BAB IV

HASIL DAN UJI COBA

IV.1. Jalannya Uji Coba

Implementasi sistem dalam aplikasi ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*).

IV.2. Hardware/Software yang dibutuhkan

Program ini dijalankan dengan menggunakan perangkat keras (*hardware*) yang direkomendasikan sebagai berikut :

1. *Prosesor Intel*

2. Memory 3 GB.

3. *Harddisk* 320 GB.

4. VGA *card* 128 MB.

5. Monitor dengan resolusi 800 X 600 *pixel*.

6. Keyboard dan Mouse

7. Hub dan Kabel LAN

Adapun perangkat lunak (*software*) yang direkomendasikan untuk menjalankan aplikasi ini adalah sebagai berikut:

1. Microsoft Windows XP SP3 dan Microsoft Windows 7 Ultimate

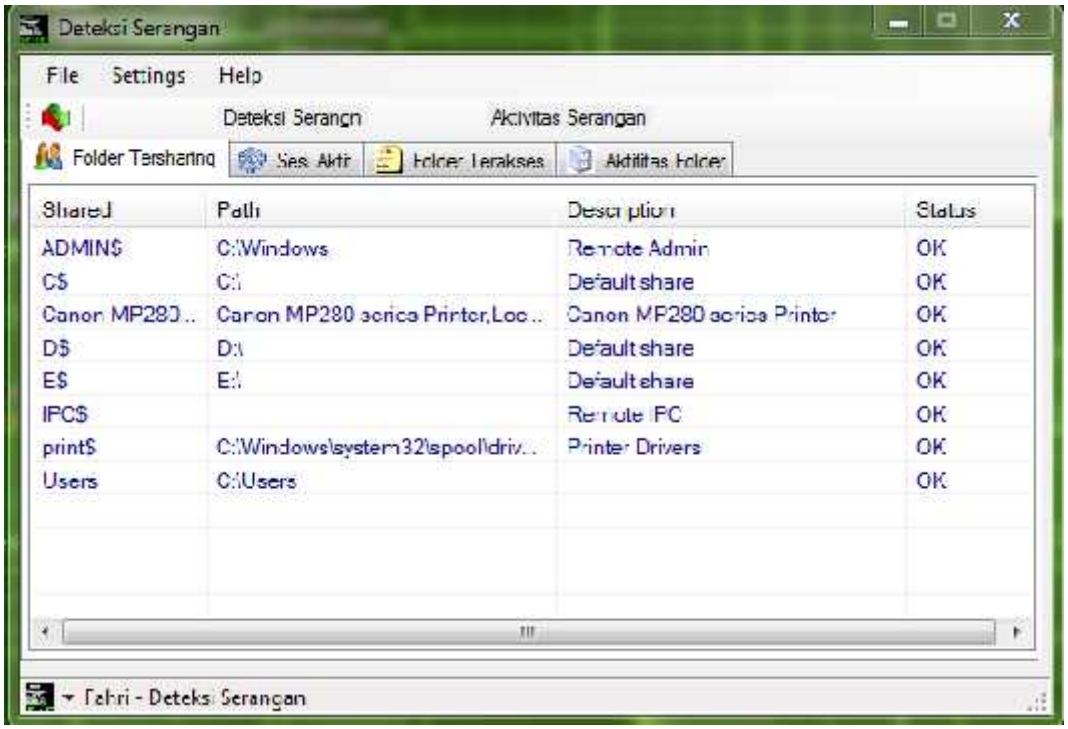
2. Microsoft Visual C# 2008

3. Microsoft *Network Libary*

4. Microsoft *Winsock Class*

IV.3. Pengujian Program

Untuk pengujian program bisa dilakukan dari *visual studio C#* atau berikut adalah tampilan utama ketika aplikasi dijalankan.

