Monitoring Layer Aplikasi (Protokol HTTP) menggunakan Wireshark

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

Application Layer merupakan layer paling atas, baik pada model OSI, maupun model TCP/IP. Layer ini menyediakan antarmuka antara aplikasi-aplikasi yang kita gunakan, dengan jaringan yang digunakannya untuk melakukan pertukaran informasi. Pada pertukaran informasi antar aplikasi yang berjalan pada host pengirim dan host tujuan digunakan berbagai protokol Application Layer.

Protokol pada application layer menentukan bagaimana pesan dipertukarkan antara host pengirim dan tujuan, sintaks dari perintah-perintah kontrol (control command), jenis dan format data yang dipertukarkan, metode yang digunakan untuk mengetahui terjadinya kesalahan dan bagaimana mengatasi kesalahan tersebut, serta bagaimana interaksi dengan layer yang berada di bawahnya.

Terdapat banyak protokol untuk apllication layer, antara lain Domain Name Service Protocol (DNS), Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Telnet, Filet Transfer Protocol (FTP), dan sebagainya.

Cara Menjalankan Wireshark: Meng-capture paket data pada protokol HTTP

Hypertext Transfer Protocol (HTTP), pada awalnya merupakan prokol yang dikembangkan untuk mempublikasikan maupun mengunduh halaman HTML. Saat ini, HTTP yang merupakan protokol pada application layer yang paling sering digunakan juga dimanfaatkan untuk transfer data. HTTP menentukan mendefinisikan protokol dalam melakukan request dan

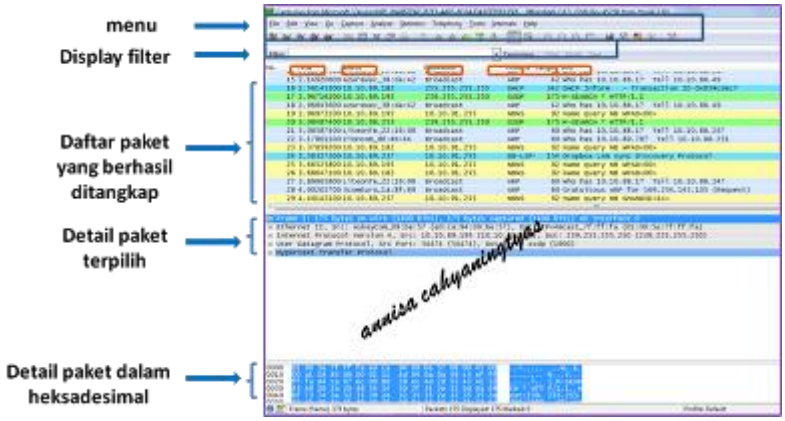
response antar klien dan server. Dengan HTTP, terdapat tiga jenis pesan yang dipertukarkan, yaitu GET, POST, dan PUT. GET digunakan oleh klien untuk melakukan request. POST dan PUT digunakan untuk melakukan upload data ke server.

Dan berikut tampilan cara meng-capture paket data melalui Wireshark yang dikirimkan saat sedang membuka web browser, sehingga paket melewati protokol HTTP:

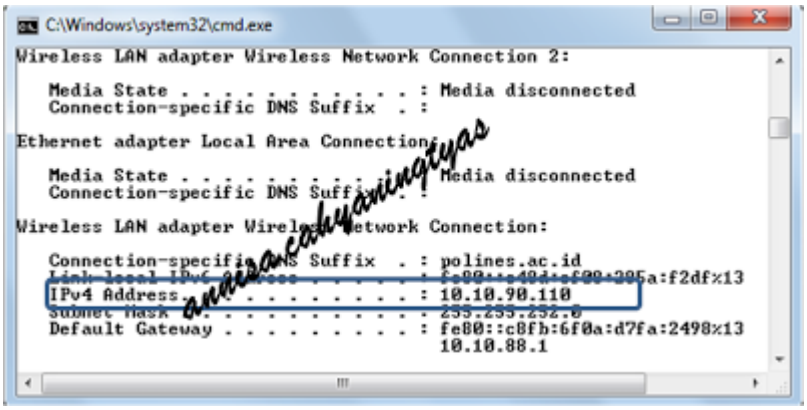
a. Menjalakan program Wireshark, kemudian memilih interface (dalam hal ini memilih interface **Microsoft**) lalu checklist kemudian Start

b. Setelah itu, buka web browser (contoh Mozilla Firefox) kemudian buka situs apapun (contoh Google, Facebook, dan Bhinneka)

