DAFTAR ISI

LEMBAR PERNYATAAN i
LEMBAR PENGESAHAN ii
ABSTRAK iii
ABSTRACT iv
LEMBAR PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR GAMBAR ix
DAFTAR TABEL x
1 PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Perumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan 3
1.5 Hipotesis 3
1.6 Metodologi Penelitian 3
2 TINJAUAN PUSTAKA 5
2.1 Komputer Forensik 5
2.1.1 Traditional Forensics 6
2.1.2 Live Forensics 7
2.1.3 Barang Bukti 8
2.1.4 Forensics Memory 9
2.2 Citadel Malware 10
2.3 Malware Analysis 10
2.3.1 Malware Life Cycle 11
2.3.2 Malware Investigation 12
2.4 Philip Schwartz Malware Analysis 13
2.5 Website VirusTotal 14
3 PERANCANGAN SISTEM INVESTIGASI 16
3.1 Gambaran Umum 16
3.2 Perancangan Sistem Investigasi 16
3.2.1 Instalasi Sistem Uji 17
3.2.2 Inisialisasi Skema 19
3.3 Live Forensics 22
3.3.1 Live Acquisition 22

3.3.2 Penanganan Bukti Digital 23
3.3.3 Analisis Process 24
3.4 Malware Forensics 24
3.4.1 Analisis Network 25
3.4.2 Analisis Apihooks 25
3.4.3 Analisis Registry 25
3.4.4 Analisis Dump Process 26
3.4.5 Analisis File Dump 26
3.5 Evaluasi Kerangka Investigasi 26
4 ANALISIS HASIL INVESTIGASI 28
4.1 Live Forensics 28
4.1.1 Live Acquisition 28
4.1.2 Penanganan Bukti Digital 28
4.2 Malware Forensics 35
4.2.1 Analisis Network 35
4.2.2 Analisis Apihooks 38
4.2.3 Analisis Registry 40
4.2.4 Analisis Dump Process 42
4.2.5 Analisis File Dump 43
4.3 Evaluasi Kerangka Investigasi 48
5 PENUTUP 51
5.1 Kesimpulan 51
5.2 Saran 51
DAFTAR PUSTAKA 52