

## Daftar Isi

Lembar Pengesahan Pembimbing.....	<b>Error! Bookmark not defined.</b>
Lembar Pengesahan Penguji .....	<b>Error! Bookmark not defined.</b>
Abstrak .....	iii
Abstract .....	iv
Pernyataan Keaslian Tulisan .....	<b>Error! Bookmark not defined.</b>
Daftar Publikasi .....	vi
Halaman Kontribusi.....	vii
Halaman Persembahan.....	viii
Kata Pengantar.....	ix
Daftar Isi.....	x
Daftar Tabel.....	xiii
Daftar Gambar .....	xiv
Glosarium .....	xvii
BAB 1 Pendahuluan.....	1
1.1    Pendahuluan .....	1
1.2    Rumusan Masalah.....	4
1.3    Batasan Masalah .....	4
1.4    Tujuan Penelitian.....	4
1.5    Manfaat Penelitian.....	5
1.6    Metode Penelitian .....	5
BAB 2 Kajian Pustaka .....	7
2.1    Penelitian Terdahulu .....	7

2.2	Landasan Teori .....	10
2.2.1	Sistem Komputer .....	10
2.2.2	Sistem Operasi.....	10
2.2.3	RAM (Random Access Memory).....	10
2.2.4	Komputer Forensik .....	10
2.2.5	Live Forensik.....	11
2.2.6	Bukti Digital.....	12
2.2.7	Metasploit.....	12
2.2.8	Exploit.....	13
2.2.9	FTK Imager .....	13
2.2.10	Payload.....	14
2.2.11	Volatility Memory Forensics Tools.....	14
BAB 3 Metodologi Penelitian .....		15
3.1	Studi Pustaka .....	15
3.2	Persiapan Sistem dan Identifikasi Kebutuhan.....	15
3.2.1	Kebutuhan Perangkat Keras .....	16
3.2.2	Kebutuhan Perangkat Lunak .....	17
3.3	Skenario dan Simulasi Kasus .....	17
3.3.1	Simulasi Kasus .....	17
3.3.2	Simulasi Serangan .....	18
3.4	Investigasi RAM Forensik .....	19
3.5	Pembuatan Laporan .....	21
BAB 4 Hasil dan Pembahasan.....		22
4.1	Simulasi Serangan .....	22
4.2	Pencarian Bukti Digital dan akuisisi RAM.....	22
4.3	Proses Analisis.....	22

4.3.1	Akuisisi USB Drive yang menyimpan hasil capture FTK Imager pada RAM Windows 8.....	23
A.	Analisis file win8_infected.mem .....	24
4.3.2	Akuisisi USB Drive yang menyimpan hasil capture Magnet Forensics RAM Capturer pada RAM Windows 8 .....	30
A.	Analisis win8_infected.raw .....	32
4.3.3	Akuisisi USB Drive yang menyimpan hasil capture Dumpit pada RAM Windows 8.....	37
A.	Analisis KORBANEXPLOIT-20180816-222949.dmp.....	39
4.3.4	Akuisisi USB Drive yang menyimpan hasil capture FTK Imager pada RAM Windows 10.....	44
A.	Analisis win10_infected.mem .....	45
4.3.5	Akuisisi USB Drive yang menyimpan hasil capture Magnet Forensics RAM Capturer pada RAM Windows 10 .....	49
A.	Analisis win10_infected_magnet.raw .....	51
4.3.6	Akuisisi USB Drive yang menyimpan hasil capture Dumpit pada RAM Windows 10.....	57
A.	Analisis DESKTOP-2BUI657-20180823-033359.dmp.....	59
4.3.7	Analisis .....	64
BAB 5 Kesimpulan dan Saran.....		67
5.1	Kesimpulan.....	67
5.2	Saran .....	67
Daftar Pustaka.....		69

