BAB III

ANALISIS MASALAH DAN RANCANGAN PROGRAM

III.1. Analisis Sistem

Network mapping merupakan salah satu fitur yang ada didalam komputer yang berbasiskan windows, secara sederhana network mapping dapat dikatakan merupakan fasilitas untuk share drive dari suatu komputer agar bisa diakses komputer lain, tetapi juga network mapping bisa digunakan untuk mengakses komputer tertentu tanpa harus dishare drive tersebut dikarenakan adanya fasilitas share yang terus terbuka oleh port tertentu yang sudah ada di windows. Maka dari itu penulis hanya membuat aplikasi pendeteksian serangan seperti pengambilan file, data yg di hapus, dan file yg di ganti oleh hacker agar dapat mengetahui keamanan dari komputer tersebut.

a. Jenis perangkat lunak yang dipakai adalah *Microsoft Visual C#* 2008 karena lebih mudah digunakan.
b. Sistem operasi yang dipakai pada rancangan aplikasi ini ialah *windows seven.*

III.2. Strategi Pemecahan Masalah

Untuk menyelesaikan masalah yang telah diuraikan sebelumnya, maka diperlukan strategi pemecahan masalah, yaitu :

a. Untuk mengetahui adanya serangan *hacker* pada sebuah jaringan komputer.

b. Dengan adanya perancangan dan pembuatan pendeteksi serangan hacker ini bisa membuat *user* lebih wapada akan data atau file yang disimpannya pada sebuah komputer.
c. Untuk bisa menjaga keamanan data *user* harus adanya pengecekan berkala akan tiap data atau file yang disimpan oleh *user* disuatu komputer.

III.3. Perancangan Umum

Langkah yang dilakukan dalam perancangan sistem adalah merancang sistem tersebut secara logika yang pada akhirnya dapat dikembangkan menjadi suatu aplikasi. Pada tahap ini disusun model fungsi awal dengan menggunakan :

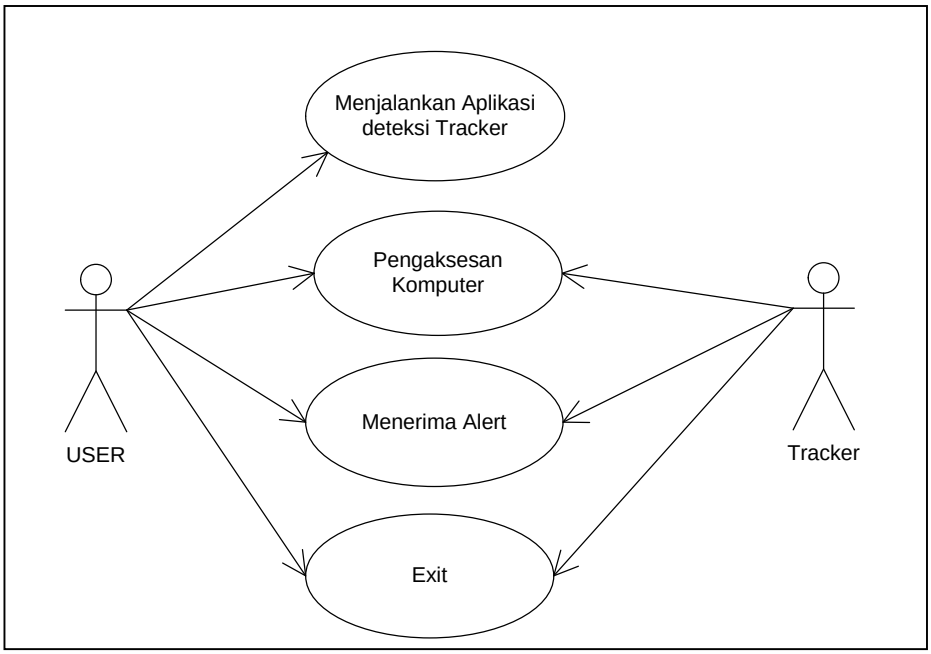
1. *Use Case Diagram*
2. *Sequence Diagram*
3. *Activity Diagram*

III.3.1. Use Case Diagram

Pada perancangan ini melibatkan *user* yang menjalankan aplikasi secara keseluruhan. Interaksi *user* tersebut dapat dilihat pada pemodelan berikut :

