Remote PC menggunakan SSH Server dan Telnet Server serta Monitoring Jaringan menggunakan Wireshark

Yama Fresdian Dwi Saputro
fds.yama@gmail.com
http:// from-engineer.blogspot.com

Lisensi Dokumen:
Copyright © 2003-2007 IlmuKomputer.Com
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Pendahuluan

1.1 Wireshark

Wireshark merupakan salah satu dari software monitoring jaringan yang biasanya banyak digunakan oleh para administrator jaringan untuk mengcapture dan menganalisa kinerja jaringan. Salah satu alasan kenapa Wireshark banyak dipilih oleh seorang administrator adalah karena interface nya menggunakan Graphical User Unit (GUI) atau tampilan grafis. Bila anda adalah seorang admin, pasti software ini bisa sangat membantu. Dengan menggunakan software ini kita bisa mengcapture packet packet data yang berkeliaran pada jaringan yang sedang dimonitoring. Dengan kata lain admin bisa mengetahui apa saja informasi yang sedang di akses oleh para user dan bisa menganalisa nya. Software Wireshark juga memungkinkan bagi seorang admin untuk memperoleh informasi informasi penting dari user seperti password email atau account lain yang sedang diakses dengan menganalisa packet packet yang bisa kita tangkap dengan software ini.

1.2 Telnet (*Telecommunication network*)

Telnet (Telecommunication network) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan. Telnet menyediakan komunikasi dua arah berbasis teks atau terminal emulator antara client dan server. Dengan kata lain, Telnet memungkinkan kita untuk mengendalikan, memberi perintah, menjalankan perintah, merubah konfigurasi, meremote komputer lain (server) melalui komputer di depan meja kita sendiri (client). Program Telnet biasanya digunakan untuk mengakses komputer berbasis Linux/Unix. Karena memang Linux/Unix banyak digunakan sebagai server. Namun saat ini Telnet sudah jarang digunakan karena memiliki celah atau lubang keamanan sebab komunikasi teks yang dilakukan tanpa enkripsi artinya bisa disadap oleh orang lain. Untuk memulai sesi Telnet, biasanya Anda harus mengisikan username serta password yang valid sebagai verifikasi atau legalitas dari account yang Anda miliki. Dan account tersebut di dapat atau Anda buat sendiri jika Anda bertindak sebagai administrator dari sebuah jaringan.

Telnet berjalan dengan 2 software yang masing-masing software dipasang pada komputer server (Telnet Server) dan pada komputer client (Telnet Client). Namun biasanya istilah Telnet sering digunakan untuk menunjuk software yang digunakan atau dipasang pada komputer client saja (Telnet Client).

- **Tugas dari Telnet Client adalah :**

1. Membuat koneksi network TCP (Transfer Control Protocol) dengan server.
2. Menerima inputan dari user.
3. Menformat kembali inputan dari user kemudian mengubah dalam bentuk format standard dan dikirim ke server.
4. Menerima output dari server dalam format standard.
5. Mengubah format output tadi untuk ditampilkan pada layar.

Copyright © 2003-2007 IlmuKomputer.Com

6. Menginformasikan software jaringan bahwa komputer itu siap menerima koneksi.
7. Menunggu permintaan dalam bentuk format standard.
8. Melaksanakan permintaan tersebut.
9. Mengirim kembali hasil ke client dalam bentuk format standard.
10. Menunggu permintaan selanjutnya.

Telnet sendiri mempunyai port defaultnya, port tersebut mempunyai nomor yaitu bernomor 23. Artinya telnet beroperasi pada port 23 di dalam sebuah komunikasi yang di bangun di jaringan komputer.

1.3 SSH (*Secure Shell*)

Secure Shell atau SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan. Terutama banyak digunakan pada sistem berbasis Linux dan Unix untuk mengakses akun shell, SSH dirancang sebagai pengganti Telnet dan *shell remote* tak aman lainnya, yang mengirim informasi, terutama kata sandi, dalam bentuk teks sederhana yang membuatnya mudah untuk dicegat. Enkripsi yang digunakan oleh SSH menyediakan kerahasiaan dan integritas data melalui jaringan yang tidak aman seperti Internet.

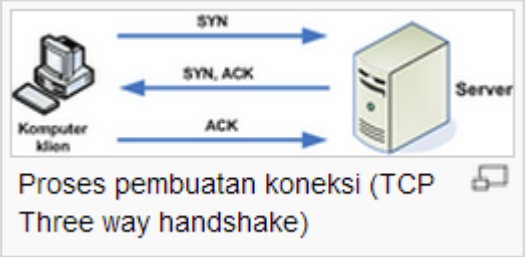
1.4 Transmission Control Protocol (TCP)

TCP adalah suatu protokol yang berada di lapisan transport (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (*connection-oriented*) dan dapat diandalkan (*reliable*). Proses pembuatan koneksi TCP disebut juga dengan "**Three-way Handshake**". Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor acknowledgement yang dikirimkan oleh kedua pihak dan saling bertukar ukuran TCP Window. Prosesnya dapat digambarkan sebagai berikut:

- *Host* pertama (yang ingin membuat koneksi) akan mengirimkan sebuah segmen TCP dengan flag SYN diaktifkan kepada *host* kedua (yang hendak diajak untuk berkomunikasi).

Copyright © 2003-2007 IlmuKomputer.Com

- *Host* kedua akan meresponsnya dengan mengirimkan segmen dengan *acknowledgment* dan juga SYN kepada *host* pertama.
- *Host* pertama selanjutnya akan mulai saling bertukar data dengan host kedua.



TCP menggunakan proses jabat tangan yang sama untuk mengakhiri koneksi yang dibuat. Hal ini menjamin dua *host* yang sedang terkoneksi tersebut telah menyelesaikan proses transmisi data dan semua data yang ditransmisikan telah diterima dengan baik. Itulah sebabnya, mengapa TCP disebut dengan koneksi yang *reliable*.

Langkah Kerja

- Dalam percobaan kali ini akan membahas tentang fungsi dari Telnet Server dan SSH Server, yang merupakan jenis software untuk meremote PC di sebuah jaringan komputer. Yang pertama adalah percobaan menggunakan Telnet Server, dengan ketentuan dalam percobaan ini adalah sebagai berikut :

- **Alat Dan Bahan :**

  2 Komputer Desktop atau Laptop

  1 kabel cross over

  Software Putty ->> di install pada kedua laptop yang terhubung

  Software FreeSSHd ->>di install pada kedua laptop yang terhubung

- **Pengalamat IP :**

  Dalam percobaan kali ini masing-masing Laptop di berikan alamart IP kelas C, dengan rincian sebagai berikut :

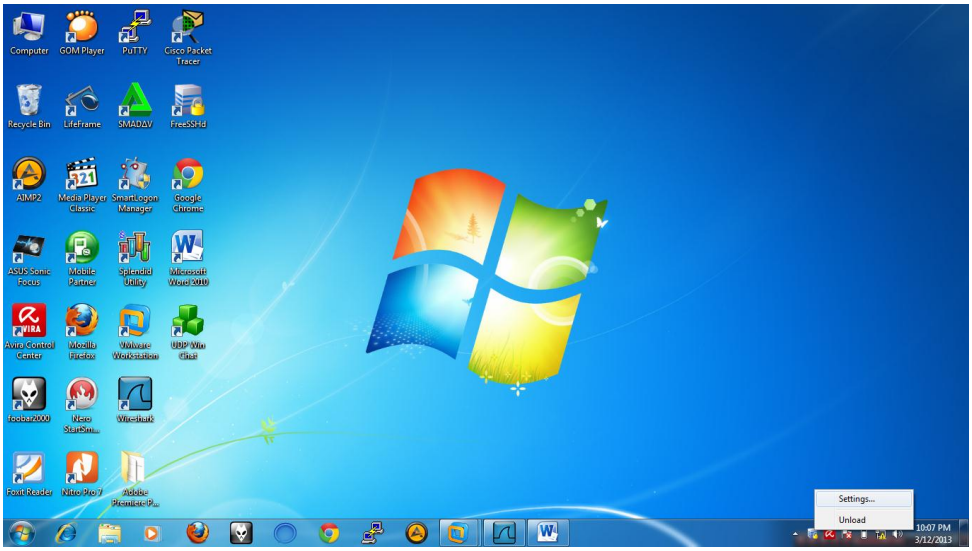
  Laptop pertama menggunakan alamat ->> 192.168.1.1

