Monitoring Layer Traansport (Protokol TCP dan UDP) menggunakan Wireshark

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

Di era modern ini, bidang telekomunikasi sangatlah dibutuhkan hingga berkembang Telah dipaparkan serta dijelaskan mengenai paket-paket di Layer Aplikasi, seperti SMTP, POP3, dan lainnya. Pada bagian ini, akan dilanjutkan untuk pembahasan paket-paket pada protokol di Layer Transport (antara lain: UDP dan TCP)

Lapisan transpor bertanggung jawab untuk menyediakan layanan untuk protokol yang berada di atasnya (lapisan aplikasi), layanan yang dimaksud antara lain:

a. Mengatur alur (*flow control*)
b. Mengurutkan paket (*packet sequencing*), dilakukan proses mengubah data menjadi segmen-segmen data (*segmentation*), dan menyusunnya kembali.
c. Penanganan kesalahan dan fitur *acknowledgment* (ACK) untuk menjamin bahwa data telah sampai di tempat tujuan dan benar, serta akan dikirimkan lagi ketika memang data tidak sampai ke tujuan (atau terjadi error).
d. *Multiplexing*, yang dapat digunakan untuk menggabungkan data dari bebeberapa sumber untuk mengirimkannya melalui satu jalur data saja.

1. Transmission Transfer Protocol (TCP)

TCP biasanya digunakan ketika protokol lapisan aplikasi membutuhkan layanan transfer data yang bersifat andal, di mana layanan tersebut tidak dimiliki oleh protokol lain sebab TCP berperan di dalam memperbaiki pengiriman data yang benar dari suatu klien ke server di mana data dapat hilang di tengah-tengah jaringan dan TCP dapat mendeteksi error atau data yang hilang dan kemudian melakukan transmisi ulang sampai data diterima dengan benar dan lengkap. . Contoh dari protokol yang menggunakan TCP adalah HTTP dan FTP.

Segmen-segmen TCP akan dikirimkan sebagai datagram-datagram IP (datagram merupakan satuan protocol data unit pada lapisan *internetwork*). Sebuah segmen TCP terdiri atas sebuah *header* dan segmen data (*payload*), yang dienkapsulasi dengan menggunakan *header* IP dari protokol IP. Sebuah segmen TCP dapat memiliki flag (tanda-tanda) khusus yang mengindikasikan segmen yang bersangkutan,

