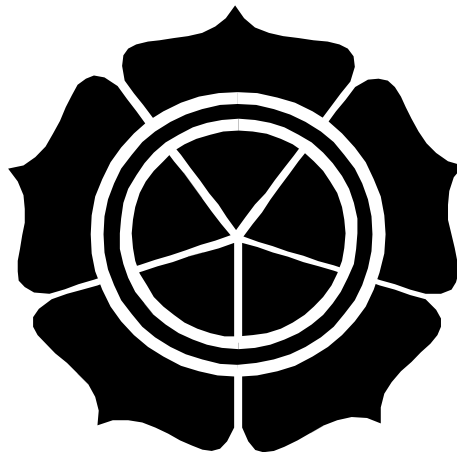


**ANALISIS PENYEBARAN VIRUS ZODIAK.EXE
TERHADAP SISTEM OPERASI
WINDOWS XP**

SKRIPSI

**Diajukan Guna Memenuhi Persyaratan
Untuk Memperoleh Gelar Sarjana Teknik Informatika**



Disusun oleh :

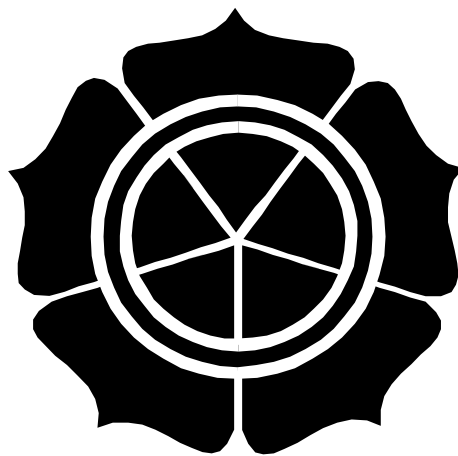
**ABD. BASITH
02.11.0033**

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
STMIK “AMIKOM” YOGYAKARTA**

2007

**ANALISIS PENYEBARAN VIRUS ZODIAK.EXE
TERHADAP SISTEM OPERASI
WINDOWS XP**

SKRIPSI



Disusun oleh :

ABD. BASITH
02.11.0033

**PROGRAM STRATA-1
JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
STMIK "AMIKOM" YOGYAKARTA**

2007

HALAMAN PENGESAHAN

**ANALISIS PENYEBARAN VIRUS ZODIAK.EXE
TERHADAP SISTEM OPERASI
WINDOWS XP**

Diajukan Sebagai Syarat Menyelesaikan Jenjang Starta-1

Jurusan Teknik Informatika

STMIK "AMIKOM" Yogyakarta

Diajukan oleh:

ABD. BASITH
02.11.0033

Mengetahui:

Disetujui dan Disahkan oleh :

Ketua STMIK "AMIKOM"

Diperiksa dan Disetujui oleh :

Dosen Pembimbing

Drs. Muhammad Suyanto, MM

Kusrini, M.Kom

HALAMAN BERITA ACARA

**ANALISIS PENYEBARAN VIRUS ZODIAK.EXE
TERHADAP SISTEM OPERASI
WINDOWS XP**

Diajukan Sebagai Syarat Menyelesaikan Jenjang Starta-1

Jurusan Teknik Informatika

STMIK "AMIKOM" Yogyakarta

Telah dipresentasikan dan dipertahankan di depan pengju:

Pada hari : Sabtu

Tanggal : 03 Maret 2007

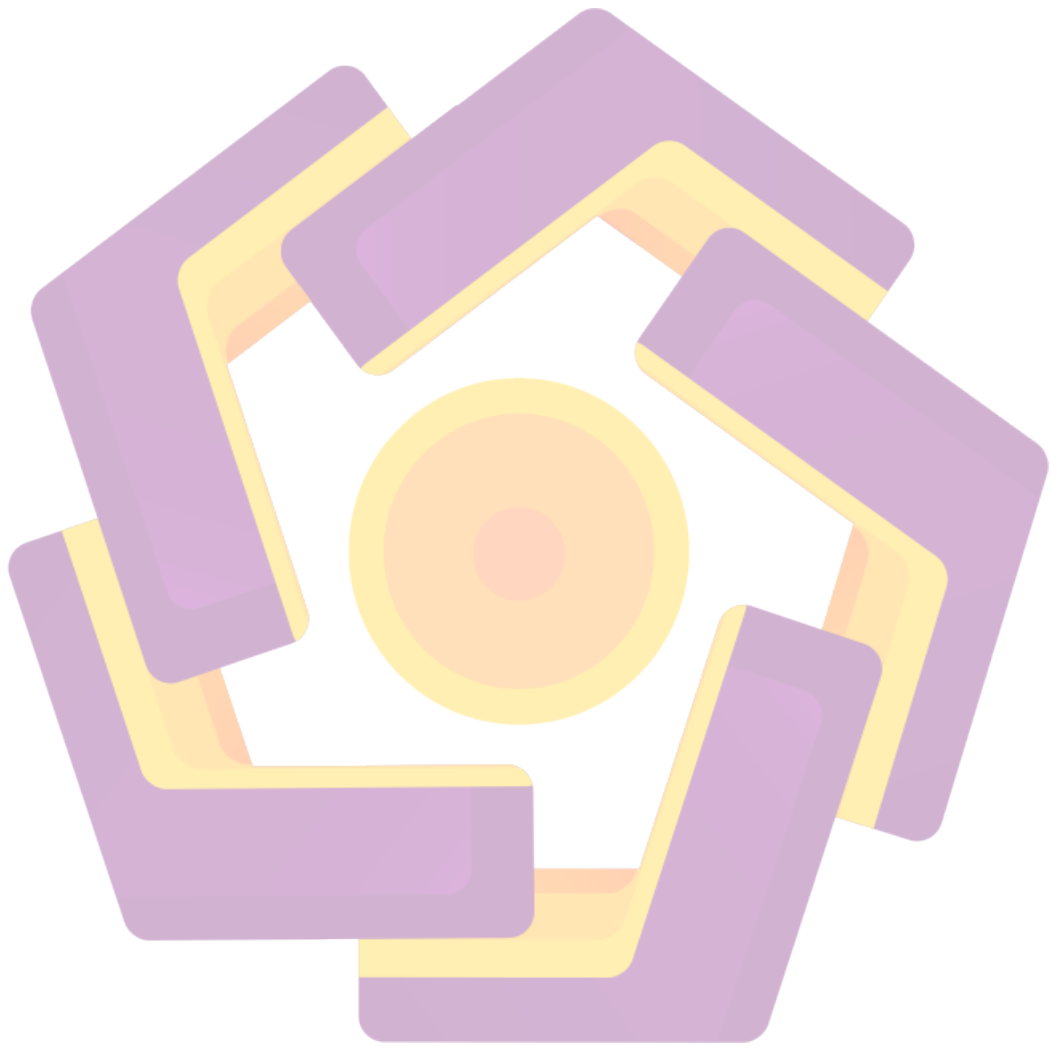
Jam : 08.30 WIB

Tempat : Kampus Terpadu Condong Catur

Tim Penguji

Tanda Tangan

1. Kusrini, M.Kom
2. Emma Utami, M.Si
3. Heri Sismoro, M.Kom



KATA PENGANTAR

Puji dan Syukur penulis panjatkan kehadirat ALLAH SWT serta kepada junjungan kita Nabi Besar Muhammad SAW yang telah melimpahkan Rakhmat dan Hidayahnya sehingga penyusun dapat menyelesaikan Skripsi.

Skripsi ini disusun guna memenuhi syarat memperoleh gelar Sarjana pada Program Starta-1 Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Pada kesempatan ini penyusun ingin menyampaikan terima kasih kepada:

1. Allah SWT atas segala Karunia dan Hidayah-Nya sehingga penulis dapat menyelesaikan Skripsi ini.
2. Bapak dan Ibu yang selalu mendoakan dan membimbing anak-anaknya
3. Bapak Drs. Muhammad Suyanto, selaku ketua STMIK "AMIKOM" Yogyakarta.
4. Ibu Kusrini, M.Kom. selaku dosen pembimbing Skripsi ini.
5. Semua pihak yang telah membantu, baik materiil maupun spiritual yang tidak dapat Penulis sebutkan satu persatu, semoga apa yang telah diberikan merupakan amalan baik.

Penyusun menyadari sepenuhnya bahwa penyusunan Skripsi ini masih jauh dari kesempurnaan, oleh sebab itu, penyusun mengharapkan kritik dan saran yang bersifat konstruktif demi kesempurnaan Skripsi ini, sehingga dapat bermanfaat bagi penulis, serta pihak-pihak yang membutuhkannya.