III.3.1.2 Use Case Global Deteksi Tracker

Adapun *Use Case Global* deteksi serangan dapat dilihat pada gambar III.1



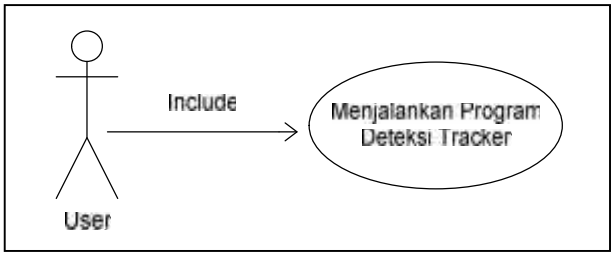
Gambar III.1. Use Case Global Deteksi Tracker

Keterangan :

Gambar diatas merupakan *use case* Global deteksi Tracker yang terdiri dari menjalankan aplikasi Deteksi Tracker, kemudian aktivitas Pengaksesan komputer yang dituju. Dan kemudian alert aplikasi. Yaitu Tracker atau melakukan tindak kejahatan seperti menghapus data mengganti nama folder supaya tidak diketahui oleh *user*.

III.3.1.3 Use Case Diagram Menu Aplikasi Deteksi Tracker

Adapun *Use Case Diagram* menu aplikasi Deteksi Tracker dapat dilihat pada gambar III.2.



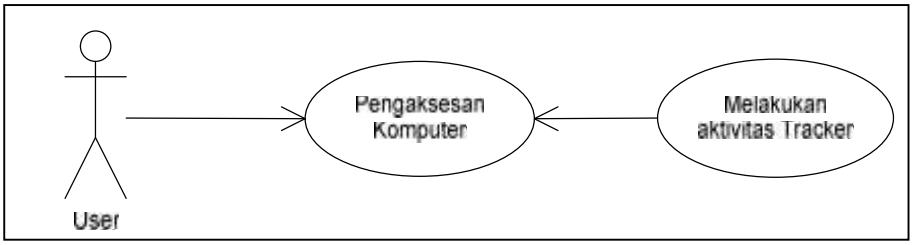
Gambar III.2. Use Case Diagram Aplikasi Deteksi Tracker

Keterangan :

user mulai menjalankan aplikasi Deteksi Tracker pada komputer

III.3.1.4 Use Case Diagram Pengaksesan Komputer

Adapun *Use Case Diagram* Pengaksesan Komputer dapat dilihat pada gambar III.3.



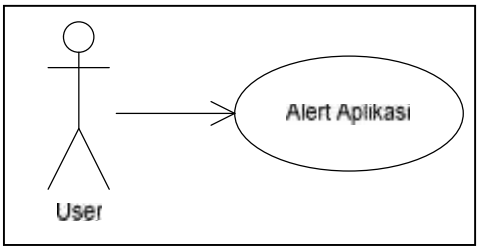
Gambar III.3. Use Case Diagram Pengaksesan Komputer

Keterangan :

User dapat sharing data atau file dan juga bisa mengambil file pada suatu komputer. Begitu juga dengan Tracker. Tetapi Tracker merusak data yang dapat merugikan *user*

III.3.1.5 Use Case Diagram Menu Alert Aplikasi

Adapun *Use Case Diagram* menu alert aplikasi dapat dilihat pada gambar III.4.



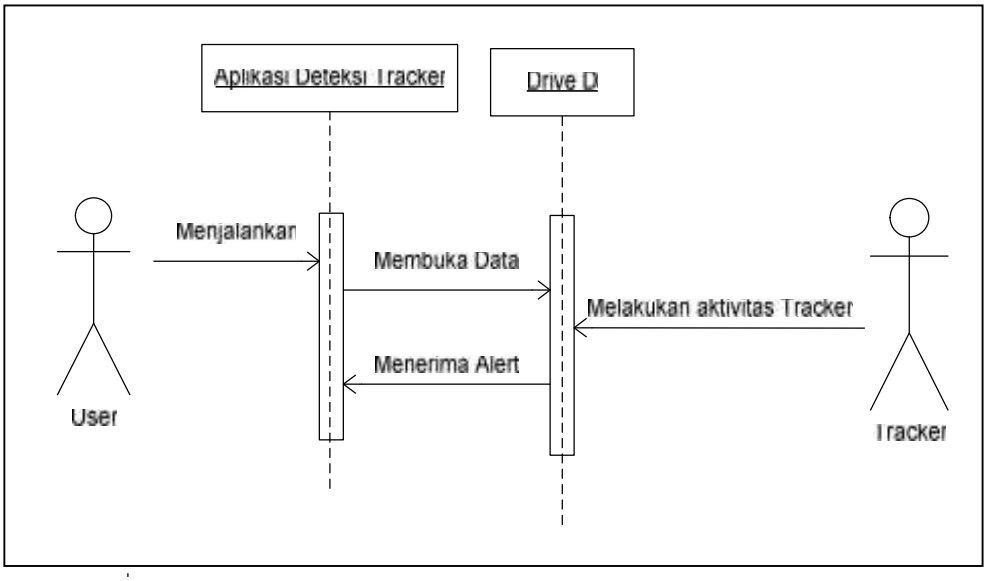
Gambar III.4. Use Case Diagram Menu Deteksi Serangan

