

Daftar Gambar

Gambar 2.1 Proses <i>Network forensic</i>	4
Gambar 2.2 <i>Flowchart</i> proses <i>Traditional Forensic</i>	5
Gambar 2.3 <i>Flowchart</i> proses <i>Live Forensic</i>	6
Gambar 3.1 Blok diagram sistem.....	11
Gambar 3.2. <i>Flowchart</i> Proses Penanganan Kasus menggunakan Aplikasi RAD	11
Gambar 3.3 <i>Flowchart</i> aplikasi RAD	12
Gambar 3.4 Proses <i>dumping</i> RAM menggunakan mdd.....	14
Gambar 3.5 Proses <i>dumping</i> RAM menggunakan Dumpit	14
Gambar 3.6 Antarmuka TCPView	14
Gambar 3.7 Antarmuka Openports	15
Gambar 3.8 Proses <i>write protect</i> menggunakan BitLocker Drive Encryption	16
Gambar 3.9 Proses pemilihan sumber bukti digital dan informasi tentang bukti digital	16
Gambar 3.10 Proses <i>imaging</i> dan verifikasi nilai MD5 dan SH1	17
Gambar 3.11 Hasil verifikasi pembuatan <i>image</i>	17
Gambar 3.12 Rancangan antar muka aplikasi RAD	18
Gambar 3.13 Rancangan antar muka tabulasi <i>tools</i> pada RAD	18
Gambar 3.14 Topologi Pengujian Serangan	19
Gambar 3.15 <i>Console</i> metasploit	21
Gambar 4.1. Penggunaan <i>Physical memory</i> Kasus 1	26
Gambar 4.2. Penggunaan <i>Virtual memory</i> Kasus 1	27
Gambar 4.4. Grafik Penggunaan <i>Physical memory</i> Kasus 2	29
Gambar 4.5. Grafik Penggunaan <i>Virtual memory</i> Kasus 2.....	30
Gambar 4.6 Penggunaan <i>Physical memory</i> kasus 3.....	32
Gambar 4.7. Penggunaan <i>Virtual memory</i> kasus 3	33
Gambar 4.8 Grafik penggunaan <i>Physical memory</i> kasus 4.....	35
Gambar 4.9 Grafik penggunaan <i>Virtual memory</i> kasus 4	36
Gambar 4.10. Grafik perbandingan penggunaan kedua <i>tools</i> terhadap <i>physical memory</i> untuk tiap kasus	38
Gambar 4.11 Grafik perbandingan penggunaan kedua <i>tools</i> terhadap <i>virtual memory</i> untuk tiap kasus	39