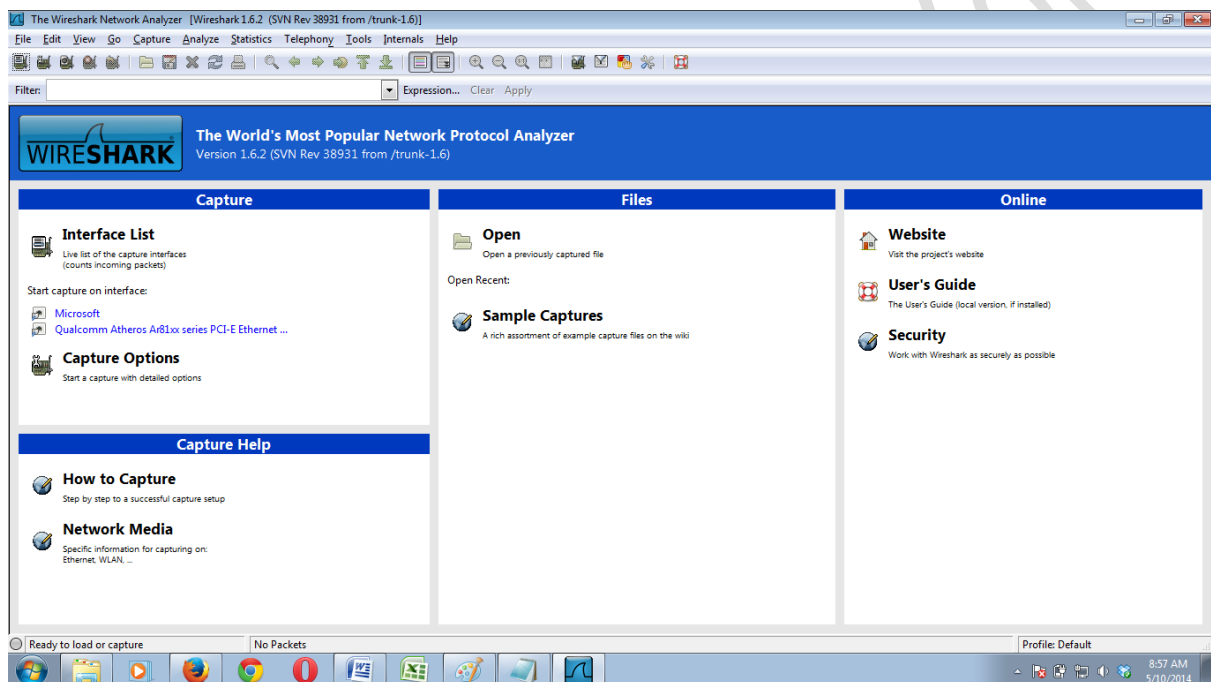


PEMANFAATAN WIRESHARK UNTUK SNIFFING

Pengertian Wireshark

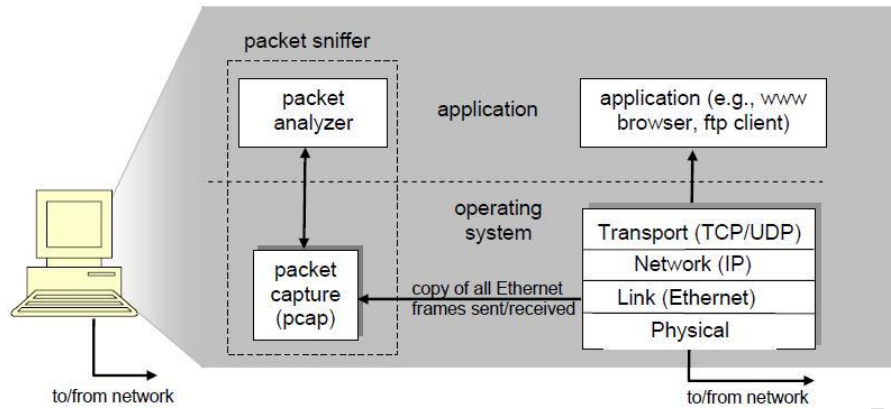
Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan.

