

**PERANCANGAN APLIKASI REMOVAL TOOLS UNTUK MENGHAPUS
VIRUS PADA SISTEM OPERASI WINDOWS XP**

SKRIPSI



**disusun oleh
GILANG RAH SATRIA
05.12.1204**

**JURUSAN SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2010**

**PERANCANGAN APLIKASI REMOVAL TOOLS UNTUK MENGHAPUS
VIRUS PADA SISTEM OPERASI WINDOWS XP**

SKRIPSI

disusun dan diajukan untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Sistem Informasi



disusun oleh
GILANG RAH SATRIA
05.12.1204

JURUSAN SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2010

PERSETUJUAN

SKRIPSI

Perancangan Aplikasi Removal Tools Untuk Menghapus Virus Pada Sistem Operasi Windows XP

yang dipersiapkan dan disusun oleh

Gilang Rah Satria

05.12.1204

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 4 Februari 2010

Dosen Pembimbing,



M. Rudyanto Arief, MT

NIK. 190302098

PENGESAHAN

SKRIPSI

Perancangan Aplikasi Removal Tools Untuk Menghapus Virus Pada Sistem Operasi Windows XP

yang dipersiapkan dan disusun oleh

Gilang Rah Satria
05.12.1204

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Februari 2010

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

M. Rudyanto Arief, MT
NIK. 190302098

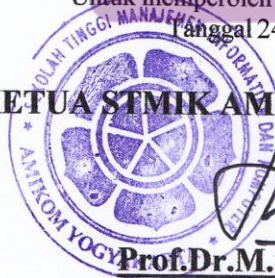
Ema Utami, S.SI, M.Kom
NIK. 190302037

Andi Sunyoto, M.Kom
NIK. 190302052



Skripsi ini telah diterima sebagai salah satu syarat
Untuk memperoleh gelar Sarjana Komputer
tanggal 24 Februari 2010

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suyanto, M.M
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 1 Maret 2010

Tanda tangan



Gilang Rah Satria

HALAMAN PERSEMBAHAN

Puji syukur kepada Allah SWT yang telah memberikan segala karunia-Nya sehingga penulis dapat menyelesaikan Skripsi ini dengan baik. Dalam kesempatan ini, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang turut memberikan dukungan, masukan, semangat dan bantuan hingga selesainya pembuatan Skripsi ini :

1. Kedua orangtuaku bapak dan ibuku tercinta, mas Seto dan Rona yang selalu memberikan yang terbaik bagi saya, terima kasih atas doanya dan dukungannya.
2. Buat Mas Jati and Mba Titiz yang selalu menyemangati ku.
3. Kawan-kawan di kelas S1 SI C angkatan 2005 Riku dan Hada yang telah memperbolehkan ngeprint skripsi memakai printer mereka. Dan kawan-kawan yang lain yang tidak bisa saya sebutkan satu-persatu.
4. Mendho, Zuko dan Icux yang telah membantu dan menyemangati saya dalam menulis skripsi ini.
5. Kawan-kawan komunitas PES dan Winning Baskoro, Alief, Andy, Zul, Kekey, Hamid. Mari kobarkan semangat fairplay dan Pwersiapkan mental kalian untuk menghadapi The Master.
6. Buat lawan bermain Billyard Hada, Rofiq, Andi, Rahman banyak – banyak lah berlatih.

KATA PENGANTAR

Atas Berkat dan Rahmat Allah SWT, yang telah memberikan Rahmat dan Hidayah serta Inayahnya sehingga penulis dapat menyelesaikan Skripsi ini dengan lancar. Dengan judul "PERANCANGAN APLIKASI REMOVAL TOOLS UNTUK MENGHAPUS VIRUS PADA SISTEM OPERASI WINDOWS XP". Tugas skripsi ini merupakan salah satu syarat studi yang harus ditempuh oleh seluruh mahasiswa Sekolah Tinggi Manajemen Informatika dan Komputer STMIK "AMIKOM" Yogyakarta, guna menyelesaikan akhir studi pada jenjang program S1. Dengan selesainya skripsi ini, penyusun mengucapkan banyak terimakasih sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM. selaku ketua STMIK "AMIKOM " Yogyakarta.
2. Bapak Drs. Bambang Sudaryatno, MM. Selaku Ketua Jurusan Sistem Informasi STMIK "AMIKOM" Yogyakarta.
3. Bapak M. Rudyanto Arief, MT yang telah berkenan menjadi Dosen Pembimbing Skripsi saya, dan atas dorongan serta bimbingannya, sehingga skripsi ini dapat selesai dengan baik.
4. Bapak, Ibu, serta seluruh keluargaku tercinta yang telah memberikan dukungan moril, materil dan spirit selama ini.
5. Dan untuk semua pihak-pihak yang telah membantu kelancaran skripsi ini serta kawan-kawan semua yang telah membantu secara tidak langsung, terima kasih atas dukungannya.