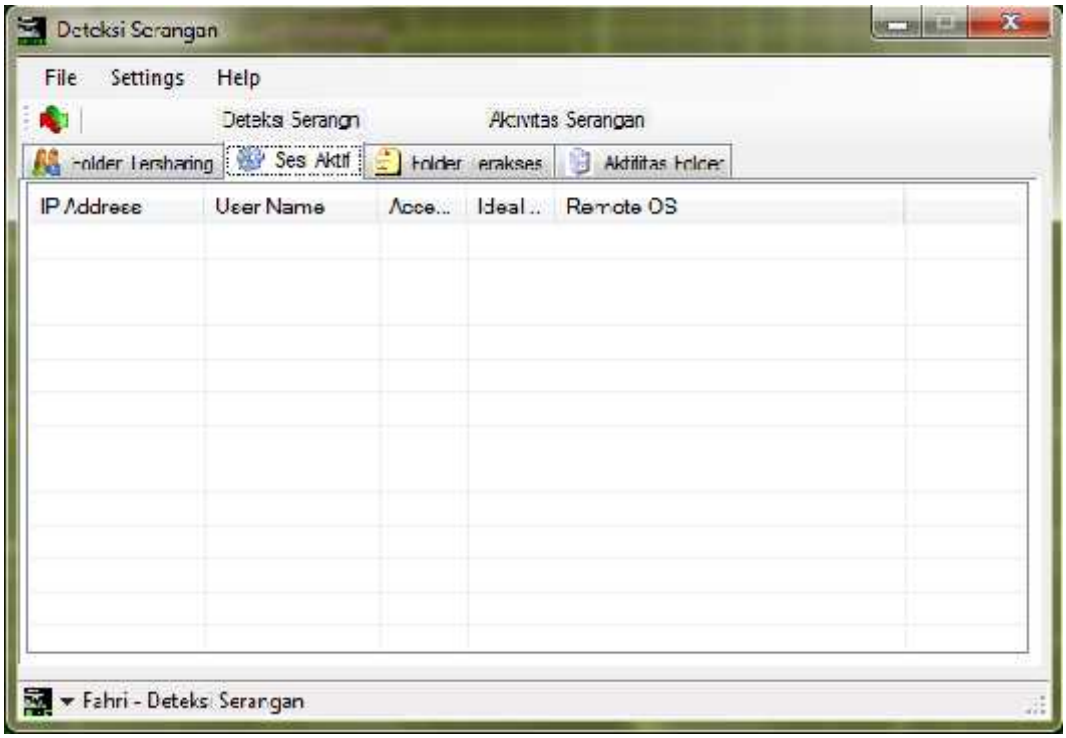


Gambar IV.1. Aplikasi Utama Folder Tersharing

Form diatas merupakan form aplikasi utama ketika dijalankan, pada aplikasi diatas terdapat beberapa tab seperti Folder sharing, Sesi Aktif, Folder terakses, Aktivitas Folder. Pada gambar IV.1. ketika aplikasi dijalankan maka secara otomatis yang aktif adalah Shared Folder.

Pada gambar diatas tampak informasi yang bisa diakses dari jaringan oleh pihak yang tidak bertanggung jawab, lokasi *folder* dan *drive* akan berbeda untuk setiap komputer dimana aplikasi dijalankan, selain *sharing folder* yang menampilkan informasi pengaksesan folder yang mungkin dimasuki oleh pihak yang bertanggung jawab, ada sebuah tab dengan nama current session yang

