# BAB V
# KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Berdasarkan penelitian tentang "Anti Komputer Forensik Dengan Menggunakan Metode Steganografi Dan Manipulasi File" maka dapat disimpulkan bahwa:

1. Teknik anti komputer forensik yang dipakai dalam penelitian ini dibagi menjadi tiga teknik yaitu: teknik menyamarkan file, teknik *data hiding,* teknik *secure delete.* Skenario percobaan yang digunakan untuk penyamaran file yaitu dengan menggunakan manual, notepad, Frhed (Free Hex Editor), PsPad Freeware Editor, Hxd Hex Editor dengan melakukan perubahan pada ekstensi file dan header ASCII. Skenario kedua data hiding menggunakan tools Openstego, Steghide, Openpuff dengan melakukan hiding ke dalam *file carrier* .jpg .png .wav. Skenario ketiga *secure delete* dilakukan dengan manual delete dan shift + delete serta menggunakan tools File Shredder dan Sdelete untuk melakukan penghapusan file.
2. Percobaan pertama penyamaran file diperoleh hasil bahwa penyamaran file menggunakan perubahan ekstensi secara manual maupun perubahan oleh notepad masih berhasil terdeteksi format file yang aslinya, sedangkan penyamaran file menggunakan *tools* tidak dapat dideteksi oleh aplikasi forensik. Percobaan kedua *data hiding* diperoleh hasil bahwa dengan menggunakan Openstego tidak dapat dideteksi oleh aplikasi forensik, sedangkan menggunakan aplikasi steghide dan Openpuff untuk *file carrier* berformat .jpg, berhasil terdeteksi sebagai stego file. Percobaan *secure delete* diperoleh hasil bahwa dengan melakukan penghapusan secara manual (delete) maupun penghapusan permanen secara manual (shift+delete) belum dikategorikan sebagai penghapusan yang aman dikarenakan masih bisa dideteksi oleh *tools* forensik dan bisa dilakukan recovery kembali, sedangkan saat dilakukan penghapusan dengan menggunakan *tools* file shredder dan

sdelete, aplikasi forensik tidak dapat mengetahui keberadaan dari file yang telah dihapus sehingga file tidak dapat dilakukan recovery.

**5.2 Saran**

Saran yang diberikan setelah penelitian ini dilakukan adalah:

1. Dapat menutupi kelemahan pada penelitian ini dengan melakukan penelitian yang lebih kompleks lagi mengenai berbagai metode anti komputer forensik yang ada.
2. Selalu *Uptodate* dalam perkembangan teknologi baik itu dari segi komputer forensik maupun anti komputer forensik.
3. Dalam penggunakan *data hiding* disarankan untuk menggunakan lebih dari satu *file carrier* supaya pelacakan menggunakan aplikasi forensik akan lebih sulit untuk dilakukan.
4. Diusahakan untuk memakai password dengan beberapa kombinasi yaitu angka, huruf maupun simbol untuk memperkuat pengamanan pada sebuah file.