

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	i
LEMBAR PENGESAHAN	ii
ABSTRAK	iii
<i>ABSTRACT</i>	iv
LEMBAR PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xiii
DAFTAR LAMPIRAN	xiv
DAFTAR ISTILAH	xv
BAB I PENDAHULUAN.....	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah.....	2
I.3 Tujuan Penelitian.....	2
I.4 Batasan Penelitian	2
I.5 Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA	4
II.1 <i>Malware (Malicious software)</i>	4
II.1.1 Jenis-jenis <i>Malware</i>	4
II.1.2 Analisis <i>Malware</i>	5
II.1.2.1 Analisis Dinamis	5
II.2 <i>Windows Registry</i>	6
II.3 <i>Dynamic Link Libraries (DLLs)</i>	7

II.4	<i>API Call</i>	7
II.5	<i>Antivirus Software</i>	8
II.5.1	<i>Signature Based Detection</i>	8
II.5.2	<i>Heuristic Based Detection</i>	9
II.6	<i>Fitur Removable Drive Protection</i>	9
II.7	<i>Computing Resources</i>	10
II.8	<i>Profiling</i>	10
II.9	<i>State of the Art</i>	11
BAB III	METODOLOGI PENELITIAN	14
III.1	Kerangka Berpikir	14
III.2	Sistematika Penelitian	15
III.2.1	Tahap Awal	17
III.2.2	Tahap Hipotesis	17
III.2.3	Tahap Desain	17
III.2.4	Tahap Simulasi dan Pengujian	18
III.2.5	Tahap Analisis	18
III.2.6	Tahap Akhir	18
III.3	Pengumpulan Data	18
III.4	Pengolahan Data	19
III.5	Metode Evaluasi	19
BAB IV	SKENARIO PENGUJIAN	20
IV.1	Perancangan Sistem	20
IV.1.1	Spesifikasi <i>Hardware</i>	20
IV.1.2	Spesifikasi <i>Software</i>	22
IV.1.2.1	Fitur Regshot	26
IV.1.2.2	Fitur Process Explorer	27

IV.1.2.3	Fitur SpyStudio	28
IV.1.3	Desain Lingkungan Virtual.....	29
IV.2	Skenario Pengujian	30
IV.2.1	Skenario Pengujian Aktivitas <i>Malware</i>	31
IV.2.2	Skenario Pengujian Analisis Fitur Antivirus	33
IV.3	Sampel <i>Malware</i>	34
IV.4	Tujuan Pengujian	36
BAB V	PENGUJIAN	37
V.1	Pengujian	37
V.1.1	Pengujian <i>Malware</i> Menggunakan <i>Tools</i> Analisis Dinamis.....	37
V.1.1.1	Sampel <i>Malware</i> 1 <i>Trojan</i>	38
V.1.1.2	Sampel <i>Malware</i> 2 <i>Trojan</i>	41
V.1.1.3	Sampel <i>Malware</i> 3 <i>Ransomware</i>	43
V.1.1.4	Sampel <i>Malware</i> 4 <i>Ransomware</i>	46
V.1.1.5	Sampel <i>Malware</i> 5 <i>Downloader</i>	49
V.1.1.6	Sampel <i>Malware</i> 6 <i>Downloader</i>	51
V.1.2	Pengujian Antivirus	54
V.1.2.1	Pengujian <i>Removable Drive Protection</i>	54
V.1.2.1.1	Antivirus Avast.....	54
V.1.2.1.2	Antivirus Kaspersky	59
V.1.2.1.3	Antivirus Avira.....	62
V.1.2.1.4	Antivirus McAfee.....	66
V.1.2.1.5	Antivirus Windows Defender.....	69
BAB VI	ANALISIS	72
VI.1	Hasil Analisis	72
VI.1.1	Analisis <i>Malware</i> Pada <i>Tools</i> Analisis Dinamis.....	72

VI.1.2	Analisis Hasil pada Antivirus	78
VI.1.2.1	Analisis Hasil Fitur <i>Removable Drive Protection</i>	78
VI.2	Analisis Perbandingan	99
VI.2.1	Perbandingan Total Aktivitas <i>Malware</i>	100
VI.2.2	Perbandingan Metrik pada Sampel <i>Malware</i>	101
VI.2.3	Perbandingan Total Aktivitas <i>Malware</i> dengan Metrik Antivirus .	106
VI.2.4	Perbandingan <i>Software</i> Antivirus	110
BAB VII	KESIMPULAN DAN SARAN.....	118
VII.1	Kesimpulan	118
VII.2	Saran	119
DAFTAR PUSTAKA	120
LAMPIRAN	124