Analisis Paket Data Wireshark

Nama: Thomi Irfansyah

NIM :09031381419093

Kelas: SIBIL 4A

Jurusan Sistem Informasi – Fakultasl Imu Komputer

Universitas Sriwijaya

2016

Analisa Paket Data Menggunakan Wireshark

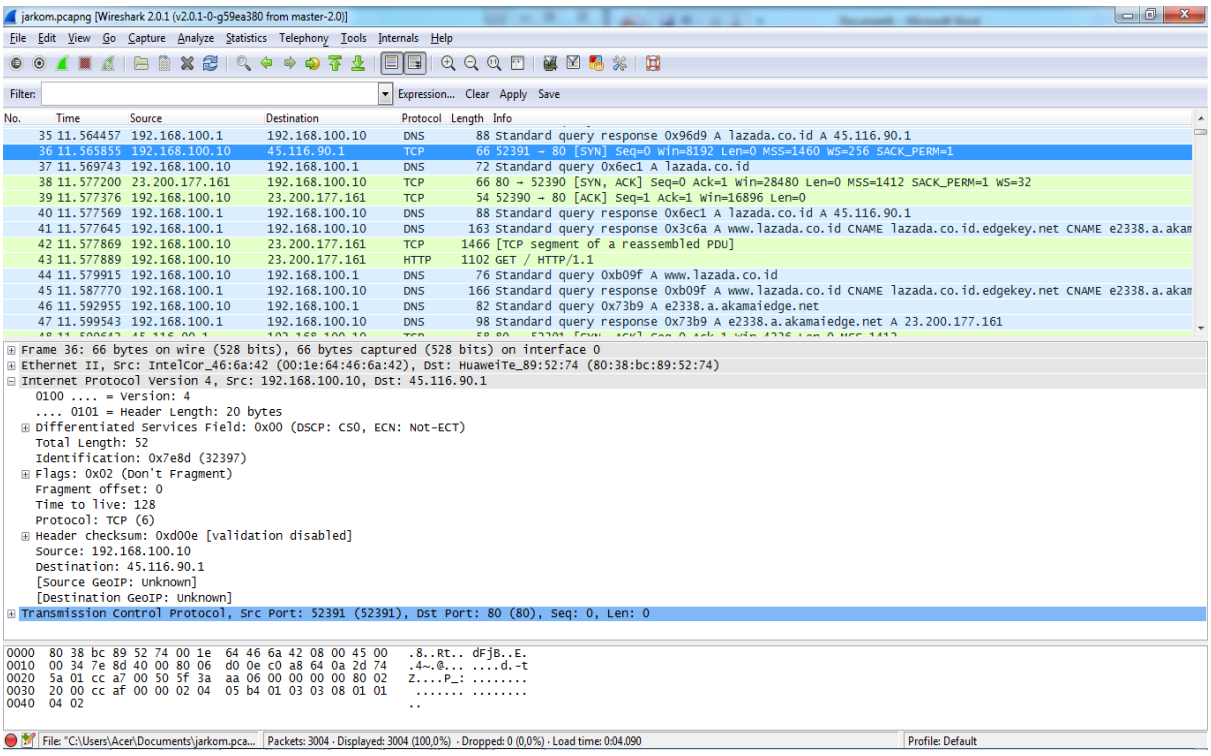
Wireshark adalah penganalisa jaringan data. Penganalisa kinerja jaringan itu melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang lewat dalam jaringan. Penangkapan data serta menampilkannya secara reltime.

