

PENGEMBANGAN PERANGKAT LUNAK UNTUK PEMANTAUAN JARAK JAUH (*REMOTE MONITORING*)

Wilfridus Bambang Triadi Handaya

Program Studi D3 Teknologi Informasi

Fakultas Teknologi Informasi, Universitas Kristen Maranatha

Jl. Prof. Drg. Suria Sumantri No. 65 Bandung 40164

email: wilfridus.bambang@eng.maranatha.edu

Abstract

The purpose of this system development to help the network administrator for doing the maintenance and monitoring. Sistem will be consist of two kind of implementation, client side and server side. Client Machine have some function to record the view of computer monitor with 2 option, based on time interval and execution. All user activities can be monitored from the server. File will be convert from JPG extension to video (AVI). This implementation of this software is running smoothly with some mechanism to prevent from security threats that can disturb the whole operation of the system

Keywords : *spy, client server, remote monitoring.*

1. Pengantar

Berbicara mengenai dunia spionase saat ini adalah tidak terbatas hanya pada masalah intelijen militer dengan alasan keamanan negara ataupun spionase pada dunia bisnis dimana kompetitor dapat mengetahui data penting yang terdapat pada sistem perusahaan pesaingnya. Kemudian penerapannya dikembangkan lagi pada dunia *Personal Computer* (PC) yang secara langsung akan mengawasi serta mengeliminasi privasi kepentingan dari seorang pengguna komputer.

Sebenarnya masalah spionase pada dunia komputer telah dimulai dalam jangka waktu yang lama, dan boleh dibilang telah ada semenjak dunia komputer itu diciptakan. Contoh kasus yang dapat dianalisa secara lebih sederhana dari uraian di atas adalah keingintahuan seseorang mengenai data dari komputer publik yang sedang digunakan, ataupun pula dalam administrasi jaringan, dengan menggunakan program *Remote Control*, sudah sejak lama para administrator sistem tidak hanya dapat mengendalikan PC dalam jaringan, tapi juga mengawasinya. Program yang pada awalnya hanya dibuat segelintir produsen seperti Novell (*Remote Management*) atau Symantec (*PC Anywhere*) ini belakangan telah tersedia dalam aplikasi sistem operasi Microsoft Windows XP. Walaupun peruntukan utamanya adalah untuk mengendalikan PC *client* dari jauh (*remote*), kini fungsinya telah jauh diperluas dengan fungsi-fungsi tambahan.

Sebagai sebuah teknologi yang sifatnya netral, aplikasi spionase pada PC pun dipengaruhi oleh latar-belakang mengapa program tersebut di-*install*. Penerapannya secara nyata dapat berfungsi untuk melakukan monitoring pada seseorang untuk mencegah terjadinya penyelewengan yang dilakukan oleh seorang bawahan. Juga berfungsi untuk menguji loyalitas seseorang. Pada sisi yang lain,

program ini dapat pula diarahkan sebagai program untuk melakukan kegiatan yang *illegal* seperti pencurian nomor rekening, *password*, data pribadi, dan lain-lain. Bahkan program ini dapat menjalankan peran sebagai mata–mata yang jitu. Sehingga bukan tidak mungkin aplikasi ini mengambil peran cukup penting dalam dunia spionase.

2. Latar Belakang Masalah

Dalam sebuah jaringan komputer (LAN) yang memiliki disiplin pemakaian yang tinggi, dibutuhkan pengawasan dan pengendalian terhadap pemakaian tiap-tiap *workstation* di dalamnya. Untuk alasan tersebut maka perlu dipikirkan suatu aplikasi yang dapat digunakan untuk membantu melakukan tugas pengawasan dan pengendalian.

Dari kondisi tersebut di atas akan dirancang pengembangan suatu perangkat lunak pemantauan jarak jauh (*remote monitoring*), yaitu perangkat lunak dimana seorang administrator dapat dengan mudah mengetahui siapa saja yang telah menggunakan komputer, serta apa saja yang dilakukan saat menggunakan komputer tersebut. Aplikasi ini memiliki kinerja seperti sebuah kamera keamanan yang diletakkan secara rahasia dan berfungsi memonitor penggunaan komputer. Untuk hasil perekaman akan berbentuk *file* grafis JPEG yang selanjutnya dapat dikonversi menjadi suatu *file* video dengan format AVI.

