TEKNIK PEMBUATAN ANTIVIRUS DENGAN METODE PENCARIAN DENGAN MEMBACA INFORMASI STRUKTUR FILE PORTABLE EXECUTABLE(PE) SEBAGAI POLA VIRUS

SKRIPSI

disusun oleh

Syamsul Syarif

08.21.0375

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA

2011

PERSETUJUAN

SKRIPSI

Teknik Pembuatan Antivirus Dengan Metode Pencarian Dengan Membaca Informasi Struktur File Portable Executable(PE) Sebagai Pola Virus

yang dipersiapkan dan disusun oleh

Syamsul Syarif

08.21.0375

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 04 Maret 2011

Dosen Pembimbing,

Ir. Abas Ali Pangera, M.Kom.
NIK. 190302010

PENGESAHAN

SKRIPSI

Teknik Pembuatan Antivirus Dengan Metode Pencarian Dengan Membaca Informasi Struktur File Portable Executable(PE) Sebagai Pola Virus

yang dipersiapkan dan disusun oleh

Syamsul Syarif

08.21.0375

telah dipertahankan didepan Dewan Penguji
pada tanggal 04 Maret 2011

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Sudarmawan, S.T., M.T. NIK. 190302035	
Armadyah Amborowati, S.Kom., M.Eng. NIK. 190302063	
Afelwin Syafrizal, S.Kom., M.Eng. NIK. 190302105	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 04 Maret 2011

KETUA STMIK AMIKOM YOGYAKARTA

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

PERNYATAAN

Saya yang bertanda tangan 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, 03 Maret 2011

Tanda tangan

Syamsul Syarif
08.21.0375

MOTTO

- *Membahagiakan orang disekitar kita merupakan salah satu unsur untuk belajar ilmu ikhlas*
- *Belajar ikhlas adalah belajar untuk memberi tanpa mengharapkan timbal balik apapun dari siapa pun karena ada ZAT yang sangat memperhatikan kita ……*
- *Hidup adalah sebuah pilihan, maka pilih lah jalan yang terbail untuk mu*
- *Dan jika kamu salah memilih jangan lah kamu menyesalinya……*
- *Hari ini lebih baik dari kemarin dan hari esok lebih baik dari hari ini*
- *Demi Waktu itu sangat berharga dan amat berguna bagi siapa saja yang mempergunakan nya, tetapi membawa rugi bagi siapa yang membuangnya dengan percuma. (**QS. AL' Ashr**)*
- *Putus asa merupakan salah satu hal yang dibenci oleh Allah SWT, jadi tetaplah mempunyai harapan demi tercapainya harapan dan cita-cita. (**QS. Al. Qalam 31**)*

PERSEMBAHAN

Syukur Alhamdulillah kita panjatkan kehadirat Allah SWT yang telah memberikan rahmat serta hidayat-Nya

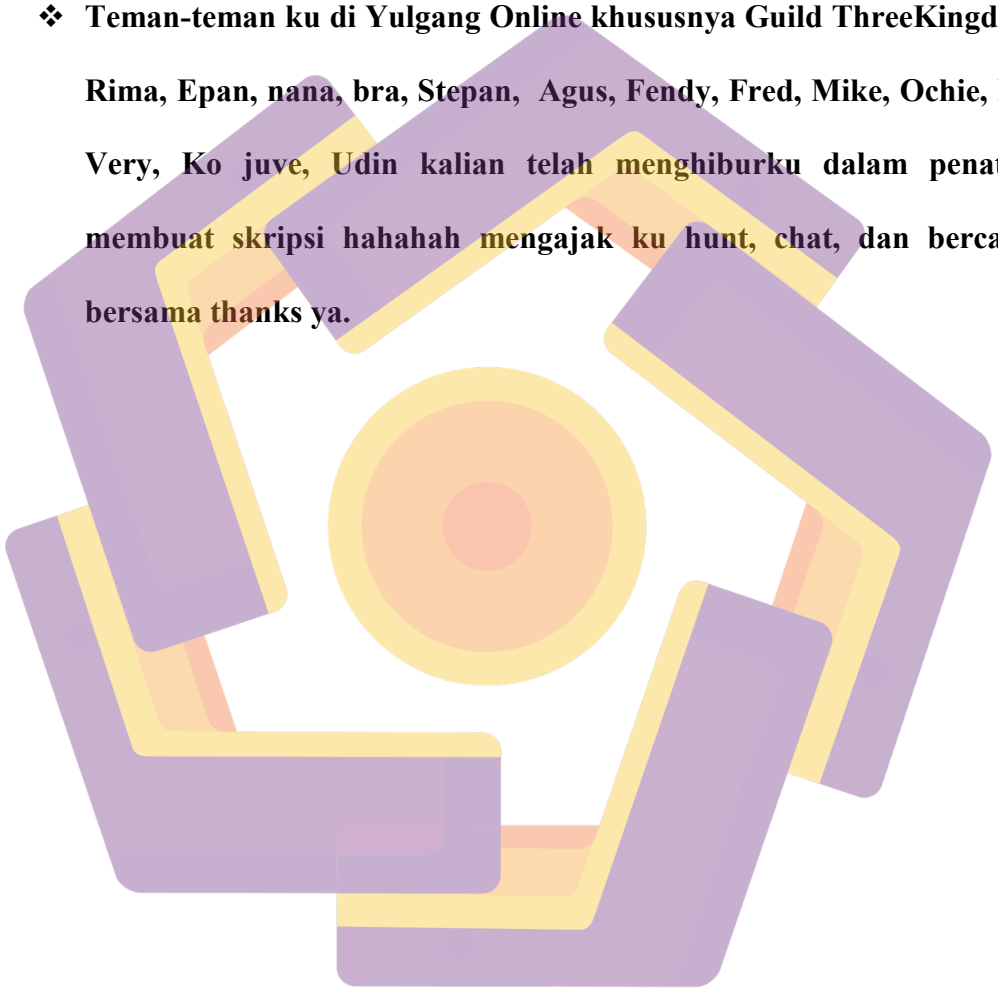
Sholawat serta salam kepada Nabi Muhammad SAW serta seluruh pengikut setianya hingga akhir zaman….