## Daftar Tabel

Tabel 2.1 Literature Review.....	8
Tabel 3.1 Laptop 1 .....	16
Tabel 3.2 Laptop 2 .....	16
Tabel 3.3 Laptop 3 .....	16
Tabel 3.4 Router MiFi.....	16
Tabel 3.5 USB drive .....	16
Tabel 3.6 Proses yang berjalan.....	20
Tabel 3.7 Barang bukti digital yang ditemukan .....	20
Tabel 4.1 Verifikasi nilai hash barang bukti 1 .....	23
Tabel 4.2 Tabel nama proses, PID dan direktori explorer.exe .....	28
Tabel 4.3 Koneksi IP mencurigakan.....	30
Tabel 4.4 Verifikasi nilai hash barang bukti 2 .....	31
Tabel 4.5 Nama proses, PID dan direktori explorer.exe.....	35
Tabel 4.6 Koneksi IP mencurigakan.....	37
Tabel 4.7 Verifikasi nilai hash barang bukti 3 .....	38
Tabel 4.8 Nama proses, PID dan direktori explorer.exe .....	42
Tabel 4.9 Koneksi IP mencurigakan.....	43
Tabel 4.10 Verifikasi nilai hash barang bukti 4 .....	45
Tabel 4.11 Verifikasi nilai hash barang bukti 5 .....	50
Tabel 4.12 Nama proses, PID dan direktori explorer.exe.....	55
Tabel 4.13 Koneksi IP mencurigakan.....	57
Tabel 4.14 Verifikasi nilai hash barang bukti 6.....	58
Tabel 4.15 Nama proses, PID dan direktori explorer.exe.....	62
Tabel 4.16 Koneksi IP mencurigakan.....	64
Tabel 4.17 Proses <i>malicious</i> yang berjalan pada Windows 8. ....	64
Tabel 4.18 Proses <i>malicious</i> yang berjalan pada Windows 10. ....	64
Tabel 4.19 Artefak digital yang ditemukan pada Windows 8.....	65
Tabel 4.20 Artefak digital yang ditemukan pada Windows 10.....	66

## Daftar Gambar

Gambar 1.1 Berita Serangan Siber di Indonesia (Sumber: nasional.kompas.com).....	1
Gambar 1.2 Presentase motivasi dibalik serangan (Sumber: Hackmageddon.com). ....	2
Gambar 2.1 Gambar Tampilan AccessData FTK Imager.....	13
Gambar 3.1 Alur Metodologi Penelitian.....	15
Gambar 3.2 Gambaran Umum Topologi Skenario Kasus .....	18
Gambar 3.3 Gambaran umum simulasi serangan.....	18
Gambar 3.4 Diagram Alur Proses Akuisisi RAM Komputer Windows.....	19
Gambar 4.1 Proses verifikasi nilai hash.....	23
Gambar 4.2 Proses Imaging dengan dc3dd tool.....	23
Gambar 4.3 Proses mount pada file fd_evidence.dd .....	24
Gambar 4.4 Direktori /mnt/evidence. ....	24
Gambar 4.5 Mencari informasi awal file win8_infected.mem.....	25
Gambar 4.6 Perintah menggunakan pslist.....	25
Gambar 4.7 Proses yang sedang berjalan dalam sistem .....	26
Gambar 4.8 Baris perintah menggunakan pstree.....	26
Gambar 4.9 Proses terlihat dalam tampilan <i>tree</i> .....	27
Gambar 4.10 Baris perintah menggunakan cmdline.....	27
Gambar 4.11 Hasil ketika perintah cmdline dijalankan.....	28
Gambar 4.12 Proses dump explorer.exe pada PID 3512 .....	29
Gambar 4.13 Perintah menggunakan plugin netscan.....	29
Gambar 4.14 Koneksi antar IP .....	29
Gambar 4.15 Nilai hash USB drive fisik. ....	30
Gambar 4.16 Proses Imaging USB drive fisik barang bukti.....	31
Gambar 4.17 Proses mount fd_evidence_magnet.dd.....	31
Gambar 4.18 Membuka direktori /mnt .....	32
Gambar 4.19 Menggunakan perintah imageinfo .....	32
Gambar 4.20 Proses yang sedang berjalan pada sistem.....	33
Gambar 4.21 Perintah menggunakan pstree.....	34
Gambar 4.22 Proses terlihat dalam tampilan <i>tree</i> .....	34
Gambar 4.23 Baris perintah menggunakan cmdline.....	34
Gambar 4.24 Hasil dari perintah cmdline. ....	35
Gambar 4.25 Proses dump explorer.exe PID 756.....	36