Penulis menyadari bahwa Skripsi ini masih jauh dari sempurna, baik dari segi isi, penulisan maupun pembahasan. Oleh karena itu segala kritik dan saran yang sifatnya membangun sangat penulis harapkan. Semoga skripsi ini dapat berguna dikemudian hari dan dipergunakan dengan sebaik - baiknya. Akhir kata penulis ucapkan Terima Kasih yang sebanyak - banyaknya.

Yogyakarta, 1 Maret 2010



(Penulis)

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiv
INTISARI	xv
ABSTRACT	xvi
BAB I PENDAHULUAN	1
I.1 Latar Belakang Masalah	1
I.2 Rumusan Masalah	3
I.3 Batasan Masalah	3
I.4 Tujuan Penelitian	4
I.5 Metodologi Penelitian	5
I.6 Sistematika Penulisan Laporan	6
BAB II LANDASAN TEORI	8

II.1	Virus.....	8
II.1.1	Sejarah Virus Komputer.....	8
II.1.2	Pengertian Virus Komputer	9
II.1.3	Kriteria Virus Komputer	10
II.1.4	Jenis-jenis Virus Komputer	13
II.1.5	Media Penyebaran Virus	15
II.2	CRC32	16
II.2.1	Pengertian CRC32	16
II.2.2	Implementasi CRC32 ke Pendeteksian Virus	19
II.3	Sistem Operasi	20
II.3.1	Definisi Sistem Operasi	20
II.3.2	Fungsi Dasar Sistem Operasi	21
II.4	Microsoft Visual Basic 6.0	21
II.4.1	Pengenalan Microsoft Visual Basic 6.0	21
II.4.2	Variabel, Konstanta dan Tipe Data	24
II.4.3	Operator	28
II.4.4	Prosedur	29
II.4.5	Fungsi	31
II.4.6	Struktur Percabangan dan Perulangan	34
II.5	Windows API (Aplication Programing Interface)	38
II.6	Dynamic Link Library (<i>DLL</i>)	42
II.7	<i>Registry Windows</i>	42
II.7.1	Pengertian <i>Registry Windows</i>	42

II.7.2	Hirarki <i>Registry Windows</i>	43
BAB III	ANALISIS DAN PERANCANGAN SISTEM	49
III.1	Alat Penelitian	49
III.2	Bahan Penelitian	50
III.3	Tahap Penelitian	50
III.3.1	Analisa Cara Kerja dan Aksi Yang Dilakukan Beberapa Virus Lokal	50
III.3.2	Cara Mengatasi dan Menanggulangi Virus	54
III.4	Perancangan Sistem	55
III.4.1	Perancangan Flowchart	55
III.4.2	Struktur Kode Program	58
III.4.3	Perancangan Antarmuka (<i>Interface</i>)	60
III.5	Pembuatan Program	66
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	81
IV.1	Hasil dan Pembahasan Program	81
IV.2	Implementasi Program	94
IV.2.1	Instalasi Program	95
IV.2.2	Testing Program	97
BAB V	KESIMPULAN	103
V.1	Kesimpulan	103
V.2	Saran	104

