

HALAMAN PENGESAHAN

PEMBUATAN VIRUS 23SEPTEMBER BESERTA ANTIVIRUSNYA MENGGUNAKAN QBFC DAN BEDAH RESOURCE TANPA DECOMPILE

TUGAS AKHIR

Laporan Tugas Akhir ini disusun guna memenuhi persyaratan kelulusan Diploma III Jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.

Disahkan dan disetujui oleh :

Ketua STMIK "AMIKOM"
Yogyakarta



Dr. M. Suyanto, MM.

Dosen Pembimbing

A handwritten signature in black ink, which appears to be "Melwin Syafrizal", is written over the text "Dosen Pembimbing".

Melwin Syafrizal, S.Kom.

HALAMAN BERITA ACARA

**PEMBUATAN VIRUS 23SEPTEMBER BESERTA
ANTIVIRUSNYA MENGGUNAKAN QBFC DAN BEDAH
RESOURCE TANPA DECOMPILE**

Diajukan Sebagai Syarat Meraih Gelar Ahli Madya Pada Jurusan Teknik Informatika,
Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta


Telah dipresentasikan dan dipertahankan didepan penguji

Pada Hari : Selasa
Tanggal : 22 Januari 2007
Jam : 14.00 WIB
Tempat : Ruang Folder

Oleh :
Sofiyudin 05.01.1967

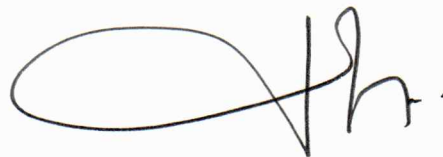
Para Penguji :

Penguji I



Heri Sismoro, S.Kom., M.Kom.

Penguji II



Emha Taufiq L, ST. M.Kom.

HALAMAN BERITA ACARA

**PEMBUATAN VIRUS 23SEPTEMBER BESERTA
ANTIVIRUSNYA MENGGUNAKAN QBFC DAN BEDAH
RESOURCE TANPA DECOMPILE**

Diajukan Sebagai Syarat Meraih Gelar Ahli Madya Pada Jurusan Teknik Informatika,
Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta

Telah dipresentasikan dan dipertahankan didepan penguji

Pada Hari : Rabu
Tanggal : 23 Januari 2007
Jam : 09.30 WIB
Tempat : Ruang Folder

Peserta :

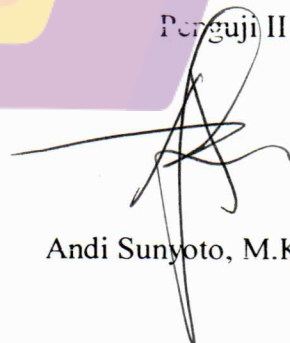
Dafika Kusuma Dara 05.01.2022

Para Penguji :

Penguji I


Hanif Al Fatta, M.Kom.

Penguji II


Andi Sunyoto, M.Kom.

MOTTO



Pengalaman adalah guru terbaik ←

Dimana ada kemauan disitu ada jalan ←

Barang siapa yang bersungguh-sungguh maka mendapatlah ia ←

Tuhan tidak akan merubah nasib suatu kaumnya kecuali kaum itu sendiri yang merubahnya ←

Lelah pun tak kan terasa olehmu bila kau yakin dengan arahmu bila citamu tercapai nanti ←

Lakukan pekerjaanmu kejar cita-citamu serta ucapkan Do'a-mu kepadaNya ←

Tak ada hal yang sulit setelah kita mengetahuinya ←

Halaman Persembahan

Sofie Thanks to :

- **ALLAH SWT** beserta para Rosulnya **Nabi Muhammad SAW** yang telah memberi tuntunan rahmat karunia dan hidayahnya.
- **'My Parent H.Asmui and Hj.Nafisah'** yang telah memberikan dukungan baik berupa *spirit*, nasehat, materi maupun lainnya yang telah menjadi begitu berarti dalam perjalananku hingga sampai disini dan untuk langkah selanjutnya. (Salut buat kedua orang tuaku).
- **My Sister and Brother (Atiyah, S.Pd.I & Faishal)** semoga kita akan menjadi orang yang berarti untuk kedua orang tua kita, untuk semua orang disekeliling kita, serta bangsa dan negara. for my **New family** Atiyah Husband Tirdan S.Pd and Gadis kecilnya 'Aulia Zukhruf'.
- **My Dinda'** Faiqotul Asma (thanks for spirit and all has gived to me)
- Sahabat Karibku Reni, Tia, Septi. Mas Bagus
- **All My Big Family**
- Sahabat perjuangan Tugas Akhir **Dafiex** (Dafika)
- Dosen Pembimbing dan Penguji Tugas Akhir
- All My Friend at **NangkaComm Djogja** (specially for Elyas, Mamat, Dafiex, Ucok, Sembod, arik, linto, Abenk)
- All My Friend at **D3TI Angk'05** kelas B

Tak lupa buat semua yang membuat aku berarti.