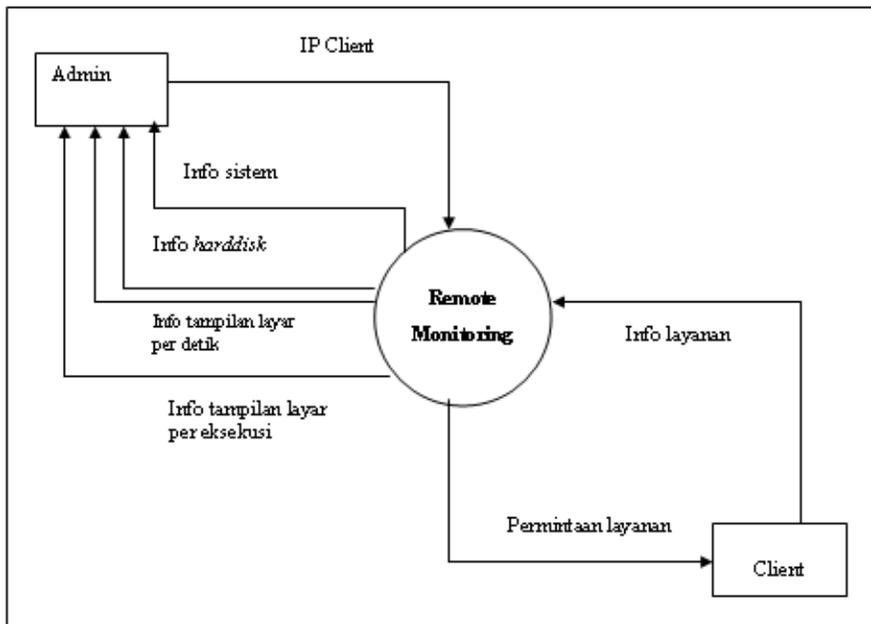
Kemampuan tambahan yang terdapat dalam aplikasi spionase ini adalah melakukan penelusuran (*explore*) ke sumber daya *harddisk* dari sistem target, kemudian dapat pula mengetahui tingkat kinerja dari memori *virtual* selama dilakukannya proses perekaman, dan terakhir adalah menghentikan kerja dari sistem komputer target apabila dianggap melakukan kegiatan yang membahayakan sistem publik secara keseluruhan.

3. Analisa Dalam Penentuan Pengembangan Aplikasi

Pada bagian ini akan diberikan gambaran dan penjelasan mengenai konsep pengawasan dan perekaman tampilan monitor pada sistem target sebagaimana yang menjadi fokus utama pembangunan perangkat lunak pemantauan jarak jauh (*remote monitoring*) berikut secara teknis, yang terdiri dari analisis sistem, perancangan sistem dan spesifikasi perangkat lunak serta perangkat keras sistem.

Untuk perancangan perangkat lunak terbagi atas : *Data Flow Diagram* (DFD), diagram yang menjelaskan mengenai aliran data dan proses yang terlibat di dalamnya. Analisis sistem digunakan untuk mempelajari lebih rinci mengenai tiap bagian yang ada dalam perancangan. Tahap selanjutnya adalah membuat perancangan masukan dan perancangan keluaran yang diharapkan, kedua hal tersebut perlu dilakukan untuk menentukan bagaimana dan darimana suatu data akan dimasukkan serta bagaimana keluaran harus dibuat. Untuk proses dan aliran data akan dijelaskan pada tahap perancangan.

