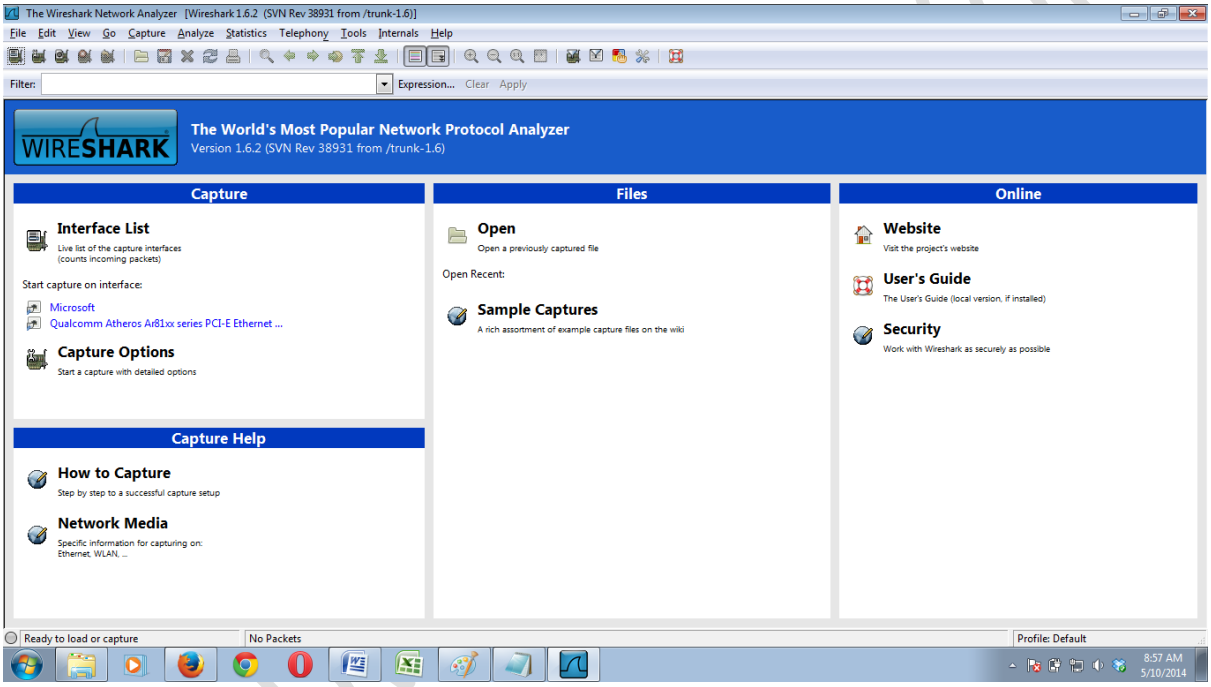
PEMANFAATAN WIRESHARK UNTUK SNIFFING

Pengertian Wireshark

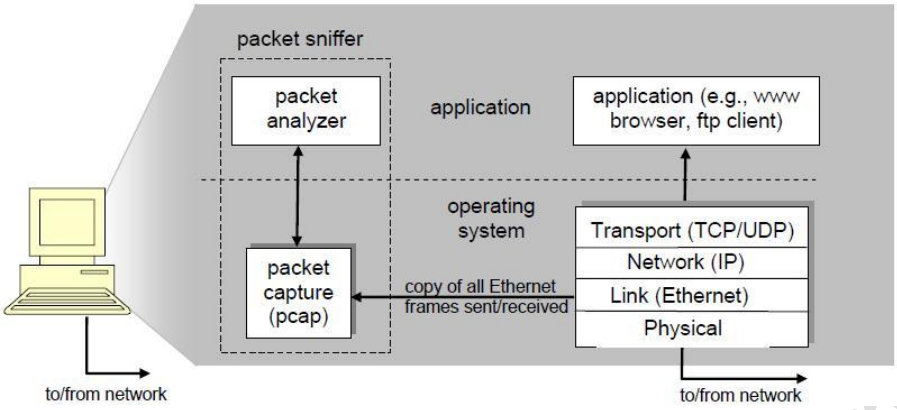
Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan.

Wireshark dapat membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN , dan koneksi ATM.