Karakteristik TCP

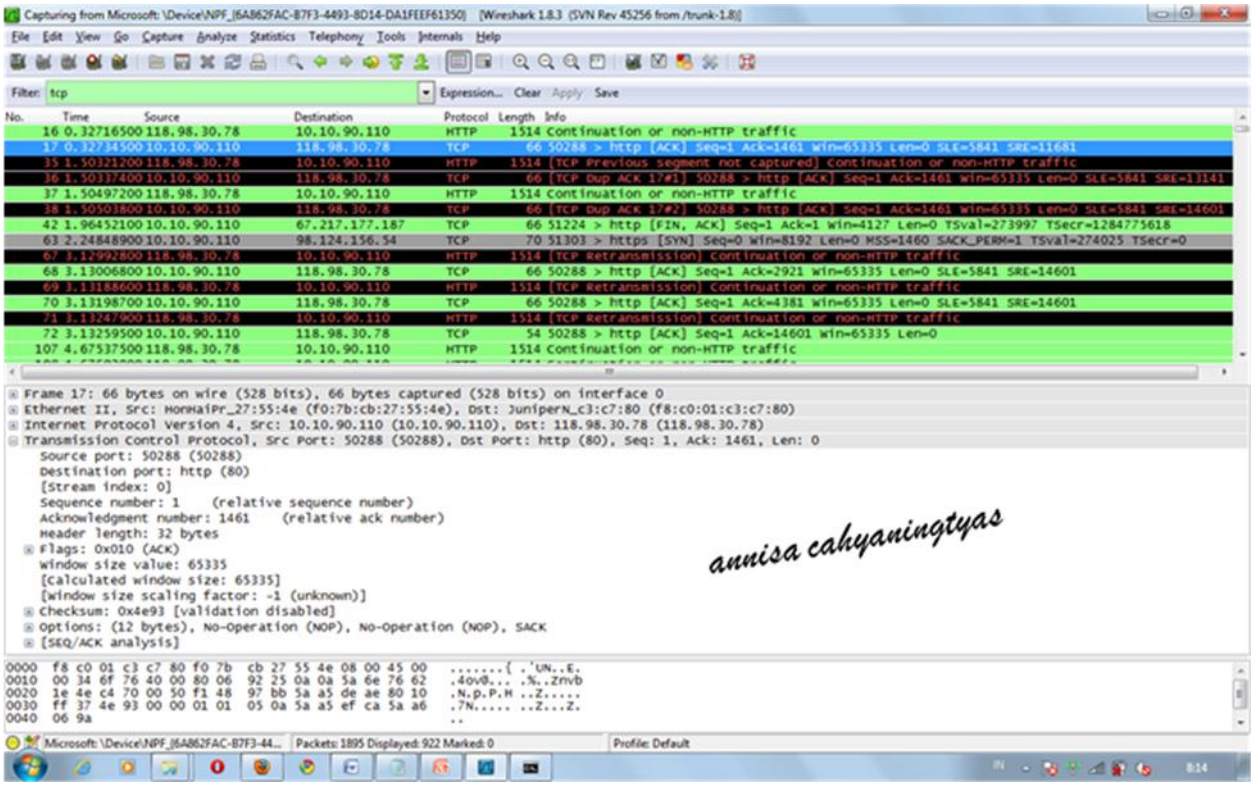
a. *Connection-oriented*: mekanisme komunikasi data di mana dua perangkat yang akan saling berkomunikasi diharuskan membuat sesi koneksi terlebih dahulu.
b. *Full-duplex*: koneksi yang terjadi antara dua host terdiri atas dua buah jalur, yakni jalur keluar dan jalur masuk., maka data secara simultan diterima dan dikirim.
c. Dapat diandalkan (*reliable*): data yang dikirimkan ke koneksi TCP akan diurutkan dengan urutan paket dan akan mengharapkan paket *positive acknowledgment* dari penerima. Jika tidak ada paket Acknowledgment dari penerima, maka segmen TCP akan ditransmisikan ulang. Untuk menjamin integritas setiap segmen TCP, diimplementasikan penghitungan TCP Checksum.
d. *Byte stream*: TCP melihat data yang dikirimkan dan diterima melalui dua jalur masuk dan jalur keluar TCP sebagai sebuah *byte stream* yang berdekatan
e. Memiliki layanan *flow control*: untuk mencegah data terlalu banyak dikirimkan pada satu waktu, pada jaringan internetwork IP, TCP mengimplementasikan layanan *flow control* yang dimiliki oleh pihak pengirim dan pihak penerima.
f. Memiliki fungsi *error detectioni*: pengirim dan penerima juga melengkapi data dengan sejumlah informasi yang bisa digunakan untuk memeriksa data yang dikirimkan bebas dari kesalahan.

