ABSTRAKSI

ANALISA WORM DENGAN KOMPRESI BERBASIS JAVA

Oleh :

TB. ARIS RISALUDIN
10103284

Beberapa tahun terakhir, terjadi peningkatan tajam dari internet *Worm* seperti *Sasser* dan *MsBlaster*, dimana menyebabkan kerusakan jutaan sistem di seluruh dunia. *Worm* adalah program otomatis yang mengexploit kelemahan dari komputer yang terkoneksi pada jaringan diamana bertujuan untuk mengambil alih komputer tersebut. Setelah mereka berhasil menginfeksi sistem, mereka (*Worm*) melanjutkan kembali untuk mencari dan menginfeksi system yang baru. *Worm* akan menginfeksi system baru yang memiliki kelemahan. *Worm* menyebar melalui jaringan dengan sendrinya.

Internet Worm telah menjadi ancaman yang tersebar luas pada sistem dan operasi jaringan. Untuk mengatasi mereka (*Worm*) dengan lebih efisien, dibutuhkan penganalisaan *Worm* yang baru ditemukan dan pola serangannya. Tugas Akhir ini menunjukkan bagaimana teknik berdasarkan pada *Kolmogorov Complexity* dapat membantu dalam menganalisa *Internet Worm*. Dengan kompresi. Spesies berbeda dari *Worm* dapat digolongkan sesuai dengan tipenya berdasarkan nilai atau skor kedekatan dari data. Ini akan mempermudah kita dalam menentukan apakah suatu binary *Unknown Worm* merupakan versi terbaru dari *Worm* yang ada sebelumnya (*Known Worm*) Aplikasi ini akan menjadi alat yang berguna dalam analisa awal terhadap binary berbahaya.

Worm yang dihasilkan dari hasil analisa dan pengujian, dengan membandingkan antara kedua data dan mencari nilai kedekatannya. Beberapa *Unknown Worm* (yang belum belum terindetifikasi) adalah termasuk kedalam *varian* dari *Worm* yang sudah diketahui baik dari teknik Worm menyerang, menyebar, dan menggandakan dirinya (*Worm*). Terbukti dengan analisa menggunakan aplikasi ini cukup efektif untuk menentukan jenis atau varian dari *Worm.*

Kata Kunci : *Worm*, Kompresi, Gravhiz, Analisa Worm

ABSTRACT

WORM ANALYSIS UNDER JAVA-BASED COMPRESSION

By

TB. ARIS RISALUDIN
10103284

In the last few years, there is an incisive escalation of internet Worm such as Sasser and MsBlaster causing damage to millions of system in the whole word. Worm is an automatic program exploiting the laxity of computer system connected to a network, which intending to take over the computer system. After successfully infected system, Worm will continue its action to seek out and infected a new system. Worm will infected the new system shich laxities, then it will disseminate through a network by it self.

Internet worms have become a widespread threat to system and network operations. In order to fight them more efficiently, it is required and analyzing of Worms which is new found and identifying how its attack pattern. This project points out how the technique which based on Kolmogorov Complexity shall be able to help in analyzing if internet Worm. With a different species compression of Worm, it can be classified as according to its type. This will water down us in specifying if a binary of the Unknown Worm denotes a newest version from the previous one (Known Worm), and this application will be a beneficial implement in an initial analysis about a dangerous binary.

Ther generated Worm is a progress from the analysis and examination by compared between the both data and quarrying their adjacent values. Some Unknown Worm (unidentified) belongs to the variant of worm which has been known either from its technique in charging, scattering, and reduplicating it self. It is proven by analysis using this application is effective enough to specify the type or variant of Worm.

Keyword : Worm, Compression, Gravhiz, Worm Analysis

KATA PENGANTAR



Assalamu'alaikum Wr. Wb.