Gambar 1. Tampilan wireshark

Tools ini bisa menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti password email atau account lain) dengan menangkap paket-paket yang berjalan di dalam jaringan dan menganalisanya. Namun tools ini hanya bisa bekerja didalam dalam jaringan melalui LAN/Ethernet Card yang ada di PC Untuk struktur dari packet sniffer terdiri dari 2 bagian yaitu packet analyzer pada layer application dan packet capture pada layer operating system (kernel).



Gambar 2. Struktur Packet Sniffer

Struktur dari wireshark graphical user interface adalah sebagai berikut :

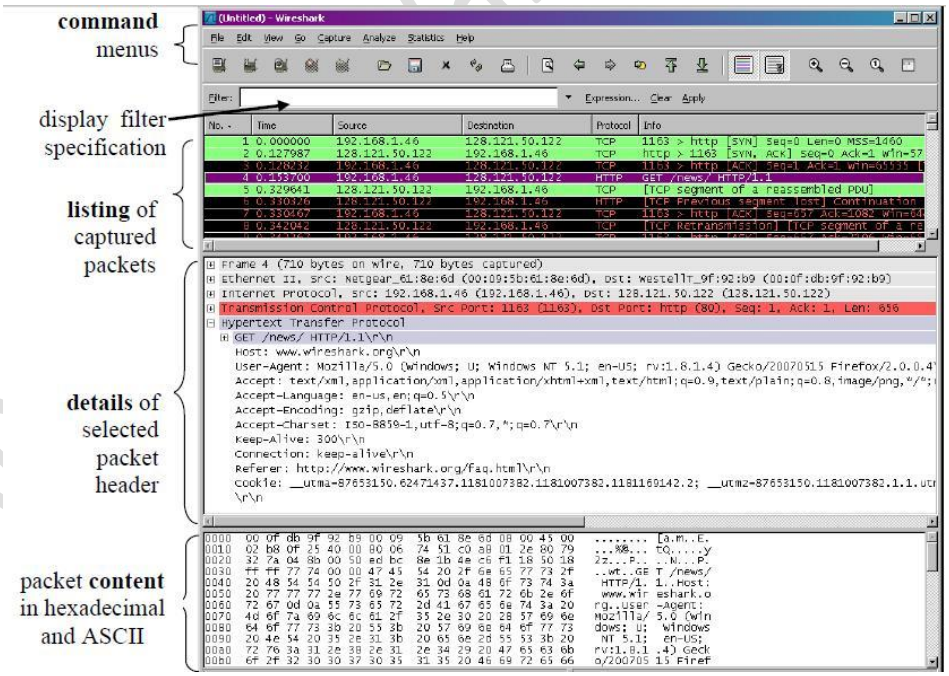
a. Command menu

b. Display filter specification : untuk memfilter packet data

c. Listing of captured packets : paket data yang tertangkap oleh wireshark

d. Details of selected packet header : data lengkap tentang header dari suatu packet