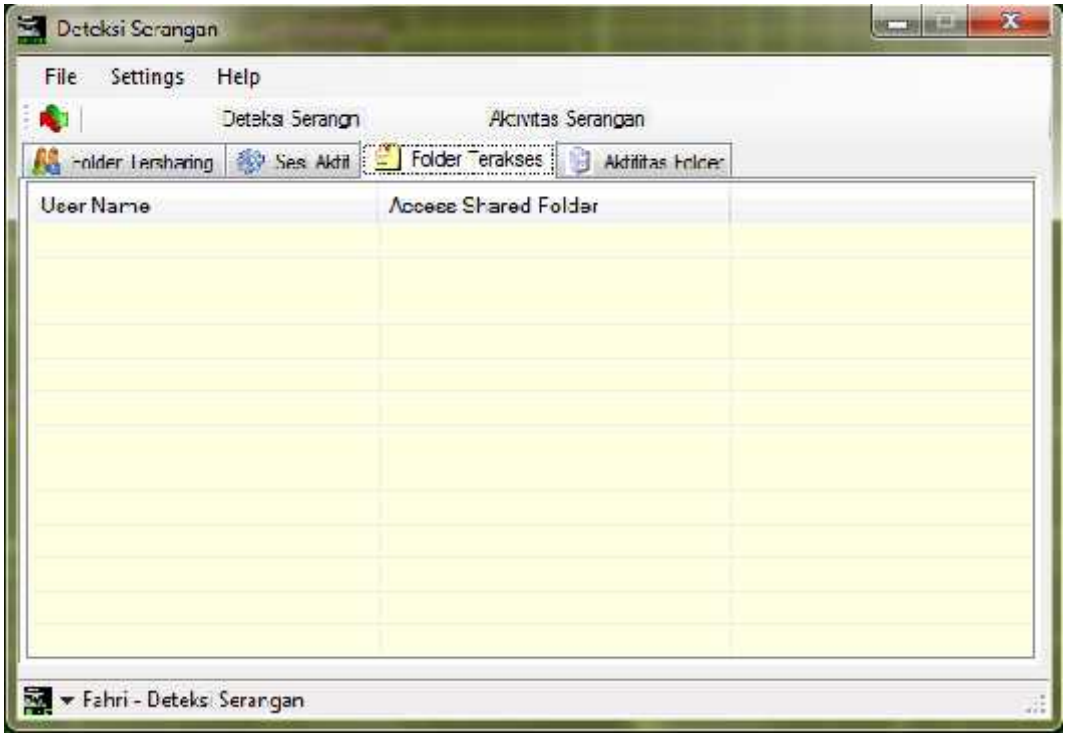
menampilkan nomor IP atau nama komputer yang mengakses komputer pengguna dari jaringan, berikut adalah *formnya*.



Gambar IV.2. Aplikasi Utama Sesi Aktif

Aplikasi utama Sesi aktif menampilkan informasi nomor IP atau nama komputer yang mengakses, *username* dari komputer ketika *mengakses*, lama pengaksesan dan waktu yang ideal pengaksesan serta sistem operasi yang digunakan.

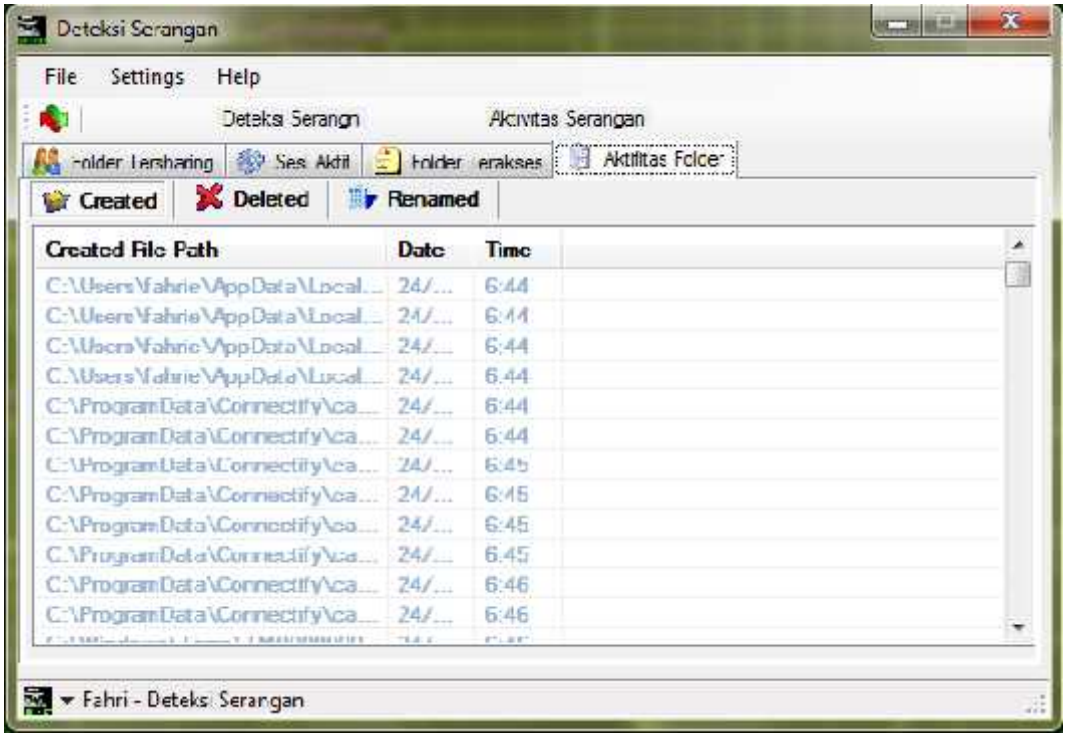
Folder yang terakses juga bisa diketahui siapa saja yang mengakses dikarenakan adanya fasilitas untuk monitoring folder, berikut adalah tampilan dama form Folder terakses.