IP address komputer yang akan digunakan

```
C:\Users\Acer>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection 7:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f59d:3882:7b5d:3a26%21
   IPv4 Address. . . . . . . . . . . : 192.168.100.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1

Ethernet adapter Local Area Connection 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{6058DD3A-C7B0-41B0-95CD-237842439523}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Bagian Pertama

Pada bagian pertama menunjukan penggunaan wireshark dengan membuka sebuah website yaitu request dari komputer ke www.lazada.co.id



Gambar 1

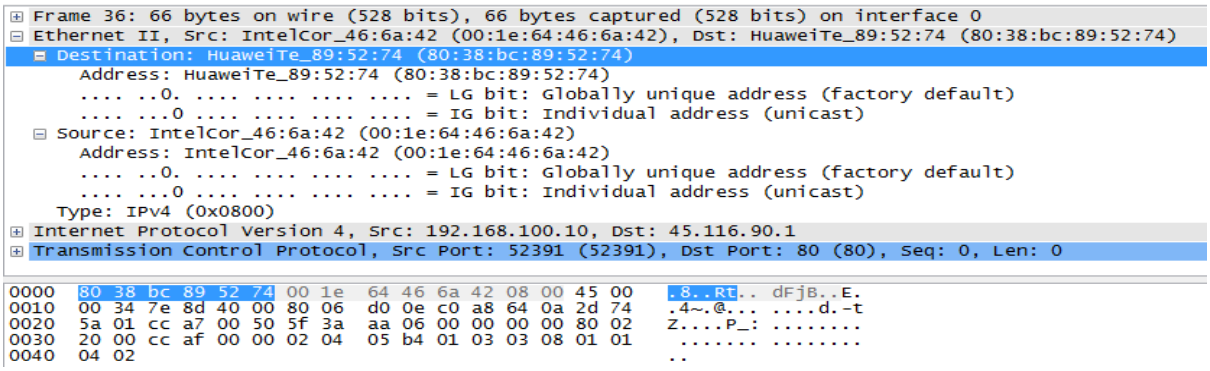
Pada gambar 1 menunjukan bahwa sebuah komputer dengan IP address 192.168.100.10 saat memasukan www.lazada.co.id maka akan terjadi pengiriman paket data dari computer menuju ke server dan selanjutnya data tersebut akan dikirim ke DNS untuk mengetahui IP nya. IP akan diterjemahkan oleh DNS dan DNS akan mengirimkan kembali ke komputer yaitu IP website yang telah diterjemahkan. Kemudian setelah dilakukan terjemahan dari www.lazada.co.id menjadi 45.116.90.1 yang merupakan IP lazada.co.id maka setelah itu komputer dengan IP 192.168.100.10 melakukan request ke destimation 45.116.90.1 dengan menggunakan protocol TCP.

TCP adalah suatu protokol pengiriman data yang berbasis Internet Protocol (IP) dan bersifat connection oriented.

Pada bagian Internet Protocol Version dapat terlihat bahwa header length nya adalah 20 bytes, source port adalah 52391

Flag yang terdapat pada wireshark

- Flag URG berfungsi untuk diidentifikasi bahwa bagian dari TCP itu mengandung data yang sangat penting.
- Flag ACK berfungsi untuk mengetahui apakah yang dikirimkan sudah diterima atau belum dikomputer client.