e. Packet contents : isi dari suatu packet data

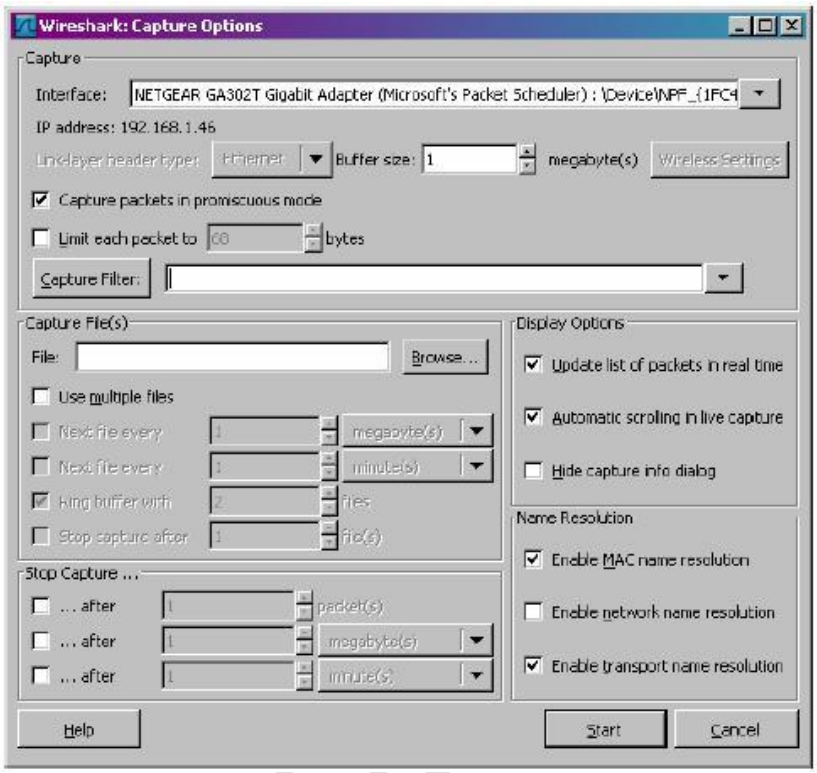


Gambar 3. Struktur Wireshark

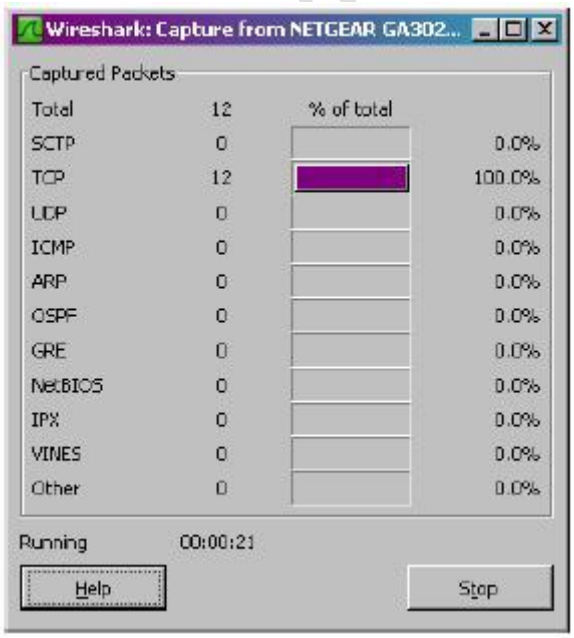
PERCOBAAN

A. Pengenalan Wireshark

1. Bukalah wireshark. Dan mulai mengcapture paket data dengan memilih Capture | Options. Pilihlah interface card yang digunakan untuk menangkap paket data yang lewat seperti gambar berikut.



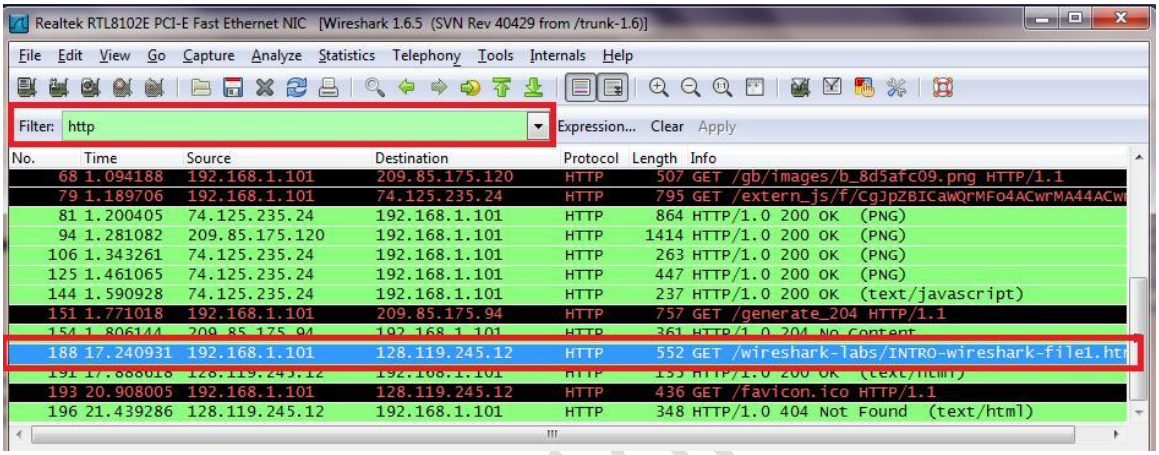
2. Mulai lakukan pengamatan data dengan menekan tombol start :



3. Sementara wireshark jalan, lakukan koneksi ke : http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html Setelah muncul tampilan pada browser kemudian stop wireshark, Capture | Stop.