Gambar IV.3. Aplikasi Utama Folder Terakses

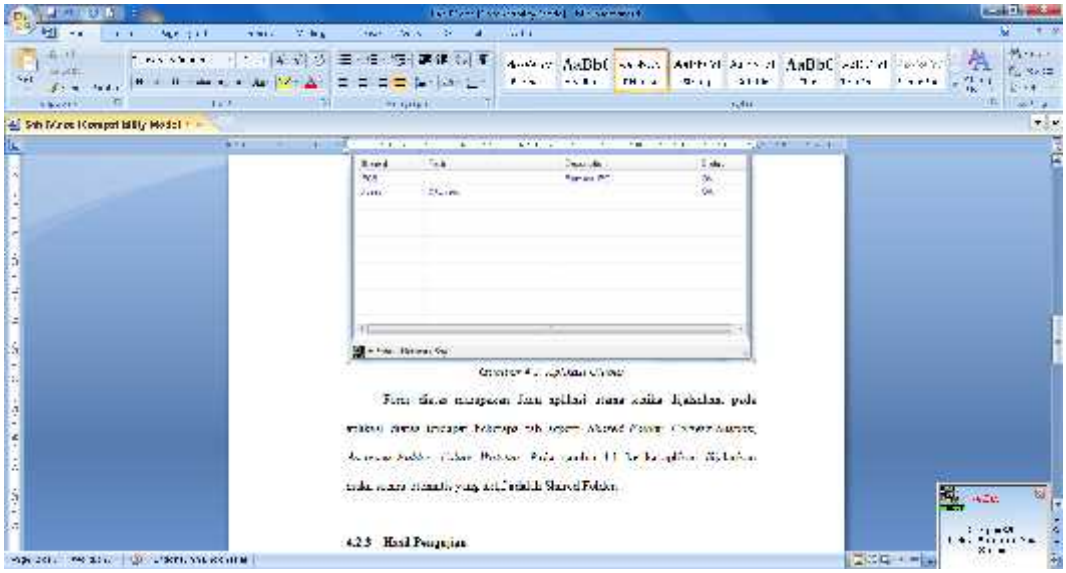
Form ini akan menampilkan informasi pengaksesan folder yang dilakukan didalam jaringan, informasi yang ditampilkan adalah username dari jaringan dan nama folder yang diakses.

