**Analisis Jaringan Menggunakan Wireshark**

Dalam konsep komunikasi data suatu jaringan komputer, ada mekanisme pengiriman data dari komputer sumber ke komputer tujuan dimana proses pengiriman paket data tersebut sampai dengan benar ke komputer yang dituju. Tentunya dalam proses pengiriman yang terjadi tidak semudah yang dipikirkan. Alasan pertama, komputer tujuan berada jauh dari komputer sumber sehingga paket data yang dikirimkan bisa saja hilang atau rusak di tengah jalan. Kedua, komputer tujuan sedang menunggu/mengirimkan paket data dari/ke komputer yang lain. Tentunya paket data yang akan dikirimkan diharapkan sampai dengan tepat tanpa terjadi kerusakan. Untuk mengatur mekanisme komunikasi data tersebut dibutuhkan pengaturan proses pengiriman data yang dikenal sebagai protokol. Protokol di sini adalah sebuah perangkat lunak yang melekat pada setiap sistem operasi tertentu.

**Analisis Menggunakan Wireshark**

Melihat Segment TCP yang ada dalam jaringan bisa dilakukan dengan menggunakan program aplikasi, salah satu contohnya adalah wireshark. Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap dan paket-paket data/informasi yang ada di dalam jaringan, sehingga data tersebut dapat kita analisa untuk berbagai keperluan, diantaranya:

* Troubleshooting masalah di jaringan
* Memeriksa keamanan jaringan
* Sniffer “ data-data privasi di jaringan

Beberapa tujuan penggunaan wireshark:

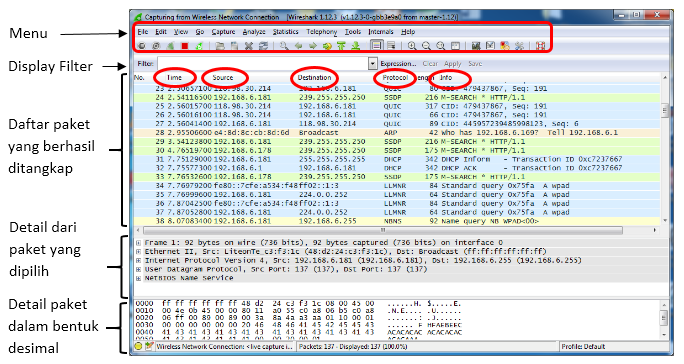
* Administrator jaringan menggunakannya untuk memecahkan masalah jaringan
* Insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan
* Pengembang menggunakannya untuk men-debug implementasi protokol
* Beberapa orang menggunakannya untuk mempelajari protokol jaringan internal

WireShark dapat menangkap paket-paket data atau informasi dalam suatu jaringan komputer. Wireshark dapat membaca:

* Ethernet
* Token-Ring
* FDDI
* Serial(PPP dan SLIP)
* 802.11 wireless LAN
* Koneksi ATM
* Mengetahui IP chatter(seseorang)
* Proses transmisi dan
* Transmisi data antar computer

**Fitur dan kelebihan WireShark:**

* Tersedia untuk Linux dan Windows.
* Menangkap paket data secara langsung dari sebuah network interface.
* Mampu menampilkan informasi yang sangat terperinci mengenai hasil tangkapan tersebut.
* Dapat melakukan import dan export hasil tangkapan dari atau ke komputer lain.
* Pencarian paket menggunakan berbagai macam kriteria filter/pemilahan.
* Dapat membuat berbagai macam tampilan statistika.



**Keterangan:**

* **Menu** : disini kita bisa bernavigasi antar menu-menu yang tersedia di wireshark
* **Display Filter** : kolom untuk mengisi sintaks-sintaks untuk memfilter paket data apa saja yang akan ditampilkan pada list paket
* **Daftar Paket**: Menampilkan paket-paket yang berhasil di tangkap oleh wireshark, berurutan mulai dari paket pertama yang ditangkap dan seterusnya.
* **Detail paket**: Sebuah paket tentunya membawa informasi tertentu yang bias berbeda-beda antar paketnya, disini akan ditampilkan sari detail paket yang terpilih pada daftar paket di atasnya.
* **Detail Heksa**: Detail paket ini akan ditampilkan dalam bentuk heksa, terkadang akan lebih mudah bagikita mendapatkan informasi dari bagian ini.
* **Time** : Menampilkan waktu saat paket tersebut tertangkap
* **Source** : Menampilkan IP sumber dari paket data tersebut
* **Destination** : Menampilkan tujuan dari paket data tersebut
* **Protocol** : Menampilkan protocol apa saja yang dipakai sebuah paket data
* **Info** : Menampilkan informasi detail tentang paket data tersebut