BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Setiap orang pasti memiliki data penting yang harus mereka lindungi agar tidak hilang atau dicuri oleh pihak yang tidak bertanggungjawab. Terlebih pada suatu perusahaan yang memiliki lebih banyak data. Data yang dimiliki suatu perusahaan dapat menjadi salah satu aset penting untuk kelangsungan hidup perusahaan tersebut. Sebuah media penyimpanan data dengan sistem keamanan penuh sangat diperlukan.

Masalah yang timbul bukan hanya pada media penyimpanan data tetapi bagaimana media penyimpanan data tersebut dilengkapi dengan sistem keamanan yang baik pula. Oleh karena itu digunakanlah teknik enkripsi data, teknik enkripsi yang umum digunakan adalah enkripsi yang dilakukan pada file atau *file encryption*. File encryption sudah dilakukan bertahun-tahun dan masih memiliki manfaat dari segi keamanan. Namun, *file encryption* juga memiliki kekurangan apabila dihadapkan pada kondisi jika file tersebut berjumlah banyak seperti file-file yang dimiliki oleh suatu perusahaan.

Selain menggunakan teknik enkripsi yang baik, media penyimpanan yang digunakan nanti harus memiliki tempat yang aman pula dikarenakan file yang di simpan berjumlah banyak dan sangat penting. File yang telah kita simpan dalam

sebuah media penyimpanan tersebut kadang sudah tidak diperlukan lagi oleh karena itu agar tidak terjadi penumpukan file, file harus dapat dimodifikasi atau dihapus.

Untuk teknik enkripsi diperlukan adanya standart algoritma yang benar-benar aman dan tidak mudah dipecahkan oleh teknologi saat ini. Maka dari itu pembangunan media penyimpanan data harus dilengkapi dengan teknik enkripsi yang menggunakan standart algoritma dengan tingkat keamanan tinggi.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana mengimplementasikan sebuah virtual disk yang telah terenkripsi dengan algoritma SHA di dalamnya menggunakan system operasi windows.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penelitian ini adalah bagaimana membuat atau membangun aplikasi enkripsi virtual disk menggunakan algoritma SHA (Secure Hash Algorithm)

Adapun Tujuan dari penelitian ini adalah:

1. Diperlukan sebuah media penyimpanan data dan teknik enkripsi yang baik
2. Membangun sebuah aplikasi enkripsi data dengan teknik disk encryption.

3. Membuat sebuah virtual disk yang dapat digunakan seperti physical disk lainnya namun tidak dalam bentuk disk yang nyata, secara fisik dapat menyimpan file serta file tersebut dapat dimodifikasi atau dihapus.
4. Mengimplementasikan teknik disk encryption menggunakan algoritma SHA.

1.4 Batasan Masalah/Ruang Lingkup Kajian

Adapun batasan masalah dari Aplikasi Enkripsi Virtual Disk Menggunakan Algoritma SHA ini adalah sebagai berikut:

1. Pengguna Aplikasi ini digunakan oleh user biasa
2. *Procedure*
   a. Implementasi yang dilakukan tidak memberikan solusi keamanan terhadap segala perlakuan yang dikenakan pada file volume, terutama penghapusan terhadap file tersebut.
   b. Operasi yang dilakukan pada suatu file hanya sebatas mengenkripsi saja tanpa adanya proses kompresi.
3. Model analisis perangkat lunak yang digunakan adalah pemodelan analisis terstruktur. Alat yang digunakan adalah flowmap dan diagram E-R, dan untuk menggambarkan proses yang digunakan adalah DFD (Data Flow Diagram).
4. Data yang diolah :

   Data yang tersimpan dalam virtual disk
5. Informasi yang dihasilkan diantaranya :

a. Informasi kapasitas virtual disk

b. Informasi jenis data yang tersimpan dalam virtual disk

6. Perangkat Lunak

Perangkat Lunak yang digunakan dalam membangun aplikasi enkripsi virtual disk menggunakan algoritma SHA ini adalah :