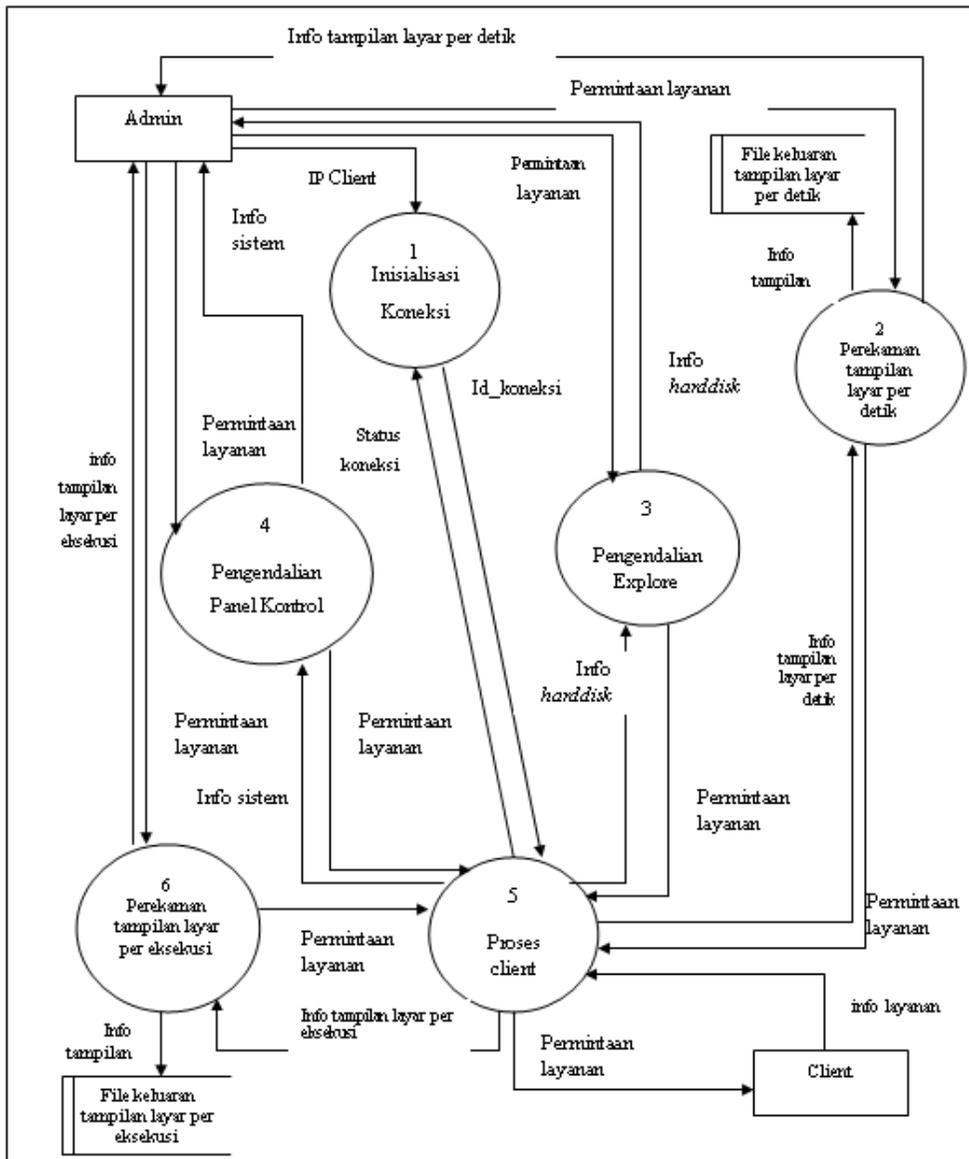
Pada gambar 1 akan ditampilkan desain DFD level 0 dari aplikasi :



Gambar 1. Desain level 0

Sistem akan bekerja untuk memonitor secara keseluruhan aktivitas dari komputer target, dengan lebih terfokus pada perekaman tampilan layar berdasarkan pada dua (2) opsi yaitu perekaman tampilan per eksekusi atau perekaman tampilan berdasarkan nilai interval waktu yang diberikan oleh sisi *server*. Akan tetapi, terdapat pula dua (2) fungsi tambahan yaitu administrator dapat melakukan pengaksesan ke *harddisk client* serta mengetahui informasi sistem yang ter-*install*.

