

## BAB VI

### KESIMPULAN DAN SARAN

#### 6.1 Kesimpulan

Setelah menyelesaikan pembuatan software maka penulis dapat menyimpulkan sebagai berikut :

- Pengenkripsian *PE File* pada suatu *file executable* dan menjalankan *PE File* tersebut di *memory* dapat meningkatkan keamanan *file executable* dari tindakan *cracking* karena *PE File* dari program yang terproteksi tidak dapat di-*debug*.
- Suatu *file executable* yang terproteksi dari *software debugger* atau *emulator* dapat menghindari *file executable* tersebut dari tindakan *debugging* ataupun pelacakan/*tracing* yang dapat mengarah ke tindakan ilegal dalam pemakaian *software*.
- Dengan menjaga keamanan suatu *software* maka dapat membantu menjaga hak cipta dan hak atas kekayaan intelektual pada *software*.

#### 6.2 Saran

Berikut saran-saran yang penulis sampaikan setelah menyelesaikan program dan melihat permasalahan yang muncul :

- Saat program mendapatkan icon pada *file executable* yang akan diproteksi, program hanya mengambil *icon* pertama pada *file executable* tersebut, sebaiknya program membandingkan *icon-icon* yang terdapat pada *file executable* dengan *icon* yang sedang digunakan *file executable*.
- Setelah proses pemroteksian dan menggunakan fitur kompresi pada *file executable* berukuran kecil, maka *file executable* yang terproteksi akan

bertambah besar. Hal ini dapat dihindari jika file loader dcompile menggunakan murni bahas *assembler* seperti *MASM* atau *TASM*.

- Pada rutin enkripsi *PE File*, kualitas pengenkripsian dapat ditingkatkan dengan menggunakan enkripsi yang lebih kompleks seperti *RC4* atau *API Crypt*.
- Program proteksi banyak menggunakan kode yang mengakses memory dan pada beberapa antivirus, hal ini dapat dideteksi antivirus sebagai trojan. Untuk menghindari kejadian ini dapat dilakukan pengenkripsian kode-kode pada program.