a. Pembangunan Aplikasi menggunakan Borland Delphi 7

b. Sistem Operasi menggunakan Microsoft Windows XP Service Pack 2

c. Editor Notepad++ v4.0.2

7. Perangkat Keras

a. Prosesor Intel Core2Duo E8200 2,7 GHz

b. RAM 2 Gb

c. Harddisk 160Gb

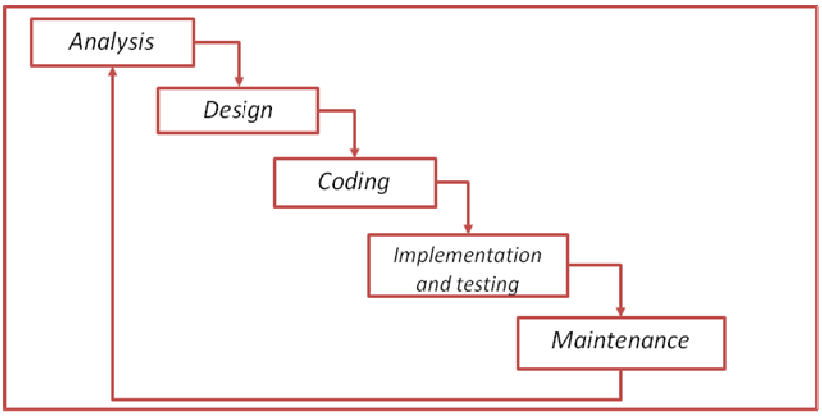
d. Perangkat keluaran berupa monitor

e. Perangkat masukan berupa keyboard

1.5 Metodologi Penelitian

Metodelogi Penelitian yang digunakan untuk membangun aplikasi enkripsi virtual disk menggunakan algoritma SHA ini sebagai berikut :

Teknik dalam pembangunan perangkat lunak menggunakan paradigma perangkat lunak secara waterfall.



Gambar 1.1 Gambar *waterfall*

1) Analisis

Merupakan tahap menganalisis hal-hal yang diperlukan dalm pelaksanaan pembangunan perangkat lunak. Pada tahap analisis dilakukan metode pengumpulan data yaitu sebagai berikut :

a. Studi Pustaka

Metode pengumpulan data dengan mencari data, mempelajari banyak data dari berbagai sumber buku, modul, artikel baik perpustakaan maupun internet yang berhubungan dengan permasalahan yang dibahas.

b. Wawancara (*interview*)

Pengumpulan data yang dilakukan dengan cara berkomunikasi langsung dengan pihak-pihak yang dianggap mampu memberikan informasi

(narasumber) yang lebih terinci terhadap permasalahan yang sedang diteliti.

c. Observasi

Pengumpulan data melalui pengamatan dan pencatatan data oleh pengumpul data terhadap peristiwa yang diselidiki pada objek penyusunan. Dalam melakukan observasi penulis melakukan beberapa pengamatan terhadap sistem kerja, proses pengolahan data yang sedang berjalan.

2) Desain

Proses ini digunakan untuk mengubah kebutuhan-kebutuhan diatas menjadi representasi ke dalam bentuk rancangan aplikasi sebelum *coding* dimulai. *Design* harus dapat mengimplementasikan kebutuhan yang telah disebutkan pada tahap sebelumnya. Seperti aktivitas sebelumnya, maka proses ini juga harus didokumentasikan sebagai konfigurasi dari aplikasi yang dibangun.

3) Pengkodean / implementasi

Untuk dapat dimengerti oleh mesin, dalam hal ini adalah komputer, maka desain tersebut harus diubah bentuknya menjadi bentuk yang dapat dimengerti oleh mesin, yaitu ke dalam bahasa pemrograman melalui proses *coding*. Tahap ini merupakan implementasi dari tahap *design.*

4) Pengujian

Aplikasi yang telah dibangun harus dilakukan ujicoba. Semua fungsi-fungsi aplikasi tersebut harus diujicobakan, agar aplikasi bebas dari *error,* dan hasilnya harus benar-benar sesuai dengan kebutuhan yang sudah didefinisikan sebelumnya.

5) Pemeliharaan

Pemeliharaan sebuah aplikasi sangat diperlukan, termasuk di dalamnya adalah pengembangan, karena aplikasi yang dibangun tidak selamanya hanya seperti itu. Ketika dijalankan mungkin saja masih ada *error* kecil yang tidak ditemukan sebelumnya, atau ada penambahan fitur-fitur yang belum ada pada aplikasi tersebut. Pengembangan diperlukan ketika adanya perubahan dari *eksternal* perusahaan seperti ketika ada pergantian sistem operasi, atau perangkat lainnya.

1.6 Sistematika Penulisan

Laporan terdiri dari beberapa bab dan tersusun berdasarkan sistematika penulisan sebagai berikut :

BAB I. PENDAHULUAN

Dalam bab ini penulis menguraikan mengenai hal-hal umum yang berkaitan mengenai latar belakang, rumusan persoalan, maksud dan tujuan dari tugas akhir, ruang lingkup dan batasan yang diacu, metodologi yang digunakan serta sistematika pembahasan.

BAB II. TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai beberapa teori pendukung tugas akhir ini

BAB III. ANALISIS DAN PERANCANGAN

Membahas spesifikasi kebutuhan perangkat lunak, yang dijelaskan dengan pemodelan diagram, hasil analisis ini kemudian diaplikasikan dengan rancangan aplikasi yang terdiri dari rancangan struktur program hasil analisis dan perancangan.

BAB IV. IMPLEMENTASI DAN PENGUJIAN

Bab ini merupakan bab penutup laporan yang berisi tentang Kesimpulan dan Saran-saran.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan bab penutup laporan yang berisi tentang Kesimpulan dan Saran-saran yang dijadikan masukkan bagi instansi.