BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang pesat berpengaruh terhadap cara masyarakat berkomunikasi dan bertukar informasi, dengan adanya teknologi memungkinkan manusia untuk berkomunikasi dengan jarak yang sangat jauh baik itu menggunakan sarana telepon, email dan internet, maka dari itu, masalah pengamana file sangatlah penting dan menjadi perhatian banyak orang. Salah satunya adalah pengamanan menggunakan steganografi. Steganografi adalah sebuah seni untuk menyembunyikan file atau pesan rahasia ke dalam sebuah wadah yang bernama *file carrier* sehingga tidak mudah terdeteksi oleh kegiatan forensik yang dilakukan oleh pihak lain.

Steganografi dapat dikatakan sebagai pisau bermata dua, disamping bisa digunakan untuk melakukan proteksi dan pengamanan file, steganografi juga bisa digunakan untuk sarana kejahatan seperti penyembunyian malware ke dalam sebuah file. Saat ini steganografi digunakan untuk melakukan *watermaking* pada sebuah gambar untuk memastikan proteksi terhadap suatu hak cipta tetap terjaga. Tipe-tipe dokumen yang diberikan watermaking antara lain *Image Watermaking, Video Watermaking, Text Watermaking, Audio Watermaking*[1]

Berdasarkan segi pengamanannya, steganografi lebih cocok digunakan bersamaan dengan menggunakan metode yang lain seperti contohnya enkripsi maupun manipulasi file. Steganografi mempunyai dua proses utama untuk melakukan pengamanan pada file, yaitu proses penyisipan dan proses ekstaksi. Pada proses penyisipan dilakukan penyembunyian *secret file* atau pesan rahasia ke sebuah wadah yang diberi nama sebagai *file carrier,* sehingga nantinya akan timbul sebuah file baru yang disebut sebagai *stego file*. Sedangkan untuk proses ekstraksi merupakan proses yang dilakukan untuk melakukan pengembalian terhadap objek maupun pesan yang telah disembunyikan ke dalam file cover.[2]

Steganografi dalam penggunaannya sebagai sarana pengamanan file

terdapat beberapa masalah. Permasalahan yang sering terjadi saat ini adalah tentang *software* forensik yang tersebar luas di internet dan bisa dengan mudah didownload dan diakses. Jika ditinjau dari tujuannya, *software* forensik ini bisa digunakan untuk menyelidiki sebuah fakta maupun kebenaran, akan tetapi banyak juga penyalahgunaan yang dapat merugikan orang lain dan membahayakan orang banyak seperti: mencari file pribadi seseorang, memantau log dan history aktivitas atau bahkan *recovery* file yang seharusnya sudah dihapus dengan tujuan kejahatan.

Berdasarkan permasalahan diatas dapat diminimalisir dengan menggunakan *software* anti komputer forensik yang nantinya berguna untuk melindungi data-data penting yang bersifat pribadi, baik itu dilakukan dengan cara data *hiding* maupun pengubahan terkait integritas data.

Selain bertujuan untuk menyembunyikan sebuah data, *software* maupun teknik anti komputer forensik ini bisa digunakan sebagai tolak ukur penilaian terhadap *software-software* forensik yang sudah beredar luas saat ini kemudian bisa mendorong para ahli dibidang komputer forensik untuk membuat *software* forensik yang lebih baik lagi kedepannya.[3]

Penelitian ini nanti akan dilakukan percobaan teknik anti komputer forensik menggunakan skenario penyamaran file, *data hiding, secure delete*. Tujuan dilakukannya penelitian ini adalah untuk menguji keefektifan dari teknik-teknik anti komputer forensik guna melakukan pengamanan data supaya data pribadi bisa dikatakan lebih aman.

1.2 Perumusan masalah

Berdasarkan latar belakang penelitian tentang anti komputer forensik diatas maka dapat dirumuskan beberapa masalah seperti berikut ini:

1. Bagaimana cara mengimplementasikan metode manipulasi file yaitu dengan menggunakan teknik penyamaran file, *secure delete* dan steganografi dengan menggunakan *data hiding* untuk melakukan anti komputer forensik?
2. Bagaimana hasil dari pengujian menggunakan teknik penyamaran file, *data hiding, secure delete* dalam penerapannya didalam anti komputer forensik?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk:

a. Menyembunyikan dan memanipulasi data file yang sebenarnya sehingga sulit untuk dilakukan analisa forensik.
b. Merubah format dan penyisipan pesan didalam file yang lainnya guna untuk memepersulit proses analisa forensik.
c. Melakukan penghapusan file maupun history serta jejak-jejak digital yang dibuat oleh sistem maupun aplikasi sehingga tidak dapat diketahui oleh orang lain.

1.4 Batasan Masalah

Batasan pada penelitian ini meliputi:

1. Membahas tentang anti komputer forensik yaitu dengan menggunakan metode steganografi dan metode manipulasi file.
2. Pada metode manipulasi file terdapat beberapa teknik yang digunakan, seperti: penyamaran format file, percobaan *data hiding*, melakukan penghapusan secara aman (*secure delete*).
3. Menggunakan satu *tools* forensik untuk melakukan pengujian di tiap-tiap teknik.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Menambah pengetahuan tentang steganografi dan teknik anti forensik komputer
2. Dapat menggunakan berbagai teknik anti komputer forensik untuk melindungi data data pribadi di dalam komputer.
3. Membuktikan bahwa data itu bersifat rapuh dan dapat dimanipulasi sedemikian rupa sehingga tidak terdeteksi oleh tools forensik komputer
4. Sebagai tolak ukur penilaian terhadap sebuah *tools* forensik maupun anti komputer forensik
5. Mendorong perkembangan teknik komputer forensik menjadi lebih baik kedepannya.