Sedangkan untuk level 1 dapat dilihat pada gambar 2 di bawah ini :



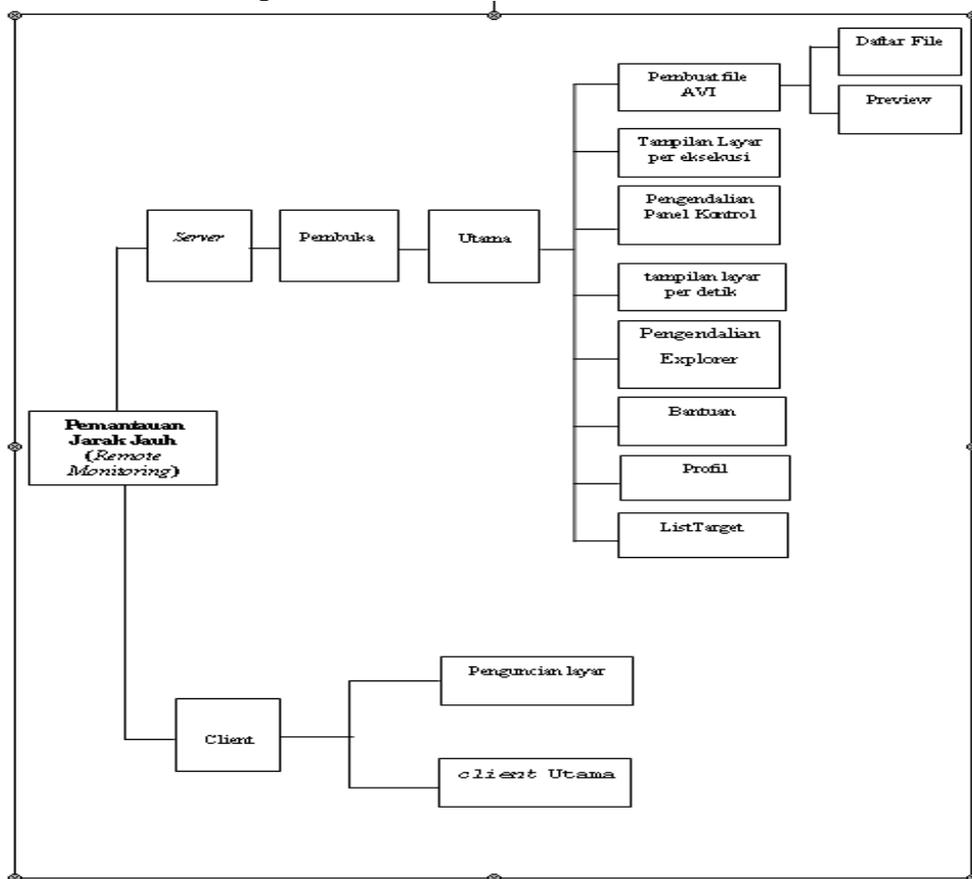
Gambar 2. Desain Level 1

Tahap-tahap perancangan aplikasi pemantauan jarak jauh (*remote monitoring*) dimulai dengan menginventarisasi semua kejadian pada mesin *client* yang mungkin dikendalikan dari *server*, kemudian menuliskannya sebagai suatu daftar kejadian (*Event List*). Untuk setiap kejadian ditentukan segala informasi yang terlibat, ditentukan alirannya (sumber dan tujuan) dan digambarkan dalam bentuk DFD. Berikut ini akan dijelaskan fungsi-fungsi yang terdapat di dalamnya.

Fungsi-fungsi yang terdapat pada aplikasi ini adalah :