  Laptop kedua menggunakan alamat ->> 192.168.1.2

Copyright © 2003-2007 IlmuKomputer.Com

Selanjutnya akan dijelaskan tentang langkah-langkah beserta fungsinya dari penggunaan Telnet server di dalam sebuah jaringan :

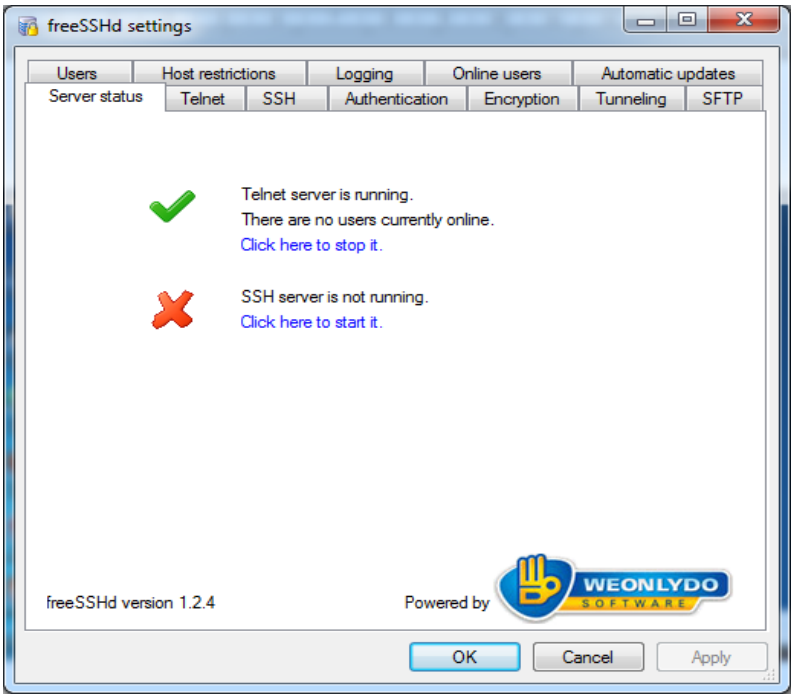
1. Pertama buka aplikasi software FreeSSHd yang telah terinstall, jika ada pesan error abaikan dan beralih pada icon yang muncul setelahnya, yang terletak pada bagian pojok kanan taskbar yang ada di dekstop. Klik kanan icon tersebut lalu pilih ***setting*** untuk masuk ke jendela FreeSSHd. Lihat gambar dibawah ini :



Gambar 1

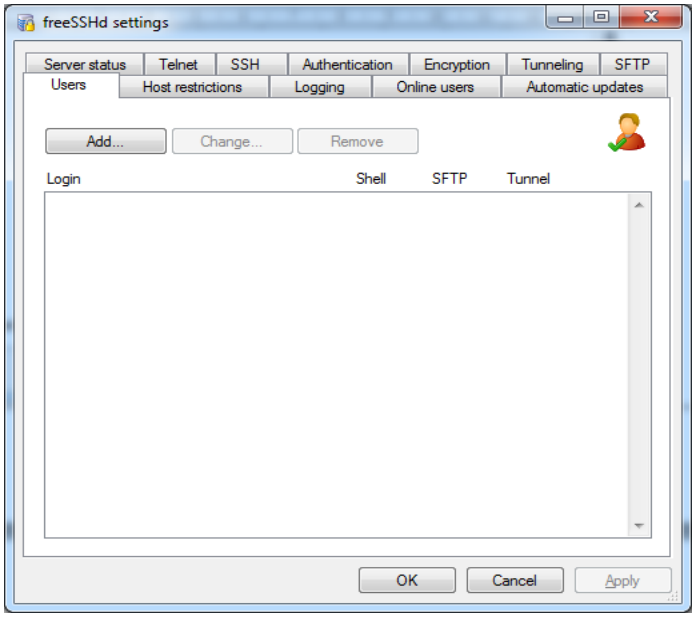
2. Kemudian setelah itu akan muncul jendela FreeSSHd seperti gambar di bawah ini. Klik pesan yang terdapat pada *Telnet server not running* agar menja di *running*. Jika icon sudah berubah menjadi centang, artinya Telnet server sudah bisa dioperasikan. Lihat gambar dibawah ini :

Copyright © 2003-2007 IlmuKomputer.Com



Gambar 2

3. Selanjutnya pilih Telnet yang ada di menu bar jendela FreeSSHd. Hala tersebut untuk membuat user baru yang akan coba di remote menggunakan Telnet client. Lihat gambar dibawah ini :

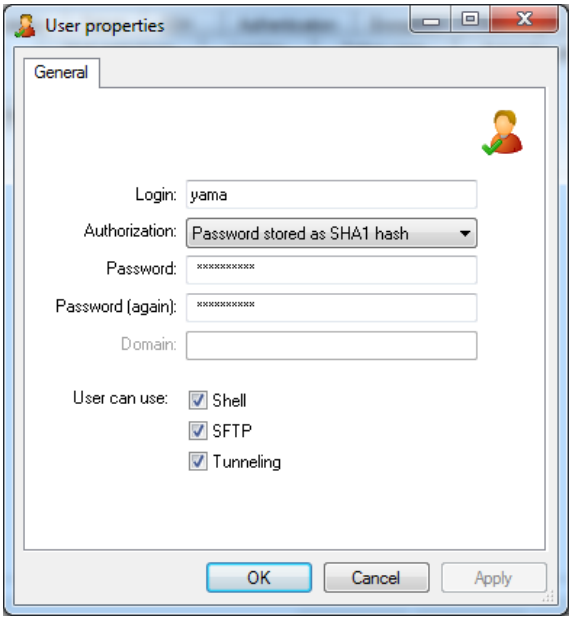


Gambar 3

4. Setelah masuk di jendela Telnet, klik Add untuk menambahkan user baru yang nantinya akan di remote oleh laptop yang terhubung dengan laptop ini. Di bagian login isikan nama user (bebas), untuk bagian *Authorization* pilih Password stored as SHA1 hash, kemudian isikan pula password (bebas).

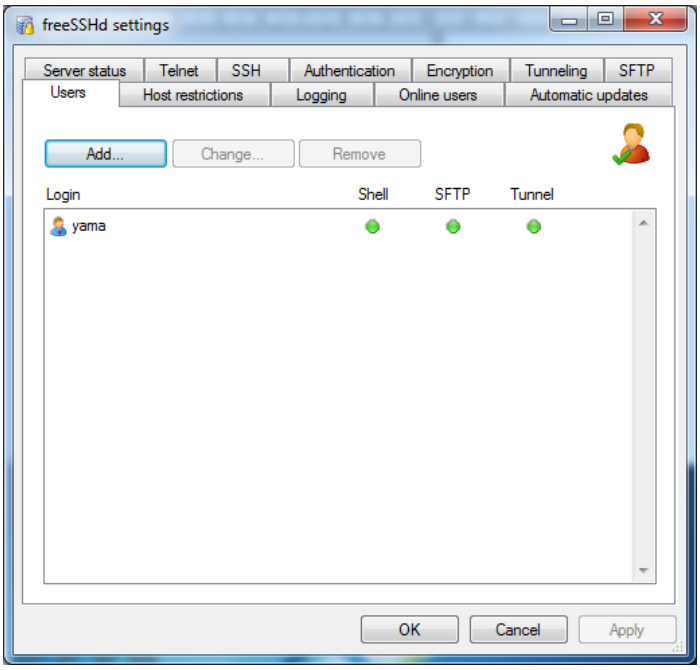
Copyright © 2003-2007 IlmuKomputer.Com

Selanjutnya check box Shell, SFTP, Tunneling yang ada di bagian User can Use. Kemudian Ok. Lihat gambar dibawah ini :



