daftar Pengujian Fasilitas Aktivasi Disable Command Prompt pada Protection Tools .....	127
Tabel 4.12. Daftar Pengujian Fasilitas Daftar Pilihan Tipe Drive dan Pembatasan Command Prompt pada Protection Tools .....	128
Tabel 4.13. Daftar Pengujian Fasilitas Perintah Execute pada Protection Tools	129

Tabel 4.14. Daftar Pengujian Fasilitas Perintah Select All, Clear All, dan About pada Protection Tools ..... 131

Tabel 4.15. Objek-objek Penting dalam Program ..... 139

Tabel 4.16. Parameter-parameter dalam Prosedur setReg ..... 140

Tabel 4.17. Penjelasan Bagian Program Protection Tools ..... 145



## DAFTAR GAMBAR

Gambar 2.1.	Ilustrasi Bagian Fisik Komputer Secara Umum .....	12
Gambar 2.2.	Hubungan Sistem Operasi dengan Pengguna .....	19
Gambar 2.3.	Penempatan File Pada Struktur Direktori .....	29
Gambar 2.4.	Struktur registry dalam Regedit .....	38
Gambar 2.5.	Tampilan IDE Microsoft Visual Basic 6.0 .....	48
Gambar 2.6.	Flowchart Proses If Then Else .....	63
Gambar 2.7.	Flowchart Proses Do Loop .....	64
Gambar 2.8.	Tampilan Command Prompt Window .....	68
Gambar 3.1.	Tampilan Isi VCD pada Windows Explorer .....	70
Gambar 3.2.	Tampilan Isi VCD pada Windows Explorer setelah Proses “Show Hidden Files and Folder” .....	72
Gambar 3.3.	Tampilan Hasil Eksekusi file “auto.cmd” .....	84
Gambar 3.4.	Tampilan hasil eksekusi file “shutdown.exe” pada Sistem Operasi Windows XP SP1 (atas) dan SP2 (bawah) .....	86
Gambar 3.5.	Flowchart Recovery Tools .....	95
Gambar 3.6.	Modifikasi salah satu key pada Registry System .....	100
Gambar 3.7.	Flowchart Protection Tools .....	101
Gambar 4.1.	Fasilitas Aktivasi Disable Autorun .....	105
Gambar 4.2.	Fasilitas Aktivasi Disable Command Prompt .....	107
Gambar 4.3.	Fasilitas Tombol Perintah Execute .....	110
Gambar 4.4.	Fasilitas Tombol Perintah Restore .....	115
Gambar 4.5.	Fasilitas Tombol Perintah Select All, Clear All, dan About .....	117
Gambar 4.6.	Tampilan Form About .....	120

## INTISARI

Permasalahan pendistribusian *malware* melalui VCD sangatlah merugikan bagi pengguna komputer, khususnya VCD dengan label “Om Sera” yang kami jadikan sebagai objek penelitian. *Malware* yang kami maksud di sini adalah *malware autorun* yang terdapat pada VCD yang kami jadikan objek penelitian. Berdasarkan kasus sistem komputer yang kacau setelah dimasukkan VCD di atas ke dalam komputer, hal ini mengindikasikan bahwa di dalam VCD tersebut terdapat sesuatu/program yang bersifat merusak/mengacaukan sistem dan tentu saja hal ini memiliki faktor kesengajaan dari produsen atau penerbit VCD tersebut dengan tujuan yang implisit dengan banyak kemungkinan. Karena kemungkinan besar yang dituju adalah pengguna komputer, karena file yang disembunyikan tersebut hanya akan aktif sebagai *malware* apabila VCD dimasukkan ke dalam komputer khususnya yang menggunakan sistem operasi Windows XP.

Barisan perintah merusak yang terdapat dalam VCD tersebut yang kami sebut sebagai *malware* dapat aktif karena bantuan file yang berfungsi sebagai *shortcut* (pintasan) yang memanfaatkan fasilitas *Autorun* pada Sistem Operasi, yang dalam penelitian ini terbatas pada Sistem Operasi Windows XP. File *shortcut* tersebut adalah file *autorun.inf* bertugas memanggil file *auto.cmd* yang merupakan sebuah file *batch* dengan barisan perintah untuk mengacaukan sistem.

Sebagai tindak lanjutnya, kami buat dua buah program sederhana yang dapat membantu mengatasi permasalahan di atas. Kedua program tersebut kami sebut sebagai *Recovery Tools* dan *Protection Tools*. *Recovery Tools* berfungsi untuk mengembalikan konfigurasi sistem yang rusak khususnya yang diakibatkan oleh *malware* dari dalam VCD tersebut, sedangkan *Protection Tools* berfungsi memasukkan konfigurasi pada sistem dengan tujuan mencegah terjadinya perusakan yang dilakukan oleh *malware* sejenis di waktu yang akan datang.

## ABSTRACT

Distribution of malware through VCD was very harmful for computer user, especially VCD that we use as object in this research. Based on those computer systems have intruded after VCD inserted to it, this case indicated that the VCD contains a harmful program file or more and of course it have intention factor by producer or publisher of the VCD with implicit purposes and many probability. Possibly such targets are computer users, because the hidden files will just activated if VCD inserted to the computer especially in Windows XP operating system.

The harmful command-line included in the VCD that called as malware can activated by an autorun file as a shortcut through Autorun feature in operating system, especially operating system that known as Windows XP. The shortcut file that talked about is the file named "autorun.inf" which ordered to call file named "auto.cmd" is a batch file that contains command line for harm the system.

As its follow, we design two simple programs that can help to handle those problems. They called as "Recovery Tools" and "Protection Tools". Recovery Tools used for overcome the damage because of malware from the VCD in this case by returning the broken system configuration, and then Protection Tools used for input some configuration to the system to prevent those problems by the same kind of malware later.