Dipersembahkan Kepada,

- **Keluarga ku, papa, mama, kak Rul, kak Arman, adik sepupu ku larry dan keluarganya yang telah banyak memberikan support baik dalam hal material dan spiritual sehingga kuliah ku selama ini bisa terselesaikan. Syamsul Sayang kalian semua.**
- **Seseorang yang telah lama menemani ku selama ini, memberi semangat, saran dan ide yang membantu dalam menyelesaikan skripsi ini dan juga yang telah meninggalkan ku … kamu akan tetap dihati ku tuk aku kenang slamanya.**
- **Sahabatku Avik dan keluarga, Rayz-Vina dan keluarga, Titem dan keluarga Riki, Sally, Sugeng, Surya, Dewi, Arman, Jicky, Teman-teman D3-TI 2004, Teman-teman S1-T1 2010 dan teman/sahabat ku yang tidak bisa saya sebutkan satu-persatu yang telah banyak membantu ku selama di ini Terimakasih.**

- **Team Codepth Om Fahmi, Mas Faiq, Mba feti dan Mulia, Terima kasih karna ku pernah menjadi bagian dari team ini yang banyak memberikan ilmu dan pengalaman yang begitu banyak…Sukses Slalu.**

- **Teman-teman ku di Yulgang Online khususnya Guild ThreeKingdomz Rima, Epan, nana, bra, Stepan, Agus, Fendy, Fred, Mike, Ochie, Rin, Very, Ko juve, Udin kalian telah menghiburku dalam penatnya membuat skripsi hahahah mengajak ku hunt, chat, dan bercanda bersama thanks ya.**



KATA PENGANTAR

Puji Syukur Penulis panjatkan kepada Allah SWT, yang telah memberikan limpahan niat, barokah dan hidayah kepada setiap makhluk-Nya, sehingga penulis mampu menyelesaikan laporan skripsi dengan judul "**TEKNIK PEMBUATAN ANTI VIRUS DENGAN METODE PENCARIAN DENGAN MEMBACA INFORMASI STRUKTUR FILE PORTABLE EXECUTABLE(PE) SEBAGAI POLA VIRUS**" ini sesuai dengan yang direncanakan.

Penyusunan laporan ini dimaksudkan untuk memenuhi persyaratan kelulusan program srata 1 jurusan Teknik Informatika pada Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.

Pada kesempatan ini penulis ingin memberikan penghargaan dan ucapan terima kasih yang sebanyak-banyaknya kepada:

1. Bapak Prof. Dr. M. Suyanto, MM selaku Ketua STMIK AMIKOM Yogyakarta
2. Bapak Ir. Abas Ali Pangera selaku ketua jurusan Teknik Informatika dan selaku dosen pembimbing yang telah banyak membantu dan dengan sabar memahami setiap keluhan dan ketidak mengertian penulis.
3. Seluruh dosen, asisten dosen, dan asisten praktikum STMIK AMIKOM Yogyakarta yang telah memberikan pemahaman dan mau berbagi ilmu kepada penulis selama penulis menjadi mahasiswa.

4. Ibu, Bapak dan Keluarga yang lain yang telah memberikan support baik material dan spiritual sehingga penulis mampu menyelesaikan tanggung jawabnya.

5. S1-T1 ’08 disanalah aku bertemu kalian semua teman-temanku, ma’af tak bisa sebutkan satu persatu yang pasti, terima kasih telah terima aku.

Akhirnya penulis mengharapkan laporan skripsi ini dapat berguna dan bermanfaat terutama bagi STMIK AMIKOM Yogyakarta, rekan-rekan serta pihak-pihak yang berkepentingan.