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

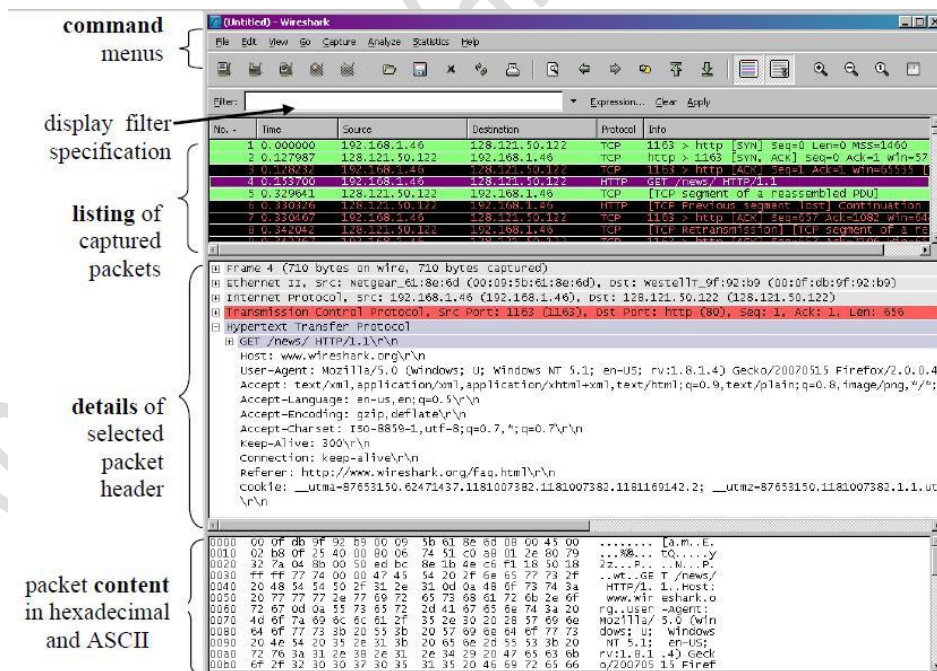
Tools ini bisa menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti password email atau account lain) dengan menangkap paket-paket yang berjalan di dalam jaringan dan menganalisisnya. 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 :

- Command menu
- Display filter specification : untuk memfilter packet data
- Listing of captured packets : paket data yang tertangkap oleh wireshark
- Details of selected packet header : data lengkap tentang header dari suatu packet
- Packet contents : isi dari suatu packet data

