BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Setelah melalui semua tahapan dalam penelitian dari persiapan, analisis, perancangan, dan implementasi serta pengujian dan hasil maka sampai pada bagian kesimpulan, kesimpulan yang dapat diambil adalah :

1. Penerapan metode *behavior approach* untuk deteksi malware berdasarkan perilaku aplikasi terhadap data dilakukan dengan melewati beberapa tahapan yaitu, tahapan persiapan analisi yaitu mempersiapkan semua hal yang dibutuhkan untuk analisis mencakup komputer dan *tools* yang akan digunakan, tahapan kedua dinamik analisis yaitu proses mengamati malware dengan cara menjalankan malware dan aplikasi secara langsung pada mesin virtual untuk mendapatkan informasi *behavior*, selanjutnya membuat rancangan sistem deteksi malware berdasarkan informasi *behavior* yang didapat dari analisis, kemudian tahapan implementasi rancangan sistem deteksi kedalam bahasa pemrograman python serta hasil berupa sistem dapat mendeteksi malware.
2. Berdasarkan hasil pengujian terhadap sistem deteksi malware berdasarkan perilaku aplikasi terhadap data meggunakan metode *behavior approach* menunjukkan bahwa penggunaan metode *behavior approach* sebagai metode deteksi malware memperlihatkan indikasi keberhasilan, dengan indikasi keberhasilan berupa tingginya jumlah perbedaan angka *behavior* antara *behavior* normal dan *behavior* yang tidak normal setelah dilakukan pengujian berulang kali terhadap sistem deteksi malware, tingginya dua nilai *behavior* tersebut dapat digunakan untuk menentukan sebuah aplikasi itu sebagai malware atau aplikasi normal.

5.2 Saran

Berdasarkan hasil penelitian ini terdapat beberapa hal yang dapat dikembangkan, hal ini menjadi masukan saran untuk pengembangan penelitian selanjutnya, yaitu :

1. Memperluas dengan menambah objek pembahasan khususnya pada *behavior operations*, yaitu pembahasan pada topik registry *operation* dan *network operation* dalam lingkungan metode *behavior based detection*.
2. Menggunakan metode *signature based detection* sebagai teknik tambahan untuk deteksi malware dalam salah satu tahapan untuk deteksi malware berbasi *behavior.*