DAFTAR PUSTAKA

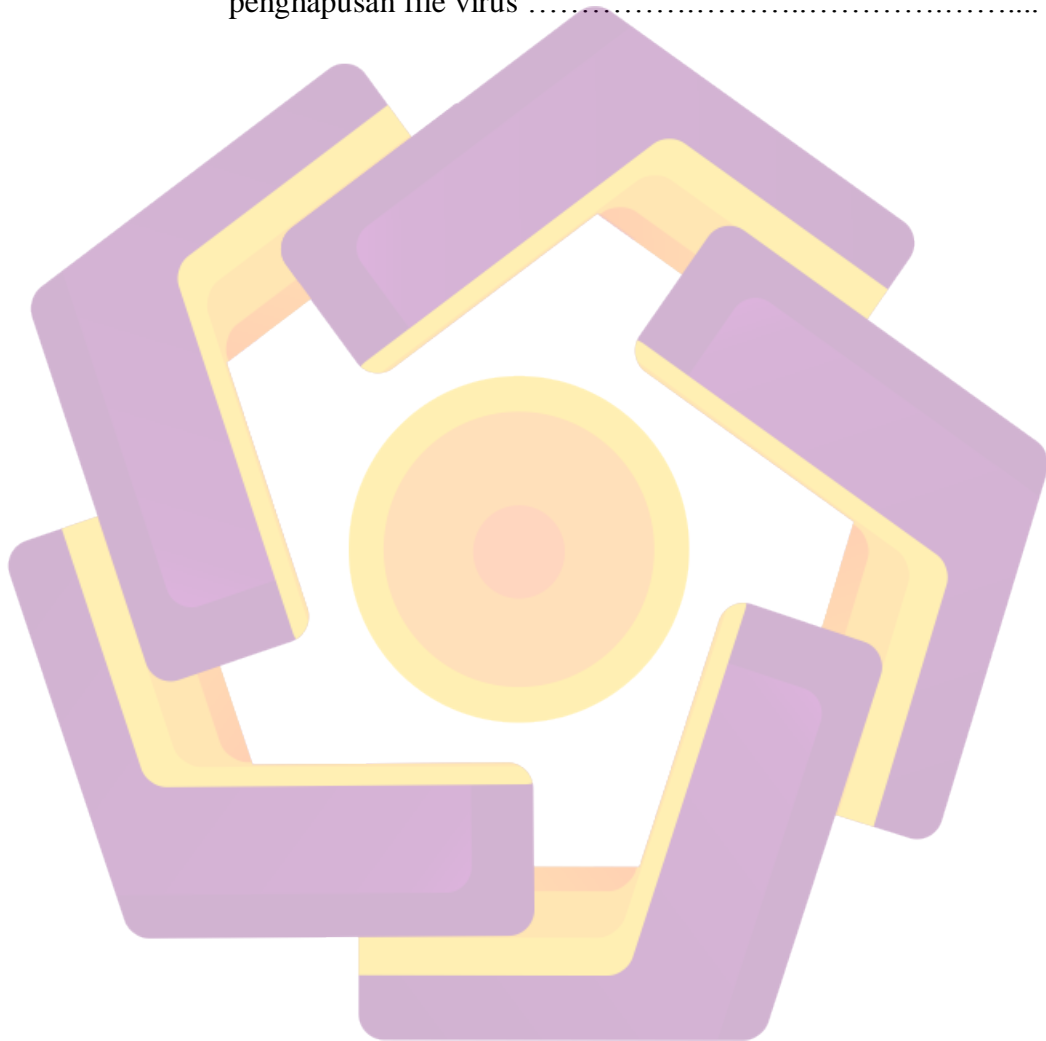
LAMPIRAN

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Tampilan IDE Visual Basic 6.0.....	22
Gambar 2.2 Tampilan Registry Editor	45
Gambar 2.3 Dword Value (REG_DWORD).....	46
Gambar 2.4 Binary Value (REG_BINARY).....	46
Gambar 2.5 String Value (REG_SZ).....	47
Gambar 2.6 Multi-String Value (REG_MULTI_SZ).....	47
Gambar 2.7 Expandable String Value (REG_EXPAND_SZ).....	48
Gambar 3.1 File duplikat folder untuk mengelabui user	51
Gambar 3.2 Pesan yang ditampilkan jika mengakses Registry Editor.....	52
Gambar 3.3 Proses dari virus Doomsday yang aktif di memory	53
Gambar 3.4 Flowchart proses pendeteksian dengan daftar signature virus.....	56
Gambar 3.5 Flowchart proses pendeteksian dengan daftar signature “File virus (lanjutan).....	57
Gambar 3.6 Perancangan tampilan form scan	61
Gambar 3.7 Perancangan tampilan form signature.....	62
Gambar 3.8 Perancangan tampilan form process manager	63
Gambar 3.9 Perancangan tampilan form settings	64
Gambar 3.10 Perancangan tampilan form about	65
Gambar 3.11 Perancangan tampilan form deteksi proses	65
Gambar 3.12 Perancangan tampilan form scan report	66
Gambar 3.13 Tampilan pembuatan form Menu	70
Gambar 3.14 Tampilan pembuatan form Scan	71
Gambar 3.15 Tampilan pembuatan form Signature	72
Gambar 3.16 Tampilan pembuatan form Process Manager	73
Gambar 3.17 Tampilan pembuatan form Settings	74