Yogyakarta, Februari 2007

Penyusun

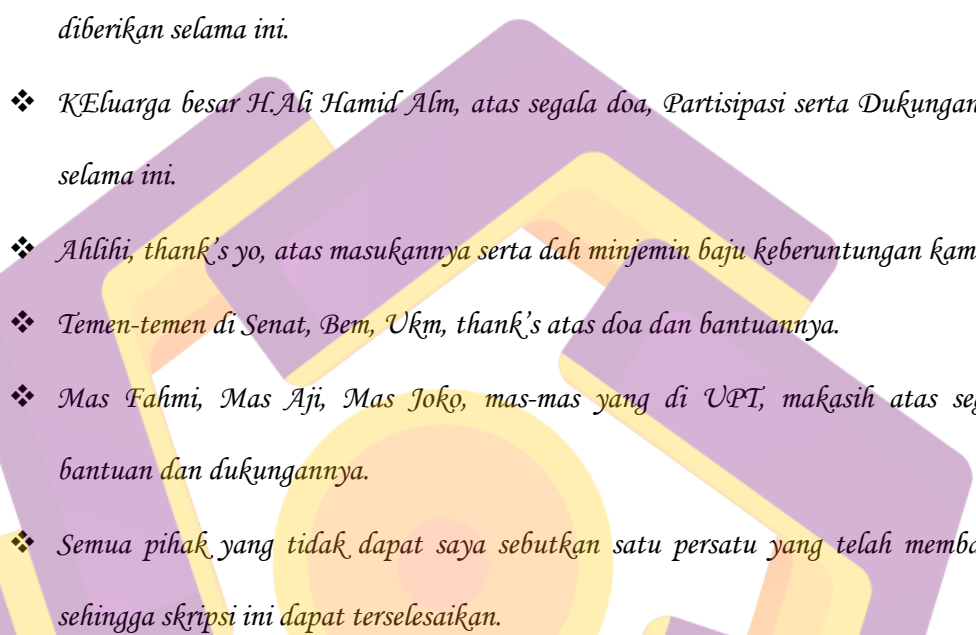
MOTTO

- ❖ *Barang siapa ditanya tentang suatu ilmu lalu merahasiakannya maka dia akan datang pada hari kiamat dengan kendali (di mulutnya) dari api neraka (HR. Abu Dawud)*
- ❖ *Barang siapa memanggakan dirinya sendiri dan berjalan dengan angkuh maka dia akan menghadap Allah dan Allah murka kepadanya. (HR. Ahmad)*
- ❖ *Kau mungkin saja kecewa jika percobaanmu gagal, tetapi kau pasti takkan berhasil jika tidak mencoba. (Beverly Sills)*
- ❖ *Hal yang benar-benar kauyakini pasti akan selalu terjadi, dan keyakinan akan suatu hal menyebabkannya terjadi. (Frank Lloyd Wright)*
- ❖ *Jika kau menginginkan kebahagiaan... Untuk sejam, tidurlah selama itu. Untuk sehari, pergilah memancing. Untuk sebulan, menikahlah. Untuk setahun, warisi harta. Untuk seumur hidup, tolonglah orang lain. (Peribahasa cina, Chicken Soup For The Soul)*
- ❖ *Teman sejati merupakan karunia terbesar dan yang paling sedikit kita pikirkan untuk memperolehnya. (Francois, Duc de La Rochefoucauld)*

PERSEMBAHAN

Dengan mengucapkan puji syukur Alhamdulillah atas segala Rahmat dan HidayahNya, maka izinkan Kupersembahkan Skripsi ini kepada :