- a. Fungsi Client Utama
Form ini mencakup inisialisasi program (*remote monitoring*) ke sistem yang diinginkan. Fungsi-fungsi yang tercakup di dalamnya antara lain untuk pengecekan *port-port* koneksi antara *server* dengan *client*, kemudian membuat suatu *file* teks yang menandakan bahwa koneksi berhasil dibangun. Selanjutnya terdapat penyiapan lingkungan sistem komputer *client* untuk dapat dijalankan sumber dayanya melalui sisi *server*.
Fungsi selanjutnya adalah melakukan perekaman dari tampilan layar monitor *client* yang dapat diinisialisasi waktu perekamannya dengan interval nilai antara 1 - 10 detik. Digunakan *file* pustaka *cjpg.dll* dalam mengkonversi hasil perekaman dari layar yang pada awalnya berbentuk *file* bitmap menjadi *file* JPEG.
Selanjutnya, terdapat fasilitas menciptakan tampilan koneksi yang dibangun oleh *client* ke *server* dengan halaman web (HTML).
- b. Fungsi Penguncian Layar
Form ini jika fungsinya dieksekusi akan menutup tampilan layar komputer *client* dengan latar depan berwarna hitam. Kemudian akan melakukan penguncian terhadap keyboard, sehingga tidak ada tombol yang bekerja.
- c. Fungsi Pengendalian Explorer
Form Pengendalian Explorer ini merupakan pengendalian sumber daya *harddisk* pada sistem target, sehingga *server* (pengintai) dapat melakukan beberapa fungsi seperti halnya aplikasi windows explorer, yaitu *download*, *upload*, melakukan eksekusi, membuat direktori, dan terakhir, dapat menghapus *file* yang diinginkan.
- d. Fungsi Pengendalian Panel Kontrol
Melakukan pemantauan kinerja dari sistem dengan melihat pergerakan status dari nilai memori komputer yang ada. Hal ini memberikan informasi pendeteksian awal apabila terjadi penurunan kinerja yang cukup signifikan pada pemantauan jarak jauh, untuk mengantisipasi kemungkinan-kemungkinan yang tidak diinginkan.
- e. Fungsi Tampilan Layar per Eksekusi
Untuk melakukan perekaman tampilan layar dari komputer target berdasarkan hasil eksekusi dari *mouse*, dengan menitikberatkan pada penekanan tombol kiri ataupun kanan dari tombol *mouse* tersebut. Hasil rekamannya akan disimpan pada direktori yang telah ditentukan dalam bentuk *file* JPEG.
- f. Fungsi Pembuat File AVI
Menggabungkan *file-file* gambar hasil perekaman sebelumnya yang telah tersimpan di *harddisk* menjadi *file video* dengan format AVI.
- g. Fungsi ListTarget
Menampilkan nomor IP komputer yang aktif sebagai *client* dari aplikasi ini.

4. Arsitektur Perangkat Lunak



Gambar 3. Arsitektur Perangkat Lunak

5. Hasil Implementasi Aplikasi

Perangkat lunak pemantauan jarak jauh (*remote monitoring*) dibangun menggunakan aplikasi pemrograman Microsoft Visual Basic 6.0 dengan memanfaatkan fasilitas komponen utama Microsoft Winsock Control untuk membangun koneksi, jalur komunikasi, serta kemampuan pengontrolan serta pengendalian dari jarak jauh (*remote*).

Pada sisi *server* yang berfungsi sebagai pemantau, diperlukan pula beberapa inisialisasi yang harus dilakukan agar dapat mengkoneksikan keberadaannya dengan komputer *client*. Salah satu contoh yang dapat disebutkan adalah konsistensi dari penggunaan *port*. Pada perancangan kode sumbernya, digunakan banyak fungsi dalam WIN32API dalam pencapaian tujuan utama aplikasi ini dibangun. Desain antarmuka aplikasi dibangun menggunakan *form* MDI, dengan maksud untuk memudahkan pemakaian serta penambahan beberapa visualisasi gambar pada *form*. Untuk komunikasi, menggunakan protokol TCP melalui soket identifier sebagai sarana pengiriman permintaan layanan kepada *client*.

Tampilan aplikasi akan terlihat seperti pada gambar 4 berikut ini :