Gambar 4

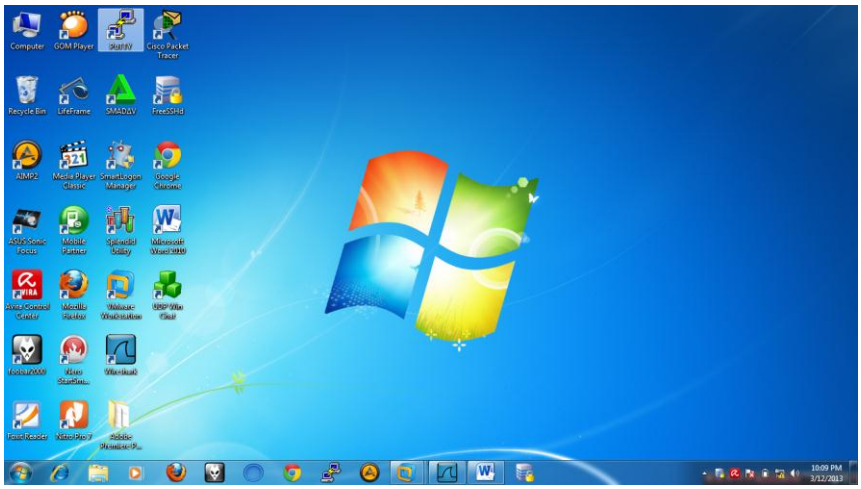
5. Selanjutnya setelah melakukan konfigurasi diatas akan tampil user baru seperti pada gambar dibawah ini :



Gambar 5

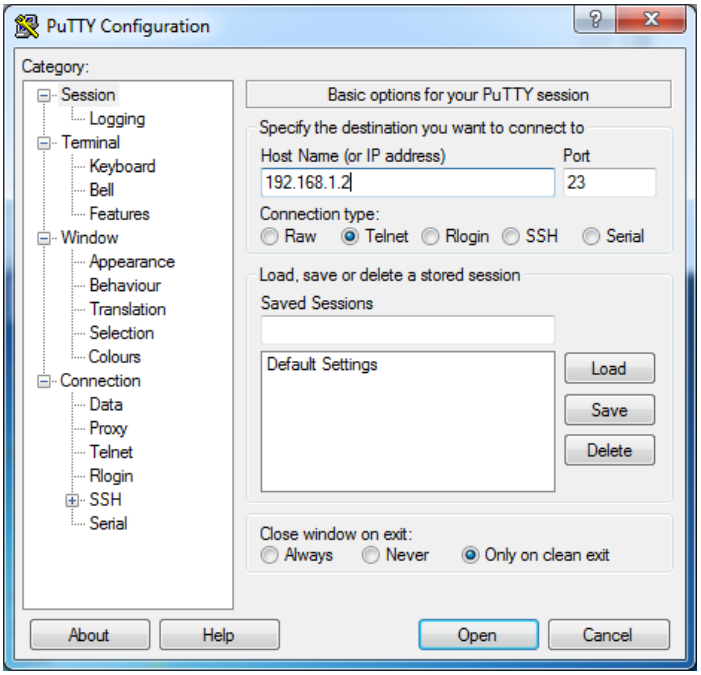
6. Lakukan langkah seperti di atas pada laptop 2 atau laptop satunya yang terhubung dengan laptop ini. Pada percobaan ini laptop satunya menggunakan user bernama **haidar** dan dengan password **rahasia.**

7. Selanjutnya buka aplikasi Putty yang telah di install. Kita akan mencoba meremote PC /laptop satunya, menggunakan Telnet Server yang telah di sediakan didalam aplikasi Putty. Lihat gambar di bawah ini :



Gambar 7

8. Kemudian setelah itu akan tampil jendela awal Putty seperti gambar di bawah ini :

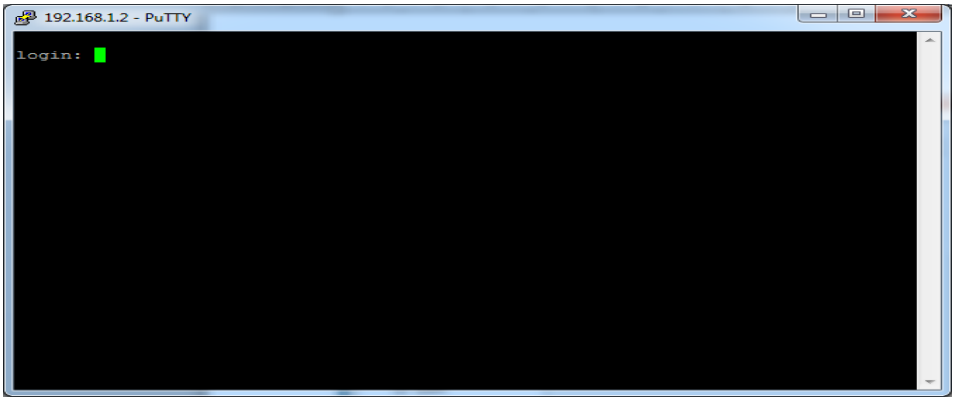


Gambar 8

9. Pada gambar di atas terdapat kolom Hostname, isikan dengan alamat tujuan laptop 2 atau laptop yang akan kita remote menggunakan Telnet server. Kita isikan dengan alamat 192.168.1.2 kemudian pilih conection type menjadi

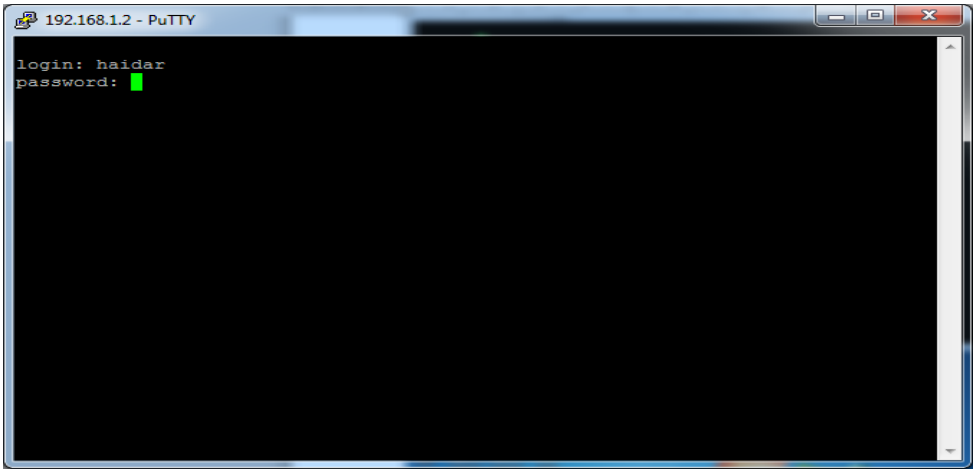
Copyright © 2003-2007 IlmuKomputer.Com

Telnet, karena kita akan meremote menggunakan Telnet Server. Selanjutnya Open, kemudian akan muncul jendela login seperti di bawah ini :



