

## DAFTAR ISI

PENGESAHAN PEMBIMBING.....	i
PENGESAHAN PENGUJI.....	ii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR .....	iii
ABSTRAK.....	iv
<i>ABSTRACT</i> .....	v
HALAMAN PERSEMBAHAN DAN MOTTO.....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR .....	xiii
BAB I PENDAHULUAN.....	I-1
1.1. Latar Belakang .....	I-1
1.2. Rumusan Masalah .....	I-4
1.3. Tujuan Penelitian.....	I-4
1.4. Batasan Masalah.....	I-4
1.5. Manfaat Penelitian.....	I-5
1.6. Metodologi Penelitian .....	I-5
1.7. Sistematika Penulisan.....	I-7

BAB II TINJAUAN PUSTAKA.....	II-1
2.1. <i>Malware</i> .....	II-1
2.2. Klasifikasi <i>Malware</i> .....	II-1
2.3. <i>Malware AQUVAPRN.exe</i> .....	II-4
2.4. Analisis <i>Malware (Malware Analysis)</i> .....	II-5
2.5. <i>Reverse Engineering</i> .....	II-8
2.6. <i>Memory Forensics</i> .....	II-10
2.7. <i>State Of The Art</i> .....	II-10
2.8. Matriks Penelitian.....	II-15
 BAB III METODOLOGI PENELITIAN.....	 III-1
3.1. Metodologi Penelitian .....	III-1
3.2. Penelitian Dasar.....	III-2
3.2.1. Identifikasi Masalah.....	III-2
3.2.2. Studi Literatur .....	III-2
3.3. <i>Malware Analysis</i> .....	III-3
3.3.1. <i>Static Analysis</i> .....	III-3
3.3.2. <i>Dynamic Analysis</i> .....	III-3
3.3.3. <i>Reverse Engineering</i> .....	III-4
3.3.4. <i>Memory Forensics</i> .....	III-5
 BAB IV HASIL DAN PEMBAHASAN .....	 IV-1

4.1.	Penelitian Dasar.....	IV-1
4.1.1.	Identifikasi Masalah Penelitian.....	IV-1
4.1.2.	Studi Literatur.....	IV-2
4.2.	Kebutuhan Sistem.....	IV-2
4.3.	<i>Malware Analysis</i> .....	IV-3
4.3.1.	Mengambil Sampel <i>Malware</i> .....	IV-3
4.3.2.	Analisa Jumlah Hash.....	IV-4
4.3.3.	<i>Setting Up Virtual Machine</i> .....	IV-7
4.3.4.	<i>Setting Up Virtual Network</i> .....	IV-7
4.3.5.	<i>Starting Process Explorer</i> .....	IV-10
4.3.6.	<i>Reverse Engineering</i> .....	IV-18
4.3.7.	<i>Memory Forensics</i> .....	IV-19
BAB V SIMPULAN DAN SARAN.....		V-1
5.1.	Simpulan.....	V-1
5.2.	Saran.....	V-2
DAFTAR PUSTAKA		
LAMPIRAN		