Halaman Persembahan

Dafika Thanks to :

- Kepada *ALLAH SWT* dan Rosulnya *Nabi Muhammad SAW* yang telah memberi tuntunan rahmat karunia dan hidayahnya.
- Buat **orang tua** dan keluarga besarku yang telah memberikan kasih sayang perhatian serta dorongan kepada ku.
- Buat keluarga mas tanto mba nika, mba novi dan adik-adik ku.
- Buat sahabat-sahabatku nangkacomm djogdja, sahabat seperjuangan dalam menyelesaikan Tugas Akhir (ifos), **D3-TI-B 2005** amikom yogyakarta. @d4mnphr34k3r (thanks buat koneksi gretz nya) @pejantan_kuda (thanks 4 free m8 nya) @ uki aqietza @idx_linuxer @meitha @azwarAnas @sonya.
- Sahabat – sahabat cyber ku :
 @adam13@fef_cc@abuma_z@dar_cisco@elpranto2000
 @gue_andika@scooter_program@hack_bisnis@nam_inspiro
- Arma
- All my friends*

UNTUK SEMUA ORANG – ORANG TERDEKATKU (thanks 4 all ☺)

Semua inspirasi yang ada tidak terlepas dari 'MEREKA', thanks..

KATA PENGANTAR

Dengan mengucapkan syukur Alhamdulillah laporan tugas akhir “**PEMBUATAN VIRUS 23SEPTEMBER BESERTA ANTIVIRUSNYA MENGGUNAKAN QBFC DAN BEDAH RESOURCE TANPA DECOMPILE**” ini dapat kami selesaikan. Dorongan keluarga serta keinginan kami untuk menggapai masa depan yang lebih cerah membuat kami terpacu untuk segera menyelesaikannya. Pengalaman kami di bidang IT baik web program, Editing Registry, CMD Programming memberikan bumbu pada pembuatan program tugas akhir kami ini.

Pembuatan virus 23september beserta Antivirusnya menggunakan QBFC dan bedah resource tanpa decompile ini memberikan gambaran bagaimana cara kerja sebuah virus local beserta antivirusnya, serta bagaimana mengembangkan CMD programming.

Laporan ini pada Bab I penulis mengemukakan tentang sejarah sebuah *virus* serta kriteria-kriteria sebuah program virus.

Pada Bab II dibahas tentang virus, antivirus, dan program batch serta registry editor.

Pada Bab III dibahas tentang rancangan pembuatan program, serta hardware dan software yang digunakan dalam pembuatan.

Pada Bab IV dibahas tentang konsep pembuatan virus beserta antivirusnya yang dibuat menggunakan bahasa pemrograman QBFC, dan bedah Resource tanpa decompile.

Pada akhir yaitu Bab V penulis membahas tentang kesimpulan dan saran dari perumusan masalah yang telah dibahas pada Bab I.

Laporan ini diharapkan dapat membantu para pengguna komputer khususnya kalangan IT dalam pembelajaran logika pemrograman khususnya pada batch programming, serta untuk mengatasi masalah/problem pada sebuah komputer yang terkena virus local.

Penulis sadar laporan/tugas akhir ini, jauh dari sempurna, maka saran dan kritik pembaca yang membangun amatlah penulis harapkan demi sempurnanya laporan maupun program ini.

Semoga laporan ini dapat bermanfaat dan dipakai sebagai bahan pengembangan Batch programming khususnya dikalangan mahasiswa teknik informatika, dan pengguna komputer pada umumnya. Amien...

Sofie & Dafika

DAFTAR ISI

| | |
|-----------------------------------|------|
| HALAMAN JUDUL | i |
| HALAMAN PENGESAHAN | ii |
| HALAMAN BERITA ACARA | iii |
| HALAMAN MOTTO | v |
| HALAMAN PERSEMBAHAN | vi |
| KATA PENGANTAR | viii |
| DAFTAR ISI | x |
| DAFTAR GAMBAR | xiv |
| DAFTAR TABEL | xv |
| BAB I PENDAHULUAN | 1 |
| A. Latar Belakang | 1 |
| B. Rumusan Masalah | 3 |
| C. Batasan Masalah | 3 |
| D. Maksud dan Tujuan | 4 |
| E. Manfaat Penelitian | 5 |
| F. Sistematika Penulisan | 5 |
| G. Jadwal Penelitian | 6 |
| BAB II DASAR TEORI | 7 |
| A. Virus | 7 |
| 1. Sejarah Virus | 7 |
| 2. Pengertian Virus | 8 |
| 3. Kriteria Virus | 9 |

| | |
|---|-----------|
| a. Kemampuan untuk mendapatkan Informasi | 9 |
| b. Kemampuan untuk memeriksa suatu file | 9 |
| c. Kemampuan untuk menggandakan diri | 10 |
| d. Kemampuan untuk melakukan manipulasi | 10 |
| e. Kemampuan untuk menyembunyikan diri | 11 |
| 4. Siklus Hidup Virus | 11 |
| a. Dormant Phase | 11 |
| b. Propagation Phase | 11 |
| c. Triggering Phase | 12 |
| d. Execution Phase | 12 |
| 5. Beberapa Cara Penyebaran Virus..... | 12 |
| B. Batch Program..... | 13 |
| 1. Pengenalan Program Batch..... | 13 |
| 2. Program Bacth Dengan Notepad | 16 |
| C. Registry..... | 17 |
| 1. Pengenalan Registry..... | 17 |
| 2. Jenis Data Registry..... | 20 |
| 3. Edit Registry Menggunakan Script/Bahasa Pemrograman..... | 23 |
| 4. Akses Registry Dengan File BAT..... | 23 |
| BAB III RANCANGAN PROGRAM..... | 26 |
| A. Alat..... | 26 |
| 1. Hardware..... | 26 |
| 2. Software..... | 27 |
| 3. Gambar | 27 |