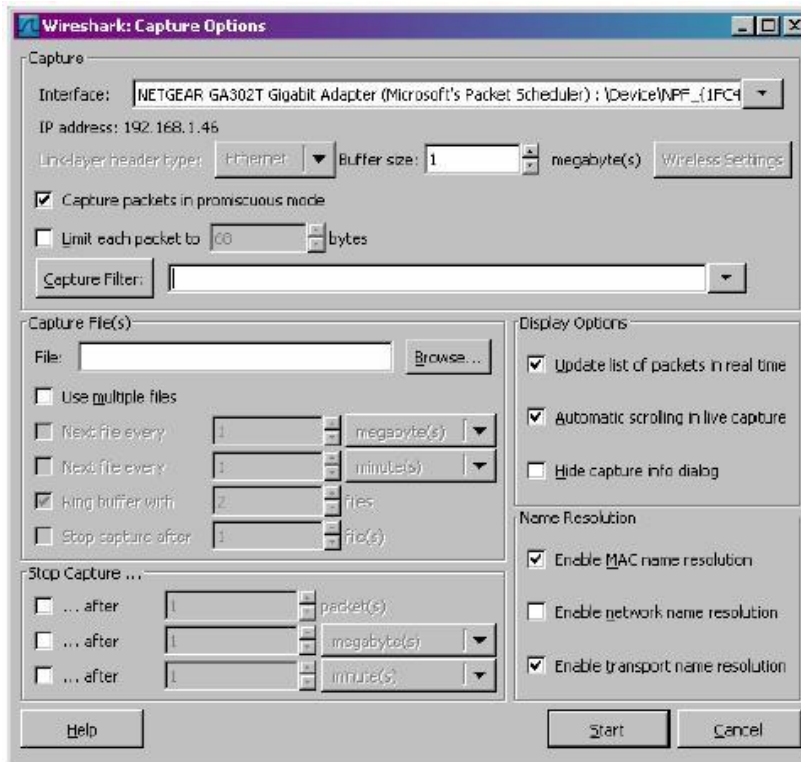


Gambar 3. Struktur Wireshark

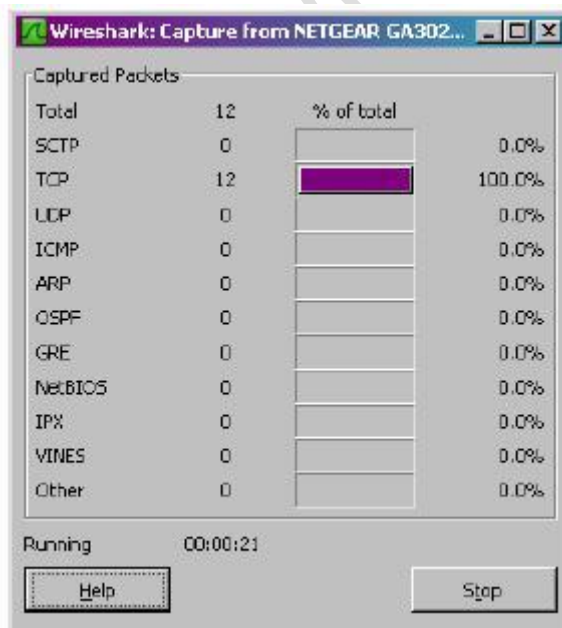
PERCOBAAN

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.



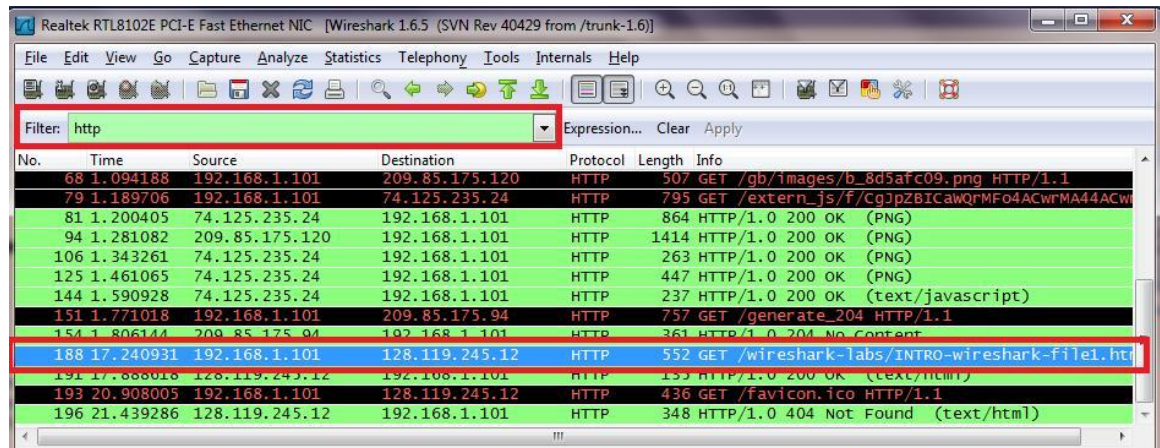
2. Mulai lakukan pengamatan data dengan menekan tombol start :



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 :