Dengan mengucapkan puji syukur kepada Allah SWT, atas segala rahmat dan hidayah-Nya, serta perlindungan, pertolongan dan ridho-Nya kepada penulis sehingga penulis dapat menyelesaikan Tugas Akhir ini tepat pada waktunya, serta tak terlupakan iringan salam dan sholawat bagi junjungan penulis Nabi Muhammad SAW.

Dengan segala kemampuan dan usaha penulis akhirnya penulis dapat menyelesaikan Tugas Akhir penulis yang berjudul :

" ANALISA WORM DENGAN KOMPRESI BERBASIS JAVA"

Tugas akhir ini dibuat sebagai salah satu syarat kelulusan pada program Strata 1 Fakultas Teknik dan Ilmu Komputer, Program Studi Teknik Informatika di Universitas Komputer Indonesia.

Dalam menyelesaikan Tugas Akhir, penulis melaksanakan berdasarkan teori-teori yang telah penulis peroleh dalam perkuliahan maupun dari internet dan bimbingan dari dosen pembimbing serta pihak-pihak lain yang telah banyak memberikan semangat dan bantuan. penyusun ingin menyampaikan rasa hormat dan terima kasih yang sebesar–besarnya kepada :

1. Kedua orang tua dan keluarga penulis yang telah memberikan dukungan moril maupun materil selama ini. Untuk Abi yang selalu memberi dukungan kepada penyusun dan untuk (Alm) Umi yang telah mencurahkan kasih sayangnya kepada penyusun.
2. Bapak Ir. Eddy Suryanto Soegoto M.S.c. Selaku Rektor Universitas Komputer Indonesia, Bandung.
3. Bapak Prof. Dr. Ir. Ukun Sastra Prawira M.S.c. Selaku Dekan Universitas Komputer Indonesia
4. Ibu Mira Kania Sabariah, M.T. selaku Ketua Jurusan Teknik Informatika Fakultas Teknik dan Ilmu Komputer UNIKOM.
5. Bapak Budhi Irawan, S.Si, M.T. Selaku pembimbing yang telah meluangkan waktu serta bantuan kepada penulis dalam penyusunan skripsi ini.
6. Bapak Irfan Maliki. S.T. dan Bapak Irawan Afrianto, S.T. Selaku Dosen Penguji atas kritik dan sarannya sehingga Tugas Akhir ini menjadi lebih baik dan lebih bermanfaat keberadaanya.
7. Ibu Tati Harihayati M, M.T. selaku Dosen Wali. Terimakasih selama ini telah membimbing dan menjadi Orang Tua di selama Perkuliahan.
8. Dosen – dosen Teknik Informatika UNIKOM atas bimbingan dan ilmunya.
9. Teh ita yang selama ini selalu memberikan dorongan dan semangat untuk selalu berjuang.

10. Kakak-kakak Wawan, Aendin, Teh Yanti yang selalu memberikan perhatian dan kasih sayang yang lebih kepada penulis serta dorongan moril dan metaril.
11. Kak Fery yang banyak membantu penulis dan memberikan dorongan moril.
12. Iwan yang telah banyak membantu hingga penyusunan tugas akhir ini selesai.
13. Iqbal, Pedro, Insan, yang banyak membantu terima kasih untuk tumpangan motor dan informasinya.
14. Adi, Nurul, Rudi, Mildan, terima kasih selalu sama-sama selama bimbingan dan sharing.
15. Seluruh teman-teman IF seperjuangan angkatan 2003 dan juga semua pihak yang telah banyak membantu dalam penyusunan tugas akhir ini.

Penulis sadar bahwasanya masih banyak kesalahan-kesalahan dan kekurangan dalam penyusunan buku laporan Tugas Akhir ini, utnuk penulis mohon maaf dan mengharapkan kritik dan saran dari pembaca. Selain itu juga diharapkan pembaca dapat mengembangkan Tugas Akhir ini. Semoga buku ini memberikan manfaat dalam menghasilkan sumber daya manusia yang berkualitas dan kreatif selalu. Amien.