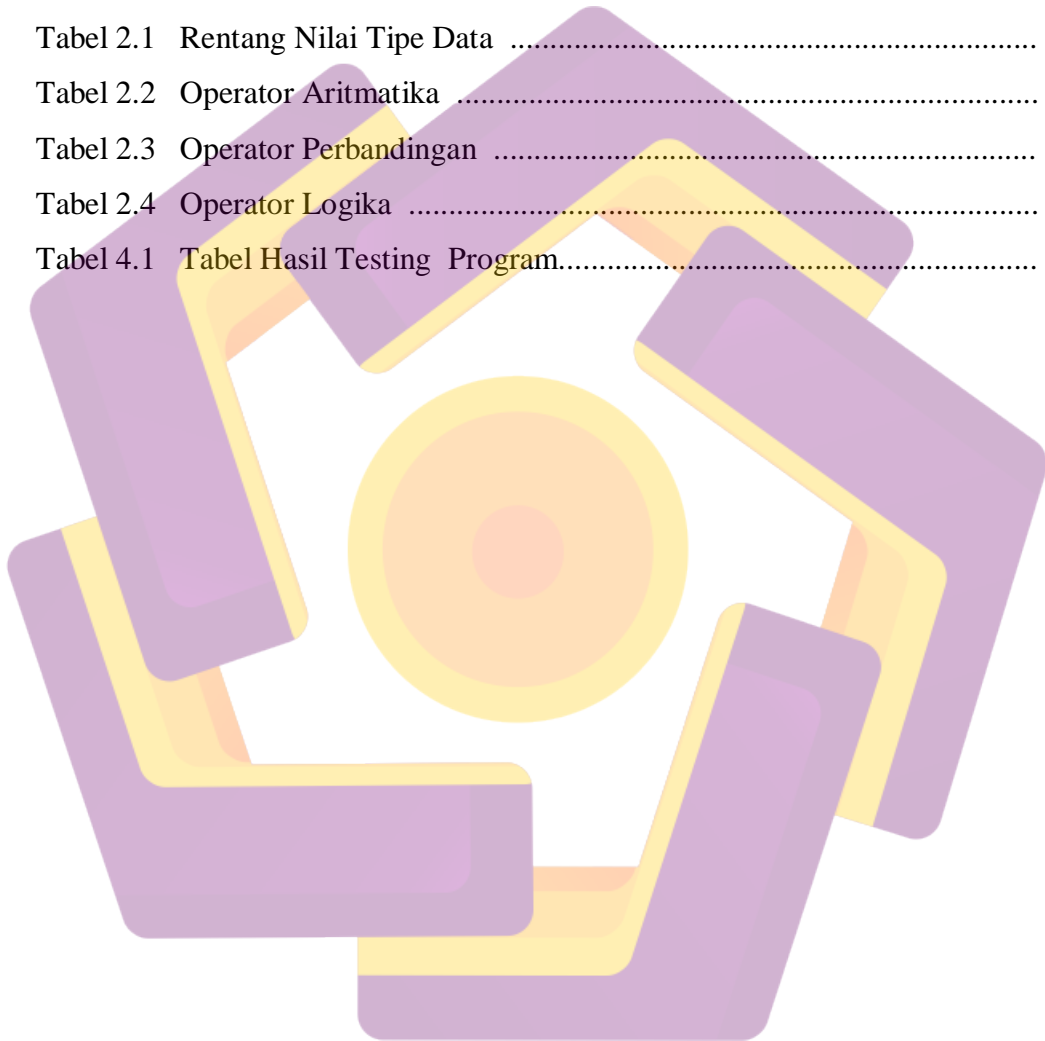
Gambar 3.18	Tampilan pembuatan form About	75
Gambar 3.19	Tampilan pembuatan form Deteksi Proses	76
Gambar 3.20	Tampilan pembuatan form Scan Report	77
Gambar 3.21	Tampilan program Notepad	78
Gambar 3.22	Tampilan isi file signature	78
Gambar 3.23	Tampilan dialog Save As	79
Gambar 3.24	Tampilan VB Resource Editor	80
Gambar 3.25	Tampilan Resource Editor setelah sign.db dimasukkan.....	80
Gambar 4.1	Tampilan Form Menu.....	81
Gambar 4.2	Tampilan Form Scan.....	82
Gambar 4.3	Daftar file virus yang tertangkap.....	83
Gambar 4.4	Tampilan scan report	84
Gambar 4.5	Tampilan folder karantina yang telah dibuat	85
Gambar 4.6	File-file yang terdapat dalam folder Karantina	85
Gambar 4.7	Tampilan Form Signature	86
Gambar 4.8	Pesan apabila terdapat hasil checksum yang sama dalam daftar signature	86
Gambar 4.9	Pesan apabila ada kesamaan dalam penulisan nama	86
Gambar 4.10	Cara menghapus signature virus	88
Gambar 4.11	Tampilan Form Process Manager	89
Gambar 4.12	Tampilan Proses Virus	90
Gambar 4.13	Tampilan Form Settings	90
Gambar 4.14	Tampilan Menu Set Attribute File	91
Gambar 4.15	Tampilan Menu Aplikasi Windows	92
Gambar 4.16	Tampilan Menu Pengaturan	93
Gambar 4.17	Tampilan Form About	93
Gambar 4.18	Tampilan Form Deteksi Proses	94
Gambar 4.19	File-file yang terdapat dalam HIT_Removal_tools.rar	95
Gambar 4.20	Tampilan awal program HIT_Removal_tools.exe	96
Gambar 4.21	File Sign.db yang telah diekstrak.....	96

