BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan uraian pada bab-bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut, yaitu :

1. Untuk meningkatkan keamanan komputer dari maraknya program berbahaya (*Malicious Code/Malicious Software "Malware"*) terutama Virus Komputer, diperlukan pemahaman mengenai kinerja sistem komputer, terutama krangka *struktur windows* dan *database setting* sistem operasi pada *registry Windows* karena tempat-tempat tersebut merupakan target serangan Virus.
2. Untuk mengenali teknik penyebaran Virus Worm.Win32/Amburadul sehingga bisa mengenali seluruh Virus yang ada dari informasi yang didapat dari Virus Worm.Win32/Amburadul yaitu dengan memahami cara kerja Virus, pola lalu lintas penyebarannya, sehingga mampu mengenali *file-file* yang dibuat Virus dan perubahan *registry* yang dilakukan Virus.
3. Untuk melakukan penghentian program Virus menggunakan perintah *end proses* (menutup id proses suatu program yang sedang berjalan dalam priode waktu tertentu) sebelum melakukan proses pencarian Virus pada komputer menggunakan nilai *ceksum Algoritma CRC32* Virus kemudian menghapusnya menggunakan teknik *Delete* dan *Shif Delete*.

6.2 Saran

Berdasarkan kesimpulan diatas maka penulis mencoba mengemukakan saran guna melengkapi rangkaian penelitian Virus Worm.Win32.Amburadul, diantaranya :

1. Proses Analisis Virus bisa dilakukan dengan cara lain disamping melalui proses perekaman aktivitas virus yang ada dalam laporan skripsi ini, seperti melihat jalannya Virus dengan *debugger* atau melalui cara *dekompilasi* yaitu mengembalikan file *application (*.exe)* kedalam *source code* aslinya namun sangat *low level language,* sehingga sangat sulit dimengerti kecuali dengan kesabaran dan banyak latihan. Ataupun dengan cara menggabungkan teknik *debugger* dan *dekompilasi.*
2. *Algoritma CRC32* hanyalah satu dari sekian banyak teknik yang digunakan dalam mendeteksi Virus komputer, pendekatan lain yang digunakan yang bisa dikembangkan secara lebih mendalam seperti *Md5, behavior-blocking detection* dengan cara mengisolasi kode-kode berbahaya yang dicurigai sebagai Virus tanpa adanya update *database* Virus dan teknik lainya yang diterapkan dalam *Intrusion Detection System (IDS).*