Keterangan :

User juga bisa mendapatkan peringatan dari program deteksi serangan apabila data atau file user dirusak oleh Tracker

III.4.1 Sequence Diagram

Squence Diagram biasa digunakan untuk menggambarkan skenario atau rangkaian langkah-langkah yang dilakukan sebagai *respons* dari sebuah *event* untuk menghasilkan *output* tertentu. *Diagram* ini menunjukan sejumlah contoh *obyek* dan *message* yang diletakkan diantara objek –objek didalam *use case.* Komponen utama *squensce diagram* terdiri dari objek yang digambarkan dengan kotak segi empat bernama.message diwakili oleh garis dengan tanda panah dan waktu yang ditunjukkan dengan proses *vertical* diawali dari apa yang mentriger aktivitas tersebut, proses dan perubahan apa saja yang terjadi secara internal dan output apa yang dihasilkan.



Gambar III.5. *Sequence Diagram* Proses Deteksi Tracker

III.4.2 Activity Diagram

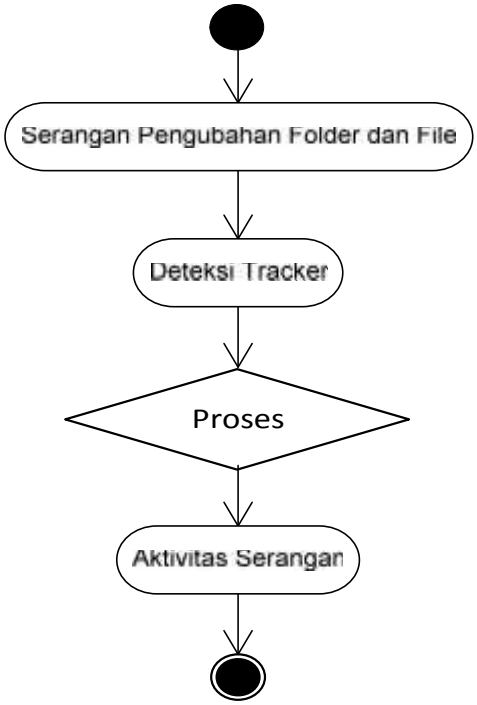
Menggambarkan rangkaian aliran dari aktivitas, digunakan untuk mendeskripsikan aktivitas yang dibentuk dalam suatu operasi sehingga dapat juga digunakan untuk aktivitas lainnya seperti *use case* atau interaksi.

III.4.2.1 Activity Diagram Menu Deteksi Tracker

Adapun prosedur ketika *user* akan menjalankan aplikasi deteksi serangan sebagai berikut :

1. Pertama *user* membuka aplikasi *Deteksi* Tracker
2. Setelah itu terdapat menu *Deteksi* Tracker
3. Jika *user* memilih tombol penjelasan dan fungsi maka *user* akan masuk ke menu utama dan terdapat *Shared Folder, Current Session, Accessed Folder, Folder Watcher* dan apabila dklik nama tiap menu tersebut akan muncul penjelasan dan fungsi pada bawah menu pertama.