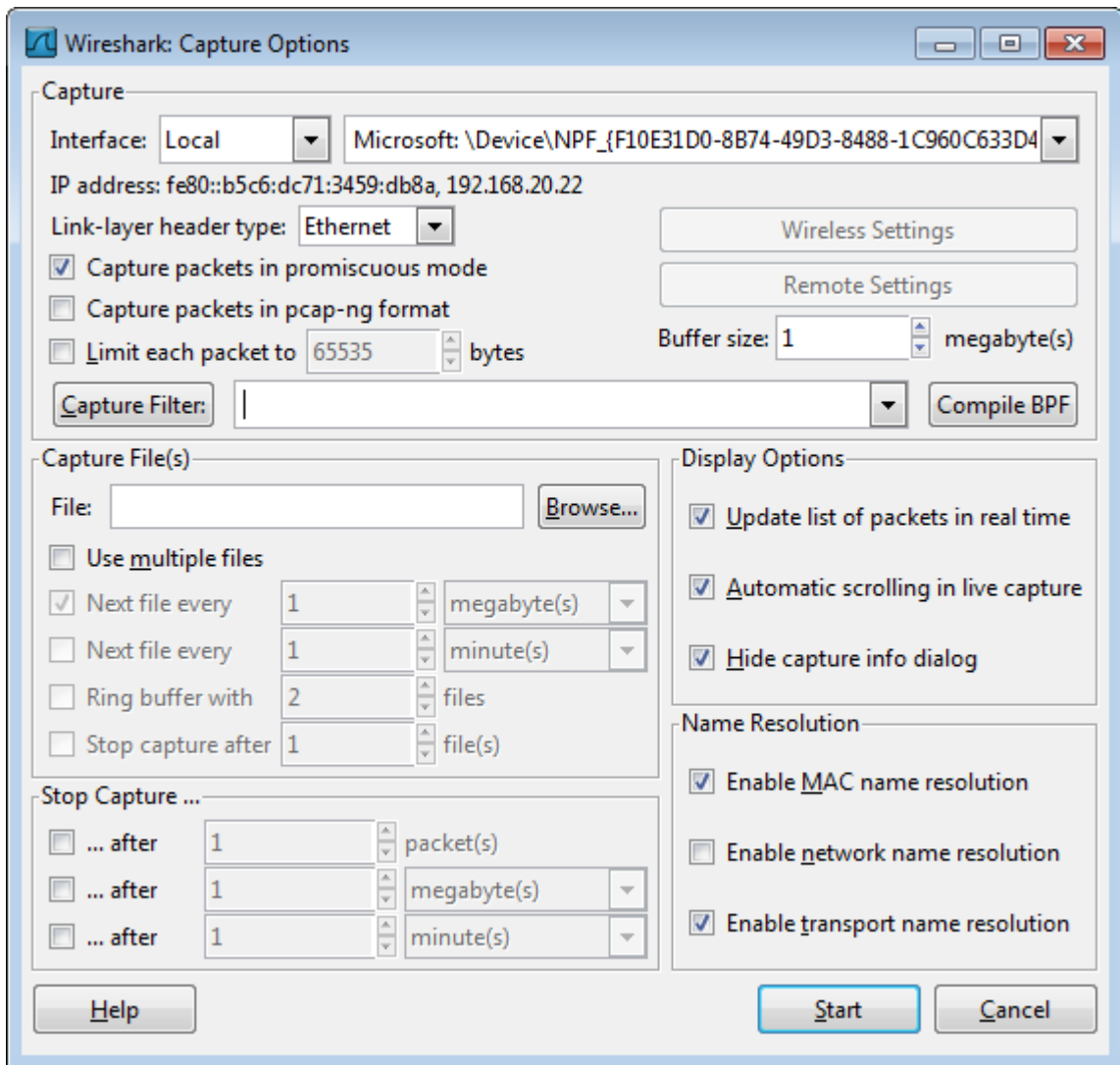
Catat dan amati header paket dan content datanya.

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 capturennya 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

Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
5545	40.553446	fe80::f8ac:e42a:e43ff02::c	103::	SSDP	208	M-SEARCH * HTTP/1.1
5580	41.666999	192.168.21.9	103.30.223.254	HTTP	127	POST /forum/login.php?do=login HTTP/1.1 (application/x-www-form-urlencoded)
5591	41.862533	103.30.223.254	192.168.21.9	HTTP	1514	[TCP Out-Of-Order] HTTP/1.1 200 OK (text/html)
5594	41.917877	192.168.21.9	103.30.223.254	HTTP	1227	GET /forum/css.php?styleid=4&langid=2&i=1397454668&d=ltr&sheet=bbcode.css,editor.css,popupmenu.css HTTP/1.1
5600	41.942456	192.168.21.9	103.30.223.254	HTTP	1127	GET /forum/css.php?styleid=4&langid=2&i=1397454668&d=ltr&sheet=additional.css HTTP/1.1
5602	42.064352	103.30.223.254	192.168.21.9	HTTP	1012	HTTP/1.1 200 OK (text/css)
5603	42.139317	103.30.223.254	192.168.21.9	HTTP	1514	[TCP Out-Of-Order] HTTP/1.1 200 OK (text/css)
5626	42.180886	192.168.21.9	103.30.223.254	HTTP	1089	GET /forum/cron.php?code=1399693836 HTTP/1.1
5629	42.255137	103.30.223.254	192.168.21.9	HTTP	112	HTTP/1.1 200 OK (GIF/89a)
5643	42.577835	192.168.21.9	173.19.138.13	HTTP	716	GET /collect?v=1&v=j208a-1000905870&t=pageview&s=1&d=1-http%3A%2Flogin.php HTTP/1.1
5654	42.624661	173.19.138.13	192.168.21.9	HTTP	490	HTTP/1.1 200 OK (GIF/89a)
5659	42.742033	192.168.21.9	208.115.120.13	HTTP	993	GET /stats/0.php?2155430&F16&G0&H24&I2&J1399693916552&K69 HTTP/1.1
5666	42.816177	fe80::d4dd:d5af:f84ff02::c	192.168.21.9	SSDP	181	M-SEARCH * HTTP/1.1
5667	42.816181	192.168.21.9	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
5668	42.816650	fe80::d4dd:d5af:f84ff02::c	192.168.21.9	SSDP	179	M-SEARCH * HTTP/1.1