- ❖ Bapak dan Ibu tercinta, Terima kasih atas segala doa, kasih sayang, dukungan, Pengorbanan serta Support yang tiada hentinya selama ini.
- ❖ Lato Congge dan Mayo', makasih ya atas doanya selama ini.
- ❖ My Sweet Heart Zara Yunizar, Thanks ya say...., atas segala doa, Pengertian, pengorbanan, serta dukungan dan Support tiada hentinya sehingga Mamas dapat menyelesaikan Skripsi ini, Harapan dan Doa Mamas semoga sayang cepat menyelesaikan Skripsi juga, Amin.
- ❖ Abah dan mama, makasih atas doa dan dukungannya selama ini.
- ❖ Ibu Kusri, M.Kom. Terima kasih atas segala bimbingan dan masukan yang diberikan selama proses penyelesaian Skripsi ini.
- ❖ Om-om dan Tante-tante ku yang tercinta, yang tak dapat Itte sebutkan satu persatu, Makasih ya atas doa serta dukungannya selama ini, terutama Om muddin dan Tante Lia, makasih ya Om, Nte, atas semua masukannya selama mengerjakan Skripsi ini.
- ❖ Om Aji dan Mbu thank's ya atas doa, dukungan, bantuan serta supportnya selama ini
- ❖ Adik-adikku yang ku sayangi, terutama appe, Lisa, Amir thank's ya atas doa, dukungan, serta supportnya selama ini.
- ❖ Abba, Assa, Wiwi, Iting, De'Dian, Iyong, Puput, thank's ya atas doa dan pengertiannya selama ini.

- 
- ❖ *Rolis, Joko, Anton serta teman-teman Bododotcom, thank's atas bantuan, doa serta dukungannya.*
 - ❖ *Tim KRI 2007 Pak Rustom, Pak Emha, Pak Andi Sunyoto, Heri, Naskah, Eddy, Nizar, Sabar, thank's ya atas doa serta dukungannya serta Pengertian yang diberikannya selama ini.*
 - ❖ *Keluarga besar H. Ali Hamid Alm, atas segala doa, Partisipasi serta Dukungannya selama ini.*
 - ❖ *Ahlilahi, thank's yo, atas masukannya serta dah minjemin baju keberuntungan kamu.*
 - ❖ *Teman-teman di Senat, Bem, Ukm, thank's atas doa dan bantuannya.*
 - ❖ *Mas Fahmi, Mas Aji, Mas Joko, mas-mas yang di UPT, makasih atas segala bantuan dan dukungannya.*
 - ❖ *Semua pihak yang tidak dapat saya sebutkan satu persatu yang telah membantu sehingga skripsi ini dapat terselesaikan.*

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN.....	ii
HALAMAN BERITA ACARA.....	iii
KATA PENGANTAR	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xiii
BAB I : PENDAHULUAN.....	1
A. Latar Belakang Masalah.....	1
B. Perumusan Masalah	3
C. Batasan Masalah.....	3
D. Tujuan dan Manfaat	4
E. Metode Penelitian.....	5
F. Sistematika Penulisan	6
BAB II : DASAR TEORI	8
A. Definisi Virus	8
A.1. Sejarah Virus Komputer.....	10
A.2. Perkembangan Virus dari Tahun ke Tahun.....	12
A.3. Kriteria Virus.....	17
A.4. Siklus Hidup dan Komponen Virus	20
A.5. Jenis – jenis Virus	22
A.5.1. Berdasarkan Teknik Pembuatannya	23
A.5.2. Berdasarkan Infeksi yang Dilakukan	24

A.5.3. Berdasarkan Media Penyebarannya	26
B. Pengenalan Sistem Operasi Windows.....	27
B.1. Definisi Sistem Operasi.....	27
B.2. Fungsi Dasar Sistem Operasi	28
B.3. Tujuan Mempelajari Sistem Operasi	29
B.4. Sasaran Sistem Operasi	29
B.5. Sejarah Sistem Operasi.....	30
C. Pengenalan Registry Windows	31
C.1. Definisi Registry Windows	31
C.2. Memahami Struktur Registry	33
C.2.1. Perbandingan Struktur Registry dengan Windows Explorer.....	33
C.2.2. Bagian Registry dan Fungsinya.....	34
D. Pengenalan Visual Basic	38
D.1. Sejarah Microsoft Visual Basic 6.0.....	39
D.2. Konsep Kerja Visual Basic 6.0	41
D.3. Kelebihan dan Kekurangan Microsoft Visual Basic 6.0	42
D.4. Komponen Visual Basic 6.0	43
D.2. Versi - versi Visual Basic 6.0.....	45
E. Penyebaran dan Penanggulangan Virus.....	46
E.1. Penyebaran Virus.....	46
E.2. Pencegahan dan Penanggulangan Virus	48
F. Teknik dan Langkah – langkah Melindungi Komputer dari Virus	50
BAB III : ANALISIS DAN PERANCANGAN PROGRAM PENDETEKSI VIRUS.....	56
A. Definisi Virus Zodiak.exe	56