Gambar 9

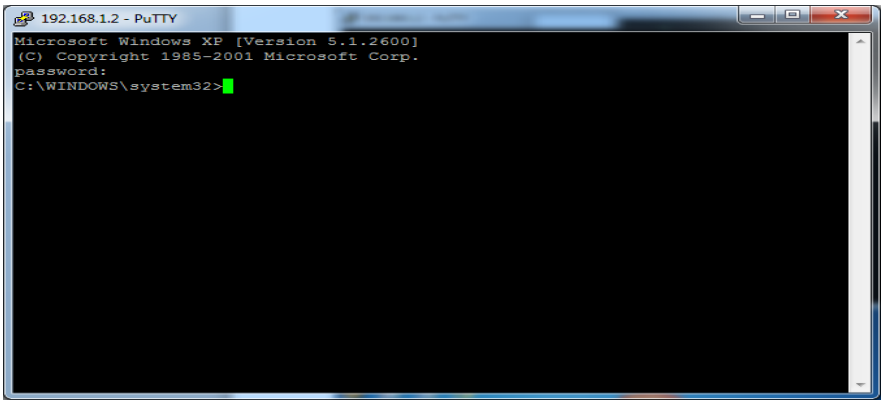
10. Isikan login dengan nama user laptop 2 yaitu haidar kemudian isikan pula passwordnya yaitu rahasia lalu Enter. Lihat gambar di bawah ini :



Gambar 10

11. Selanjutnya jika benar dan berhasil maka kita bisa login sebagai user haidar yang dimiliki oleh laptop 2 yang terhubung dengan laptop ini. Sehingga memungkinkan kita untuk mengendalikan, memberi perintah, menjalankan perintah, merubah konfigurasi, meremote komputer lain (server) melalui komputer di depan meja kita sendiri (client). Lihat gambar login sebagai haidar di bawah ini :

Copyright © 2003-2007 IlmuKomputer.Com

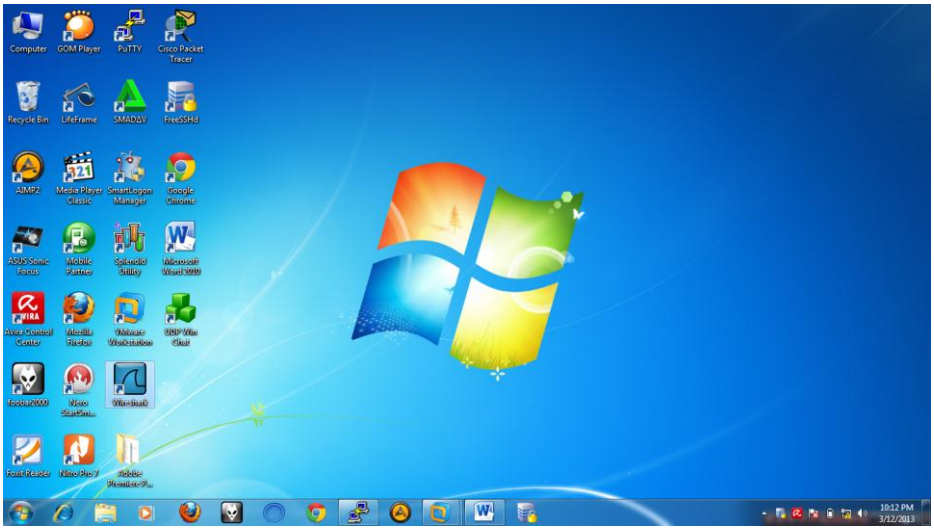


Gambar 11

Proses dan langkah-langkah meremote PC menggunakan Telnet Server di atas telah selesai, sekarang kita mencoba memonitoring kegiatan yang terjadi pada saat kita meremote PC tadi menggunakan aplikasi Wireshark. Aplikasi wireshark memiliki fungsi sebagai alat monitoring jaringan. Sedangkan monitoring disini dapat berupa informasi-informasi penting dari user seperti password email atau account lain yang sedang diakses dengan menganalisa packet-packet yang bisa kita tangkap dengan software ini.

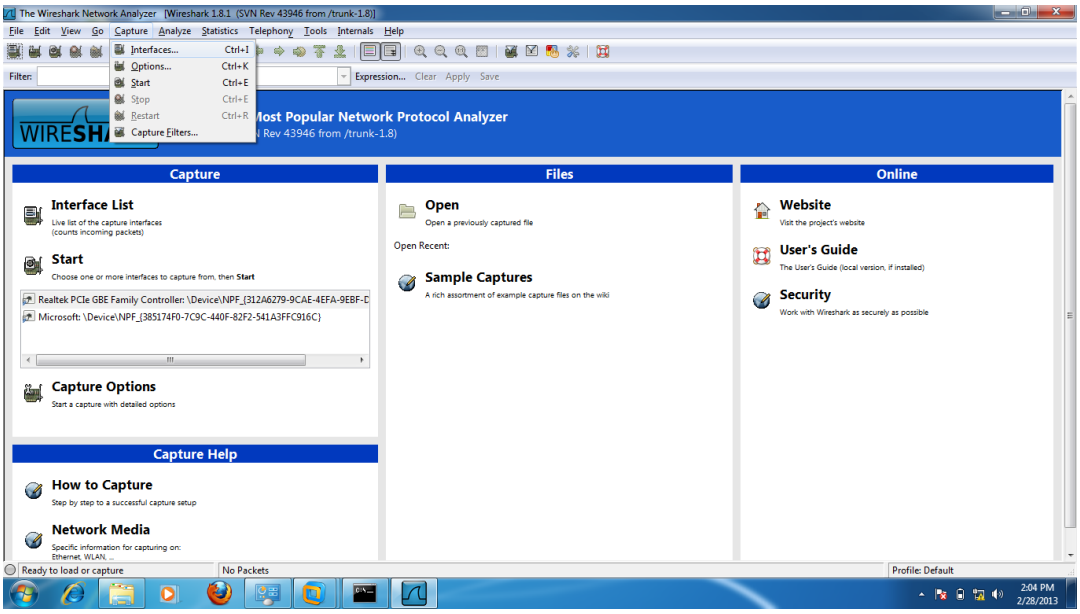
Langkah-langkahnya adalah sebagai berikut :

