BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan dari pembahasan pada penulisan skripsi ini, maka dari itu didapatkan kesimpulan sebagai berikut ini:

1. Dari hasil pengujian *malware* untuk dilakukan proses *memory forensics* menggunakan aplikasi FTK Imager penulis berhasil mendapatkan sample RAM yang kemudian digunakan untuk proses *memory forensics*.
2. Dari hasil pengujian *Yara rule* pada aplikasi Geleaner melakukan banyak pemasangan aplikasi tanpa sepengetahuan korban yang digunakan untuk mengakses komputer korban.
3. Dari hasil pengujian sample memori yang telah diakuisisi penulis membuktikan bahwa pada PID 4996 telah terinfeksi oleh *malware redline stealer*, dan melakukan komunikasi dengan IP 2.56.59.42.

5.2 Saran

Pada penelitian ini masih banyak terdapat kekurangan dan masih membutuhkan pemahaman yang lebih baik agar dapat menghasilkan laporan analisis yang baik dan mudah dimengerti orang yang masih awam. Maka dari itu peneliti memberikan saran untuk peneliti ke depan nya yaitu:

1. Untuk peneliti selanjutnya, dapat dilakukan penelitian pada koneksi jaringan menggunakan analisis jaringan untuk mendapatkan komunikasi apa saja yang terjadi pada aktivitas jaringan komputer korban dengan *attacker* sehingga dapat menemukan aktivitas *attacker* melalui jaringan
2. Mempelajari lebih dalam pada bahasa *assembly* karena butuh pemahaman lebih dalam menjelaskan hasil dari proses *memory forensics*.