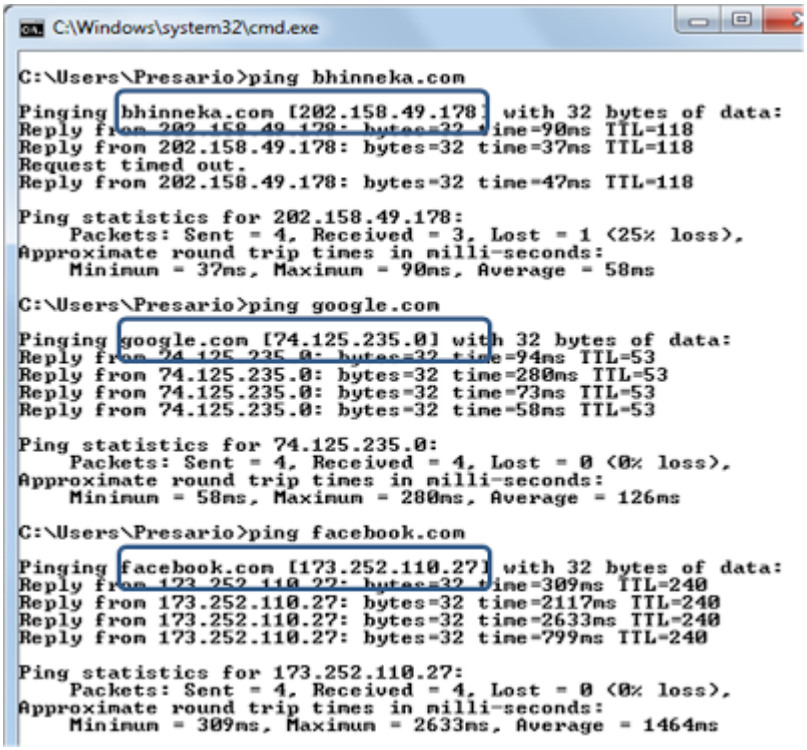
c. Saat situs-situs diakses dan terbuka, maka saat itu pula data-data telah dimasuk ke Wireshark dan paket-paket data pun akan ditampilkan.



d. Kemudian, melakukan pengecekan IP Address laptop kita (untuk keperluan pembuktian), dengan cara : klik Start>mengetik cmd pada kotak Search> OK. Setelah muncul kotak dialog Command Prompt, mengetikkan ‘ipconfig’ dan terbacalah bahwa IP Address Laptop kita yaitu 10.10.90.110

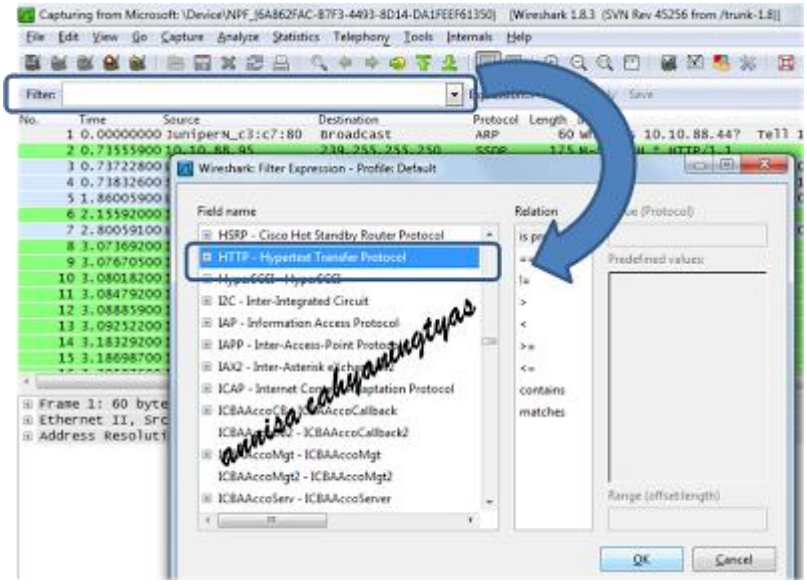


e. Setelah itu melakukan pengecekan IP Address dari situs yang kita buka melalui Command Prompt, antara lain: Google (IP Address: 74.125.235.0); Facebook (IP Address: 173.252.110.27); dan Bhinneka (IP Address: 202.158.49.178).