B. Penyebaran Virus Zodiak.exe	56
C. Mendeteksi Penyebaran Virus Zodiak.exe.....	65
D. Mengatasi Penyebaran Zirus Zodiak.exe	67
E. Perencanaan Pembuatan Program Removal Virus	
Zodiak.exe.....	73
E.1. Hasil Analisa yang Didapat	73
E.2. Implementasi Program.....	76
BAB IV : HASIL DAN PEMBAHASAN	77
A. Pembahasan Program	77
A.1. Fasilitas AntiZod.exe Remover.....	77
A.2. Cara Penggunaan.....	78
B. Uji Coba Program	79
BAB V : PENUTUP	84
A. Kesimpulan	84
B. Saran.....	85
DAFTAR PUSTAKA	87
LAMPIRAN.....	89

DAFTAR GAMBAR

GAMBAR 2.1 TAMPILAN VIRUS CRETAION LAB (VCL)	15
GAMBAR 2.2 TAMPILAN AWAL SEBELUM MEMULAI REGEDIT	32
GAMBAR 2.3 TAMPILAN AWAL JENDELA REGISTRY EDITOR	33
GAMBAR 2.4 TAMPILAN MICROSOFT VISUAL BASIC 6.0.....	43
GAMBAR 2.5 PROCESS EXPLORER DALAM HEX EDIT SEBELUM MODIF	53
GAMBAR 2.6 TAMPILAN PROCESS EXPLORER DALAM HEX EDIT SETELAH MODIF ...	54
GAMBAR 2.7 PROCESS EXPLORER SEBELUM MODIF.....	54
Gambar 2.8 Tampilan process explorer sesudah modif.....	54
Gambar 3.1 Hasil setelah Desktop.ini diaktifkan.....	57
Gambar 3.2 Konfirmasi untuk meng-copy-kan konfirmasi zodiak.reg ke registry.....	58
Gambar 3.3 Tampilan Zodiak.html.....	59
Gambar 3.4 File Startup yang dibuat virus	60
Gambar 3.5 Kondisi Task Manager pasca penyerangan virus	60
Gambar 3.6 Tampilan file admin.html.....	61
Gambar 3.7 Tampilan file ucapanterimakasih.txt.....	62
Gambar 3.8 Pesan eror yang dideteksi oleh cmd.exe.....	62
Gambar 3.9 Tampilan file restart.txt.....	62
Gambar 3.10 Informasi peng-copy-an informasi di zodiac.reg telah sukses	63
Gambar 3.11.a Tampilan registry Editor bagian explorer	63
Gambar 3.11.b Tampilan Registry editor bagian system policies	64
Gambar 3.11.c Tampilan Registry editor bagian system windows.....	64
Gambar 3.12.a Tampilan properties Zodiak.exe.....	66
Gambar 3.12.b Compani zodiac.exe	66
Gambar 4.12.c File versi Zodiak.exe	67
Gambar 3.13 Tampilan run untuk menjalankan perintah anti shutdown/restart...	68
Gambar 3.14 Tampilan awal FreshUI.....	70
Gambar 3.15 Tampilan FreshUI untuk mengaktifkan Regedit.....	70
Gambar 3.16 Tampilan untuk mengaktifkan Regedit.....	71

Gambar 3.17 Tampilan Registry Editor untuk mengaktifkan Task Manager	71
Gambar 3.18 Tampilan awal Hijackthis.....	72
Gambar 3.19 Tampilan Form Removal Zodiak.exe.....	76
Gambar 4.1 Tampilan AntiZod.exe Remover.....	80
Gambar 4.2.a Tampilan Task Manager masih Disable	80
Gambar 4.2.b Tampilan Task Manager sudah diaktifkan	80
Gambar 4.3.a Tampilan Regedit masih Disable.....	81
Gambar 4.3.b Tampilan Regedit sudah diaktifkan.....	81
Gambar 4.4.a Tampilan file startup windows sebelum virus dimatikan.....	81
Gambar 4.4.b Tampilan file startup windows sesudah virus dimatikan	81
Gambar 4.5.a Tampilan Folder Option yang didisable oleh virus	82
Gambar 4.5.b Tampilan Folder Option yang sudah diaktifkan.....	82
Gambar 4.6.a Tampilan pada saat program akan meng-attrib file dengan tujuan drive E:\.....	82
Gambar 4.6.b Tampilan beberapa file yang dirubah attributnya menjadi Super hiden oleh virus	83
Gambar 4.6.c Tampilan beberapa file yang sudah dirubah attributnya menjadi No hiden.....	83

