

# Daftar Isi

Abstrak.....	ii
Abstract.....	v
Pernyataan keaslian tulisan .....	v
Publikasi selama masa studi .....	vi
Publikasi yang menjadi bagian dari tesis.....	vi
Halaman Persembahan .....	viii
Kata Pengantar .....	ix
Daftar Isi .....	x
Daftar Tabel .....	xiii
Daftar Gambar .....	xiii
Takarir dan Singkatan .....	xvi
Bab 1 Pendahuluan .....	1
1.1 Latar Belakang Penelitian .....	1
1.2 Identifikasi Masalah .....	3
1.3 Rumusan Masalah .....	3
1.4 Tujuan Penelitian .....	3
1.5 Batasan Masalah .....	3
1.6 Manfaat Penelitian .....	4
a. Manfaat Bagi Peneliti .....	4
b. Manfaat Bagi Instansi .....	4
c. Manfaat Bagi Pihak Lain .....	4
1.8 Metodologi Penelitian .....	5
1.9 Sistematika Penulisan .....	5
Bab 2 Landasan Teori .....	7
2.1 Penelitian Terdahulu.....	6
2.2 Landasan Teori .....	14
2.2.1 Forensik Digital .....	14
a. Pengertian Forensik Digital.....	14
b. Klasifikasi barang bukti Forensik .....	14
c. Barang Bukti Elektronik .....	15
d. Barang Bukti Digital .....	15
2.2.2 Malware .....	18
a. Malware tipe infeksi.....	18
b. Malware tipe Terselubung .....	18

c. Malware tipe <i>Profit –oriented</i> .....	19
2.2.3 Cryptolocker .....	19
2.2.4 Kriptografi Algoritma RSA .....	19
2.2.5 Teknik Analisa Malware .....	21
a. Teknik Analisa <i>Surface</i> .....	21
b. Teknik Analisa <i>Runtime</i> .....	21
c. <i>Teknik Analisa Static Code</i> .....	21
2.7 Malware Sandbox Online .....	21
2.8 Packed dan Obfuscated Program .....	22
2.9 Deobfuscated .....	22
2.10 Debugging .....	22
2.11 Linked Libraries dan Function .....	23
2.12 Reverse Engineering .....	23
2.13 Assembly .....	23
Bab 3 Metodologi Penelitian .....	25
3.1 Studi Literatur .....	25
3.2 Sampel Malware .....	25
3.3 Membuat Real Environment .....	26
3.4 Analisa Malware .....	26
3.5 Laporan Analisa Malware .....	28
3.6 Langkah - Langkah Penelitian .....	29
3.7 Pengujian terhadap Solusi Pencegahan Malware TT.exe .....	30
3.8 Hipotesa .....	30
Bab 4 Analisis dan Pembahasan .....	31
4.1 Menemukan Sampel Malware .....	31
4.2 Analisa Ransomware Surface Analysis .....	32
4.2.1 Menguji sampel malware menggunakan Antivirus .....	33
4.2.2 Hashing pada Malware .....	33
4.2.3 Mendeteksi Packed / Obfuscated .....	34
4.2.4 Analisa Portable Executable (PE) .....	35
4.2.5 Malware Sandbox untuk Analisa Malware .....	37
4.2.6 Kesimpulan dari hasil Analisa Malware .....	34
4.3 Analisa Ransomware Runtime Analysis .....	41
4.3.1 Menyiapkan Real Environment (Physical Lab) .....	42
4.3.2 Melakukan Analisa pada registry.....	43
4.3.3 Memonitor aktifitas Malware menggunakan Process Monitor .....	45
4.3.4 Mendeteksi aktifitas DNS .....	47
4.3.5 Analisa Paket Data menggunakan Wireshark .....	49
4.3.6 Kesimpulan dari hasil Analisa Malware .....	51

4.4	Analisa Ransomware Static Code Analysis .....	52
4.4.1	Analisa Linked Libraries dan Function .....	53
4.4.2	Analisa String pada Malware .....	56
4.4.3	Analisa Debugging pada Malware .....	57
4.4.4	Kesimpulan dari hasil Analisa Malware .....	59
4.5	Laporan Karakter Malware .....	60
4.6	Rekomendasi pencegahan malware .....	61
4.7	Bukti digital yang diperoleh .....	62
Bab 5	Kesimpulan dan Saran .....	66
5.1	Kesimpulan .....	66
5.2	Saran .....	67
	Daftar Pustaka .....	68
	Lampiran .....	71



## Daftar Tabel

Tabel 2.1	Literatur Review.....	10
Tabel 3.1	Hasil pengujian analisa Malware surface analysis.....	28
Tabel 3.2	Hasil pengujian analisa Malware Runtime analysis .....	28
Tabel 3.3	Hasil pengujian analisa malware static Code analysis.....	29
Tabel 3.4	Laporan analisa malware.....	29
Tabel 4.1	Data Section Cryptolocker .....	37
Tabel 4.2	Kesimpulan dari Surface Analysis .....	41
Tabel 4.3	Kesimpulan dari Runtime Analysis .....	51
Tabel 4.4	Linked Library Kernel32 .....	54
Tabel 4.5	Linked Library User32 .....	55
Tabel 4.6	Linked Library SHELL32 .....	55
Tabel 4.7	Linked Library Advapi32 .....	55
Tabel 4.8	Linked Library Version .....	55
Tabel 4.9	Kesimpulan dari Static Code Analysis .....	59
Tabel 4.10	Setting Rekomendasi Pencegahan .....	62
Tabel 4.11	Bukti digital yang didapatkan menggunakan metode Surface Analisis.....	62
Tabel 4.12	Bukti digital yang didapatkan menggunakan metode Runtime Analisis .....	63
Tabel 4.13	Bukti digital yang didapatkan menggunakan metode Static code Analisis ....	64