1. Buka aplikasi wireshark yang telah terinstall, lihat gambar dibawah ini :

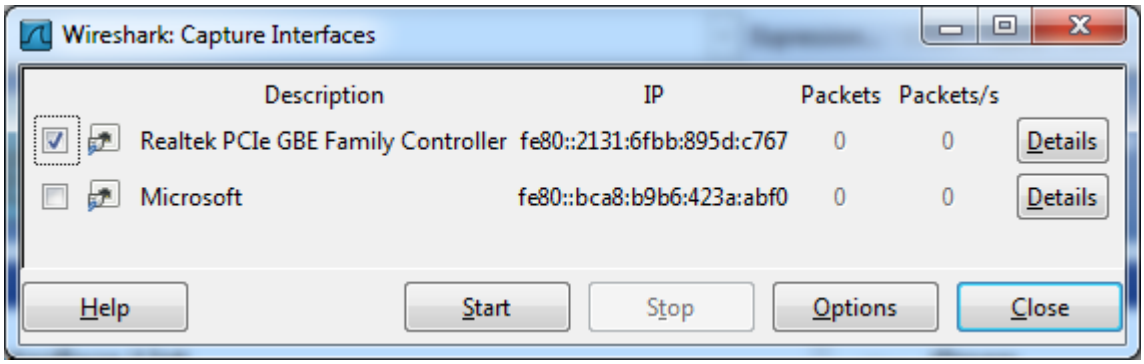


2. Selanjutnya akan tampil gambar jendela awal dari program wireshark. Lihat gambar dibawah ini :

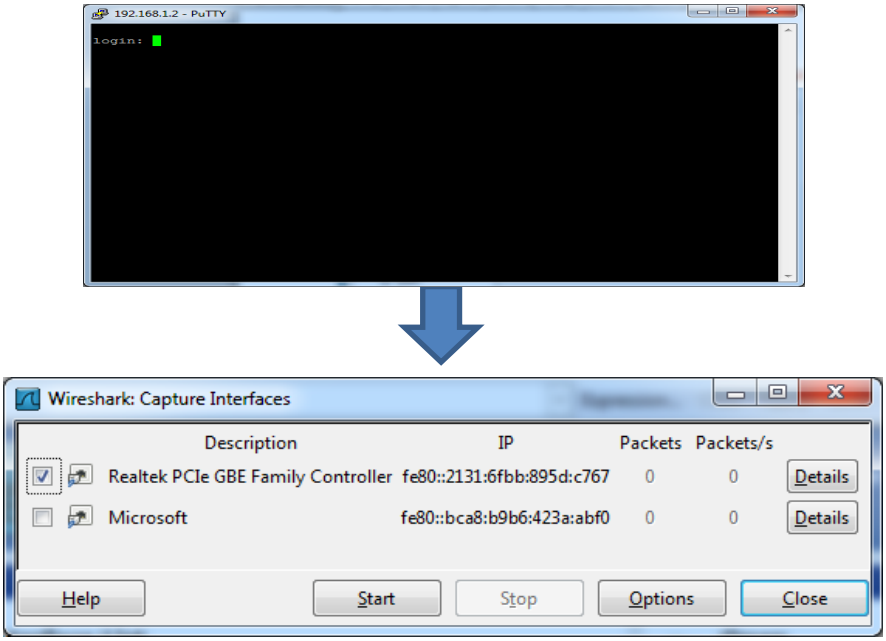
Copyright © 2003-2007 IlmuKomputer.Com



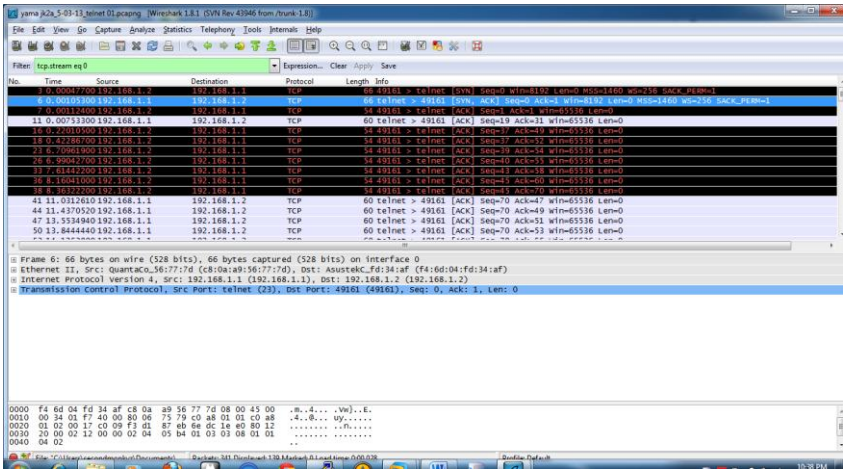
3. Pilih Capture yang terdapat di menu bar jendela wireshark kemudian pilih interfaces. Hal tersebut dimaksudkan untuk memulai proses monitoring yang akan di lakukan pada laptop ini atau laptop 1 terhadap laptop 2.
4. Setelah memilih interface yang terdapat di menu capture maka akan muncul jendela Capture Interfaces. Dalam jendela ini kita disuguhkan dengan beberapa pilihan mana kartu jaringan atau Network Interfaces yang akan kita gunakan. Kita pilih ***Realtek PCIe GBE…*** berhubung kita menggunakan network interface tersebut untuk melakukan hubungan kepada laptop 2. Lihat gambar dibawah ini :



5. Kemudian selanjutnya kita klik Start, namun lngkah pengeklikan Start dilakukan ketika kita masuk di halaman awal login Telnet server. Berikut gambaran langkah-langkahnya :

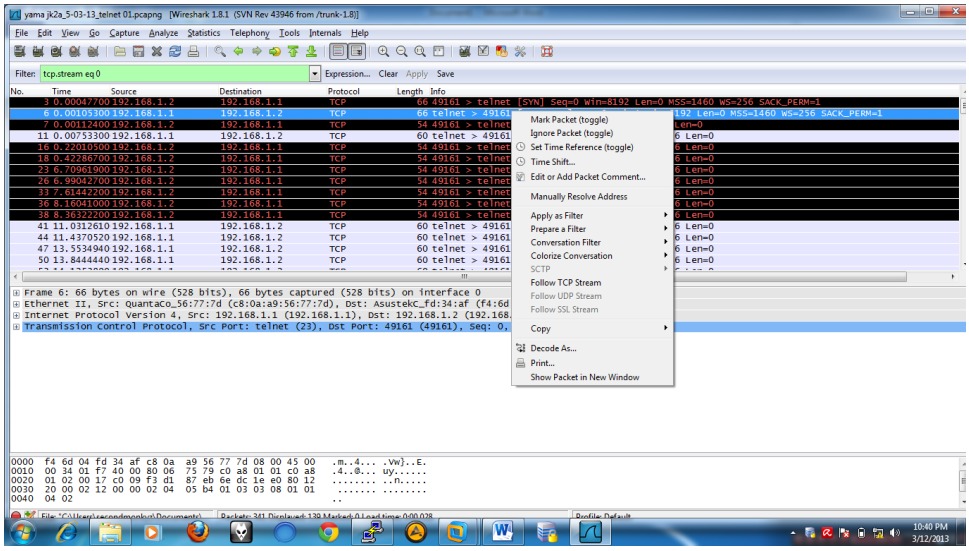


6. Selanjutnya setelah kita klik Start, maka akan tampil jendela di bawah ini yang berisi packet-packet dan aliran data yang berjalan dalam lalu lintas jaringan yang terhubung antara kedua laptop. Dalam proses yang tertampil di wireshark akan terlihat proses ***3 way handshake*** yang dilakukan protokol TCP pada saat melakukan koneksi atau komunikasi jaringan. lihat gambar dibawah ini :

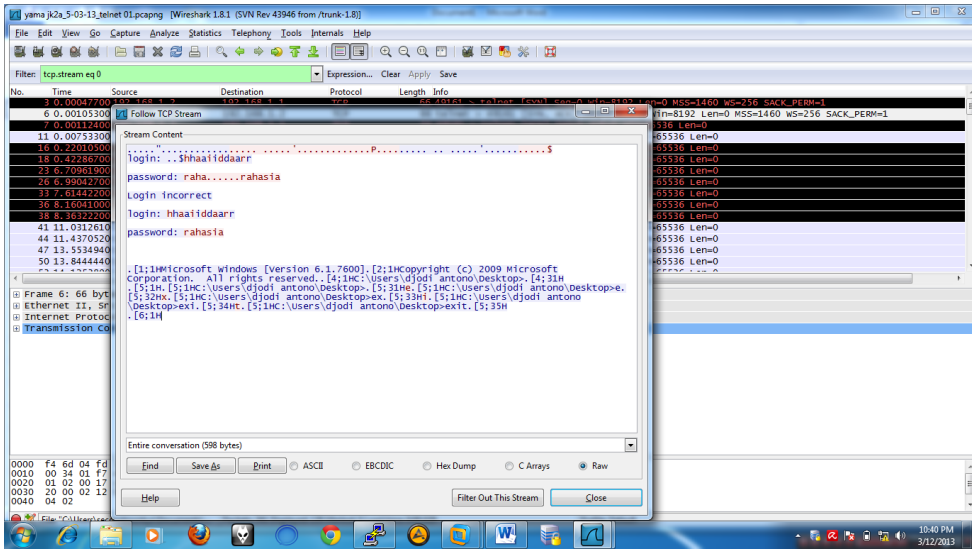


7. Selanjutnya klik kanan pada bagian packet yang menunjukan destinasi ke alamat 192.168.1.2 dan mempunyai pesan "***telnet>..>[SYN,ACK]….***" . Pilih *Follow TCP Stream* untuk melihat hasil informasi yang dapat di peroleh dari penyadapan yang di lakukan di lalu lintas jaringan menggunakan wireshark. Lihat gambar di bawah ini :

