

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN ORISINALITAS	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR DAN ILUSTRASI	viii
DAFTAR TABEL	ix
DAFTAR ISTILAH	x
DAFTAR SINGKATAN	xii
DAFTAR LAMPIRAN	xiv
Bab I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	3
I.3 Tujuan Penelitian	3
I.4 Manfaat Penelitian	3
I.5 Batasan Masalah	4
I.6 Batasan Implementasi	4
I.7 Sistematika Penulisan	4
Bab II LANDASAN TEORI	6
II.1 <i>Malware</i>	6
II.1.1 Jenis-jenis <i>malware</i>	6
II.2 <i>Malware Analysis</i>	7
II.2.1 <i>Static Analysis</i>	7
II.2.1.1 <i>Signature-based</i>	7
II.2.1.2 <i>Heuristic-based</i>	8
II.2.2 <i>Dynamic Analysis</i>	8
II.2.2.1 <i>Behavior-based</i>	8
II.3 <i>API Windows</i>	9
II.3.1.1 <i>API Network</i>	9

II.4	<i>State of Art</i>	10
Bab III	METODOLOGI PENELITIAN	12
III.1	Konseptual Model	12
III.2	Sistematika Penelitian	13
III.2.1	Tahap Awal	15
III.2.2	Tahap Design	15
III.2.3	Tahap Simulasi dan Pengujian	15
III.2.4	Tahap Analisis	15
III.2.5	Tahap Akhir	16
Bab IV	SKENARIO PENGUJIAN	17
IV.1	Rancangan Sistem	17
IV.1.1	Instrumen <i>Hardware</i>	17
IV.1.2	Instrumen <i>Software</i>	18
IV.2	Skenario Pengujian	20
IV.3	Tujuan Pengujian	23
Bab V	PENGUJIAN DAN ANALISIS HASIL	24
V.1	Pengujian	24
V.1.1	Pengujian dengan Cuckoo Sandbox	24
V.1.2	Pengujian dengan Wireshark	25
V.1.2.1	Behavior Malware pada Trafik Jaringan	25
V.1.2.2	<i>Payload</i>	28
V.1.2.3	<i>Bandwidth</i> Trafik Jaringan	30
V.2	Analisis	31
V.2.1	Hasil Analisis dengan Urutan API <i>Network</i>	31
V.2.2	Hasil Analisis Terhadap Trafik Jaringan	32
V.2.3	Dampak <i>Malware</i> Terhadap Trafik Jaringan	34
Bab VI	KESIMPULAN DAN SARAN	48
VI.1	Kesimpulan	48
VI.2	Saran	49
	DAFTAR PUSTAKA	50