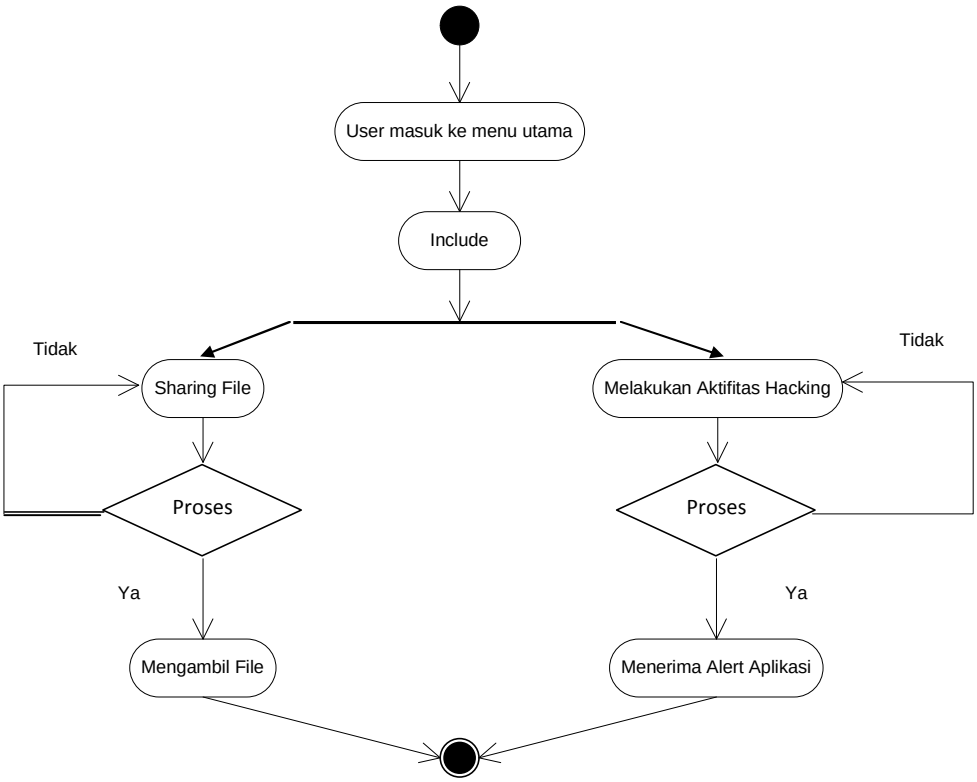
Adapun Activity Diagram Menu Penjelasan dan Fungsi dapat dilihat pada gambar III.6.



Gambar III.6. Activity Diagram Deteksi Tracker

III.4.2.2 Activity Diagram Menu Proses

User memilih menu *star* maka akan tampil kembali ke menu proses deteksi serangan . Adapun *Activity Diagram Option* dapat dilihat pada gambar III.7.



Gambar III.7. Activity Diagram Menu Proses

III.5 Perancangan Tampilan

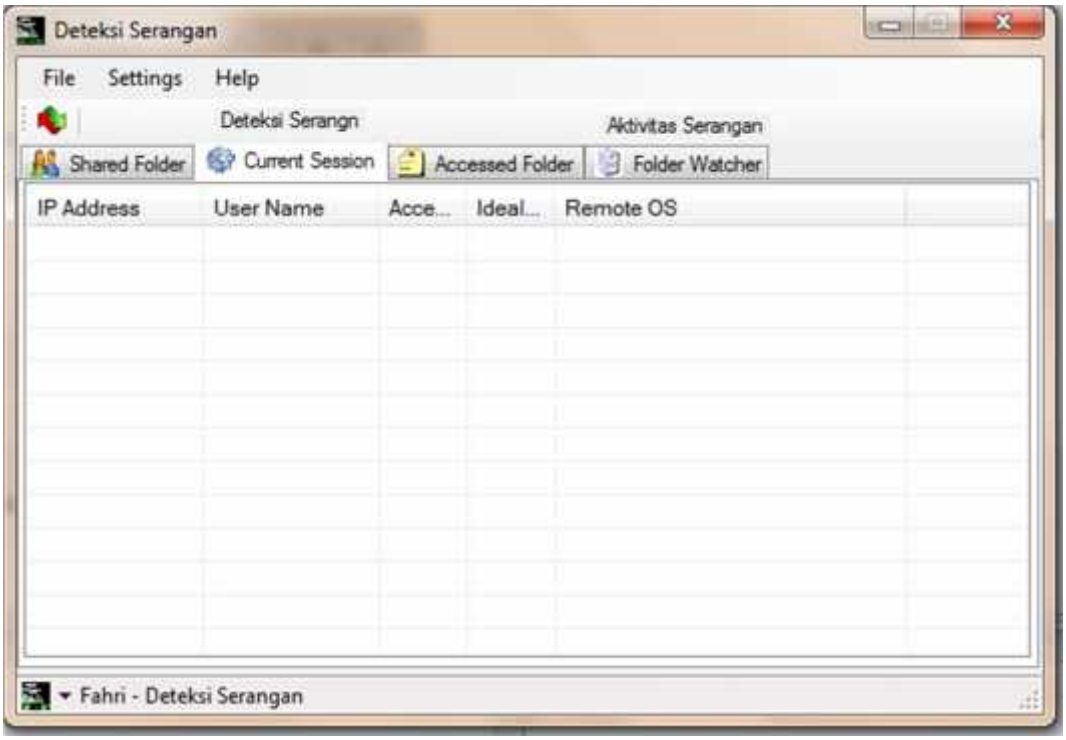
Perangkat lunak pembelajaran ini dirancang dengan menggunakan bahasa pemrograman *Microsoft Visual C# 2008* dengan menggunakan beberapa komponen (*tools*) yang dimiliki. Dalam perancangan perangkat lunak *network spy* ini, penulis juga menggunakan beberapa gambar sebagai tambahan untuk mempercantik aplikasi

Form – form yang terdapat dalam perangkat lunak pembelajaran ini yaitu,

1. *Form* Utama
2. *Form Password*

III.5.1 Form Utama

Form utama merupakan form yang digunakan untuk melakukan proses monitoring terhadap pengaksesan komputer yang dilakukan dari jaringan, berikut adalah desainnya.