Wassalamu'alaikum Wr. Wb.

Bandung, Januari 2008

Penulis

DAFTAR ISI

LEMBAR JUDUL
LEMBAR PENGESAHAN
ABSTRAK ..... **i**
ABSTRACT ..... **ii**
KATA PENGANTAR ..... **iii**
DAFTAR ISI ..... **vi**
DAFTAR TABEL ..... **xi**
DAFTAR GAMBAR ..... **xiii**
DAFTAR SIMBOL ..... **xvi**
DAFTAR LAMPIRAN ..... **xvii**

BAB I PENDAHULUAN **1**
1.1 Latar Belakang Masalah 1
1.2 Identifikasi Masalah 2
1.3 Maksud dan Tujuan 2
1.4 Batasan Masalah 2
1.5 Metode Penelitian 3
1.5.1 Tahap pengumpulan Data 3
1.5.2 Tahap Pembuatan Perangkat Lunak 4
1.6 Sistematika Penulisan 5

BAB II LANDASAN TEORI **7**
2.1 *Worm* 7
2.1.1 *Email Worm* 7
2.1.2 Instam Message Worm (IMW) 7
2.1.3 Internet Worm 8
2.1.3.1 Karakteristik *Worm* 9
2.1.3.2 Kemampuan Attack Secara Spesifik 9

2.1.3.3 Command Interface 10
2.1.3.4 Kemampuan Worm Dalam Melakukan Attack 11
2.1.4 IRC Worm 13
2.1.5 File Sharing Network Worm atau P2P Worm 13
2.2 Jenis-jenis Malware Yang Menyerang Komputer 14
2.3 Kompresi 16
2.3.1 UPX Commpretion 16
2.3.2 Kompresor *BZip2* 17
2.3.3 Kompresor *Zlib* 17
2.4 Kolmogorof Kompleksitas 17
2.5 NCD (Normalized Compression Distance) 19
2.6 Quartet Method (Metode kuartet) 21
2.7 Complearn Toolkit 22
2.8 Gravhiz 23
2.9 Java dan Netbeans 23
2.9.1 Java 23
2.9.1.1 Wrappree Class 24
2.9.1.2 Deklarasi Class dan Java 25
2.9.1.3 Deklarasi Konstruktor pada Java 26
2.9.1.4 Deklarasi Member Variabel pada Class Java 27
2.9.1.5 Deklarasi Method pada Class java 27
2.9.1.6 Deklarasi Objek pada Class Java 28
2.9.1.7 GUI (*grafic user interface*) 28
2.9.1.8 Java *class Libelary* 29
2.9.2 Netbeans 30
2.10 UML (Unifield Modeling language) 31
2.10.1 Use Case 31
2.10.2 Aktor 32
2.10.3 *Class Diagram* 35
2.10.4 *Statechart Diagram* 36

2.10.5 *Activity Diagram*.....36
2.10.6 *Squence Diagram*.....37
2.10.7 *Deployment Diagram*.....39

BAB III ANALISIS DAN PERANCANGAN SISTEM.....40
3.1 Analisis Masalah.....40
3.2 Langkah-langkah Penyelesaian Masalah.....41
3.3 Analisis Proses *Complearn Toolkit*.....43
3.3.1 Analisis *Toolkit NCD*.....44
3.3.2 Analisis *Toolkit Maketree*.....45
3.4 Karakteristik Worm.....46
3.5 Analisis Kebutuhan Sistem.....49
3.5.1 Analisis Perangkat Keras.....49
3.5.2 Analisis Perangkat Lunak.....49
3.5.3 Analisis Kebutuhan Pengguna (*User*).....50
3.6 Perancangan Sistem.....50
3.6.1 Tujuan Perancangan Sistem.....51
3.6.2 *Use Case Diagram*.....51
3.6.3 *Class Diagram*.....52
3.6.4 Squence Diagram.....53
3.6.4.1 Squence Diagram Proses *Setting*.....53
3.6.4.2 *Squence DiagramProses Create New Project*.....54
3.6.4.3 *Squence DiagramProses Input Data Known Worm*.....55
3.6.4.4 *Squence DiagramProses Input Data Unknown Worm*.....56
3.6.4.5 *Squence Diagram Proses Run Analyzer*.....57
3.6.4.6 *Squence Diagram Proses View Result*.....58
3.6.5 *Activity Diagram*.....59
3.6.5.1 *Activity Diagram Proses NCD*.....60
3.6.5.2 *Activity Diagram Proses Maketree*.....61