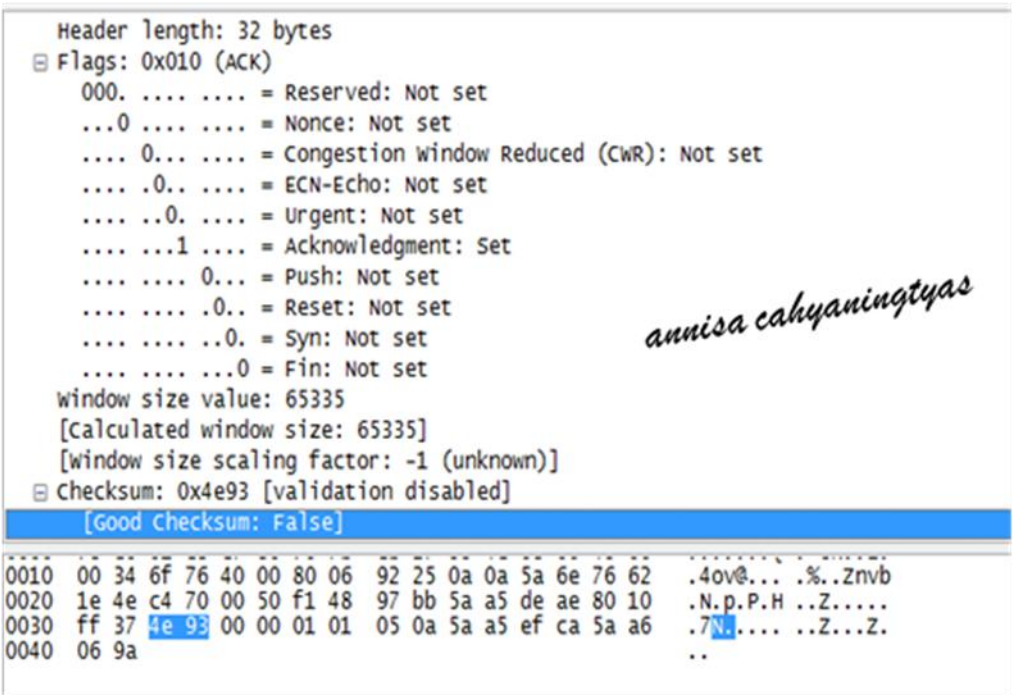
Proses pembuatan koneksi TCP disebut juga dengan "Three-way Handshake". Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor acknowledgement yang dikirimkan oleh kedua pihak, dan prosesnya dapat digambarkan sebagai berikut:

a. *User* pertama (yang ingin membuat koneksi) akan mengirimkan sebuah segmen TCP dengan flag SYN diaktifkan kepada *user* kedua (yang akan diminta untuk berkomunikasi).
b. *User* kedua akan menjawabnya permintaan tersebut dengan mengirimkan segmen berisi *acknowledgment* dan juga SYN kepada *user* pertama.
c. *User* pertama selanjutnya akan mulai saling bertukar data dengan *user* kedua.

TCP menggunakan proses jabat tangan yang sama untuk mengakhiri koneksi yang dibuat. Hal ini menjamin dua *host* yang sedang terkoneksi tersebut telah menyelesaikan proses transmisi data dan semua data yang ditransmisikan telah diterima dengan baik. Dan itu alasan TCP memiliki koneksi yang *reliable* atau dapat diandalkan.

Berikut tampilan monitoring protokol TCP dengan meng-capture melalui Wireshark :





Tampilan capture di atas, adalah saat protokol TCP akan memulai melakukan hubungan (permintaan awal saat akan koneksi). Terlihat pada detail flags, bahwa belum mendapat banyak balasan atau informasi yang menandakan bahwa paket permintaan koneksi baru saja dikirim, namun sudah terlihat bahwa acknowledgment terlah diatur dalam kondisi '1' sebagai parameter pengecekan untuk hubungan komunikasi data selanjutnya. Pada capture lalu lintas paket data, diharapkan menghitaukan tampilan protokol lain yang ter-capture (HTTP). Sesuai dengan alur atau proses komunikasi TCP, yaitu Three-way Handshake.

2. User Datagram Protocol (UDP)

UDP (User Datagram Protocol) adalah protokol umum lainnya yang digunakan di Internet. Namun, UDP tidak pernah digunakan untuk mengirim data penting seperti halaman web, informasi database, dan lainnya. UDP biasa digunakan untuk streaming audio dan video, streaming media, dan lainnya, karena penggunaan UDP menawarkan kecepatan. Ini alasan UDP lebih cepat daripada TCP adalah karena tidak ada bentuk kontrol aliran atau koreksi kesalahan.