Tab terakhir adalah Aktivitas Folder yang menampilkan lokasi folder yang dibuat, dihapus, dirubah, terjadinya perubahan terhadap folder bisa terjadi yang dilakukan didalan jaringan seperti membuat folder ataupun menghapus folder, berikut adalah tampilannya



Gambar IV.4. Aplikasi Utama Aktivitas Folder

Selain informasi diatas terdapat juga informasi *popup message* yanng menampilkan notifikasi bahwa komputer sedang diakses oleh komputer dari jaringan, berikut adalah tampilan notifikasinya.



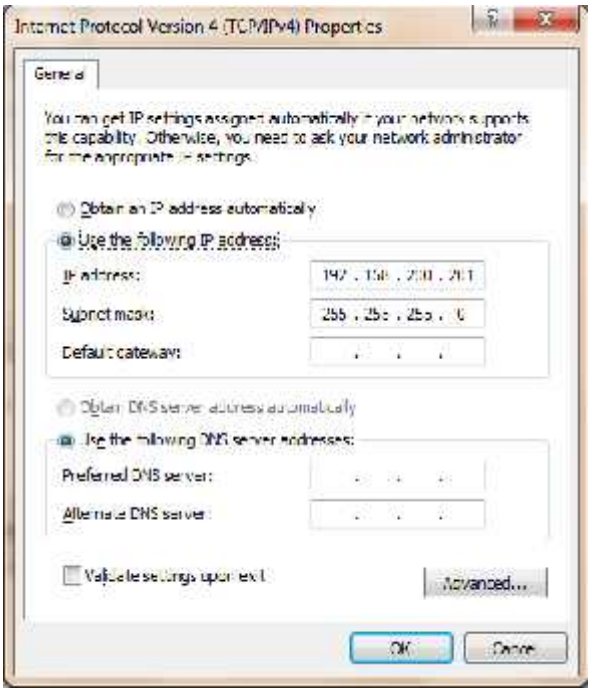
Gambar IV.5. Tampilan *Notifikasi*

IV.4. Analisa Hasil

Analisa hasil dari aplikasi deteksi serangan ini dapat mendeteksi adanya si penyerang mengakses komputer user. Aplikasi deteksi serangan ini memberikan informasi berupa data yang telah di akses oleh si penyerang. Misalkan, file, folder yang di hapus dan di rubah oleh si penyerang, dan02 aplikasi ini dapat menampilkan ip addres / nama dari pc dari penyerang yang mengakses komputer user. Dari analisa hasil percancangan aplikasi ini penulis membuat tiga poin proses sebelum terjadinya serangan yaitu,

1. Proses Serangan
2. Proses Alert
3. Aktivitas Yang Dilakukan Oleh penyerang

Berikut adalah gambar Proses untuk melakukan serangan berbasis LAN.



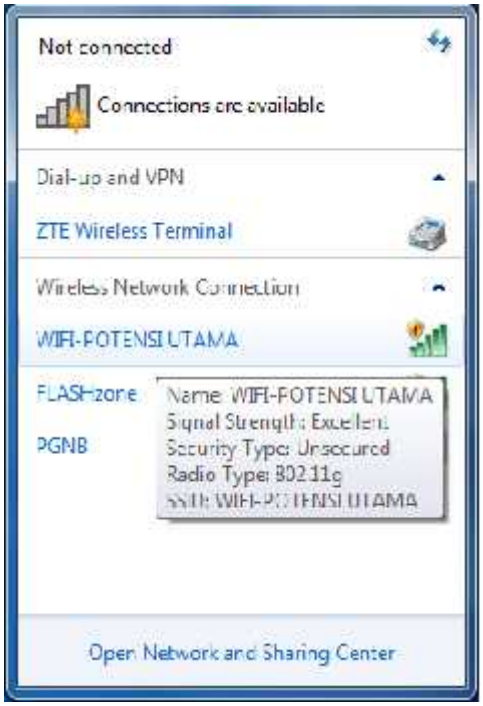
IV.6. Tampilan Proses Untuk Melakukan Serangan

Pada Gambar IV.6 menunjukan bahwa untuk memasuki komputer yang ingin di akses Tracker / sipenyerang terlebih dahulu harus mengetahui alamat ip addres dari komputer yang ingin di akses.

