Pengenalan dan Instalasi Wireshark

Imam Prasetyo
imp.masiv@gmail.com
http://superman-kartini.blogspot.com

1. Apa itu wireshark?

Wireshark merupakan sebuah Network Packet Analyzer dan salah satu tools yang digunakan untuk monitoring jaringan komputer. Dengan wireshark akan mempermudah analisa jaringan karena software ini menangkap paket dalam lalu lintas jaringan dan menampilkan data paket sedetail mungkin.

Kita bisa mengumpamakan sebuah Network Packet Analyzer sebagai alat untuk memeriksa apa yang sebenarnya sedang terjadi di dalam kabel jaringan, seperti halnya voltmeter atau digunakan untuk memeriksa apa yang sebenarnya sedang terjadi di dalam sebuah kabel listrik.

Di masa lalu, alat-alat semacam itu baik sangat mahal dan eksklusif serta biasanya dengan embel-embel hak cipta. Namun dengan munculnya Wireshark semua itu telah berubah. Oleh situs pengembangnya (www.wireshark.org) mengklaim bahwa Wireshark adalah salah satu Network Packet Analyzer yang bersifat open source terbaik saat ini. Tools ini dapat didownload di www.WireShark.org/download.html.

2. Penggunaan Wireshark

Berikut ini beberapa contoh penggunaan wireshark.

a. Admin sebuah jaringan komputer menggunakannya untuk troubleshooting masalah-masalah di jaringannya
b. Teknisi keamanan jaringan menggunakannya untuk memeriksa keamanan jaringan
c. Pengembang software bisa menggunakannya untuk "debuging" implementasi protokol jaringan dalam software mereka
d. Banyak orang memakainya untuk mempelajari protokol jaringan secara detail
e. Banyak juga orang yang menggunakannya sebagai sniffer atau "pengendus" data-data privasi di jaringan.

3. Main Features

Berikut ini adalah fitur-fitur penting dari tools wireshark.

- Tersedia buat Unix dan Windows
- Menangkap / Capture paket data secara langsung atau real time dari sebuah network interface
- Mampu menampilkan informasi yang sangat detail mengenai hasil capture tersebut
- Bisa Import dan Export hasil capture dari atau ke komputer lain
- Pencarian paket dengan berbagai macam kriteria filter
- Bisa membuat berbagai macam tampilan statistika
- Mampu mendekoderkan banyak protokol
- Open Source application
- Etc

4. System Requirements

Microsoft Windows

✓ Windows XP Home, XP Pro, XP Tablet PC, XP Media Center, Server 2003, Vista, 2008, 7, or 2008 R2

- ✓ Any modern 32-bit x86 or 64-bit AMD64/x86-64 processor
- ✓ 128MB available RAM. Larger capture files require more RAM
- ✓ 75MB available disk space. Capture files require additional disk space
- ✓ 800*600 (1280*1024 or higher recommended) resolution with at least 65536 (16bit) colors (256 colors should work if Wireshark is installed with the "legacy GTK1" Election of The Wireshark 1.0.x releases)
- ✓ A supported network card for capturing

Unix/ Linux

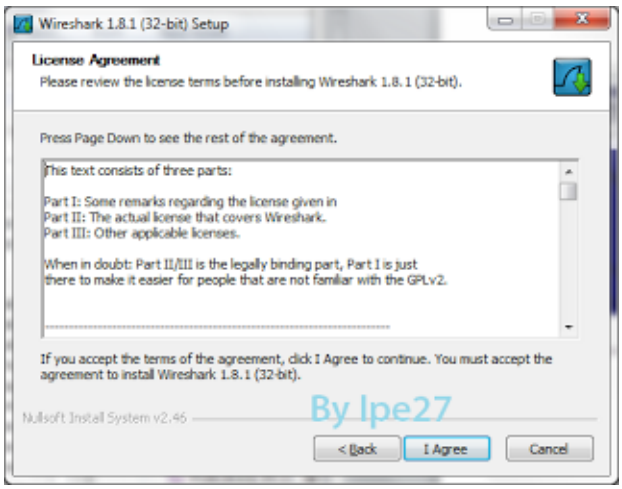
Wireshark saat ini support pada platform UNIX dan Linux kebanyakan. Persyaratan sistem harus sebanding dengan sistem requirement Windows yang tercantum di atas.

