



**ANALISA PERANCANGAN APLIKASI MANIPULASI DATA DENGAN
METODE TRAIL OBFUSCATION UNTUK MELINDUNGI DATA DARI
AUDIT FORENSIK**



**UNIVERSITAS
MERCU BUANA**

HALOMOAN

41511120108

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2016**



**ANALISA PERANCANGAN APLIKASI MANIPULASI DATA DENGAN
METODE TRAIL OBFUSCATION UNTUK MELINDUNGI DATA DARI
AUDIT FORENSIK**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

UNIVERSITAS
MERCU BUANA

Disusun oleh:

HALOMOAN

41511120108

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2016

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41511120108

Nama : Halomoan

Judul Tugas Akhir : Analisa Perancangan Aplikasi Manipulasi Data Dengan Metode Trail Obfuscation Untuk Melindungi Data Dari Audit Forensik

Menyatakan bahwa Tugas Akhir dengan judul yang tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

UNIVERSITAS
MERCU BUANA

Jakarta, 23 Juli 2016



Halomoan

LEMBAR PENGESAHAN

Nama : Mr. Halomoan
NIM : 41511120108
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul : Analisa Perancangan Aplikasi Manipulasi Data Dengan Metode Trail Obfuscation Untuk Melindungi Data Dari Audit Forensik



Jakarta, 23 Juli 2016

Disetujui dan diterima oleh,

UNIVERSITAS
MERCU BUANA

Achmad Kodar, Drs., MT

Dosen Pembimbing

DR. Yaya Sudarya Triana, M.Kom

Kaprodi Informatika

Desi Ramayanti, S.Kom, MT

Koordinator Tugas Akhir

KATA PENGANTAR

Puji syukur Alhamdulillah kehadiran Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan tugas akhir ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Achmad Kodar, Drs., MT., selaku Pembimbing Tugas Akhir yang telah membimbing penulis dalam menyelesaikan laporan tugas akhir ini.
2. Bapak DR. Yaya Sudarya Triana, M.Kom., selaku Kepala Program Studi Teknik Informatika Universitas Mercu Buana.
3. Ibu Desi Ramayanti, S.Kom, MT, selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercu Buana.
4. Orang tua tercinta yang selalu mendukung penulis baik spirit maupun materi.
5. Istriku Nurhikmah dan Bayi En tercinta yang selalu memberikan dukungan dan semangat untuk menyelesaikan skripsi ini.
6. Teman-teman Jurusan Teknik Informatika angkatan 20 yang memberikan banyak pencerahan pada skripsi ini.
7. Saudara, teman dan sahabat-sahabat yang telah memberikan dukungan moral untuk terus menyelesaikan tugas akhir ini

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

ABSTRACT

Data security is a very expensive factor the current information era. The anti-forensic computer offering one method that actually about of the box to protect the data from any irresponsible parties. Most of the data consisting of files that identified by computer using file name and header on the particular file, this is usually called file signature. In this research we are trying to manipulate the file with the trail obfuscation method. Where we disguise the type of the files to become other type of files, which is going to make the identification process harder, both from forensic user and application sides. The concept of this system application is to alter the extension and file signature, so that in the test of forensic application the file that been altered can be recognized as another type of file. After some time designing and testing the application, we manage to run it smoothly, bug free and functioning well as the basic layout in the first design.

Keywords: Anti Forensic, File Signatures, File Extension, Trail Obfuscation

xi+82 pages; 44 figures; 13 tables; 13 attachment

Bibliography: 812(1994-2016)

ABSTRAK

Keamanan data adalah barang yang mahal dalam era informasi seperti saat ini. Anti Forensik komputer menawarkan salah satu metode out of the box untuk melindungi data dari orang yang tidak bertanggung jawab. Data yang terdiri dari file biasanya diidentifikasi oleh komputer melalui ekstensi nama file dan header pada file yang biasa disebut file signature. Pada penelitian ini penulis mencoba untuk memanipulasi file sehingga file tersebut dengan metode trail obfuscation. Yaitu dengan menyamarkan jenis file menjadi jenis file lain yang mana menyulitkan dalam proses identifikasi file baik itu oleh user, sistem dan aplikasi *forensic*. Konsep sistem aplikasi ini adalah yaitu dengan mengubah ekstensi dan file signature sehingga dalam uji coba terhadap aplikasi Forensik bisa teridentifikasi menjadi jenis file lain. Setelah merancang dan menguji coba, aplikasi ini dapat berjalan dengan baik, tanpa masalah dan berfungsi sesuai rancangan.