Berikut adalah gambar proses untuk melakukan serangan bebasis wifi.

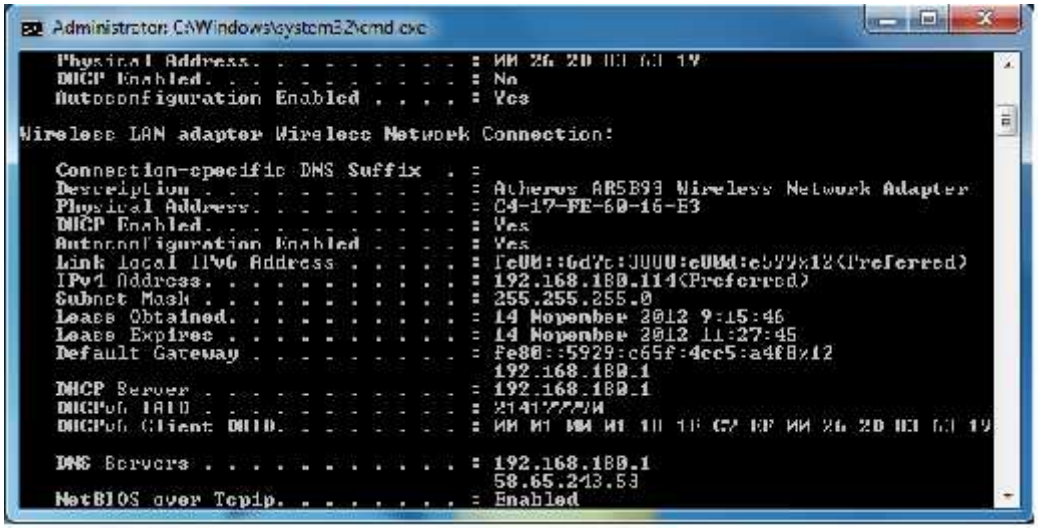
IV.7 Gambar Proses Berupa *Wifi* Yang Ingin di Akses

Kemudian Hacker memilih *wifi* korban yaitu Wifi Potensi Utama untuk memulai Serangannya. Berikut gambar proses untuk megakses komputer yang dituju.



IV.8. Gambar Wifi Yang Digunakan korban

Setelah itu Tracker memilih Wifi Potensi Utama Untuk Pengaksesan.Sebelum itu seorang penyerang terlebih dahulu harus mengetahui alamat ip addres dari komputer yang dituju. Berikut tampilan dari ip addres dari komputer yang dituju.



IV.9. Tampilan IP Addres Komputer Korban

Selanjutnya Tracker / penyerang harus mengetetahui nama dan pasword keamanan dari komputer yang dituju. Berikut tampilannya.

IV.10. Tampilan Dari Security Komputer Yang Dituju

IV.5. Kelebihan Dan Kekurangan Aplikasi

IV.5.1. Kelebihan Dari Aplikasi Yang Dirancang.

Aplikasi deteksi serangan memiliki kelebihan sebagai berikut:

a. Aplikasi yang dirancang mampu untuk merekam aktifitas yang terjadi pada komputer ketika terjadi pengaksesan oleh komputer didalam jaringan.
b. Aplikasi juga bisa mencatat semua aktiftas manipulasi folder dan file yang ada didalam drive yang ada pada komputer.
c. Terdapatnya fasilitas Log monitoring pada aplikasi.

IV.5.2. Kekurangan Dari Aplikasi Yang Dirancang.

Aplikasi deteksi serangan ini memiliki kekurangan Sebagai berikut:

a. Aplikasi belum mendukung untuk pengaksesan dalam WiFi, masih sebatas dalam jaringan Local Area Network.
b. Tidak adanya fitur untuk pemblokiran IP.
c. Aplikasi deteksi serangan ini tidak bisa mengantisipasi serangan.