Gambar 4.26 Perintah menggunakan plugin netscan.....	36
Gambar 4.27 Koneksi antar IP. ....	36
Gambar 4.28 Nilai hash md5 USB drive fisik.....	37
Gambar 4.29 Proses Imaging dengan dc3dd tool.....	38
Gambar 4.30 Proses mount pada file fd_evidence_dumpit.dd.....	38
Gambar 4.31 Membuka direktori /mnt/evidence.....	39
Gambar 4.32 Menggunakan perintah imageinfo. ....	39
Gambar 4.33 Volatility tool gagal memberikan infomasi.....	40
Gambar 4.34 Proses yang sedang berjalan.....	40
Gambar 4.35 Menggunakan perintah pstree.....	41
Gambar 4.36 Proses terlihat dalam tampilan <i>tree</i> . ....	41
Gambar 4.37 Perintah menggunakan cmdline.....	41
Gambar 4.38 Proses dump explorer.exe PID 3236.....	42
Gambar 4.39 Perintah menggunakan plugin netscan.....	43
Gambar 4.40 Koneksi antar IP ....	43
Gambar 4.41 Nilai hash md5 USB drive fisik.....	44
Gambar 4.42 Proses imaging menggunakan dc3dd.....	44
Gambar 4.43 Proses mount dan membuka direktori /mnt.....	45
Gambar 4.44 Menggunakan perintah imageinfo ....	46
Gambar 4.45 Perintah menggunakan pslist.....	46
Gambar 4.46 Proses yang berjalan ....	47
Gambar 4.47 Perintah menggunakan pstree.....	47
Gambar 4.48 Proses terlihat dalam tampilan <i>tree</i> .....	47
Gambar 4.49 Perintah menggunakan cmdline.....	48
Gambar 4.50 Hasil dari perintah cmdline. ....	48
Gambar 4.51 Proses dump explorer.exe PID 5904.....	48
Gambar 4.52 Menggunakan perintah netscan. ....	49
Gambar 4.53 Koneksi dua IP berbeda. ....	49
Gambar 4.54 Nilai hash USB drive fisik. ....	50
Gambar 4.55 Proses imaging USB drive. ....	50
Gambar 4.56 Proses mount fd_evidence_win10_magnet.dd. ....	51
Gambar 4.57 Menggunakan perintah imageinfo. ....	51
Gambar 4.58 Perintah Menggunakan pslist. ....	52
Gambar 4.59 Potongan daftar proses yang berjalan. ....	53

Gambar 4.60 Perintah menggunakan pstree.....	53
Gambar 4.61 Potongan proses yang berjalan dalam tampilan <i>tree</i> . ....	54
Gambar 4.62 Perintah menggunakan cmdline.....	54
Gambar 4.63 Hasil dari perintah cmdline. ....	55
Gambar 4.64 Proses dump explorer.exe PID 2348.....	56
Gambar 4.65 Perintah menggunakan plugin netscan.....	56
Gambar 4.66 Koneksi antar IP. ....	56
Gambar 4.67 Nilai hash pada USB drive fisik. ....	57
Gambar 4.68 Proses Imaging USB drive fisik barang bukti. ....	58
Gambar 4.69 Proses mount fd_evidence_win10_dumpit.dd.....	58
Gambar 4.70 Membuka direktori /mnt. ....	59
Gambar 4.71 Menggunakan perintah imageinfo. ....	59
Gambar 4.72 Volatility tool gagal memberikan informasi.....	60
Gambar 4.73 Perintah menggunakan pslist.....	60
Gambar 4.74 Potongan Proses yang berjalan.....	60
Gambar 4.75 Proses terlihat dalam tampilan <i>tree</i> .....	61
Gambar 4.76 Perintah menggunakan cmdline.....	61
Gambar 4.77 Potongan hasil perintah menggunakan cmdline. ....	62
Gambar 4.78 Proses dump explorer.exe PID 3612.....	63
Gambar 4.79 Perintah menggunakan netscan. ....	63
Gambar 4.80 Koneksi antar IP. ....	63

## **Glosarium**

RAM – Random Access Memory