Kata Kunci :Anti Forensik, File Signature, Ekstensi File, Trail Obfuscation,

xi+82 halaman; 44 gambar;13 tabel; 13 lampiran

Daftar acuan : 12 (1994-2016)

DAFTAR ISI

	Halaman
KATA PENGANTAR	i
ABSTRACT	ii
ABSTRAK	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL	viii
BAB I PENDAHULUAN	
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan dan Manfaat Penelitian	4
1.4.1 Tujuan Penelitian	4
1.4.2 Manfaat Penelitian	4
1.5 Metode Penelitian	4
1.6 Sistematika Penulisan	5
BAB II LANDASAN TEORI	
2.1. Algoritma	6
2.1.1 Algoritma Kriptografi Klasik	6
2.1.2 Algoritma Kriptografi Klasik Substitusi	6
2.2. Komputer Forensik	8
2.2.1 Anti Forensik	9
2.2.2 Metode Trail Obfuscation	11
2.3. Konsep File	11
2.3.1 File Signature	13
2.3.2 Ekstensi File	14
2.4. Rekaya Perangkat Lunak	14
2.4.1 Ruang Lingkup Rekayasa Perangkat Lunak	15

2.4.2	<i>Software Development Life Cycle</i>	16
2.4.3	Model Waterfall	18
2.4.4	Pengujian Perangkat Lunak	20
2.4.5	Verifikasi Pengujian	21
2.4.6	Validasi Pengujian	22
2.5.	Paradigma Berorientasi Objek	23
2.5.1	Pemodelan UML	24
2.5.1.1	<i>Use Case Diagram</i>	25
2.5.1.2	<i>Sequence Diagram</i>	27
2.5.1.3	<i>Activity Diagram</i>	30
2.6.	<i>Java</i>	33
2.6.1	Kelebihan Java	33
2.6.2	Kekurangan Java	35
2.6.3	<i>Java 2 Standard Editon</i>	37
2.7.	<i>Netbeans</i>	40

BAB III ANALISIS DAN PERANCANGAN

3.1	Analisa Sistem	41
3.1.1	Metode Trail Obfuscation	42
3.1.2	Informasi File	45
3.2	Analisa Kebutuhan	47
3.2.1	Analisa Kebutuhan Fungsional	47
3.2.2	Analisa Kebutuhan Non Fungsional	47
3.2.2.1	Kebutuhan Perangkat Keras (<i>Hardware</i>)	47
3.2.2.2	Kebutuhan Perangkat Lunak (<i>Software</i>)	47
3.3	Perancangan Sistem	48
3.3.1	Perancangan Pembuatan Sistem (<i>Use Case Diagram</i>)	48
3.3.2	Perancangan Alur Kerja (<i>Activity Diagram</i>)	50
3.3.3	Perancangan Interaksi Antar Objek (<i>Sequence Diagram</i>)	54
3.4	Perancangan Antar Muka (<i>Interface</i>)	56

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi Sistem	61
4.2 Pengumpulan Program	61
4.2.1 Implementasi Jendela Utama Aplikasi.....	62
4.2.2 Implementasi Cari File.....	64
4.2.3 Implementasi Tampilan Informasi File.....	65
4.2.4 Implementasi Manipulasi Data	69
4.3 Metode Pengujian	71
4.3.1 Skenario Pengujian	72
4.4 Analisa Hasil Pengujian	73