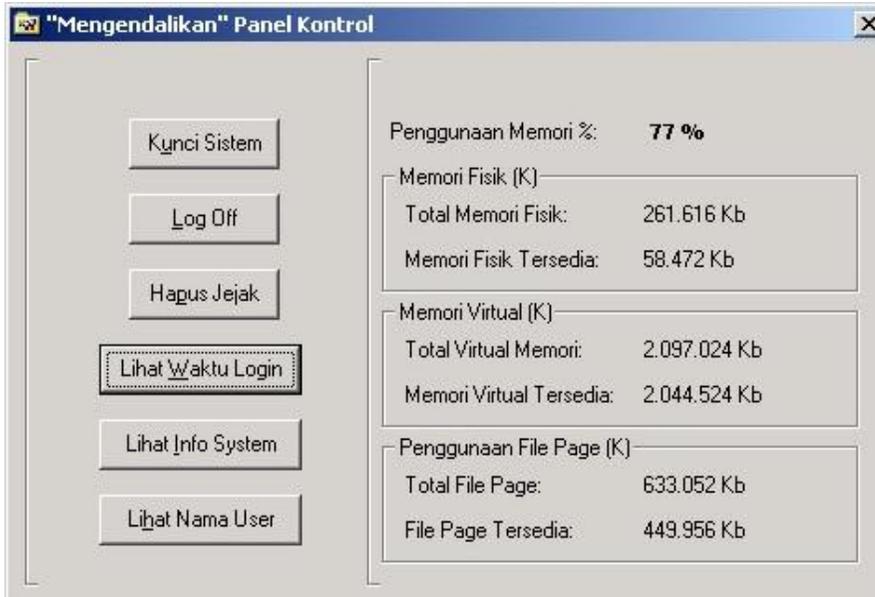


Gambar 4. Form Utama Aplikasi

Ketika aplikasi dijalankan, maka akan melakukan interupsi untuk menahan apabila terdapat upaya untuk mematikan sistem secara tidak sengaja ataupun dari pihak di luar sistem. Menggunakan *file* pustaka *user32.dll*, dan pendeklarasiannya adalah sebagai berikut :

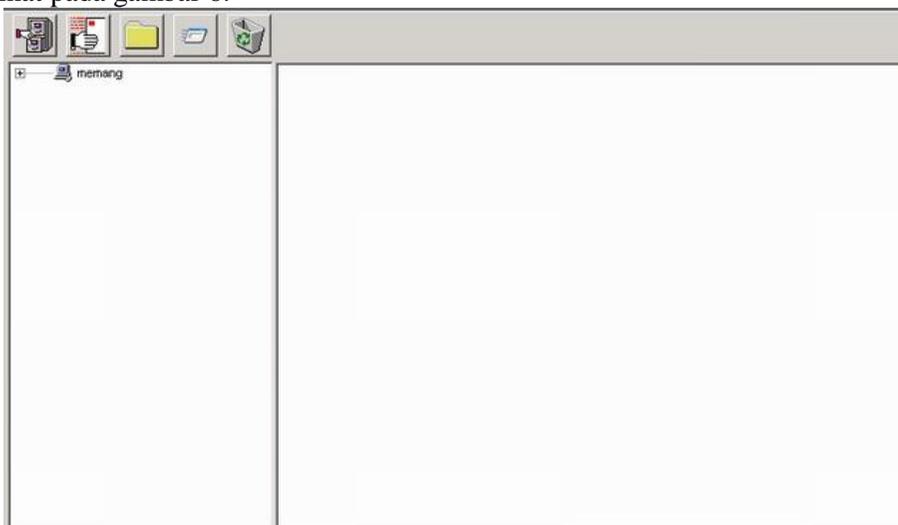
```
lpPrevWndProc = SetWindowLong(gHW, GWL_WNDPROC, AddressOf WindowProc)
```

Bagian ini merupakan fungsi untuk mendapatkan informasi dari sistem komputer dari sisi *server* ataupun dari sisi *client*. Hal ini dilakukan agar administrator (pengguna) dapat segera memutuskan solusi yang perlu dalam penanganan suatu kejadian. Disertakan beberapa objek tombol seperti untuk penghapusan registry di sistem Microsoft Windows, LogOff, penguncian layar pada *client*, serta memperoleh informasi mengenai sistem yang berhasil dipantau. Untuk rutin sebenarnya terdapat pada sisi *client*, dengan *server* hanya memberikan perintah dalam variabel tertentu bertipe *string*. Kemudian untuk tampilan dari form pengendalian panel kontrol akan terlihat pada gambar 5.



