BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Setelah melakukan berbagai percobaan maka dapat ditarik kesimpulan bahwa serangan menggunakan Framework Metasploit pada simulasi yang dilakukan dalam penelitian ini meninggalkan artefak digital yang dapat ditemukan pada RAM komputer Windows 8 dan Windows 10.

Penelitian yang telah dilakukan pada kali ini menggunakan tiga *tools* untuk melakukan *capture* pada RAM komputer, ketiganya memeliki perbedaan yang mendasar yaitu default ekstensinya berbeda-beda. Untuk FTK Imager mempunyai *default* ekstensi .mem, kemudian untuk Magnet RAM Forensics mempunyai *default* ekstensi .raw. Selanjutnya untuk Dumpit menggunakan default ekstensi .dmp.

Ketiga *tools* tersebut secara umum mampu melakukan *capture* RAM pada Windows 8 dan Windows 10 dan menemukan artefak digital serangan exploit menggunakan Framework Metasploit berupa IP Penyerang, Exploit/Trojan, Proses berjalan, Profile OS, Lokasi exploit/Trojan, dengan demikian Live Forensik pada RAM komputer dapat membantu dalam upaya investigasi kejahatan kriminal menggunakan Framework Metasploit. Selain itu dalam penelitian ini juga berhasil melakukan *dump* file binary dari malicious executable yang dicurigai sehingga hal ini dapat dijadikan penelitian lanjutan untuk melakukan malware analisis atau *reverse engineer* terhadap file binary tersebut.

Selain pengujian forensik terhadap RAM komputer dalam penelitian ini juga memberikan informasi bahwa untuk meminimalkan risiko terjadinya serangan ini adalah dengan selalu melakukan update anti virus dan melakukan konfigurasi firewall pada komputer.

5.2 Saran

Dalam penelitian ini masih menggunakan konsep dasar simulasi teknik serangan memanfaatkan sebuah exploit tertentu dalam Framework Metasploit yang masih memanfaatkan faktor *social engineering* untuk mendukung keberhasilannya, sedangkan Framework Metasploit memiliki banyak exploit lain yang dapat diteliti lebih dalam. Untuk itu saran penelitian ke depan untuk bisa melakukan serangan dengan teknik dan exploit

lain yang lebih variatif. Kemudian *tools* RAM capture yang digunakan juga masih terbatas pada tiga tools yaitu FTK Imager, Magnet Forensics dan Dumpit, selain itu untuk analisisnya juga masih menggunakan hanya satu *tools* yaitu Volatility, dengan demikian diharapkan penelitian selanjutnya bisa menggunakan *tools* lain guna menambah wawasan dan keilmuan tentang karakteristik dari *tools* yang ada untuk kemajuan keilmuan khususnya dalam bidang Digital Forensik.