3.7 Perancangan Antarmuka 62
3.7.1 Perancangan Antarmuka Form Menu Utama.....62
3.7.2 Perancangan Antarmuka Form Menu Tarik File 64
3.7.3 Perancangan Antarmmuka Form Menu Tarik Setting *Compressor* 65
3.7.4 Peerancangan Antarmuka Form Menu Tarik Setting *Tree Output* 68
3.7.5 Perancangan Antarmuka Form Menu Tarik Run (*Analyze now*).....70
3.7.6 Perancangan Antarmuka Menu Tarik Help (*How To Use*dan *About*).....72
3.7.7 Perancangan Antar Muka Form Menu *New Directory* 74
3.7.8 Perancangan Antarmuka Form The Result (*View Result*) 75
3.7.9 Perancangan Antarmuka *Form Input Known Data*.....76
3.7.10 Perancangan Antarmuka *Form Input Unknown data* 77
3.7.11 Perancangan Antarmuka *Form Open Dir* 78
3.7.12 Perancangan Antarmuka *FormCheck Tools* 79
3.7.13 Perancangan Antarmuka *Form Wait Dialog*.....80
3.7.14 Perancangan Antarmuka *Form How To Use* 81
3.7.15 Perancanan Anatarmuka *Form About* 82
3.7.16 Perancangan Antarmuka *Form Threshold* 83

BAB IV IMPLEMENTASI DAN PENGUJIAN 84
4.1 Implementasi 84
4.1.1 Batasan Implementasi 84
4.1.2 Perangkat Keras 86
4.1.3 Perangkat Lunak 86

4.1.4 Implementasi Program 86
4.1.4.1 Implementasi *Toolkit NCD* 87
4.1.4.2 Implementasi Antarmuka 87
4.2 Pengujian 92
4.2.1 Pengujian Perangkat Lunak Pendukung 92
4.2.1.1 Pengujian *Complearn Toolkit NCD* 92
4.2.1.2 Pengujian *Comlearn Toolkit Maketree* 93
4.2.1.3 Pengujian *Comlearn Toolkit Neato* 93
4.2.2 Pengujian Aplikasi (Tes Aplikasi) 94
4.2.2.1 Pengujian Tes Aplikasi dengan Kompresor *BZip2* 95
4.2.2.2 Pengujian Tes Aplikasi dengan Kompresor *Zlib* 99
4.2.3 Pengujian Aplikasi dengan Data Berupa *Worm* 102
4.2.3.1 Pengujian Aplikasi dengan Pilihan *TreeOutput Just Known Data* 103
4.2.3.2 Pengujian Aplikasi dengan Pilihan *TreeOutput Just Unknown Data* 108
4.2.3.3 Pengujian Aplikasi dengan Pilihan *TreeOutput Both Known and Unknown Data* 111