Frame 5580: 1270 bytes on wire (10160 bits), 1270 bytes captured (10160 bits) on interface 0

Ethernet II, Src: Dell_4f:1b:18 (5c:26:0a:4f:1b:18), Dst: Routerbo_ea:c1:56 (00:0c:42:ea:c1:56)

Internet Protocol Version 4, Src: 192.168.21.9 (192.168.21.9), Dst: 103.30.223.254 (103.30.223.254)

Transmission Control Protocol, Src Port: 53874 (53874), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1216

Hypertext Transfer Protocol

Line-based text data: application/x-www-form-urlencoded

Content-Disposition: form-data; name="username"; value="andidwtr"&name="password"; value="...&name="md5password"; value="a8e52217c48d05f98e2732c587d056"

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

Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
11	2.160673	172.16.17.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
23	3.639285	fe80::e43ff02::c	192.168.21.9	SSDP	208	M-SEARCH * HTTP/1.1
38	6.640339	fe80::e43ff02::c	192.168.21.9	SSDP	208	M-SEARCH * HTTP/1.1
52	9.219319	192.168.21.9	118.98.73.219	HTTP	571	POST / HTTP/1.1 (application/x-www-form-urlencoded)
54	9.315853	118.98.73.219	192.168.21.9	TCP	1514	[TCP Previous segment lost] [TCP segment of length 1514 bytes received out of order]
58	9.346649	192.168.21.9	192.168.21.9	HTTP	1514	Continuation or non-HTTP traffic
59	9.348605	192.168.21.9	192.168.21.9	HTTP	1514	Continuation or non-HTTP traffic
61	9.350989	192.168.21.9	192.168.21.9	HTTP	1514	Continuation or non-HTTP traffic
62	9.376401	192.168.21.9	192.168.21.9	HTTP	222	Continuation or non-HTTP traffic
66	9.641116	fe80::e43ff02::c	192.168.21.9	SSDP	208	M-SEARCH * HTTP/1.1
79	11.746491	192.168.21.9	118.98.73.219	HTTP	454	GET /ruang_utama_karyawan.html HTTP/1.1
80	11.746900	192.168.21.9	207.46.162.10	HTTP	831	GET /search?q=site%3Ast HTTP/1.1
81	11.747139	192.168.21.9	207.46.162.10	HTTP	461	GET /web/%/http://sta HTTP/1.1
90	11.879646	192.168.21.9	192.168.21.9	TCP	1514	[TCP Previous segment lost] [TCP segment of length 1514 bytes received out of order]
92	11.879993	192.168.21.9	192.168.21.9	HTTP	1514	Continuation or non-HTTP traffic

Frame 52: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0

Ethernet II, Src: Dell_4f:1b:18 (5c:26:0a:4f:1b:18), Dst: Routerbo_ea:c1:56 (00:0c:42:ea:c1:56)

Internet Protocol Version 4, Src: 192.168.21.9 (192.168.21.9), Dst: 118.98.73.219 (118.98.73.219)

Transmission Control Protocol, Src Port: 53911 (53911), Dst Port: http (80), Seq: 1, Ack: 1, Len: 517

Hypertext Transfer Protocol

Line-based text data: application/x-www-form-urlencoded

Content-Disposition: form-data; name="UserID"; value="20097"&name="Password"; value="me...&name="YLogin"; value="++++LOG+IN++++"