

DAFTAR ISI

LEMBAR PENGESAHAN.....	iii
PERNYATAAN KEASLIAN PROYEK AKHIR.....	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xii
INTISARI.....	xiii
ABSTRACT.....	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Proyek Akhir.....	4
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA.....	6
2.1 Tinjauan Pustaka.....	6
2.2 Dasar Teori.....	13
2.2.1 Malicious software (Malware).....	13
2.2.2 Jenis – Jenis Malware.....	13
2.2.3 WannaCry Ransomware.....	15
2.2.4 Eternal Blue.....	16
2.2.5 Double Pulsar.....	17
2.2.6 Teknik Analisis Malware.....	17
2.2.7 Reverse Engineering.....	18
2.2.8 Tool Analisis.....	18
2.2.9 Incident Response.....	22
2.2.10 Indicator of Compromise.....	22



2.2.11 Indicator of Attack (IOA)	23
BAB III METODE PROYEK AKHIR.....	24
3.1 Alat Penelitian.....	24
3.2 Bahan Penelitian.....	25
3.3 Alur Pengerjaan Proyek Akhir.....	26
3.4 Topologi Sistem.....	29
3.5 Instalasi dan Konfigurasi Sistem.....	30
3.5.1 Instalasi Perangkat Lunak Oracle VM VirtualBox.....	30
3.5.2 Instalasi Sistem Operasi Windows.....	30
3.5.3 Instalasi Flare Virtual Machine.....	34
3.5.4 Instalasi Remnux Virtual Machine.....	41
3.5.5 Instalasi dan Konfigurasi InetSim.....	42
3.5.6 Konfigurasi Transfer Malware.....	46
3.5.7 Skenario Pengujian.....	49
BAB IV HASIL DAN PEMBAHASAN.....	50
4.1 Analisis Statis Malware.....	50
4.1.1 Identifikasi File PE.....	50
4.1.2 Ekstrak String.....	56
4.1.3 File Packed pada Malware.....	61
4.1.4 Fingerprinting pada Malware.....	64
4.1.5 Scanning File Biner.....	65
4.2 Reverse Engineering menggunakan Ghidra.....	67
4.3 XIA File pada Malware.....	69
4.4 Analisis Dinamis Malware.....	77
BAB V PENUTUP.....	80
5.1 Kesimpulan.....	80
5.2 Saran.....	81
DAFTAR PUSTAKA.....	82
LAMPIRAN.....	86