

DAFTAR GAMBAR

Gambar 2.1 Flowchart traditional forensics [8].....	7
Gambar 2.2 Flowchart live forensics [8]	8
Gambar 2.3 Malware analysis life cycle [5]	11
Gambar 2.4 Kerangka investigasi : Philip	14
Gambar 3.1 Gambaran umum sistem investigasi	16
Gambar 3.2 Topologi sistem uji.....	18
Gambar 3.3 Konfigurasi VMware	19
Gambar 3.4 Inetsim yang berjalan	20
Gambar 3.5 Citadel RAT Builder & Panel	22
Gambar 3.6 Live Acquisition.....	23
Gambar 3.7 Website Virus Total	24
Gambar 4.1 soft.exe : website virus total.....	29
Gambar 4.2 Analisis soft.exe : website virus total.....	29
Gambar 4.3 imageinfo : Kali Linux	30
Gambar 4.4 Analisis process : pslist	31
Gambar 4.5 Proses tersembunyi	32
Gambar 4.6 Analisis process : psscan.....	32
Gambar 4.7 Perbandingan Task manager & Pslist	33
Gambar 4.8 Analisis process : psxview	34
Gambar 4.9 Analisis process : pstree	35
Gambar 4.10 Analisis network : netscan	36
Gambar 4.11 Koneksi Penyerang ke Korban.....	36
Gambar 4.12 Analisis network : malfind.....	37
Gambar 4.13 Analisis apihooks : handles.....	38
Gambar 4.14 Volshell : taskeng.exe	40
Gambar 4.15 Analisis registry : Hivelist.....	40
Gambar 4.16 Analisis registry : printkey winlogon.....	41
Gambar 4.17 Analisis registry : Userassist	41
Gambar 4.18 Analisis Dump process: Procdump	42
Gambar 4.19 Analisis Dump process : Malfind dump	42
Gambar 4.20 Analisis Dump process : Vaddump.....	42
Gambar 4.21 Live Scanning : Procdump.....	44
Gambar 4.22 Live Scanning : Malfinddump	45
Gambar 4.23 Live Scanning : Vaddump.....	47
Gambar 4.24 Diagram input-proses-output	48
.....	Error! Bookmark not defined.