## Daftar Gambar

Gambar 1.1	Rincian Geografis jumlah infeksi. ....	2
Gambar 1.2	Tampilan Cryptolocker di komputer korban.....	2
Gambar 2.1	Algoritma asimetris .....	20
Gambar 2.2	Contoh debugging menggunakan Ollydbg .....	22
Gambar 2.3	Contoh Dynamic Link Library (DLL) dan Function .....	23
Gambar 3.1	Metodologi Penelitian .....	25
Gambar 3.2	Metode analisa malware .....	26
Gambar 3.3	Langkah - Langkah Penelitian .....	29
Gambar 3.4	Alur Pengujian Rekomendasi .....	30
Gambar 4.1	Tampilan malwr.com .....	31
Gambar 4.2	Hasil analisa Virustotal .....	33
Gambar 4.3	Hasil Hashing .....	34
Gambar 4.4	Hasil pengujian Cryptolocker menggunakan Exeinfo PE .....	34
Gambar 4.5	Hasil pengujian Cryptolocker menggunakan PeiD v0.95.....	34
Gambar 4.6	Hasil ekstrak Cryptolocker menggunakan 7Zip .....	35
Gambar 4.7	Analisa Menggunakan PEViewer .....	36
Gambar 4.8	Informasi dari PE Header malware Menu Text .....	36
Gambar 4.9	Informasi dari PE Header malware Menu rdata .....	36
Gambar 4.10	Tampilan depan website Mastiff.....	37
Gambar 4.11	Proses analisa website Mastiff .....	38
Gambar 4.12	Proses analisa website Mastiff menu peinfo-full .....	38
Gambar 4.13	Proses analisa website Mastiff menu yara .....	39
Gambar 4.14	Hasil Analisa tentang summary dan proses created .....	40
Gambar 4.15	Hasil Analisa tentang registry dan komunikasi keluar.....	40
Gambar 4.16	Konfigurasi komputer .....	43
Gambar 4.17	Tampilan Aplikasi Regshot.....	44
Gambar 4.18	Tampilan Registry Schedule TaskCache Tasks .....	44
Gambar 4.19	registry pengawasan firewall, antivirus dan antispyware .....	44

Gambar 4.20	registry Malware membuat jalan disaat Windows dihidupkan.....	45
Gambar 4.21	Tampilan Aplikasi ProceMonitor .....	46
Gambar 4.22	Tampilan Aplikasi ProceMonitor .....	46
Gambar 4.23	Tampilan Aplikasi ProceMonitor .....	47
Gambar 4.24	Malware berusaha menghubungi beberapa domain.....	47
Gambar 4.25	Melalui ApateDNS Malware menghubungi beberapa domain .....	48
Gambar 4.26	Informasi status dari domain redtable.biz .....	48
Gambar 4.27	informasi dari pemilik domain redtable.biz .....	49
Gambar 4.28	Mengambil paket data malware menggunakan Wireshark .....	50
Gambar 4.29	mendapatkan informasi ippublic dalam bentuk plain .....	50
Gambar 4.30	Tampilan komunikasi menggunakan SSL .....	50
Gambar 4.31	Linked Libraries dan Function.....	53
Gambar 4.32	Contoh tampilan BinText dan string yang dihasilkan.....	56
Gambar 4.33	Bintext dan string yang dihasilkan.....	56
Gambar 4.34	Bintext dan string yang dihasilkan.....	57
Gambar 4.35	Bintext dan string yang dihasilkan.....	57
Gambar 4.36	Analisis malware dengan olly dbg .....	57
Gambar 4.37	Ollydbg menampilkan proses unpacking.....	58
Gambar 4.38	Ollydbg menampilkan lokasi dirinya.....	58
Gambar 4.39	Pemanggilan modul cryptbas.dll.....	58
Gambar 4.40	Karakteristik Malware Cryptolocker .....	61

## Takarir dan Singkatan

AES	: Advanced Encryption Standard
ASCII	: American Standard Code for Information Interchange
CTU	: Counter Threat Unit
CCTV	: Closed-circuit television
DHCP	: Dynamic Host Configuration Protocol
DLL	: Dynamic Link Library
DNS	: Dynamic Name Server
Email	: Electronic mail
EoC	: End of Cluster
EoF	: End of file
GUI	: Graphical User Interface
HTTP	: Hypertext Transfer Protocol
IP Address	: Internet Protocol Address
Mac Address	: Media Access Control Address
MMS	: Multimedia Message Service
MSDN Library	: Microsoft Developer Network Library
NSIS	: Nullsoft Scriptable Install System
PDA	: Personal Digital Assistant
SMS	: Short Message Service
SDM	: Sumber Daya Manusia
TKP	: Tempat Kejadian Perkara
TCP	: Transmission Control Protocol
URL	: Uniform Resource Locator