Pengenalan dan Instalasi Wireshark

Annisa Cahyaningtyas
annisacahyaningtyas@gmail.com
http://annisacahyaningtyas.blogspot.com

Wireshark merupakan sebuah software/alat penganalisa jaringan yang paling dikenal. Alat ini sangat berguna dalam menyediakan jaringan dan protokol yang ada pada protokol bagian atas yang memberi informasi tentang data yang tertangkap pada jaringan. Perangkat ini juga digunakan untuk pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Awalnya bernama Ethereal, pada Mei 2006 proyek ini berganti nama menjadi Wireshark karena masalah merek dagang.

Wireshark sering digunakan karena interfacenya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data/informasi yang berseliweran dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Oleh karena itu, *tool* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password* email atau *account* lain) dengan menangkap paket-paket yang lalu-lalang di dalam jaringan dan menganalisanya. Selain itu juga bisa mem-filter protokol lain selain ICMP, seperti HTTP dan lainnya. Selama kita bisa mendapatkan paket langsung dari jaringan, dengan tools seperti Wireshark, maka kita juga bisa memanfaatkan Wireshark untuk ‘menyadap’ pembicaraan Voice over IP.

Tool ini tidak mengenal interface modem dan hanya dapat bekerja dalam jaringan melalui LAN/Ethernet Card yang ada di PC. Wireshark bersifat *open source* atau bisa didapat dengan gratis (tidak berbayar) tanpa perlu lisensi apapun. Wireshark tersedia untuk komputer yang berbasis Windows dan juga Mac OS. Untuk mendapatkan Wireshark, dapat didownload dari web Wireshark langsung,yaitu http://www.wireshark.org/download.html

1. PENGGUNAAN WIRESHARK

Wireshark biasa digunakan untuk:

a. Admin sebuah jaringan untuk troubleshooting masalah-masalah di jaringan.
b. Teknisi keamanan jaringan (*network security engineer*) menggunakannya untuk memeriksa keamanan jaringan.
c. Pengembang sofware bisa menggunakannya untuk men-debug implementasi protokol jaringan dalam software mereka.
d. Mempelajari protokol jaringan (internal) secara detail.

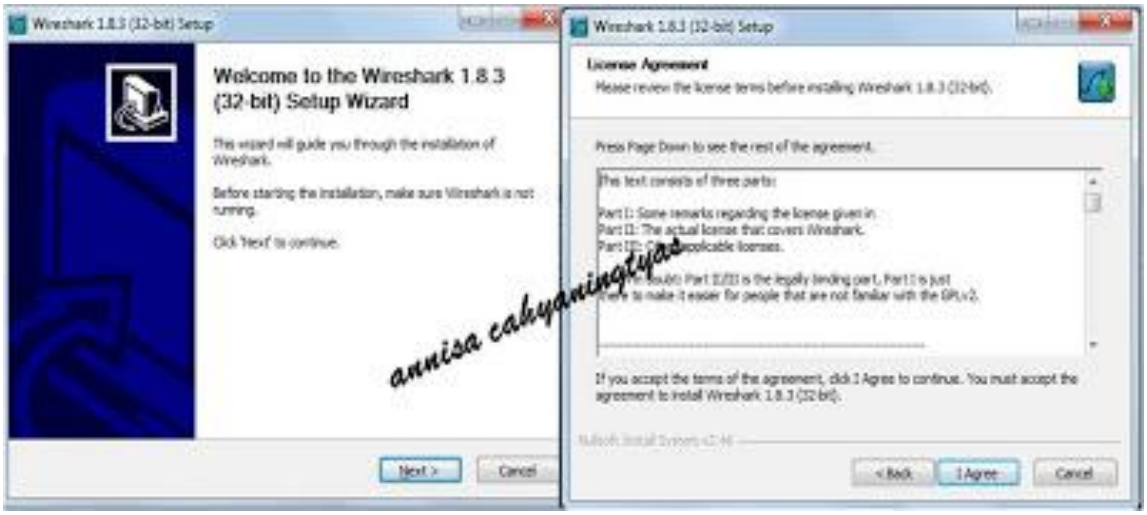
Berikut adalah beberapa fitur dan kelebihan wireshark:

a. Tersedia untuk sistem operasi Linux dan Windows.
b. Menangkap (*capture*) paket data secara langsung dari sebuah network interface.
c. Mampu menampilkan juga membuka dan menutup paket dengan informasi protokol secara detail mengenai hasil *capture* tersebut.
d. Dapat import dan export paket data atau hasil *capture* dari atau ke komputer lain.
e. Perncarian paket dengan berbagai macam kriteria filter.
f. Pemberian warna paket data yang ditampilkan berdasarkan filternya
g. Bisa membuat berbagai macam gambar tampilan statistika.

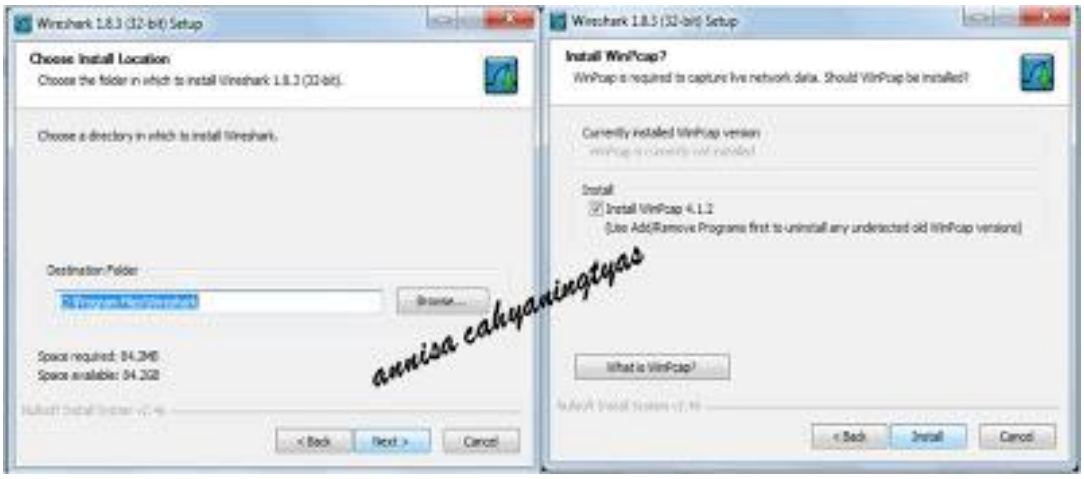
2. INSTALASI WIRESHARK

Cara instalasi Wireshark sangat mudah, berikut langkah-langkahnya:

a. Membuka **Wireshark Installer** yang telah didownload, kemudian double klik
b. Lalu akan muncul jendela **Wireshark Setup**, lalu klik **Next**.
c. Setelah itu muncul **License Agreement.** Pilih **I Agree** untuk menyetujui lisensi tersebut.



d. Kemudian akan ada pilihan komponen, pilihan fungsi tambahan, serta pilihan lokasi instalasi. Klik Next pada ketiga pilihan tersebut.



e. Lalu, akan ada pilihan dan diminta untuk menginstal **WinPcap**. WinPcap diperlukan untuk menangkap (meng-*capture*) data jaringan secara langsung.

f. Maka proses instalasi akan berjalan, tunggu hingga proses istalasi selesai, lalu pilih **Next**.

g. Setelah proses instalasi selesai, pilih **Finish**, kemudian jalankan program Wireshark tersebut.

Untuk menggunakan *tool* ini pun cukup mudah. Kita cukup memasukkan perintah untuk mendapatkan informasi yang ingin kita *capture* (yang ingin diperoleh) dari jaringan kita. Masuk ke menu Capture – Option – Start.

Biografi Penulis

Annisa Cahyaningtyas. Saat ini sedang menjalani studi D4 di Politeknik Negeri Semarang, Jurusan Teknik Elektro, Program Studi Teknik Telekomunikasi.