DAFTAR TABEL

Tabel 2.1 Perbandingan Regedit dengan Windows Explorer.....	34
---	----



DAFTAR GAMBAR

Gambar 2.1 Tampilan Virus Cretaiion Lab (VCL).....	14
Gambar 2.2 Tampilan Awal sebelum memulai regedit	32
Gambar 2.3 Tampilan awal jendela Registry Editor	32
Gambar 2.4 Tampilan Microsoft Visual Basic 6.0.....	42
Gambar 2.5 Process explorer dalam hex edit setelah modif.....	53
Gambar 2.6 Tampilan process explorer setelah modif.....	53
Gambar 2.7 Process explorer dalam hex edit sebelum modif.....	42
Gambar 2.8 Tampilan process explorer sebelum modif.....	43
Gambar 3.1 Hasil setelah Desktop.ini diaktifkan.....	55
Gambar 3.2 Konfirmasi untuk meng-copy-kan konfirmasi zodiak.reg ke registry.....	56
Gambar 3.3 Tampilan Zodiak.html.....	57
Gambar 3.4 File Startup yang dibuat virus	58
Gambar 3.5 Kondisi Task Manager pasca penyerangan virus	58
Gambar 3.6 Tampilan file admin.html.....	59
Gambar 3.7 Tampilan file ucapan terimakasih.txt.....	60
Gambar 3.8 Pesan eror yang dideteksi oleh cmd.exe.....	60
Gambar 3.9 Tampilan file restart.txt.....	60
Gambar 3.10 Informasi peng-copy-an informasi di zodiac.reg telah sukses	61
Gambar 3.11.a Tampilan registry Editor bagian explorer	61
Gambar 3.11.b Tampilan Registry editor bagian system policies	62
Gambar 3.11.c Tampilan Registry editor bagian system windows.....	62
Gambar 3.12.1 Tampilan properties Zodiak.exe.....	64
Gambar 3.12.b Compani zodiac.exe	64
Gambar 4.21 File versi Zodiak.exe	65
Gambar 3.13 Tampilan run untuk menjalankan perintah anti shutdown/restart... ..	66
Gambar 3.14 Tampilan awal FreshUI.....	68
Gambar 3.15 Tampilan FreshUI untuk mengaktifkan Regedit.....	68

Gambar 3.16 Tampilan untuk mengaktifkan Regedit.....	69
Gambar 3.17 Tampilan Registry Editor untuk mengaktifkan Task Manager.....	69
Tampilan awal Hijackthis	
Gambar 3.18 Tampilan awal Hijackthis.....	70
Gambar 3.19 Tampilan Form Removal Zodiak.exe.....	74
Gambar 4.1 Tampilan AntiZod.exe Remover.....	78
Gambar 4.2.a Tampilan Task Manager masih Disable.....	78
Gambar 4.2.b Tampilan Task Manager sudah diaktifkan.....	78
Gambar 4.3.a Tampilan Regedit masih Disable.....	79
Gambar 4.3.b Tampilan Regedit sudah diaktifkan.....	79
Gambar 4.4.a Tampilan file startup windows sebelum virus dimatikan.....	79
Gambar 4.4.b Tampilan file startup windows sesudah virus dimatikan.....	79
Gambar 4.5.a Tampilan Folder Option yang didisable oleh virus.....	80
Gambar 4.5.b Tampilan Folder Option yang sudah diaktifkan.....	80
Gambar 4.6.a Tampilan pada saat program akan meng-attrib file dengan tujuan drive E:\.....	80
Gambar 4.6.b Tampilan beberapa file yang dirubah attributnya menjadi Super hiden oleh virus.....	81
Gambar 4.6.c Tampilan beberapa file yang sudah dirubah attributnya menjadi No hiden.....	81

DAFTAR TABEL

Tabel 2.1 Perbandingan Regedit dengan Windows Explorer.....	33
---	----