BAB V KESIMPULAN DAN SARAN 118
5.1 Kesimpulan 118
5.2 Saran 119

DAFTAR PUSTAKA

DAFTAR TABEL

Tabel 2.1 *Wraper Class* 23
Tabel 2.2 Macam-macam Package pada Java 28
Tabel 3.1 Penjelasan Komponen Menu Utama 61
Tabel 3.2 Penjelasan Komponen Menu Tarik File 63
Tabel 3.3 Perancangan Antarmuka Form Menu Tarik Setting (*Compressor*) 65
Tabel 3.4 Perancangan Antarmuka *Form Menu Tarik Setting* (*Tree Output*) 67
Tabel 3.5 Perancangan Antarmuka Menu Tarik Run (*Analyze Now*) 70
Tabel 3.6 Perancangan Antarmuka Form Menu Tarik Setting (*How To Use* dan *Abut*) 71
Tabel 3.7 Perancangan Antarmuka Form *New Directory* 73
Tabel 3.8 Penjelasan Form The Result 74
Tabel 3.9 Penjelasan Form *Known Data* 75
Tabel 3.10 Penjelasan Form *Known Data* 76
Tabel 3.11 Penejelasan *JfileChooser* 77
Tabel 3.12 Penjelasan Form *Check Tools* 78
Tabel 3.13 Penjelasan *Form Wait Dialog* 79
Tabel 3.14 Penjelasan *Form How To Use* 80
Tabel 3.15 Penjelasan *Form About* 81
Tabel 3.16 Penjelasan *Form Threshold* 82
Tabel 4.1 Hasil Pengujian data Bukan *Worm* dengan kompresor Bzip2 98
Tabel 4.2 Hasil Pengujian data Bukan Worm dengan Kompresor Zlib 100
Tabel 4.3 Perbedaan Hasil Analisa dengan Menggunakan Kompresor Zlib dab Bzip2 101
Tabel 4.4 Hasil Pengujian dengan Kompresor Bzip2 (Just Known Data) 105
Tabel 4.5 Hasil Pengujian dengan Kompresor Zlib (*Just Known Data*) 107

Tabel 4.6 Hasil Pengujian dengan Kompresor Bzip2 (*Just Unknown Data*).....110
Tabel 4.7 Hasil Pengujian dengan kompresor Zlib (*Just Unknown data*).....111
Tabel 4.8 Hasil Pengujian *Known data* dengan kompresor Bzip2 (*Both Known and Unknown Data*) 113
Tabel 4.9 Hasil Pengujian Unknown Data dengan kompresor Bzip2 (*Both Known and Unknown Data*) 114
Tabel 4.10 Hasil Pengujian *Known Data* dengan Kompresor Zlib (*Both Known and Unknown Data*) 115
Tabel 4.11 Hasil Pengujian *Unknown Data* dengan kompresor Zlib (*Both Known and Unknown Data*) 116

DAFTAR GAMBAR

Gambar 2.1 *Quartet Topology tree* 20
Gambar 2.2 *Tree yang Konsisten Terhadap UV | WX* 20
Gambar 2.3 *Use Case Model* 31
Gambar 2.4 Contoh *Use Case Di Mesin ATM* 33
Gambar 2.5 *Class Diagram* 34
Gambar 2.6 *Statechart Diagram* 35
Gambar 2.7 *Activity Diagram* 36
Gambar 2.8 *Squence Diagram* 37
Gambar 2.9 *Deployment Diagram* 38
Gambar 3.1 *Flow Chart* proses Analisis *Worm* 41
Gambar 3.2 Flowchart Proses NCD 44
Gambar 3.3 Flowchart Proses Maketree (Pembentukan tree) 45
Gambar 3.4 *Use Case Diagram* Analisis *Worm* 52
Gambar 3.5 *Class Diagram* 52
Gambar 3.6 *Squence Diagram Proses Setting* 53
Gambar 3.7 *Squence Diagram Proses Create Project* (Proyek baru) 54
Gambar 3.8 *Squence Diagram* Proses *Input Known Worm* 55
Gambar 3.9 *Squence Diagram Proses Input Unknown Worm* 56
Gambar 3.10 *Squence Diagram Proses Run Analyze* (Run Aplikasi Analisis) 57
Gambar 3.11 *Squence Diagram Proses View Result* (Tampilkan *Result*) 58
Gambar 3.12 *Activity Diagram Proses NCD* 60
Gambar 3.13 *Activity Diagram Proses Maketree* 61
Gambar 3.14 Perancangan Antarmuka *Form Menu Utama* 62
Gambar 3.15 Perancangan Antarmuka Menu Tarik File 64
Gambar 3.16 Perancangan Antarmuka Form Menu Tarik Setting (*Compressor*) 66
Gambar 3.17 Perancangan Antarmuka *Form Menu Tarik Setting* (*Tree Output*) 68

