

## DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR . <b>Error! Bookmark not defined.</b>	
HALAMAN PERSEMBAHAN .....	iv
HALAMAN MOTO .....	vi
KATA PENGANTAR .....	vii
SARI.....	ix
GLOSARIUM.....	x
DAFTAR ISI.....	xi
DAFTAR TABEL .....	xiii
DAFTAR GAMBAR.....	xiv
BAB I PENDAHULUAN.....	16
1.1 Latar Belakang .....	16
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan Penelitian .....	2
1.5 Manfaat Penelitian .....	2
1.6 Metode Penelitian .....	2
1.7 Sistematika Penulisan .....	3
BAB II TINJAUAN PUSTAKA.....	5
2.1 Penelitian Sebelumnya.....	5
2.2 Landasan teori .....	5
2.2.1 <i>Ransomware</i> .....	7
2.2.2 Jenis jenis <i>Ransomware</i> .....	8
2.2.3 Sandbox .....	12
2.2.4 Cuckoo Sandbox.....	13
2.2.5 Volatility.....	14
BAB III METODE PENELITIAN .....	15
3.1 Langkah Penelitian.....	15
3.1.1 Alur Penelitian Cuckoo Sandbox .....	15
3.2 Studi Pustaka.....	17
3.3 Analisa Kebutuhan Sistem.....	17
3.3.1 Analisis Kebutuhan Perangkat Keras .....	17
3.3.2 Analisis Kebutuhan Perangkat Lunak .....	17
3.3.3 Analisis Kebutuhan Lainnya .....	18
3.3.4 Analisis kebutuhan proses .....	19
3.4 <i>Ransomware</i> Analisis.....	19
BAB IV IMPLEMENTASI DAN HASIL PENGUJIAN .....	21
4.1 Instalasi Sistem .....	21
4.1.1 Instalasi CuckooSandbox .....	21
4.2 Implementasi Perangkat Lunak.....	26
4.2.1 Membangun Lingkungan Kerja Simulasi dan Analisis.....	26
4.2.2 Instalasi Cuckoo dan Cuckoo Sandbox .....	27
4.2.3 Implementasi Analisis Cuckoo.....	30
4.1.4 Hasil Analisis Cuckoo .....	35
4.1.5 Grafik hasil analisis <i>Ransomware</i> .....	38
4.1.6 Hasil Monitoring cacti.....	40

4.1.7	Evolusi Ransomware.....	45
	BAB V KESIMPULAN DAN SARAN.....	49
5.1	Kesimpulan .....	49
5.2	Saran.....	49
	DAFTAR PUSTAKA .....	50
	LAMPIRAN .....	51



## DAFTAR TABEL

Tabel 2. 1 Tabel jurnal.....	5
Tabel 4. 1 Tabel Antivirus.....	41
Tabel 4. 2 Klasifikasi struktur serangan <i>Ransomware</i> .....	46



## DAFTAR GAMBAR

Gambar 2. 1 tampilan <i>Ransomware</i> Wannacry .....	8
Gambar 2. 2 Tampilan <i>Ransomware</i> Petya.....	10
Gambar 2. 3 Tampilan PC yang terinfeksi Petya.....	11
Gambar 2. 4 Tampilan PC yang terinfeksi Badrabbbit.....	12
Gambar 2. 5 Alur Analisis Cuckoo Sandbox.....	14
Gambar 3. 1 Alur analisis Cuckoo Sandbox .....	16
Gambar 3. 2 Dashboard Cuckoo.....	25
Gambar 3. 3 Dashboard Cuckoo.....	25
Gambar 3. 4 Menu Recent Cuckoo.....	26
Gambar 4. 1 Instalasi Virtualbox.....	26
Gambar 4. 2 Install Python .....	27
Gambar 4. 3 Instalasi Mongoddb.....	27
Gambar 4. 4 Instalasi SQLAlchemy dan BSON.....	27
Gambar 4. 5 Instalasi paket opsional .....	28
Gambar 4. 6 instalasi Cuckoo melalui terminal.....	28
Gambar 4. 7 Konfigurasi skrip cuckoo.conf.....	29
Gambar 4. 8 Konfigurasi skrip auxialary.conf.....	29
Gambar 4. 9 Konfigurasi skrip processing.conf .....	29
Gambar 4. 10 konfigurasi skrip reporting.conf.....	30
Gambar 4. 11 Perintah untuk membuka web Cuckoo .....	31
Gambar 4. 12 Halaman Submit sampel malware.....	31
Gambar 4. 13 Submit malware EXE.....	32
Gambar 4. 14 menjalankan proses analisis.....	32
Gambar 4. 15 menjalankan mesin virtual yang sudah di konfigurasi .....	33
Gambar 4. 16 menjalankan Cuckoo.....	33
Gambar 4. 17 proses analisis pada mesin virtual.....	34
Gambar 4. 18 Analisis Selesai .....	34
Gambar 4. 19 Antarmuka Web Cuckoo.....	35
Gambar 4. 20 hasil dari behaviorial analisis dari Wannacry.exe.....	35
Gambar 4. 21 proses perilaku sampel malware Wannacry.....	36
Gambar 4. 22 Diagram evolusi <i>Ransomware</i> berdasarkan jumlah file yang diakses.....	39

Gambar 4. 23 Diagram evolusi <i>Ransomware</i> berdasarkan jumlah file penting yang diakses.	40
Gambar 4. 24 proses sebelum dijalankan <i>Ransomware</i> .....	41
Gambar 4. 25 proses CPU sebelum <i>Ransomware</i> dijalankan.....	41
Gambar 4. 26 hasil setelah <i>Ransomware</i> dijalankan .....	41
Gambar 4. 27 hasil monitoring proses CPU setelah <i>Ransomware</i> dijalankan.....	42
Gambar 4. 28 proses CPU dari task manager .....	42
Gambar 4.29 hasil setelah <i>Ransomware</i> Petya dijalankan.....	41
Gambar 4.30 hasil CPU Petya dari task manager.....	42
Gambar 4.31 hasil setelah <i>Ransomware</i> NotPetya dijalankan.....	42
Gambar 4.32 hasil CPU NotPetya dari task manager.....	42
Gambar 4.33 hasil setelah <i>Ransomware</i> Badrabbid dijalankan.....	43
Gambar 4.34 hasil monitoring cacti <i>Ransomware</i> Badrabbid.....	43
Gambar 4.35 Evolusi struktur serangan <i>Ransomware</i> .....	44
Gambar 4.36 tingkatan bahaya <i>Ransomware</i> .....	45

