Pengenalan dan Dasar Penggunaan Wireshark

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

Wireshark merupakan Network Protocol Analyzer, juga termasuk salat satu network analysis tool atau packet sniffer. Wireshark memungkinkan pengguna mengamati data dari jaringan yang sedang beroperasi atau dari data yang ada di disk, dan langsung melihat dan mensortir data yang tertangkap, mulai dari informasi singkat dan detail bagi masing-masing paket termasuk full header dan porsi data, dapat diperoleh. Wireshark memiliki beberapa fitur termasuk display filter language yang banyak dan kemampuan me-reka ulang sebuah aliran pada sesi TCP.

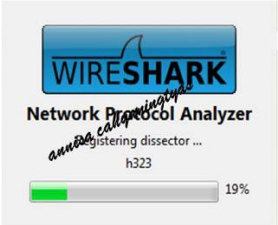
Paket sniffer sendiri diartikan sebuah tool yang berkemampuan menahan dan melakukan pencatatan terhadap traffic data dalam jaringan. Selama terjadi aliran data dalam jaringgan, packet sniffer dapat menangkap protocol data unit (PDU), melakukan decoding serta analisis terhadap isi paket. Wireshark sebagai salah satu packet sniffer yang diprogram demikian agar mengenali berbagai macam prottokol jaringan. Wireshark juga mampu menampilkan hasil enkapsulasi dan field yang ada di dalam PDU.

CARA MENJALANKAN WIRESHARK

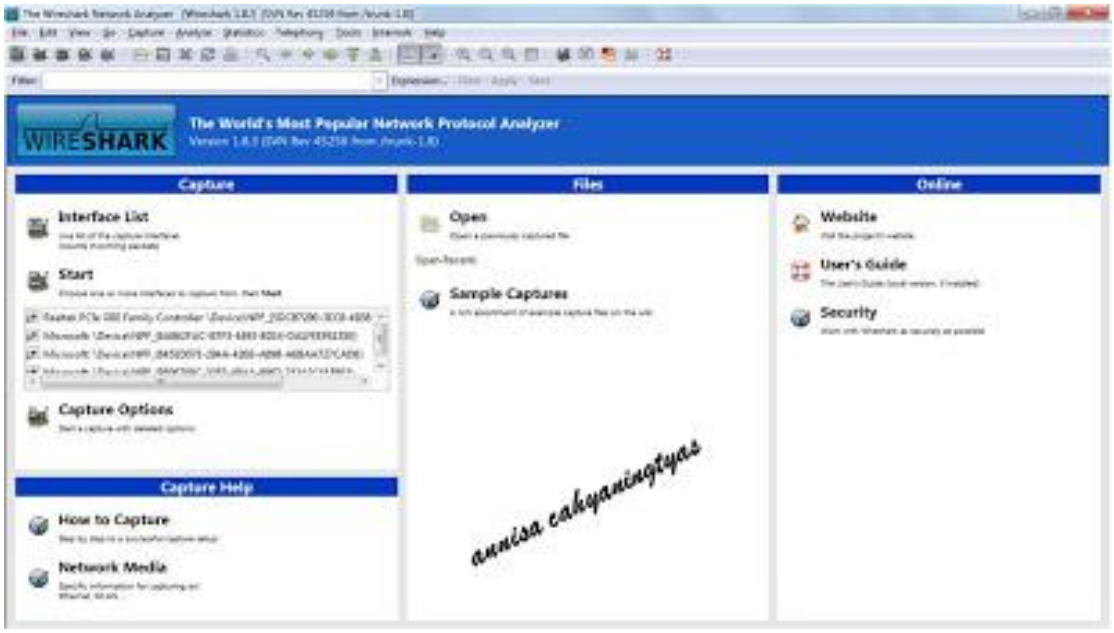
Setelah memahami cara instalasi Wireshark, berikut cara menjalankan program ini.

a. CARA MENJALANKAN WIRESHARK : Menjalankan wireshark (awal)

