DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS i
LEMBAR PENGESAHAN ii
ABSTRAK iii
ABSTRACT iv
KATA PENGANTAR v
DAFTAR ISI vi
DAFTAR GAMBAR x
DAFTAR TABEL xii
DAFTAR LAMPIRAN xiii
DAFTAR ISTILAH xiv
BAB I PENDAHULUAN 1
I.1 Latar Belakang 1
I.2 Perumusan Masalah 2
I.3 Tujuan Penelitian 2
I.4 Batasan Masalah 3
I.5 Manfaat Penelitian 3
BAB II TINJAUAN PUSTAKA 4
II.1 *Malware (Malicious Software)* 4
II.2 Antivirus *Software* 5
II.2.1 *Signature Based Detection* 6
II.2.2 *Heuristic Based Detection* 6
II.3 Fitur *Real-time Protection* 7
II.4 Analisis *Malware* 7
II.5 Analisis Statis 8

II.5.1 *Strings* 8
II.5.2 *Strings Blacklist* 8
II.5.3 *Section* 9
II.5.4 *File Ratio* 9
II.5.5 *Function* 9
II.5.6 *Libraries* 10
II.6 *Computing Resource* 10
II.7 *Profiling* 10
II.8 *State of The Art* 11
BAB III METODOLOGI PENELITIAN 15
III.1 Kerangka Konseptual 15
III.2 Sistematika Penelitian 16
III.2.1 Tahap Awal 18
III.2.2 Tahap Hipotesis 18
III.2.3 Tahap Desain 18
III.2.4 Tahap Simulasi dan Pengujian 19
III.2.5 Tahap Analisis 19
III.2.6 Tahap Akhir 19
III.3 Pengumpulan Data 19
III.4 Pengolahan Data 20
III.5 Metode Evaluasi 20
BAB IV SKENARIO PENGUJIAN 21
IV.1 Perancangan Sistem 21
IV.1.1 Instrumen *Hardware* 21
IV.1.2 Instrumen *Software* 22
IV.1.2.1 Fitur PE Studio 26

IV.1.2.2 Fitur Cuckoo Sandbox 27
IV.1.2.3 Design Lingkungan Virtual 28
IV.2 Skenario Pengujian 28
IV.2.1 Skenario Pengujian Analisis Statis pada *Malware* 29
IV.2.2 Skenario Pengujian Fitur Antivirus 31
IV.3 Sampel *Malware* 32
IV.4 Tujuan Pengujian 34
BAB V PENGUJIAN DAN DATA 36
V.1 Pengujian 36
V.1.1 Pengujian *Malware* Menggunakan *Static Tools* Analisis 36
V.1.1.1 Sampel *Malware* 1 *Trojan* 36
V.1.1.2 Sampel *Malware* 2 *Trojan* 38
V.1.1.3 Sampel *Malware* 3 *Ransomware* 39
V.1.1.4 Sampel *Malware* 4 *Ransomware* 41
V.1.1.5 Sampel *Malware* 5 *Downloader* 43
V.1.1.6 Sampel *Malware* 6 *Downloader* 44
V.1.2 Pengujian Antivirus 46
V.1.2.1 Pengujian Fitur *Real-time* 46
V.1.2.1.1 Avast 47
V.1.2.1.2 Kaspersky 51
V.1.2.1.3 Avira 53
V.1.2.1.4 McAfee 56
V.1.2.1.5 Windows Defender 58
BAB VI ANALISIS 62
VI.1 Hasil Analisis *Malware* pada *Tools* Analisis Statis 62
VI.2 Hasil Analisis Pada Antivirus 69

VI.2.1 Antivirus Avast 70
VI.2.2 Antivirus Kaspersky 73
VI.2.3 Antivirus Avira 76
VI.2.4 Antivirus McAfee 80
VI.2.5 Antivirus Windows Defender 83
VI.3 Analisis Perbandingan 91
VI.3.1 Perbandingan Total Temuan *Malware* 91
VI.3.2 Perbandingan Metrik Antivirus 92
VI.3.3 Perbandingan Total Aktivitas *Malware* dengan Metrik Antivirus ... 98
VI.3.4 Perbandingan *Software* Antivirus 102
BAB VII KESIMPULAN DAN SARAN 109
VII.1 Kesimpulan 109
VII.2 Saran 111
DAFTAR PUSTAKA 112
LAMPIRAN 115