Copyright © 2003-2007 IlmuKomputer.Com

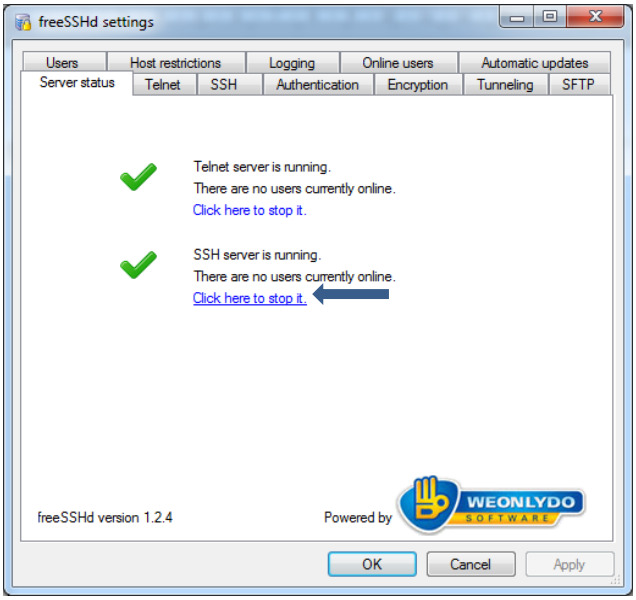


8. Setelah diklik *Follow TCP Stream*, maka akan tertampil jendela di bawah ini yang menampilkan informasi nama user serta password yang kita remote menggunakan telnet server. Lihat gambar dibawah ini :

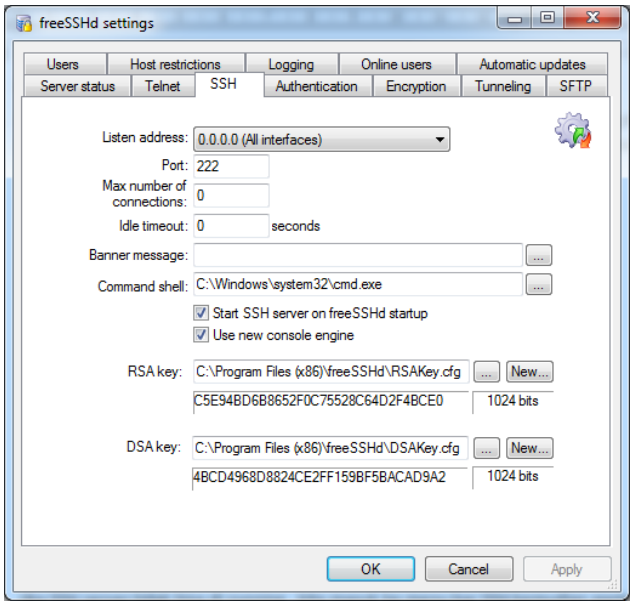


2.2 Untuk percobaan selanjutnya adalah Remote PC/ Laptop menggunakan SSH Server. Berikut langkah-langkahnya :

1. Pertama buka aplikasi FreeSSHd, kemudian jadikan SSH server menjadi running dengan mengeklik click here to running yang ada pada kolom SSH. **(Untuk user masih memakai yang seperti pada percobaan telnet server)**.Lihat gambar di bawah ini :

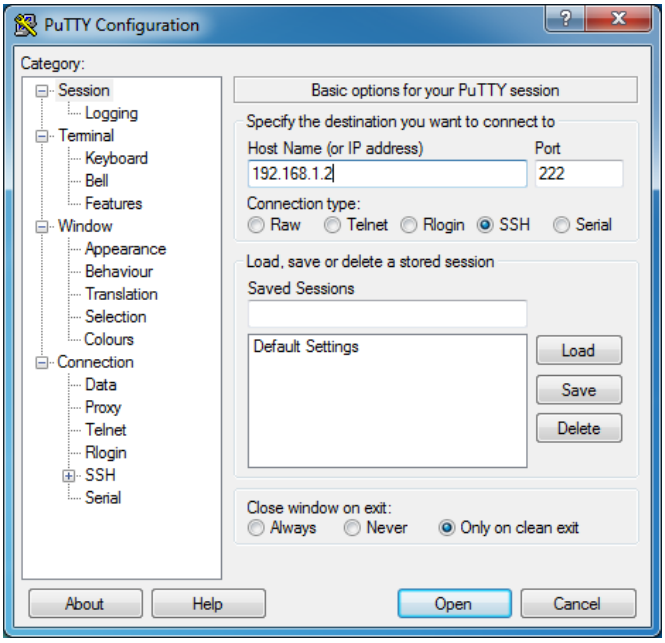


2. Jika SSH server tidak bisa di running , kita masuk ke menu bar SSH kemudian ganti port default SSH menjadi 222. Setelah itu cobalah langkah seperti diatas untuk merunningkan SSH server. Lihat gambar di bawah ini :

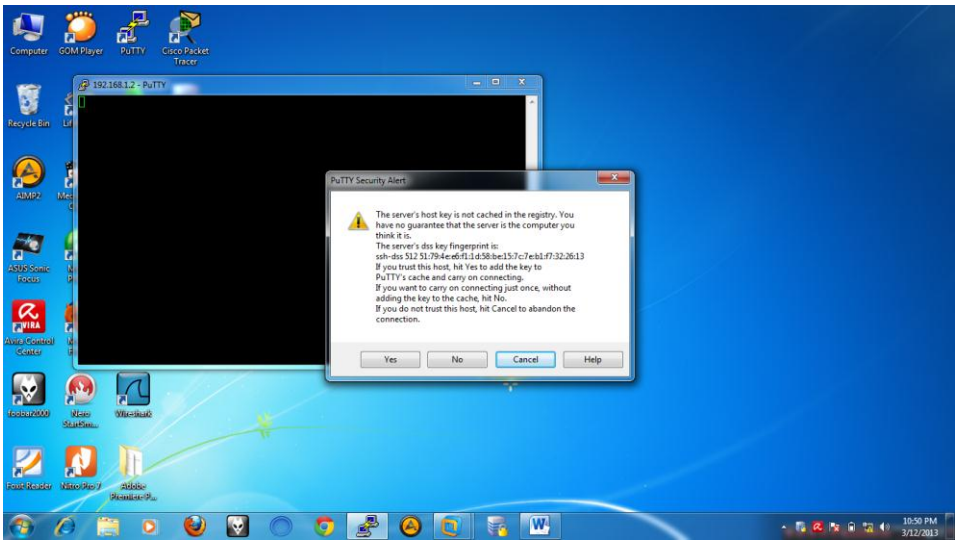


3. Langkah selanjutnya masuk ke aplikasi Putty untuk menjalankan Remote PC menggunakan fasilitas SSH server yang ada didalamnya. Isikan host name dengan alamat tujuan yaitu 192.168.1.2 kemudian ganti port default SSH yang awalnya 22 menjadi 222. Sebab pada saat settingan port SSH di aplikasi FreeSSHd port default di rubah agar dapat menjalankan atau merunning fungsi

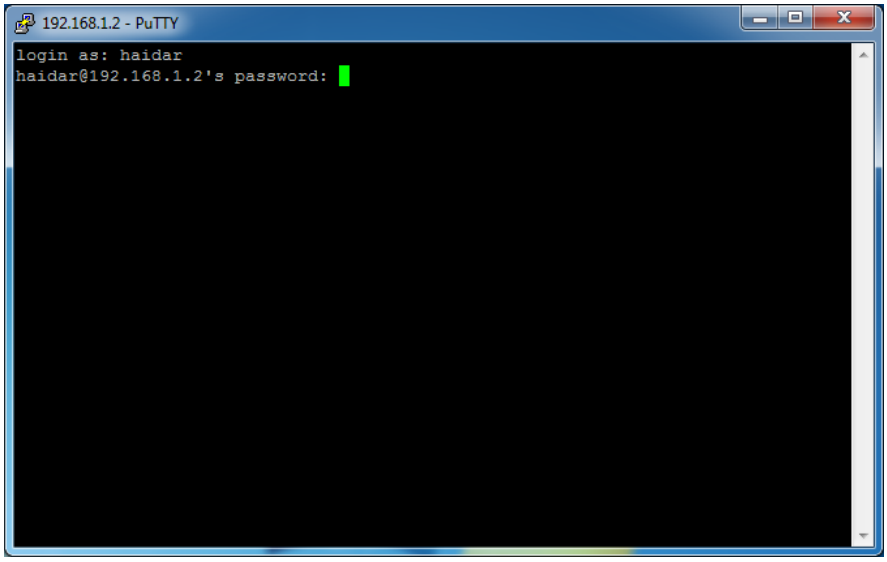
dari SSH Server itu sendiri . Setelah itu klik open untuk melanjutkan. lihat gambar di bawah ini :