- Pertama, untuk menjalankan program **Wireshark**, double-click melalui shortcut-nya di Desktop. Maka, muncullah Splash Screen Wireshark yang sedang me-load komponen-komponen yang diperlukan



Berikut tampilan halaman awal Wireshark saat pertama kali dibuka sebelum melakukan proses 'capture'

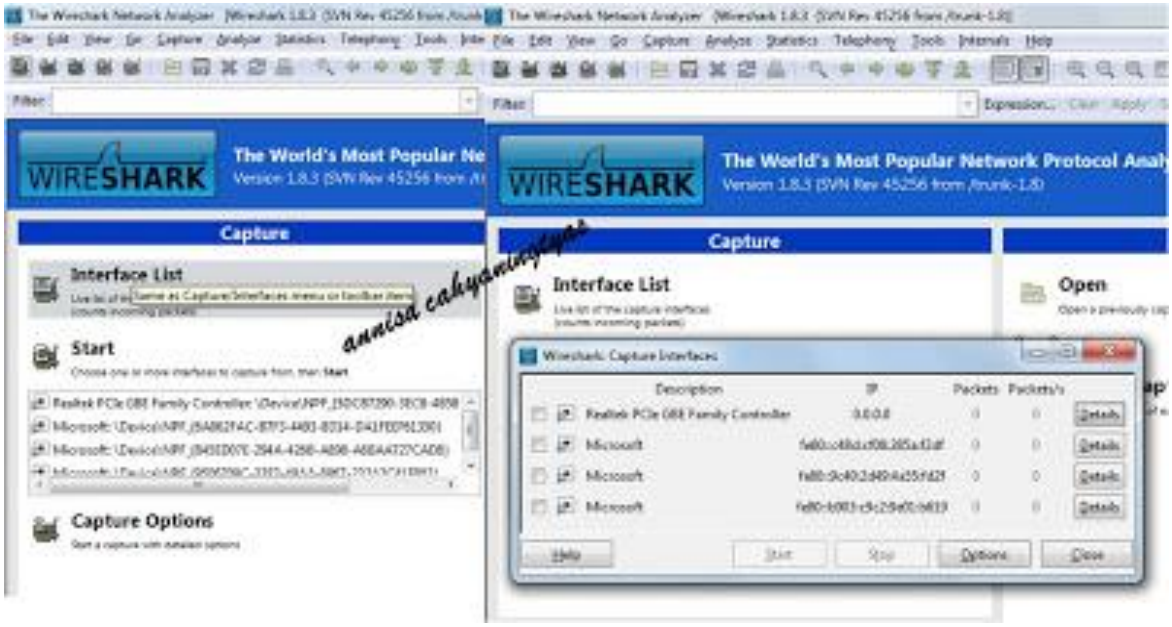


b. CARA MENJALANKAN WIRESHARK : Meng-capture paket dengan wireshark (awal)