Gambar 4.22	Daftar proses virus yang terdeteksi	99
Gambar 4.23	Pemilihan lokasi drive dan ekstensi file	100
Gambar 4.24	Proses pencarian file virus TrenD 9aya RAm8ut 2008.....	101
Gambar 4.25	Pesan konfirmasi ketika ingin menghapus file virus	101
Gambar 4.26	Pesan sukses ketika berhasil melakukan penghapusan file virus	102



DAFTAR TABEL

	Halaman
Tabel 2.1 Rentang Nilai Tipe Data	28
Tabel 2.2 Operator Aritmatika	28
Tabel 2.3 Operator Perbandingan	29
Tabel 2.4 Operator Logika	29
Tabel 4.1 Tabel Hasil Testing Program.....	98



INTISARI

Perkembangan teknologi informasi, khususnya bidang komputer, sangat penting untuk kehidupan manusia. Hal ini dikarenakan komputer memiliki kemampuan untuk memudahkan pekerjaan manusia dengan menggunakan perangkat lunak yang telah dikembangkan. Komputer adalah suatu alat elektronik yang kemampuannya dikendalikan oleh perangkat lunak. Sangat banyak perangkat lunak yang telah dibuat dan dikembangkan, ada yang bermanfaat ada pula yang merugikan. Perangkat lunak yang merugikan biasa disebut virus komputer. Virus komputer memiliki berbagai kemampuan dasar, diantaranya memanipulasi dan memperbanyak diri. Cara kerja virus yaitu dengan memanfaatkan fungsi-fungsi sistem operasi yang tersembunyi dan memanfaatkan kelemahan yang ada pada program tertentu. Sehingga untuk menanggulangi kerusakan pada komputer yang disebabkan oleh virus maka diperlukan “obat penawar”.

Tujuan dalam penelitian ini adalah untuk mengetahui bagaimana cara membangun dan cara kerja sebuah program penghapus virus dalam hal mengatasi masalah yang disebabkan oleh serangan virus computer. Adapun metodologi penelitian yang digunakan dalam proses pembuatan skripsi ini antarlain meliputi studi pustaka, pengumpulan data dengan menggunakan metode kearsipan dan metode observasi, analisa masalah, perancangan program, dan implementasi program.

Kesimpulan yang dapat ditarik dari pembahasan bab-bab sebelumnya adalah Kebanyakan virus yang beredar di Indonesia adalah virus lokal, dan mempunyai motif penyerangan yang sama untuk menginfeksi komputer korban. Dan program removal tools ini dapat menghentikan proses virus, mencari dan menghapus file virus pada media penyimpanan serta dapat mengembalikan value registry yang telah diubah oleh virus.

Kata Kunci : Virus, Komputer, Removal Tools

ABSTRACT

Information technology development, in particular computer sector, is very important for human live. Because of computer has ability to make human activities easily by use of software that expands. Computer is an electronic instrument that its ability controlled by software. Most software had been created and expanded. There is useful software but there is malware also. Malware software usually named computer virus. It has more basic capabilities among other things are manipulate and multiply it selves. Ways of working virus is utilize invisible operation system functions and weakness in certain program. Therefore, to prevent the damage of software that caused by virus so needed “antidote”.

The purpose of this research is to know how to build and how to work a virus removal programs in terms of overcoming the problems caused by computer virus attacks. The research methodology used in the manufacturing process of this thesis include the study among libraries, with data collection using archival methods and methods of observation, analysis, problem, program design, and implementation of programs.

Conclusions can be drawn from the discussion of previous chapters is Most viruses circulating in Indonesia are local viruses, and have the same motive for the attack infects the victim's computer. These tools removal program can stop the virus, find and delete virus files on the storage media and can restore the registry values that have been changed by the virus.

Keyword : Virus, Computer, Removal Tools