Gambar 3.18 Perancangan Antarmuka Form Menu Tarik Setting (*Analyze Now*) 70
Gambar 3.19 Perancangan Antarmuka Form Menu Tarik Setting (*How To Use* dan *Abut*) 72
Gambar 3.20 Perancangan Antarmuka Form New Directory 74
Gambar 3.21 Form The Result 75
Gambar 3.22 Form *Input Known Data* 76
Gambar 3.23 Form *Input Unknown Data* 77
Gambar 3.24 Form *JfileChooser* 78
Gambar 3.25 Form *Check Tools* 79
Gambar 3.26 *Form Wait Dialog* 80
Gambar 3.27 *Form How To Use* 81
Gambar 3.28 *Form About* 82
Gambar 3.29 *Form Threshold* 83
Gambar 4.1 *Isi Complearn Toolkit* 87
Gambar 4.2 Menu Utama 88
Gambar 4.3 Menu Pilih Compressor 88
Gambar 4.4 Menu Pilih *Tree Output* 89
Gambar 4.5 Menu *Threshold* 89
Gambar 4.6 Menu New (Buat *Project* Baru) 90
Gambar 4.7 Menu Input *Known* Data 90
Gambar 4.8 Menu Input *Unknown Data* 91
Gambar 4.9 Menu *Analyzer* 91
Gambar 4.10 Fungsi *NCD* pada cmd 92
Gambar 4.11 Fungsi *Maketree* pada cmd 93
Gambar 4.12 Fungsi *Neato* pada cmd 93
Gambar 4.13 Buat Proyek Baru dan Pilih direktori Penyimpanan 95
Gambar 4.14 Inputkan Data 96
Gambar 4.15 Proses Analisa 97
Gambar 4.16 Hasil Tree dari Data .txt 97

Gambar 4.17 Result Hasil Analisa.....98
Gambar 4.18 Hasil Result dengan Kompresor *Zlib*.....99
Gambar 4.19 Hasil *Tree* dari Data.txt dengan kompresor *Zlib*.....100
Gambar 4.20 Pengujian *Worm* Dengan *TreeOutput Just Known Data* 104
Gambar 4.21 *Result Just Known Data* dengan kompresor Bzip2.....105
Gambar 4.22 Hasil Analisa *Just Known Data* dengan Kompresor Zlib 106
Gambar 4.23 *Result Just Known Data* Dengan Kompresor Zlib.....107
Gambar 4.24 Pengujian *Worm* denan *TreeOutput Just Unknown Worm* 109
Gambar 4.25 *Result Just Unknown* Data Dengan Bzip2 109
Gambar 4.26 *Result Unknown data* dengan Kompresor Zlib 111
Gambar 4.27 Grafik (*Tree*) *Known Data* pada *Both known And Unknown Data* dengan Kompresor Bzip2 112
Gambar 4.28 Grafik (*Tree*) *Known Data* pada *Both known And Unknown Data* dengan Kompresor Zlib 113

DAFTAR SIMBOL

SIMBOL	KETERANGAN
	**Actor**
	**Use Case**
	**Sistem Boundary Pada Use Case**
	**Relasi antara actor dan use case**
	**Object pada sequence diagram**
	**Activate pada sequence diagram**
	Pesan antar dua objek pada sequence diagram
	**Start state**
	**End state**
	**Avtivitas pada activity diagram**
	**Titik keputusan pada aliran data**
	Sinkronisasi horizontal
	**Communication pada deployment diagram**