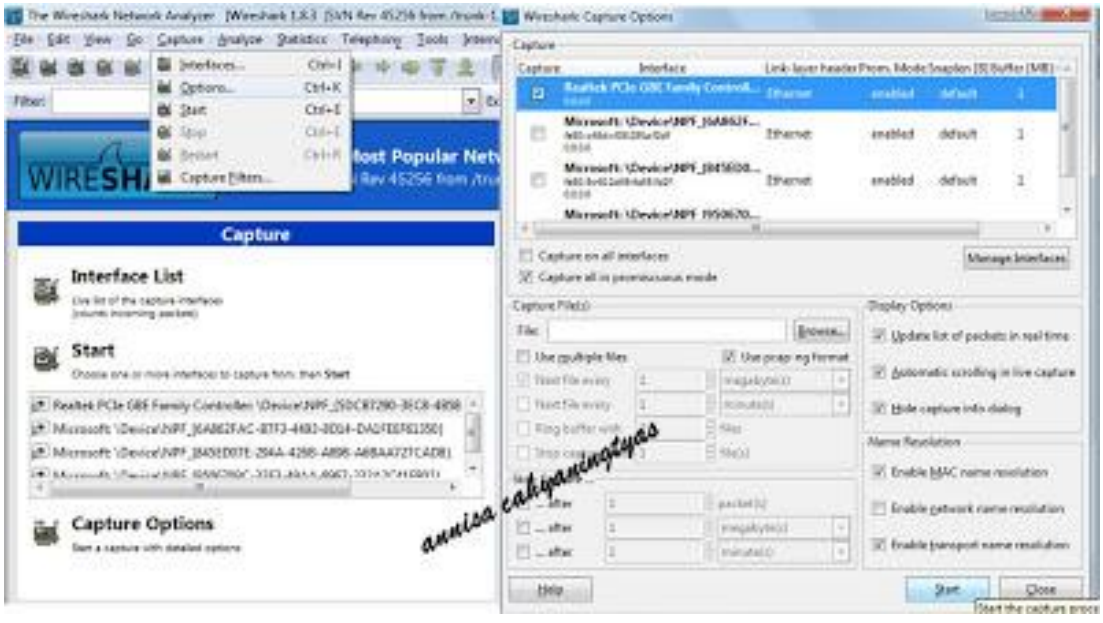
Setelah mengaktifkan dan menjalankan Wireshark, langkah berikutnya melakukan 'capture' paket data melalui Wireshark. Berikut langkah-langkahnya:

- Cara pertama: Meng-klik "**Interface List**" untuk mengaktifkannya, kemudian muncul dialog box **Wireshark Capture Interfaces** yang menampilkan semua interface-nya dan setelah memilih interface mana yang akan dipantau atau di-capture, klik saja **Start**. Maka setelah itu akan memunculkan lalu lintas jaringan komputer beserta protokol dan keterangan lainnya.

Copyright © 2003-2007 IlmuKomputer.Com



- Cara kedua: Memilih **Capture>Interfaces** untuk mengaktifkannya, kemudian muncul dialog box **Wireshark Capture Option** yang menampilkan semua interface-nya beserta pilihan-pilihan dalam 'capture' dan setelah itu dapat memilih interface mana yang akan dipantau atau di-capture, klik saja **Start**. Maka setelah itu akan memunculkan lalu lintas jaringan komputer beserta protokol dan keterangan lainnya



Setelah memilih interface dan Start, maka jaringan komputer sudah siap dipantau kemudian di-capture yang akan menampilkan bentuk traffic yang warna-warni dimana terdapat keterangan '**Time** (menampilkan waktu saat paket tersebut tertangkap); **Source** (menampilkan IP Source dari

Copyright © 2003-2007 IlmuKomputer.Com

paket tersebut); **Destination** (menampilkan IP Destination dari paket tersebut); **Protocol** (menampilkan protokol yang dipakai paket data tersebut); **Info** (menampilkan informasi dettail paket tersebut)'.

Serta ada pula keterangan lainnya yang terdapat pada tampilan utama saat Wireshark bekerja meng-capture paket data jaringan, seperti '**Menu; Display Filter; Daftar Paket; Detail Paket; Detail Heksa'**.

a. **Menu**: tampilan ini dapat bernavigasi antar menu-menu yang tersedia di Wireshark
b. **Display filter**: adalah sebuah kolom, di mana kita akan mengisinya dengan sintak-sintaks untuk memfilter (membatasi) paket apa saja yang akan ditampilkan pada daftar paket
c. **Daftar paket yang berhasil ditangkap**: menampilkan paket-paket yang berhasil ditangkap Wireshark, berurutan mulai dari paket pertama dan seterusnya.
d. **Detail paket terpilih**: menampilkan detail paket yang terpilih pada Daftar paket di atasnya.
e. **Detail paket dalam heksadesimal**: detail paket yang terpilih akan ditampilkan dalam bentuk heksadesimal sehingga memudahkan kita mendapat informasi

Biografi Penulis

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

Copyright © 2003-2007 IlmuKomputer.Com