DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR i

LEMBAR PENGUJI SIDANG TUGAS AKHIR ii

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR iii

ABSTRAK iv

ABSTRACT v

MOTTO DAN PERSEMBAHAN vi

KATA PENGANTAR vii

DAFTAR ISI x

DAFTAR GAMBAR xiii

DAFTAR TABEL I-1

I. BAB I I-2

1.1 Latar Belakang I-2

1.2 Rumusan Masalah I-4

1.3 Tujuan Penelitian I-5

1.4 Batasan Masalah I-5

1.5 Manfaat Penelitian I-5

1.6 Metode Penelitian I-6

II. BAB II I-1

TINJAUAN PUSTAKA I-1

2.1 Landasan Teori I-1

2.1.1 *Malware* I-1

2.1.2 *Analysis Static* I-2

2.1.3 *Analysis Dinamic* I-3

2.1.4 *Analysis Hybrid* I-4

2.1.5 *Signature-based Detection* I-4

2.1.6 *Reverse Engineering* I-4

2.2 *State of The Art* (SOTA) Penelitian.....I-6

2.3 Matriks Penelitian.....I-10

2.4 *Gap Research* I-19

III. BAB III..... II-1

METODOLOGI PENELITIAN II-1

3.1 *Road Map* Penelitian II-1

3.2 Tahapan Penelitian II-5

IV. BAB IV III-1

HASIL DAN PEMBAHASAN III-1

4.1 *Study Literature Review* III-1

4.2 *Observations*..... III-2

4.3 *Prepations* III-3

4.4 *Malware Using Analisis Static-Dynamic, Reverese Engineering and Signature-based Detection* III-4

4.4.1 Tahapan Analisis..... III-4

4.4.2 *Hybrid Analysis*..... III-7

4.4.3 *Reverse Engineering* III-11

4.4.4 Signature-based Detection III-19

4.5 *Report / Documentation* III-31

4.6 Persamaan dan perbandingan hasil analisis *malware wannacry* III-35

4.7 Pencegahan *Malware WannaCry* III-37

V. BAB V IV-1

SIMPULAN DAN SARAN IV-1

5.1 Simpulan IV-1

5.2 Saran IV-2

DAFTAR PUSTAKA 3

DAFTAR GAMBAR

Gambar 2.1 Deteksi *Malware* I-2

Gambar 3.1 *Road Map* 1 ..... II-1

Gambar 3.2 Road Map Penelitian 2 ..... II-3

Gambar 3.3 Alur Penelitian..... II-5

Gambar 4.1 Jenis Ransomware III-2

Gambar 4.2 Any.run..... III-5

Gambar 4.3 HashCal Malware WannaCry..... III-5

Gambar 4.4 Sampel Malware WannaCry III-6

Gambar 4.5 Virtual Machine..... III-7

Gambar 4.6 structure Hybrid analis III-8

Gambar 4.7 Apate DNS III-9

Gambar 4.8 Uji Coba Ping..... III-10

Gambar 4.9 Filter Process Monitor..... III-10

Gambar 4. 10 Proses monitoring malware WannaCry..... III-11

Gambar 4.11 Hasil Analsisis IDA PRO..... III-12

Gambar 4.12 Hasil Aanalisis Ghidra III-16

Gambar 4.13 Analisis Virus Total III-19

Gambar 4.14 Hash MD5 IDA PRO III-20

Gambar 4.15 Hash MD5 PeStudio..... III-20

Gambar 4.16 File Name aWanaCry..... III-21

Gambar 4.17 String Unik..... III-22

Gambar 4.18 Network Siganture..... III-23

Gambar 4.19 Pola Enkripsi Windows III-24
Gambar 4.20 Pola Enkripsi IDA PRO III-24
Gambar 4.21 Pemanggilan Fungsi Khusus III-25
Gambar 4.22 RegSetValueExA III-27
Gambar 4.23 fopen III-27
Gambar 4.24 memcpy III-28
Gambar 4.25 RegCreateKeyExA III-30
Gambar 4.26 Alur penyerangan ransomware III-31
Gambar 4.27 Malware WannaCry 2.0 ..... III-32
Gambar 4.28 Halaman Windows Terserang WannaCry III-32
Gambar 4.29 Wana Decryptor 2.0 ..... III-34
Gambar 4.30 File-File terserang WannaCry III-34

DAFTAR TABEL

Tabel 2.1 State of The Art (SOTA) Penelitian.....I-6

Tabel 2.2 Matriks peneltian.....I-10

Tabel 2.3 Gap Research/Terdekat I-19

Tabel 4.1 Tools/Sotware Requirement yang digunakan IV-3

Tabel 4.2 Informasi Malware.....IV-6

Tabel 4.3 Konfigurasi Windows 10 .....IV-7

Tabel 4.4 Konfigurasi Windows 11 .....IV-7

Tabel 4.5 Tab Import.....IV-12

Tabel 4.6 Disassambler Malware WannaCry.....IV-17

Tabel 4.7 Penjelasan MD5 .....IV-21

Tabel 4.8 Penjelasan File Name.....IV-21

Tabel 4.9 Penjelasan String.....IV-22

Tabel 4.10 Penjelasan Network Signature IV-23

Tabel 4.11 Penjelasan Pola Enkripsi.....IV-25

Tabel 4.12 Penjelasan Pemanggilan Fungsi Khusus.....IV-26

Tabel 4.13 Kode Instruksi.....IV-27

Tabel 4.14 Instruksi Networking.....IV-28

Tabel 4.15 Instruksi enkripsi dan dekripsi IV-29

Tabel 4.16 Instruksi Manipulasi File dan Registri IV-30

Tabel 4.17 Persamaan dua metode.....IV-35

Tabel 4.18 Parameter Signature WannaCry.....IV-36