5. Instalasi Wireshark

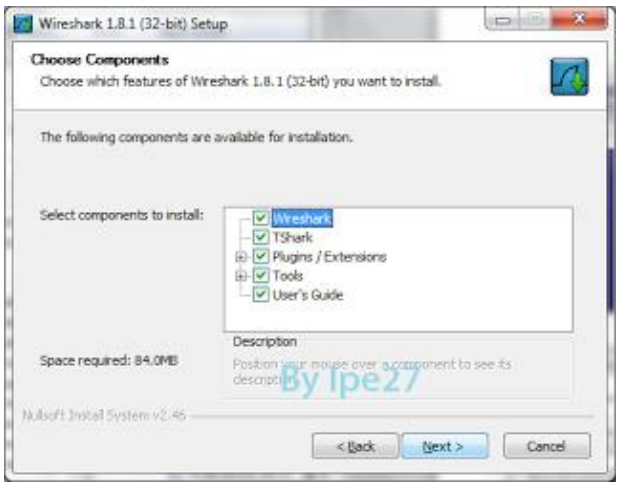
Berikut ini adalah langkah-langkah instalasi wireshark *(proses instalasi wireshark pada windows dan unix hampir sama)

1. Download installer wireshark di www.WireShark.org/download.html, pilih installer yang sesuai operating sistem yang dipakai.
2. Double klik pada ikon installer yang telah didownload sehingga muncul pop-up seperti berikut.

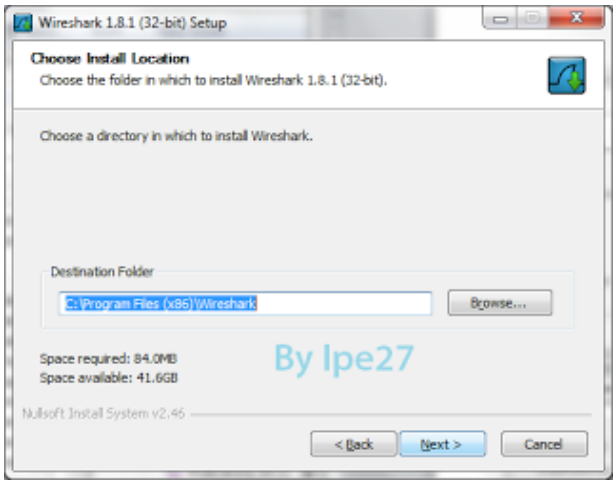
3. Ketika muncul Licence Agreement pilih “I agree”.



4. Pilih komponen yang akan diinstal.



5. Memilih lokasi menginstal wireshark, secara default akan diinstal di C: \Program Files \ “di sini” kemudian klik “next”



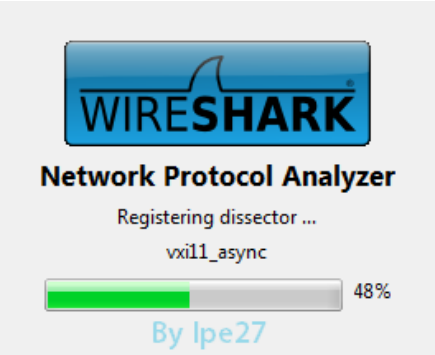
6. Lanjutkan proses instalasi dengan selalu memilih opsi “next” hingga ada pilihan untuk menginstal wincap, pilih yes jika di komputer anda belum terinstal wincap dan pilih no jika telah terinstal wincap sebelumnya.
7. Tunggu instalasi hingga ada panel “finish” yang berarti wireshark telah terinstal.

6. Start Wireshark dan Main Window

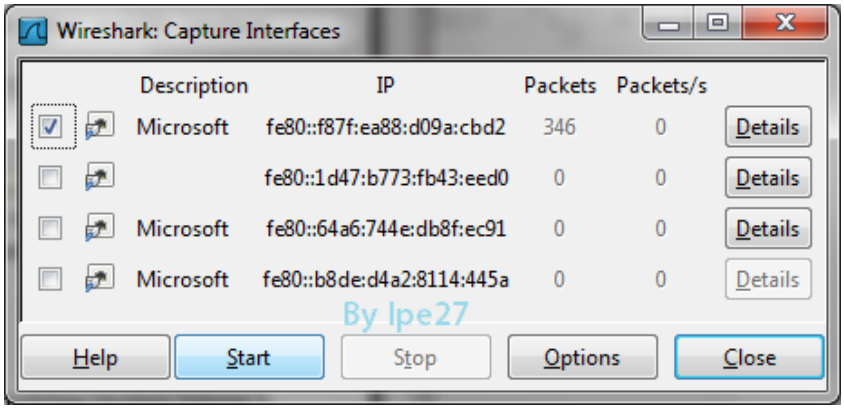
Berikut ini adalah cara untuk menjalankan wireshark (analogi pada Windows)

