BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian Pengembangan Volatrik Untuk Analisis *Fileless Malware* dengan Teknik *Memory Forensic*, dapat diambil kesimpulan sebagai berikut.

1. Berhasil membangun lingkungan sandbox menggunakan sistem operasi ubuntu 22.04 LTS.
2. Berhasil mengimplementasikan metode akuisisi pada virtualbox menggunakan fitur yang tersedia pada virtualbox yaitu menggunakan metode VboxManage Debugvm.
3. Berhasil melakukan analisis pada memori ram yang telah diakuisisi menggunakan Volatrik dengan menggunakan fitur yang tersedia pada aplikasi tersebut.
4. Dari hasil analisis didapatkan informasi yang menunjukan adanya *fileless malware* dengan terhubung ke suatu alamat IP.

5.2 Saran

Penelitian ini masih memiliki kekurangan dan membutuhkan pemahaman lebih baik lagi untuk menghasilkan laporan analisis yang dapat dipahami oleh orang awam. Maka dari itu, penulis memiliki saran untuk penelitian kedepannya yaitu sebagai berikut.

1. Melakukan riset lagi tentang *tools* yang digunakan untuk analisis *fileless malware*.
2. Mempelajari lebih lanjut tentang forensik memori, karena membutuhkan pemahaman lebih banyak karena mencakup bidang ilmu yang sangat luas.
3. Melakukan riset tentang metode lain yang digunakan untuk menjalankan *fileless malware* karena perkembangan *malware* semakin canggih dan sulit terdeteksi oleh antivirus.