Bab 5 Kesipulan Dan Saran

5.1 Kesimpulan

Setelah melakukan beberapa hal terkait dengan perancangan, pengujian dan analisis maka diperoleh beberapa kesimpulan berikut ini:

1. Penerapan ontologi sebagai *knowledge base* dasar dalam melakukan analisis karakteristik *malware* sebagai *knowledge base* sangat dibutuhkan dalam melakukan analisis karakteristik *malware*, penggunaan ontologi yang menggunkan pendekatan domain dalam penggalian data, sangat berguna dalam menentukan alur dan cara kerja *malware* yang saling berhubungan antara kelas dan sub kelas serta individu dari *malware*, sehingga dapat memudahkan proses analisis dalam menentukan jenis dan karakteristik *malware*.
2. Empat karakteristik dasar *malware* yaitu *payload, obfuscation*, *vector* dan *packer* sangat berpengaruh pada setiap aktivitas atau serangan yang dilakukan oleh *malware*, hal ini disebabkan masing-masing dari karakteristik mempunyai fungsi dalam melakukan aktivitas atau serangan. Penggunaan karakteristik dasar *malware* yang diterapkan dalam ontologi sebagai *knowledge base* dalam melakukan analisis memberikan solusi terhadap pemasalahan yang terdapat dalam penelitian ini yaitu, permasalahan analisis yang masih berfokus kepada analisis perilaku *malware*, hal ini menjadi tidak efektif ketika terdapat *malware* baru yang belum diketahui perilakunya, akan tetapi ketika analisis *malware* menggunakan karakteristik dasar sebagai *knowledge base* maka analisis yang dilakukan menjadi tidak terbatas dikarenakan karakteristik dasar terdapat pada setiap *malware* sehingga ketika analisis dilakukan pada jenis *malware* baru akan dapat dikenal sebagai sebuah program berbahaya sehingga memudahkan dalam proses analisis

5.2 Saran

Untuk pengembangan lebih lanjut pada penelitian ini maupun dalam penelitian ontologi *malware* maka dapat diberikan beberapa saran sebagai berikut:

1. Analisis dilakukan pada jenis *malware* lainnya, dengan menggunakan konsep dan *tools* yang lebih memadai.
2. Analisis *malware* dapat dilakukan dengan menggunakan ekstensi *file* yang bervariasi.
3. Penambahan karakteristik *malware* menjadi sangat menarik untuk pengembangan penelitian, dikarenakan masih terdapat jenis karakteristik *malware* dengan fungsi yang berbeda.