| | |
|---|-----------|
| 4. File Wav | 28 |
| B. Alur Program Virus 23september..... | 29 |
| 1. Flowchart program virus 23september | 29 |
| 2. Mekanisme program virus 23september..... | 30 |
| C. Alur Program Anti Virus 23september..... | 35 |
| 1. Flowchart program anti virus 23september..... | 35 |
| 2. Mekanisme program anti virus 23september..... | 36 |
| BAB IV HASIL DAN PEMBAHASAN..... | 39 |
| A. Virus 23september..... | 39 |
| 1. Infeksi virus 23september..... | 39 |
| B. Anti Virus 23september..... | 44 |
| 1. Struktur interface program anti virus 23september..... | 44 |
| a. Interface utama..... | 44 |
| b. Tampilan proses penghapusan virus..... | 45 |
| c. Tampilan proses recovery file JPG..... | 47 |
| d. Tampilan proses penghapusan Desktop.ini..... | 48 |
| e. Scanning pada drive sistem..... | 49 |
| C. Compile Menggunakan QBFC..... | 51 |
| D. Bedah Resource Tanpa Decompile | 57 |
| BAB V PENUTUP..... | 59 |
| A. Kesimpulan | 59 |
| B. Saran | 60 |
| DAFTAR PUSTAKA | |
| LAMPIRAN | |

DAFTAR GAMBAR

| | |
|---|----|
| Gambar 2-1. Ruang kerja Batch Programing (CMD) | 13 |
| Gambar 2-2. Tampilan ketika mengetikkan Help pada CMD..... | 15 |
| Gambar 2-3. Tampilan perintah copy /? Pada CMD | 15 |
| Gambar 2-4. Contoh simpel program batch (23september.bat) | 16 |
| Gambar 2-5. Struktur pohon registri key pada windows xp. | 19 |
| Gambar 2-6. Export registry | 25 |
| Gambar 3-1. Flowchart proses Virus 23september..... | 29 |
| Gambar 3-2. Proses Infeksi Registry Virus 23september..... | 30 |
| Gambar 3-3. Proses infeksi sistem..... | 32 |
| Gambar 3-4. Detail Proses Manipulasi BAT..... | 32 |
| Gambar 3-5. Alur Proses Infeksi JPG..... | 34 |
| Gambar 3-6. Blok Proses Antivirs 23september..... | 35 |
| Gambar 3-7. Proses Recovery File JPG..... | 37 |
| Gambar 3-8. Proses Recovery background..... | 37 |
| Gambar 4-1. Disable CMD..... | 39 |
| Gambar 4-2. Disable Tasck Manager..... | 40 |
| Gambar 4-3. Hide Ekstensi..... | 40 |
| Gambar 4-4. Manipulasi JPEG Type File mode Details..... | 41 |
| Gambar 4-5. Background pada Taskbar atas..... | 42 |
| Gambar 4-6. JPEG image mode View Thumbnails..... | 42 |

| | |
|--|----|
| Gambar 4-7. Tampilan interface Utama..... | 44 |
| Gambar 4-8. Tampilan proses penghapusan virus 23september..... | 46 |
| Gambar 4-9. Tampilan proses Recovery File JPG..... | 47 |
| Gambar 4-10. Tampilan proses penghapusan Desktop.ini..... | 48 |
| Gambar 4-11. Scanning selesai..... | 49 |
| Gambar 4-12. Clean dari virus 23september..... | 49 |
| Gambar 4-13. Sistem tidak terinfeksi virus 23september..... | 50 |
| Gambar 4-14. Menu utama Software QBFC..... | 51 |
| Gambar 4-15. Sub menu Open pada menu File..... | 52 |
| Gambar 4-16. Hasil ambil source code bacth programming..... | 52 |
| Gambar 4-17. Tab menu Custom Resource pada QBFC..... | 53 |
| Gambar 4-18. Tab menu Include pada QBFC..... | 53 |
| Gambar 4-19. Sub menu Option pada QBFC..... | 54 |
| Gambar 4-20. Tab menu General pada sub menu Option..... | 55 |
| Gambar 4-21. Tab menu Decompilation pada sub menu Option..... | 56 |
| Gambar 4-22. Menu Compile F9 pada QBFC..... | 56 |
| Gambar 4-23. Box Save As (untuk menyimpam program exe)..... | 57 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 1.1. Jadwal Kegiatan Penelitian..... | 6 |
| Tabel 2.1. Jenis Data Registry..... | 20 |