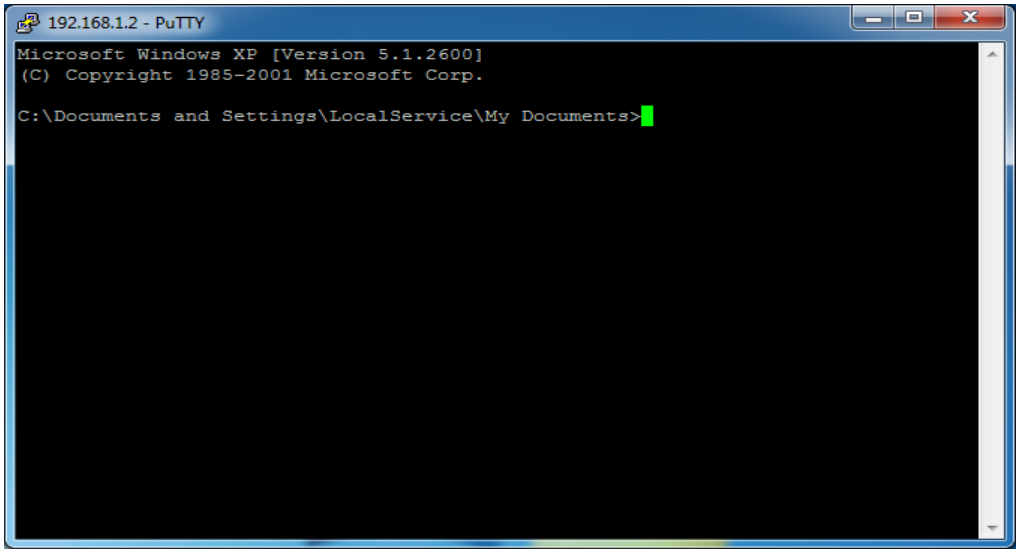
4. Kemudian selanjutnya akan tampil kotak dialog peringatan sebelum masuk ke jendela login, seperti gambar di bawah ini. Kita pilih opsi yes untuk melanjutkan. Lihat gambar :



5. Setelah itu kita akan masuk ke jendela login, isikan nama user dan password dari laptop 2 atau yang terhubung dengan laptop 1 (laptop ini). Lihat gambar :



6. Selanjutnya jika benar dan berhasil kita akan login ke user haidar atau user dari laptop 2 atau user yang dituju untuk di remote menggunakan SSH server oleh kita. Seperti hal nya telnet dalam SSH server memungkinkan kita untuk mengendalikan, memberi perintah, menjalankan perintah, merubah konfigurasi, meremote komputer lain (server) melalui komputer di depan meja kita sendiri (client). Lihat gambar dibawah ini :



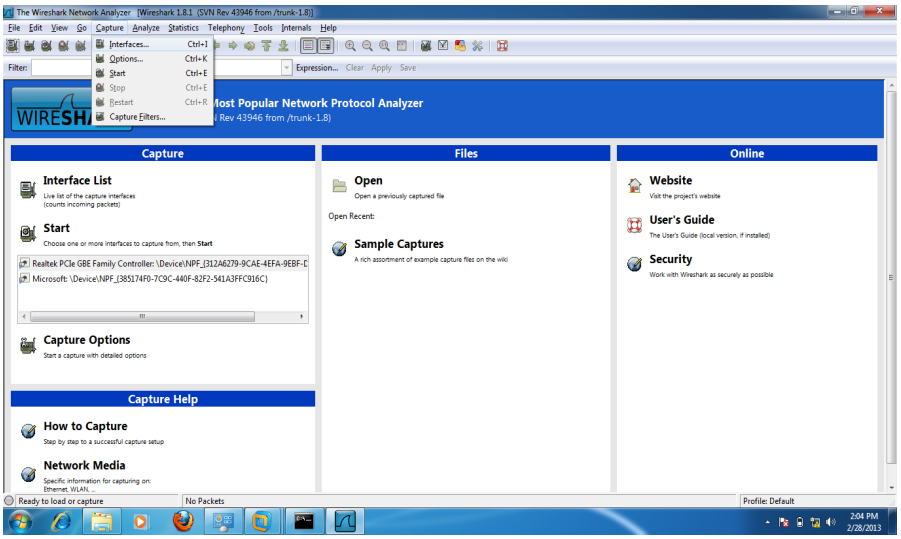
Proses dan langkah-langkah meremote PC menggunakan SSH Server di atas telah selesai, sekarang kita mencoba memonitoring kegiatan yang terjadi pada saat kita meremote PC tadi menggunakan aplikasi Wireshark. Aplikasi wireshark memiliki fungsi sebagai alat monitoring jaringan. Sedangkan monitoring disini dapat berupa informasi-informasi penting dari user seperti password email

Copyright © 2003-2007 IlmuKomputer.Com

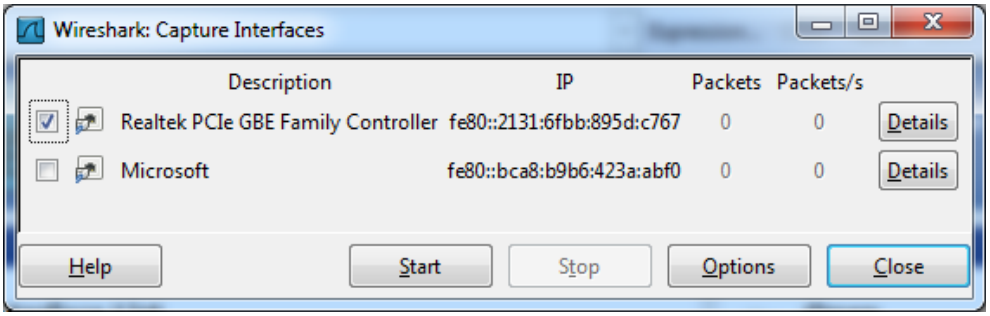
atau account lain yang sedang diakses dengan menganalisa packet-packet yang bisa kita tangkap dengan software ini.