1. Untuk memulai aplikasi wireshark dapat melalui shortcut pada start menu

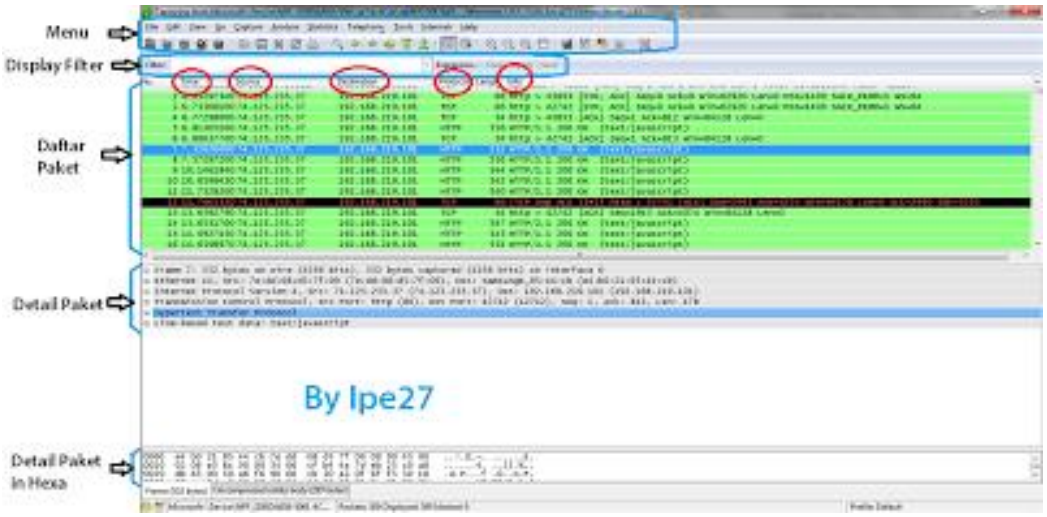
2. Setelah itu akan muncul Splash Screen dari WireShark yang sedang me-load komponen-komponen yang diperlukan



3. Kemudian kita akan dihadapkan dengan tampilan untukmemilih interface yang akan kita capture nantinya kemudian klik start, seperti ini:



4. Main Window



a. Menu : Di sini kita bisa bernavigasi antar menu-menu yang tersedia di Aplikasi Monitoring Jaringan Komputer WireShark.

b. Display Filter : Sebenarnya adalah sebuah kolom, kita akan mengisinya dengan sintaks-sintaks untuk memfilter (membatasi) paket-paket apa saja yang akan ditampilkan pada list paket.

c. Daftar Paket : Di sini akan ditampilkan paket-paket yang berhasil ditangkap oleh WireShark, berurutan mulai dari paket pertama yang ditangkap, dan seterusnya.

d. Detail Paket : Sebuah paket tentunya membawa informasi tertentu yang bisa berbeda-beda antar paketnya, di sini akan ditampilkan dari detail paket yang terpilih pada Daftar paket di atasnya.

e. Detail Heksa : Detail paket yang terpilih akan ditampilkan dalambentuk heksa, terkadang akan lebih mudah bagi kita mendapatkan informasi dari bagian ini.

Pada daftar bagian Daftar Paket, terdapat kolom-kolom seperti berikut ini:

- Time : Menampilkan waktu saat paket tersebut tertangkap
- Source : Menampilkan ip sumber dari paket data tersebut
- Destination : Menampilkan ip tujuan dari paket data tersebut

- Protocol : Menampilkan protokol apa yang dipakai sebuah paket data
- Info : Menampilkan informasi mendetail tentang paket data tersebut.

Biografi Penulis

***Imam Prasetyo**. Kuliah D4 Teknik Telekomunikasi di Politeknik Negeri Semarang. Lulusan SMA Negeri 1 Pati tahun 2010 dan SMP Negeri 1 Pati tahun 2007. Dari kecil sangat tertarik pada ilmu pengetahuan alam dan teknologi. Untuk informasi maupun tulisan menarik lain dapat diakses di situs blog http://www.superman-kartini.blogspot.com*