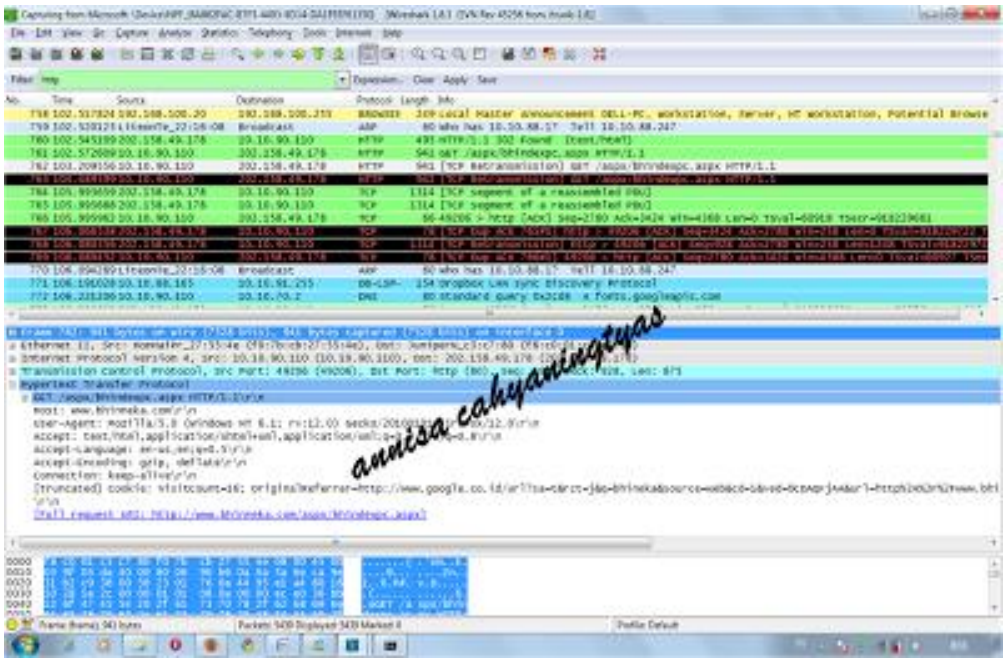


f. Kita telah mengakses situs melalui web browser dan telah menampilkan lalu lintas paket data nya melalui Wireshark. Dan saat kita hanya ingin menampilkan protokol HTTP

maka dapat dilakukan pemilihaan HTTP pada eksperi filtering, dan tampilannya akan menjadi seperti berikut



IP Address Laptop kita yaitu 10.10.90.110; Google (IP Address: 74.125.235.0); Facebook (IP Address: 173.252.110.27); dan Bhinneka (IP Address: 202.158.49.178).



Terlihat pada gambar ‘penangkapan paket data’ melalui Wireshark, telah banyak lalu lintas jaringan yang telah berjalan. Kegiatan yang telah kita coba adalah penangkapan paket data dengan menggunakan filter HTTP. Pertama kita telah mengecek IP Laptop sendiri, yaitu 10.10.90.110, lalu telah kita lakukan browsing ke beberapa situs antara lain Google (IP Address: 74.125.235.0); Facebook (IP Address: 173.252.110.27); dan Bhinneka (IP Address:

202.158.49.178). Namun, kali ini yang akan dibahas penangkapan data saat browsing situs Bhinneka.

Dari gambar di atas menunjukan banyaknya HTTP Messages yang ditangkap saat browsing situs Bhinneka. Diliat dari sumbernya ada dua jenis HTTP Messages yang ditangkap yaitu dari browser kita ke server Bhinneka dan sebaliknya, dapat dilihat dari IP source dan destination. Pada sumber, IP Laptop sendiri, yaitu 10.10.90.110 pada sumber ketika memasukkan www.bhinneka.com maka akan mengirimkan data-data ke server dan juga data tersebut akan dikirim ke DNS untuk diketahui IP nya. Setelah IP diterjemahkan oleh DNS,maka DNS akan mengirimkan kembali IP Bhinneka ke Laptop kita.Kemudian setelah dilakukan translasi dari www.bhinneka.com ke 202.158.49.178 yang merupakan IP bhinneka maka laptop kita sebagai sumber melakukan request ke destination dengan menggunakan protocol TCP. Penggunaan TCP karena TCP merupakan protocol yang digunakan untuk melakukan browsing.

Dari hasil Ethernet II (layer 2) tersebut, dapat diketahui bahwa paket frame 762 dikirimkan ke perangkat tujuan JuniperN_c3:c7:80 dengan MAC address f8:c0:01:c3:c7:80, dimana perangkat asal atau sumber adalah HonHairPr_27:55:4e dengan MAC address f0:7b:cb:27:55:4e . Pada protokol TCP, port sumbernya : 42906, dan port tujuan (http): 80, dengan seq: 19095, Ack; 928, Len: 875 .

Dari gambar di atas pula, dapat dilihat bahwa metode permintaan yang digunakan pada protokol HTTP tersebut adalah GET. Metode GET meminta representasi dari sumber tertentu. Server yang dituju untuk meminta halaman dengan sumber daya tertentu dalam frame ini adalah www.bhinneka.com\r\n. Sedangkan klien yang meminta ditunjukka pada User-Agent yaitu Mozillla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0.1\r\n karena dalam monitoring ini saya mengakses halaman bhinneka.com dengan menggunakan Mozilla Firefox 12.0.1.

Biografi Penulis

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