Langkah-langkahnya adalah sebagai berikut :

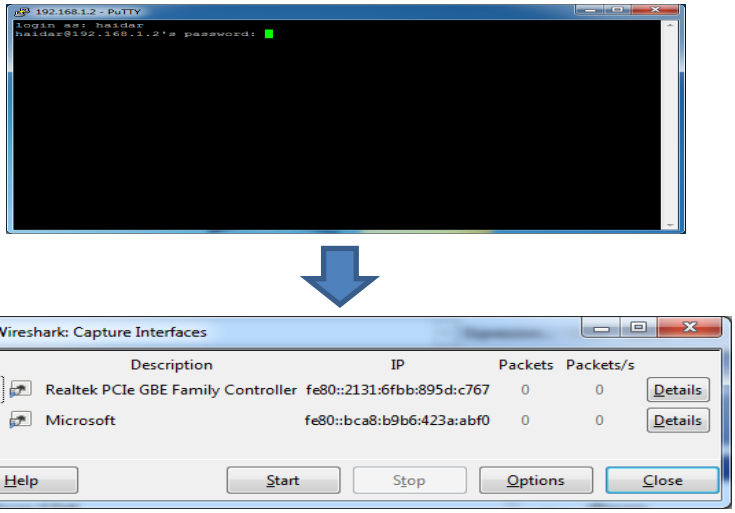
1. Buka aplikasi wireshark yang telah terinstall, Selanjutnya akan tampil gambar jendela awal dari program wireshark. Lihat gambardi bawah :



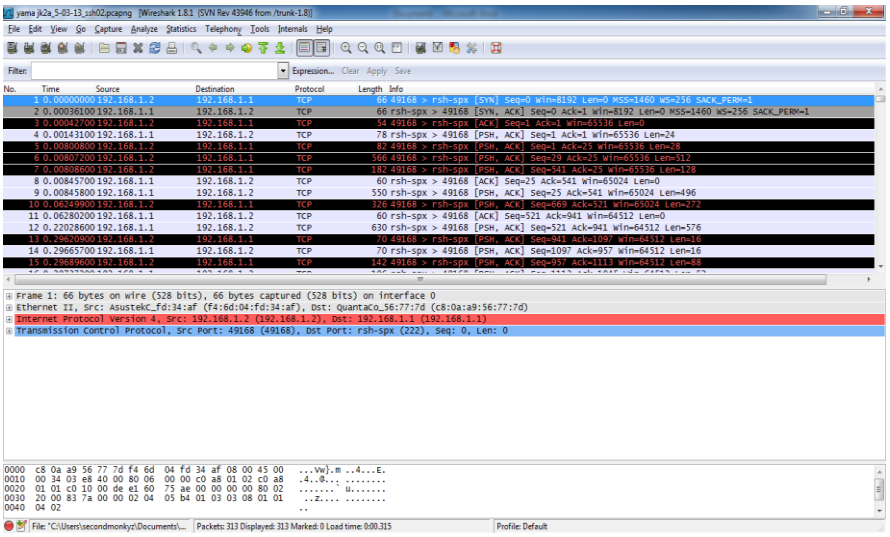
2. Pilih Capture yang terdapat di menu bar jendela wireshark kemudian pilih interfaces. Hal tersebut dimaksudkan untuk memulai proses monitoring yang akan di lakukan pada laptop ini atau laptop 1 terhadap laptop 2.
3. Setelah memilih interface yang terdapat di menu capture maka akan muncul jendela Capture Interfaces. Dalam jendela ini kita disuguhkan dengan beberapa pilihan mana kartu jaringan atau Network Interfaces yang akan kita gunakan. Kita pilih ***Realtek PCIe GBE…*** berhubung kita menggunakan network interface tersebut untuk melakukan hubungan kepada laptop 2. Lihat gambar dibawah ini :



4. Kemudian selanjutnya kita klik Start, namun lngkah pengeklikan Start dilakukan ketika kita masuk di halaman awal login Telnet server. Berikut gambaran langkah-langkahnya :

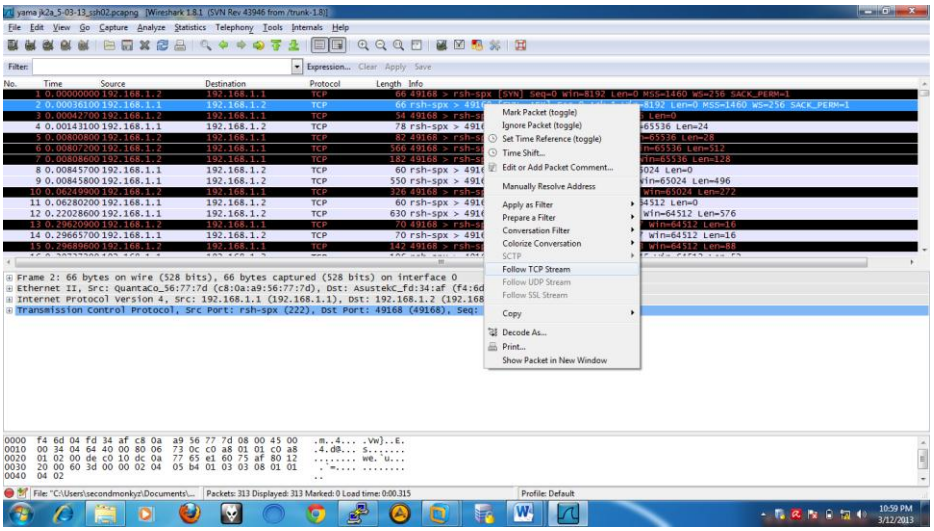


5. Selanjutnya setelah kita klik Start, maka akan tampil jendela di bawah ini yang berisi packet-packet dan aliran data yang berjalan dalam lalu lintas jaringan yang terhubung antara kedua laptop. Dalam proses yang tertampil di wireshark akan terlihat proses ***3 way handshake*** yang dilakukan protokol TCP pada saat melakukan koneksi atau komunikasi jaringan. lihat gambar dibawah ini :

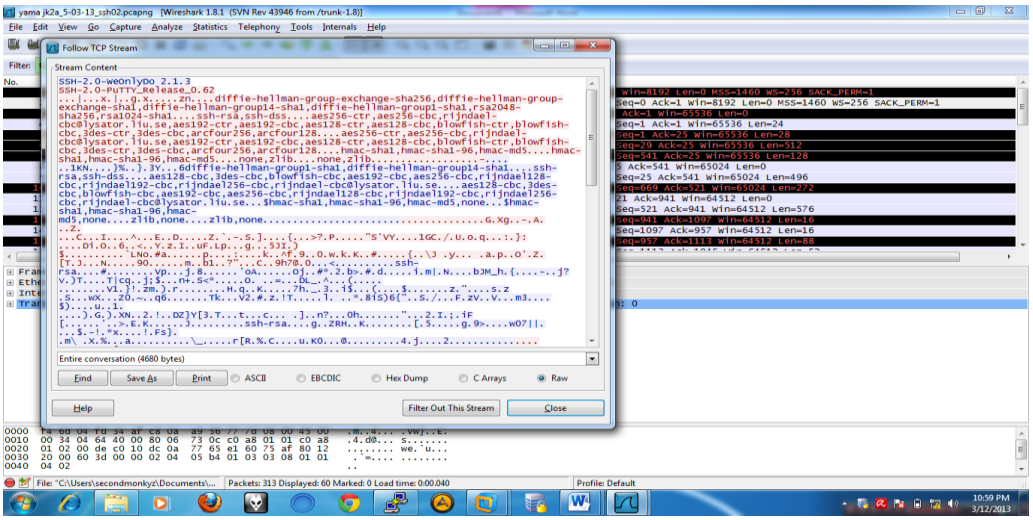


6. Selanjutnya klik kanan->> Follow TCP Stream pada bagian packet yang menunjukan destinasi ke alamat 192.168.1.2 dan mempunyai pesan "***telnet>..>[SYN,ACK]....***" . Pilih *Follow TCP Stream* untuk melihat hasil informasi yang dapat di peroleh dari penyadapan yang di lakukan di lalu lintas jaringan menggunakan wireshark. Lihat gambar di bawah ini :

Copyright © 2003-2007 IlmuKomputer.Com



7. Setelah diklik *Follow TCP Stream*, maka akan tertampil jendela di bawah ini yang menampilkan informasi nama user serta password yang kita remote menggunakan SSH Server. Namun data yang kita peroleh masih dalam kondisi terenkripsi tidak seperti halnya ketika kita memonitoring telnet server, yang semua informasinya dapat langsung terlihat. Lihat gambar dibawah ini :



8. Selesai …

Biografi Penulis

Nama Penulis : Yama Fresdian Dwi Saputro lahir 11 September 1993. Sedang menyelesaikan studi di POLITEKNIK NEGERI SEMARANG Jurusan Elektro Progdi D4 Telekomunikasi.

Copyright © 2003-2007 IlmuKomputer.Com