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan	75
5.2 Saran	75

DAFTAR PUSTAKA	76
-----------------------------	----

LAMPIRAN	77
-----------------------	----



DAFTAR GAMBAR

	Halaman
Gambar 2.1 Sebuah <i>File</i> .Exe yang dibuka oleh program <i>WinHex Editor</i>	12
Gambar 2.2 <i>Signature File</i> untuk <i>File type</i> .Exe (aplikasi)	13
Gambar 2.3 <i>Signature File</i> untuk <i>File type</i> .Pdf	14
Gambar 2.4 Ruang lingkup Rekayasa Perangkat Lunak	16
Gambar 2.5 Ilustrasi Model Waterfall	18
Gambar 2.6 Pengujian Perangkat Lunak	21
Gambar 2.7 Diagram UML 2.3	24
Gambar 2.8 Contoh <i>Use Case Diagram</i>	25
Gambar 2.9 Contoh <i>Sequence Diagram</i>	28
Gambar 2.10 Contoh <i>Activity Diagram</i>	31
Gambar 3.1 Macam-macam ekstensi <i>File</i> dan <i>Signaturenya</i>	42
Gambar 3.2 Contoh <i>File</i> dan Ekstensinya	43
Gambar 3.3 <i>Signature File</i> dokumen yang berekstensi MP3	43
Gambar 3.4 <i>Signature File</i> gambar yang berekstensi PDF	44
Gambar 3.5 <i>Signature File executable</i> yang berekstensi EXE	44
Gambar 3.6 <i>Properties File</i> lagu bertipe mp3	45
Gambar 3.7 <i>Struktur File</i> lagu bertipe MP3	46
Gambar 3.8 <i>Use Case</i> Sistem aplikasi Manipulasi data	48
Gambar 3.9 Diagram Activity Cari <i>File</i>	51
Gambar 3.10 Diagram Activity Melihat Properties dan <i>Signature File</i>	52
Gambar 3.11 Diagram Activity Mengubah Ekstensi dan <i>Signature File</i>	53
Gambar 3.12 Diagram Sequence Mencari <i>File</i>	54
Gambar 3.13 Diagram Sequence Melihat Properties dan <i>Signature File</i>	55
Gambar 3.14 Diagram Sequence Mengubah Ekstensi dan <i>Signature File</i>	56
Gambar 3.15 Rancangan Tampilan Jendela Utama Aplikasi	57
Gambar 3.16 Rancangan Tampilan Cari <i>File</i>	58
Gambar 3.17 Rancangan Notifikasi <i>File</i> belum dipilih	58
Gambar 3.18 Rancangan Tampilan informasi <i>File</i>	59

Gambar 3.19 Rancangan Tampilah Signature info	59
Gambar 3.20 Rancangan Tampilan Kategori File	59
Gambar 3.21 Rancangan Tampilan Tombol Eksekusi	60
Gambar 3.22 Rancangan Notifikasi <i>File</i> belum dipilih	60
Gambar 3.23 Rancangan Notifikasi <i>File</i> sukses dimanipulasi.....	60
Gambar 4.1 Implementasi Jendela Utama	62
Gambar 4.2 Implementasi info signature	63
Gambar 4.3 Implementasi pilih kategori	63
Gambar 4.4 Implementasi Jendela Cari File	64
Gambar 4.5 Implementasi Notifikasi Belum dipilih	64
Gambar 4.6 Implementasi Informasi <i>signature file</i>	65
Gambar 4.7 Implementasi informasi <i>Properties file</i>	67
Gambar 4.8 Informasi jenis <i>file</i> MP3.....	68
Gambar 4.9 Informasi jenis <i>file</i> EXE.....	68
Gambar 4.10 Informasi jenis <i>file</i> PDF	69
Gambar 4.11 Tombol Eksekusi	70

DAFTAR TABEL

	Halaman
Tabel 2.1 Substitusi	7
Tabel 2.2 Notasi Pada Use Case Diagram	26
Tabel 2.3 Notasi Pada <i>Sequence Diagram</i>	28
Tabel 2.4 Notasi Pada <i>Activity Diagram</i>	32
Tabel 2.5 <i>Package</i> pada Java	39
Tabel 3.1 Ekstensi File dan signature file-nya	44
Tabel 3.2 Deskripsi <i>Use Case</i> Mencari File	49
Tabel 3.3 Deskripsi <i>Use Case</i> Melihat <i>Properties</i> dan <i>Signature File</i>	50
Tabel 3.4 Deskripsi <i>Use Case</i> Mengubah Ekstensi dan <i>Signature File</i>	50
Tabel 3.5 Keterangan <i>Sequence Diagram</i> Mencari File	54
Tabel 3.6 Keterangan <i>Sequence Diagram</i> Melihat <i>Properties</i> dan <i>Signature File</i>	55
Tabel 3.7 Keterangan <i>Sequence Diagram</i> Mengubah <i>Properties</i> dan <i>Signature</i>	56
Tabel 4.1 Skenario Pengujian	72

UNIVERSITAS
MERCU BUANA