   Perhatikan pada bagian Protocol, ada banyak protocol yang ditampilkan.

   Untuk memfilter hanya protocol http saja yang ditampilkan lakukan filtering seperti berikut :



   Catat dan amati header paket dan content datanya.

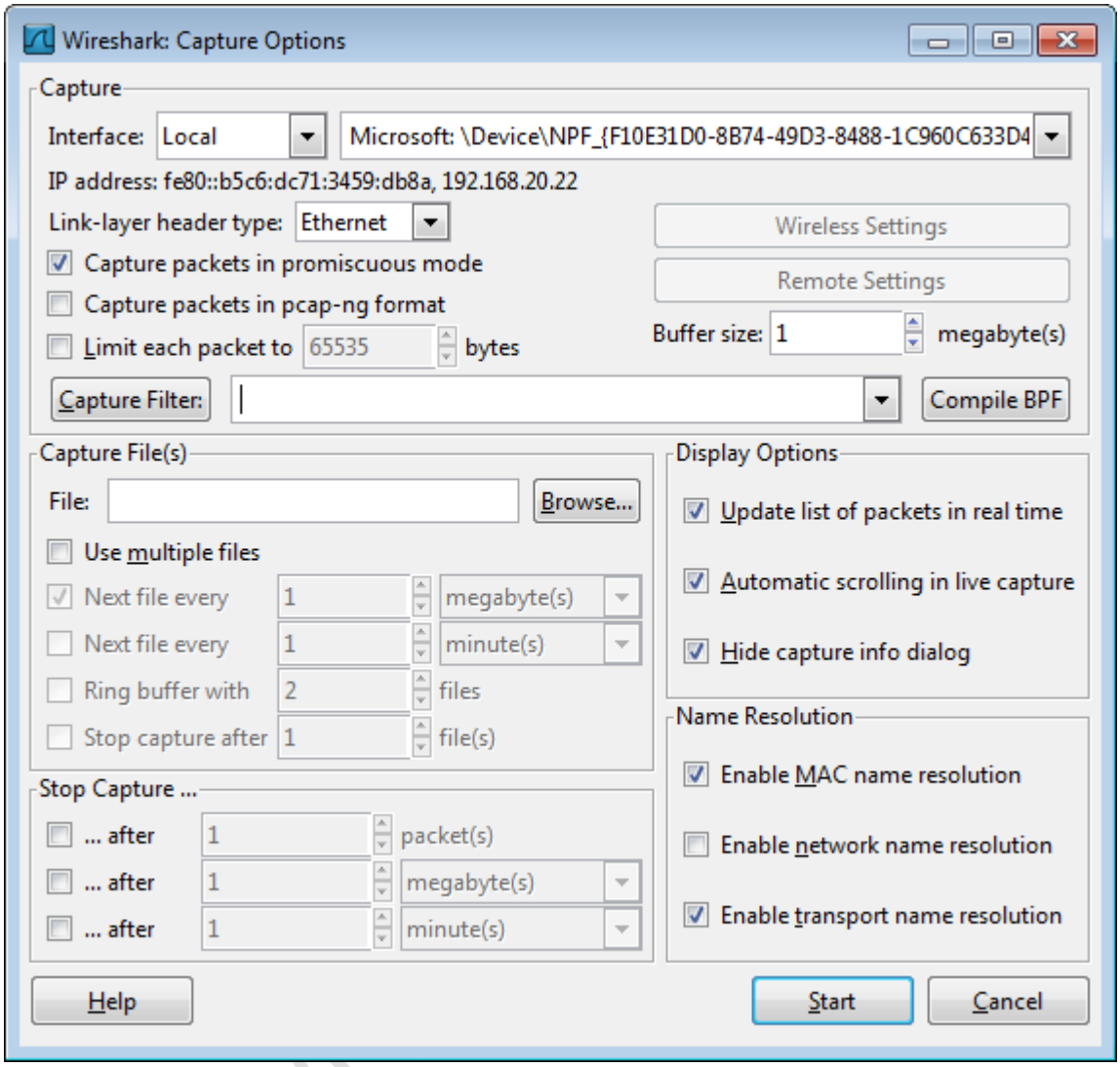
4. Dari HTTP GET message diatas yang dikirim dari komputer anda ke gaia HTTP server. Amatilah data berikut pada informasi header packet dan juga content informasi yang dikandungnya :