Gambar III.8. Rancangan Form Utama

Form utama diatas merupakan form ketika pertama sekalian program dijalankankan, pada form utama diatas terdapat opsi tab dan menu yang bisa digunakan, adapun keterangannya adalah sebagai berikut:

1. Frame yang digunakan untuk menampilkan informasi dari masing-masing tab, seperti shared folder dan current session.
2. Menu yang digunakan untuk melakukan fungsi pada aplikasi *Network Spy*, pada menu ini terdapat 3 menu utama yaitu menu file, menu settings dan menu help, berikut adalah isi dari masing-masing menu.

a. File

1. Refresh

   Sub menu ini digunakan untuk melakukan pembaruan informasi terhadap pengaksesan folder

2. Exit

   Untuk keluar dari aplikasi

b. Settings

1. Enable PopUp

   Sub menu ini digunakan untuk menampilkan informasi ketika ada pengaksesan yang dilakukan dari dalam jaringan

2. Refresh Time

   Sub menu ini digunakan untuk mengatur lamanya refresh dilakukan, interval waktu yang diberikan dari 1 detik sampai 5 detik.

c. Help

   Help

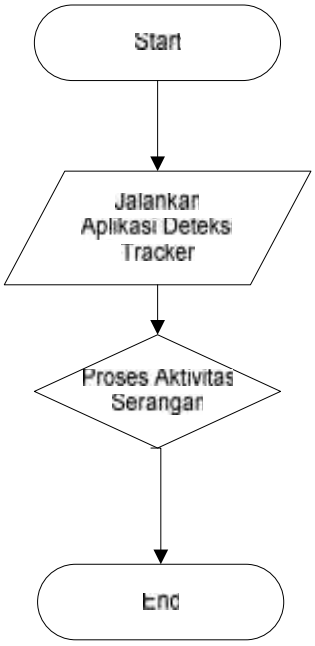
   Untuk menampilkan informasi tentang aplikasi

III.6. Analisis Flowchart

Pembuatan flowchart pada sistem ini untuk menggambarkan cara kerja dari sistem yang dirancang per modulnya, dalam perancangan ini terdapat beberapa flowchart yang menggambarkan sistem secara keseluruhan, berikut adalah flowchartnya.

1. Proses Aktifkan Deteksi Serangan

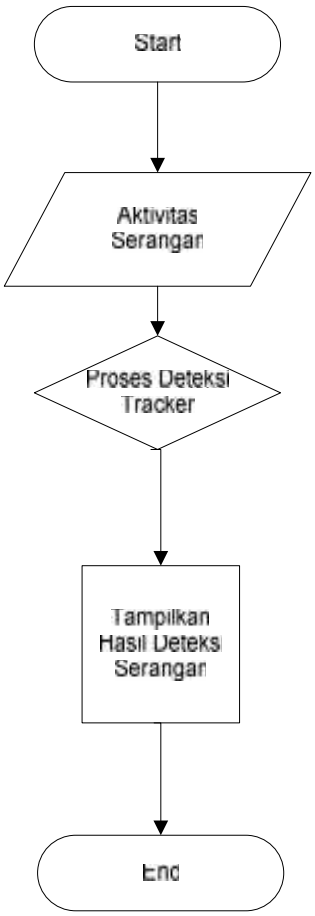
Untuk melakukan proses perekaman pada komputer target, aplikasi Deteksi serangan diaktifkan secara manual, untuk proses aktifasi Deteksi Serangan dapat diperhatikan pada flowchart dibawah ini.



Gambar III.9 *Flowchart* Aktifkan Deteksi Tracker

2. Tampilkan Hasil Pengaksesan

Tool Deteksi Serangan yang dirancang memungkinkan untuk melihat pengaksesan yang dilakukan, perubahan terhadap folder, pengaksesan folder, berikut adalah flowchart yang penulis rancang.



Gambar III.10 *Flowchart* Tampilkan Hasil Deteksi Tracker