Gambar 5. Form Pengendalian Panel Kontrol

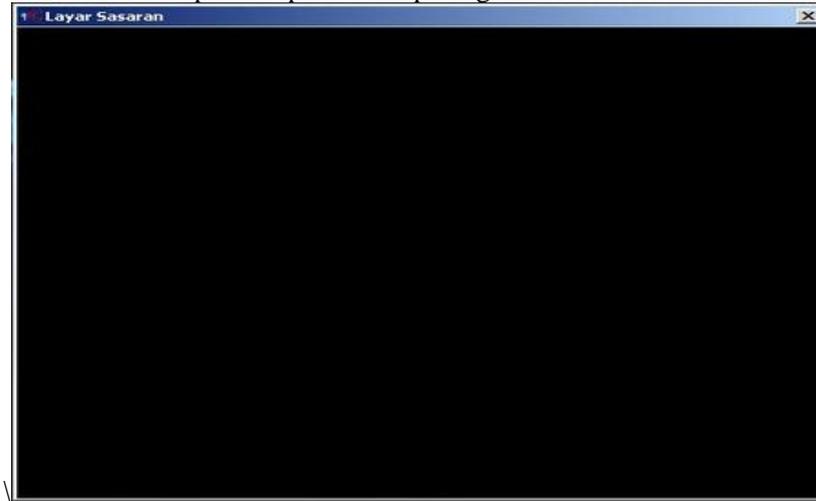
Pada modul ini, sistem akan mendapatkan tampilan *drive* dari *harddisk* sistem yang menjadi tujuan koneksi. Konsep yang digunakan adalah berbeda dengan *file sharing* seperti halnya Netbios pada Microsoft Windows, tapi lebih pada identifikasi semua *resources* yang terdapat dalam sistem yang aktif. Dapat dilihat pada gambar 6.



Gambar 6. Form Pengendalian Eksplorer

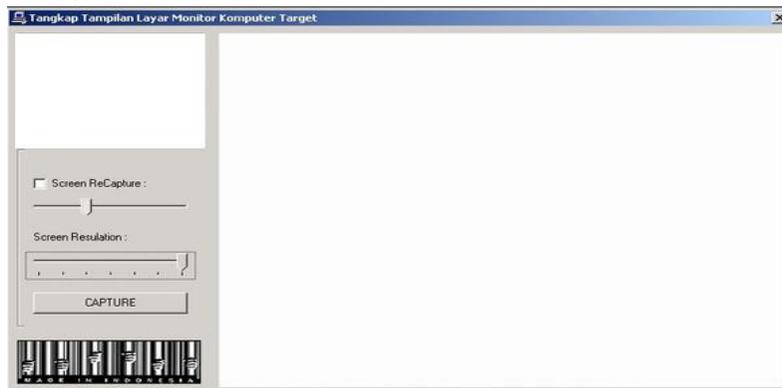
Fasilitas selanjutnya yang dihadirkan oleh aplikasi ini adalah akan menampilkan *screenshot* dari *client* berdasarkan *event* klik kiri dan kanan dari *mouse*, untuk selanjutnya akan dikirim ke komputer *server/administrator* dalam bentuk *file* grafis dengan *format* JPEG yang pada proses penamaan

penyimpanannya di sumberdaya pengguna (*harddisk*) yang sedang melakukan pengawasan akan ditambahkan nilai dari pencacah yang secara otomatis akan menaikkan nilainya setiap kali penerimaan yang sukses oleh *server*. *File-file* tersebut diletakkan pada satu direktori khusus yang telah dibuat pada waktu *form* utama dieksekusi. Tampilan dapat dilihat pada gambar 7.



Gambar 7. Form Perekaman Tampilan Layar per Eksekusi

Modul ini berfungsi untuk melakukan perekaman tampilan layar monitor dari komputer *client* berdasar interval waktu tertentu yang dimasukkan oleh administrator (pengguna). Hasil yang diperoleh merupakan *file* grafis dengan pengesetan menggunakan *format* JPEG. Untuk objek slider ada 2 kategori yaitu perubahan ukuran tampilan layar mulai dari 10-70 %, dan pengesetan interval waktu perekaman secara kontinu mulai dari 1-10 detik. Tampilan dapat dilihat pada gambar 8.