   a. Ethernet frame
   b. IP datagram
   c. TCP segment
   d. HTTP message

B. Sniffing

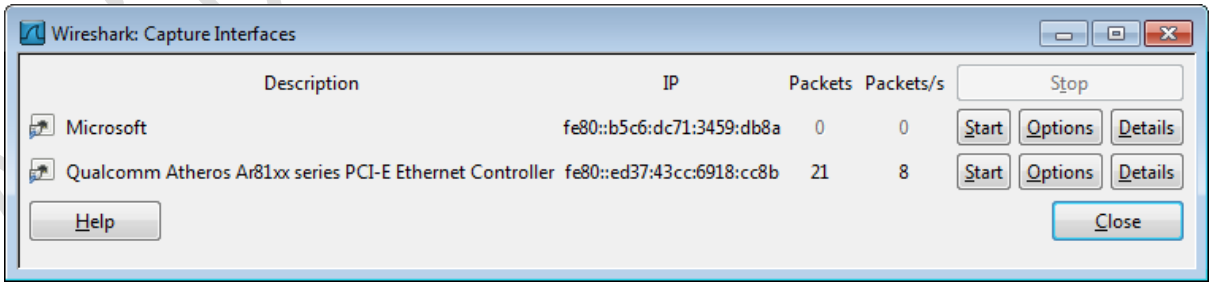
Catatan : Sniffng hanya bisa dilakukan pada jaringan yang menggunakan hub sebagai media konsentratornya.

1. Siapkan web yang memiliki fasilitas login
2. Ketahui alamat ip nya menggunakan whois tools
3. Buka wireshark, siapkan capturenya = Wireshark → Capture → Option



Start

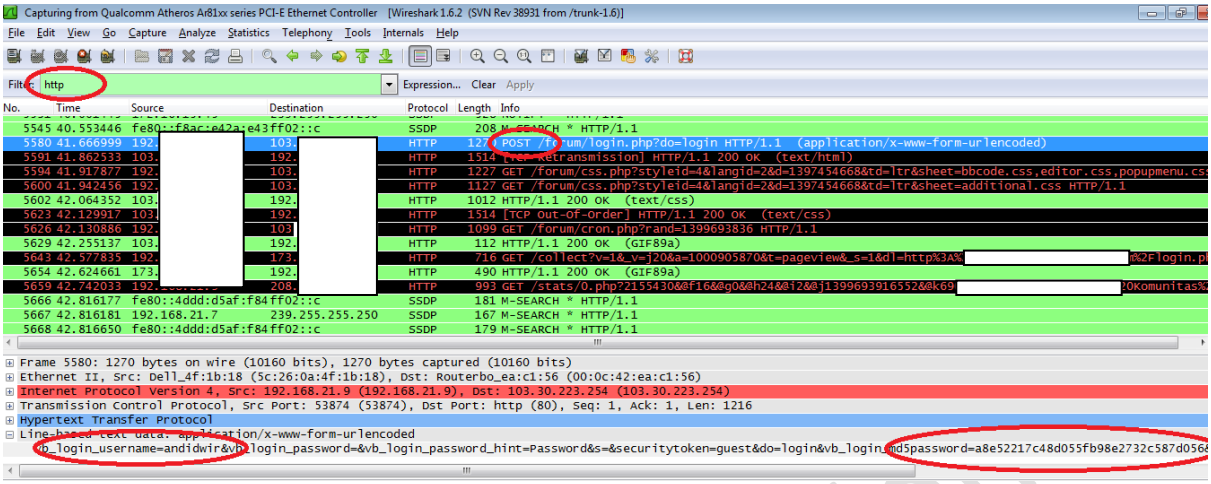
4. Atau siapkan capturenya dg cara = Wireshark → Capture → Interface



Pilih yang paket datanya aktif, Start.

5. Buka browser, masukkan alamat web yang sudah disiapkan, lakukan login.

6. Masukkan “http” pada filter capture



Perhatikan “POST”, akan terlihat login dan password meskipun di encrypt menggunakan md5.