

DAFTAR GAMBAR

Gambar 2.1 Klasifikasi <i>Malware</i> (Zalavadiya & Sharma, 2017).	II-1
Gambar 2.2 Teknik Deteksi <i>Malware</i> (Penmatsa dkk., 2020)	II-6
Gambar 2.3 Informasi <i>File</i> Memori (Kusuma, 2023)	II-9
Gambar 2.4 <i>YARA rules: syntax and example</i> (Naik dkk., 2021)	II-10
Gambar 3.1 Tahapan Penelitian	III-1
Gambar 3.2 Alur Metode <i>Memory Forensic</i>	III-4
Gambar 4.1 Sampel <i>malware</i> <i>ramez.exe</i> pada <i>website any.run</i>	IV-2
Gambar 4.2 Perhitungan <i>hash file</i> <i>ramez.exe</i>	IV-3
Gambar 4.3 Tampilan <i>ApateDNS</i>	IV-6
Gambar 4.4 Tampilan eksekusi awal <i>file</i> <i>ramez.exe</i>	IV-7
Gambar 4.5 <i>Filtering</i> pada <i>process monitor</i>	IV-8
Gambar 4.6 Detail Proses Monitor <i>remcos.exe</i>	IV-9
Gambar 4.7 <i>Process monitor network</i>	IV-10
Gambar 4.8 Hasil lacak <i>ip address malware</i>	IV-11
Gambar 4.9 Tampilan <i>Tools DumpIt</i>	IV-12
Gambar 4.10 Hasil <i>Memory Dump</i>	IV-13
Gambar 4.11 Proses <i>pslist volatility</i>	IV-14
Gambar 4.12 Proses <i>pstree volatility</i>	IV-15
Gambar 4.13 Proses <i>netscan Volatility</i>	IV-16
Gambar 4.14 Perintah untuk ekstraksi <i>string</i> dari <i>file</i> <i>ramez.exe</i>	IV-17
Gambar 4.15 File hasil ekstraksi <i>string</i>	IV-17
Gambar 4.16 <i>File YARA Rules</i> untuk deteksi <i>malware</i> <i>ramez.exe</i>	IV-18

Gambar 4.17 Hasil eksekusi <i>YARA Rule</i> terhadap file <i>ramez.exe</i>	IV-19
Gambar 4.18 Hasil <i>YARA</i> pada <i>memory dump</i> , <i>rmclient</i> , <i>sysinfo</i> , <i>dxdiag</i>	IV-21
Gambar 4.19 Hasil <i>YARA</i> pada <i>memory dump</i> , <i>dxdiag</i> , <i>cmd</i>	IV-22
Gambar 4.20 Hasil <i>YARA</i> pada <i>memory dump</i> , <i>cmd</i> , <i>image/jpeg</i>	IV-23