Gambar 8. Form Perekaman Tampilan Layar per Detik

Untuk menggabungkan *file-file* rekaman dari tampilan yang telah dijelaskan pada bagian sebelumnya, sehingga menjadi suatu *file video* berformat AVI. Rutin penggabungannya merupakan implementasi langsung dari kode sumber *modAVIDecs.bas*, yang merupakan hak cipta Ray Mercer (<http://www.shrinkwrapvb.com>). Tampilan dapat dilihat pada gambar 9.



Gambar 9. Form Pembuat Berkas AVI

6. Kesimpulan

1. Perangkat lunak ini dapat membantu administrator jaringan untuk melakukan pemantauan terhadap penggunaan komputer dalam jaringan, dengan menangkap serta merekam tampilan visual pada komputer yang dimonitor.
2. Implementasi aplikasi pada mesin *client* yang berfungsi sebagai *backdoor* dari sistem pemantau, tidak terdeteksi sebagai *virus* oleh *tool* Antivirus Norton Antivirus dengan *update database* terbaru. Untuk pendeteksian dari *tool* McAfee, tercatat sebagai *script* yang tidak membahayakan sistem.
3. Untuk mengatasi berbagai kemungkinan spesifikasi komputer pada sisi *client* yang kadangkala memiliki komputasi yang rendah, maka administrator sebagai pengguna dari sisi *server* dapat memilih opsi-opsi yang sekiranya tidak mengakibatkan penurunan kinerja dari sistem selama proses pemantauan dilakukan.
4. Aplikasi-aplikasi lain yang berjalan pada komputer *client*, terutama aplikasi utilitas sistem, dapat mempengaruhi kinerja perangkat lunak.

7. Saran

Pengembangan perangkat lunak pemantauan jarak jauh ini masih mempunyai banyak celah yang dapat dijadikan acuan untuk pembangunan di masa yang akan datang sehingga dapat diciptakan suatu sistem pemantauan yang lebih sempurna. Keberhasilan implementasi fungsi-fungsi yang ada, sangat bergantung pada tingkat mobilitas penggunaan dan konfigurasi sistem, yang seharusnya telah dari awal disiapkan berbagai macam *policy* untuk penerapan dalam suatu jaringan komputer yang digunakan sebagai fasilitas publik.

Untuk pemahaman mengenai masalah etika dari penggunaan aplikasi ini, diharapkan administrator sebagai pihak yang melakukan *maintenance* dalam sistem agar menjaga kerahasiaan serta privasi dari pengguna. Pada satu sisi, hilangnya privasi merupakan pelanggaran hak yang sangat mendasar dari pengguna, akan tetapi di sisi lain, hal tersebut dapat dilakukan, untuk kepentingan keamanan sistem secara keseluruhan.

Daftar Pustaka

1. Dumas, Arthur, *Programming Winsock*, SAMS Publishing, Indianapolis, 1995.
2. Freedman, D "The Goods on Hackers Hoods", Forbes ASAP, September 13, 1993.
3. Heywood, Drew, *Networking with Microsoft TCP/IP*, Prentice Hall Inc., 1996.
4. Judith, Jeffcoate, *Multimedia in Practice, Technology and Applications*, Prentice Hall, 1994.
5. Marchuk, Michael, *Building Internet Applications with Visual Basic*, QUE Corporation, Indianapolis, 1995.
6. Onno W. Purbo, Adnan Basalamah, Ismail Fahmi, dan Achmad Husni Thamrin, *Buku Pintar Internet : TCP/IP*, PT Elex Media Komputindo, Jakarta, 1998.
7. Pfleeger, C "Security in Computing", Englewood Cliffs, NJ, Prentice Hall 1989.
8. Saltzer, J., and Schroeder, M. "The Protection of Information in Computer Systems" Proceeding of the IEEE, September 1975.
9. Tanenbaum, A. S., *Computer Networks 3e*, Prentice Hall Inc., New Jersey, 1996.
10. Thomas, Robert M., *Introduction to Local Area Network*, SYBEX Inc., 1996.
11. Wahana Komputer, *Memahami model enkripsi dan security data*, Penerbit Andi, Yogyakarta, 2003.