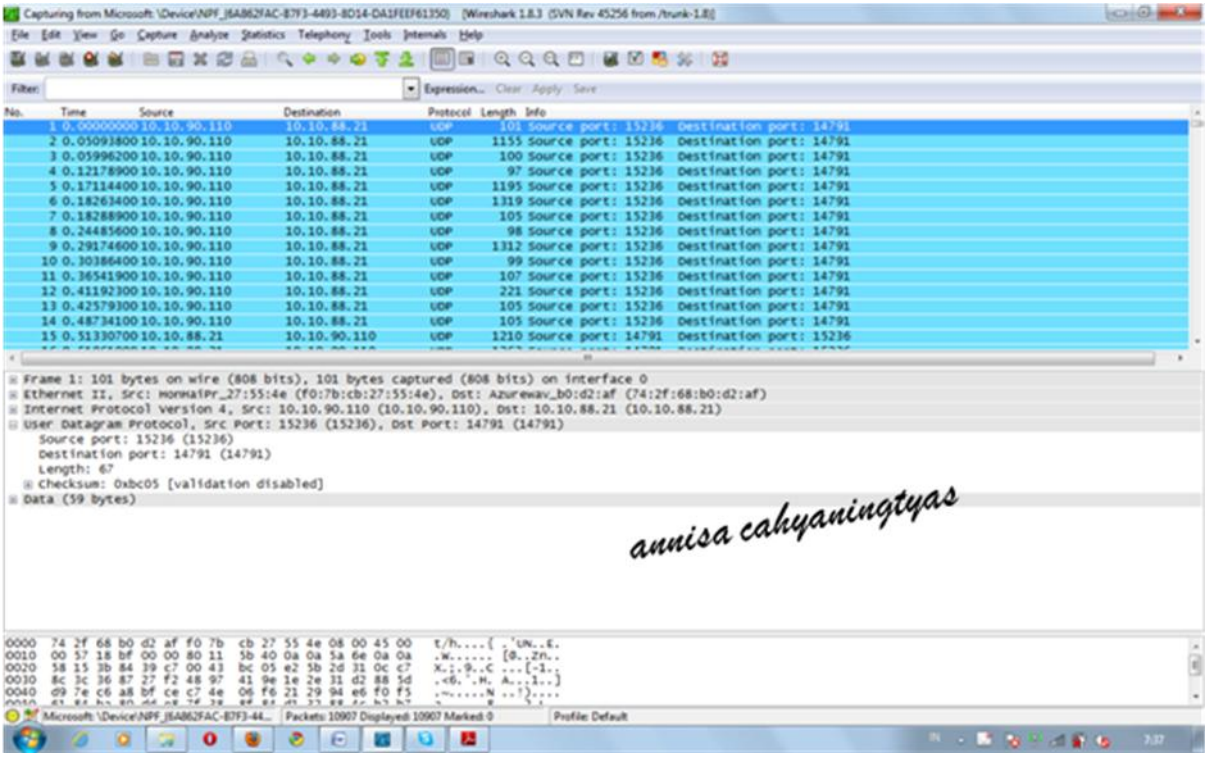
UDP adalah TCP yang connectionless. Hal ini berarti bahwa suatu paket yang dikirim melalui jaringan dan mencapai komputer lain tanpa membuat suatu koneksi. Sehingga dalam perjalanan ke tujuan paket dapat hilang karena tidak ada koneksi langsung antara kedua host, jadi UDP sifatnya tidak realibel

.

Karakteristik UDP:

a. *Connectionless* (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negoisasi/konfirmasi koneksi antara dua host yang hendak bertukar informasi. Sehingga dalam perjalanan ke tujuan paket dapat hilang karena tidak ada koneksi langsung
b. *Unreliable* (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment.

Berikut tampilan monitoring protokol TCP dengan meng-capture melalui Wireshark :



Berdasarkan tampilan capture melalui Wireshark, saat host pertama (IP: 10.10.90.110) ingin melakukan hubungan koneksi dengan host kedua (IP: 10.10.88.21), karena menggunakan UDP maka langsung terbentuk koneksi tanpa harus melakukan ijin koneksi seperti TCP. Atau secara sederhana, pada UDP koneksi langsung terhubung atau tidak terlalu rumit jika dibandingkan dengan TCP yang sangat rumit. Dan pada UDP, selain dapat terhubung langsung tanpa harus negosiasi terlebih dahulu, komunikasi data dapat terus berjalan secara kontinyu meeskipun tidak tahu apakah terdapat kesalahan pengiriman atau penerimaan paket data, atau kesalahan lainnya karena UDP tidak disertai error control. Pada tampilan di atas, terjadi komunikasi data yaitu streaming yang hanya membutuhkan kecepatan bukan kehandalan.

Biografi Penulis

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