Yogyakarta, 03 Maret 2011

Penulis

DAFTAR ISI

INTISARI

Selama lebih dari tiga dekade yang lalu, virus komputer telah berkembang dari sekedar riset akademis menjadi masalah yang umum bagi para pengguna komputer di dunia. Masalah terbesar dari virus ini berasal dari penanggulangan efek kerugian yang ditimbulkan oleh penyebarannya. Efek kerugian ini semakin menjadi dengan maraknya penggunaan internet sebagai jalur komunikasi global antara pengguna komputer di seluruh dunia. Berdasarkan hasil survei CSI/FB sejak tahun 2004-2008 pada sekitar 433-an responden dari berbagai organisasi di Amerika Serikat, tentang kejahatan komputer dan keamanannya, menyebutkan bahwa virus menempati urutan pertama sebagai kejahatan komputer yang paling merugikan. Seiring dengan perkembangannya, virus komputer mengalami beberapa evolusi dalam bentuk, karakteristik serta media penyebarannya. bentuk evolusi tersebut dikenal dengan *Worms, Spyware, Trojan horse* dan program Malcode lain.

Perkembangan penyebaran malcode di Indonesia pada awalnya lebih banyak didominasi oleh *worms* dan *virus* yang berasal dari luar negeri. Namun pada bulan Oktober 2005, dominasi ini mulai runtuh dengan menyebarnya virus-virus lokal yang hampir ada disetiap komputer di seluruh Indonesia, virus menyebar dengan sangat cepat dan sangat membuat risih bagi pengguna komputer, dengan demikian dibuatlah anti virus sebagai salah satu solusi mencegah penyebaran.

Metode pencarian virus yang paling sering di pakai oleh anti virus yaitu metode CRC-32 (*Cyclic Redundancy Code*). Metode CRC-32 merupakan teknik yang semulanya digunakan untuk mengecek kerusakan pada file. Metode ini yang sering digunakan oleh anti virus untuk mengecek signature dari virus, tetapi teknik ini tidak efesien apabila diterapkan pada malware yang sudah mengimplementasikan teknik polymorph. Teknik Polymorph secara umum adalah teknik mereplikasi diri dan tiap signature replikanya berbeda satu sama lain. Kasus virus lokal sudah ditemukan penggunaan teknik polymorph. Hal ini yang melatar belakangi mengapa "Teknik Pembuatan Anti Virus Dengan Metode Pencarian Dengan Membaca Informasi Struktur File *Portable Executeble*(PE) Sebagai Pola Virus" diangkat sebagai judul skripsi, karena berdasarkan pengamatan penulis walaupun virus sudah melakukan modifikasi menambah atau mengurangi byte-byte tertentu tetapi Informasi Struktur File *Portable Executeble*(PE) yang berupa data optimal header dari virus yang berisi informasi *SizeOfCode* dan *AddressOfEntry*, tidak akan berubah.

Kata Kunci: Antivirus, Portable Executable, PE, Virus, CRC-32, Malcode.

ABSTRACT

For more than three decades ago, computer viruses have evolved from mere academic research into a common problem for computer users in the world. The biggest problem of this virus comes from overcoming the effects of losses caused by the spread. Effect of this loss is increasingly becoming the widespread use of the Internet as a global communication path between computer users around the world. Based on survey results of the CSI / FB since the period 2004-2008 in about 433 of the respondents from various organizations in the United States, about computer crime and security, said that the virus ranks first as the most harmful computer crime. Along with its development, computer viruses have some evolution in the form, characteristics and distribution media. form of evolution is known as Worms, Spyware, Trojan horses and other Malcode program.

Developments in Indonesia spread malcode initially more dominated by worms and viruses that come from abroad. But in October 2005, this dominance began to crumble with the spread of local viruses that almost every computer is in Indonesia, the virus spreads very fast and extremely uncomfortable for the user computer, thus made an anti virus as one solution to prevent the spread.

Virus discovery method most often used by anti-virus on the method of CRC-32 (Cyclic Redundancy Code). CRC-32 method is a technique that semulanya used to check the damage to the file. This method is often used by anti-virus to check the signature of the virus, but these techniques are not efficient when applied to malware that has been implemented Polymorph technique. Polymorph technique in general is a technique to replicate itself and each signature is different from each other replicas. The case of local virus has been found using techniques Polymorph. This is the background for why the "Technical Preparation Anti Virus Search Method By Reading Portable File Structure Information Executeble (PE) As a pattern of virus" was appointed as the thesis title, because according to writer's observation, although the virus has made modifications to add or subtract certain bytes but Portable File Structure Information Executeble (PE) in the form of optimal data header from a virus that contains information SizeOfCode and AddressOfEntry, will not change.

***Keywords**: Antivirus, Portable Executable, PE, Virus, CRC-32, Malcode.*