- Flag PSH berfungsi untuk mengindikasi isi dari TCP yang diterima dikomputer client. Jika PSH bernilai 1 maka data tidak boleh satu byte pun hilang, jika hilang maka data akan dikirim ulang.
- Flag RST berfungsi untuk mengidentifikasi koneksi yang dibuat akan gagal.Untuk sebuah koneksi TCP yang sedang berjalan (aktif), sebuah segmen dengan flag RST diset ke nilai 1 akan dikirimkan sebagai respons terhadap sebuah segmen TCP yang diterima yang ternyata segmen tersebut bukan yang diminta, sehingga koneksi pun menjadi gagal
- Flag SYN berfungsi untuk mengindikasi bahwa segmen TCP yang bersangkutan mengandung Initial Sequence Number (ISN). Selama proses pembuatan sesi koneksi TCP, Jika melakukan request maka akan memberikan nilai SYN bernilai 1
- Flag FIN berfungsi untuk menandakan bahwa pengirim segmen TCP telah selesai dalam mengirimkan data dalam sebuah koneksi TCP. Ketika sebuah koneksi TCP akhirnya dihentikan (akibat sudah tidak ada data yang dikirimkan lagi), setiap host TCP akan mengirimkan sebuah segmen TCP dengan flag FIN diset ke nilai 1



Gambar 2

Pada gambar 2, terlihat pada bagian Ethernet II bahwa source (192.168.100.10) memiliki mac address 80:38:bc:89:52:74 dan pada destination (45.116.90.1) memiliki mac address 00:1e:64:46:6a:42

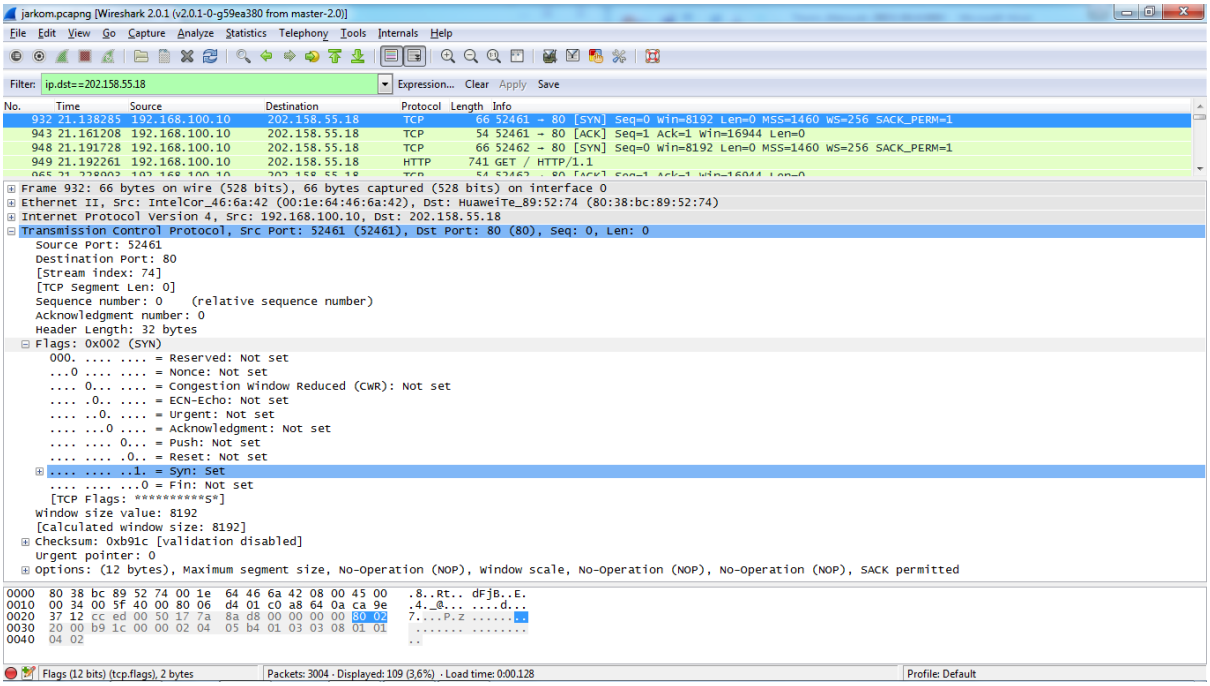
```
C:\Users\Acer>tracert lazada.co.id

Tracing route to lazada.co.id [45.116.90.1]
over a maximum of 30 hops:

  1    12 ms    42 ms     3 ms  192.168.100.1
  2     7 ms     8 ms     8 ms  10.37.0.1
  3    33 ms    33 ms    33 ms  172.16.2.137
  4     *        *        *     Request timed out.
  5    30 ms     *       29 ms  11.1.1.1
  6    25 ms    25 ms    25 ms  ip-27-50-30-185.cepat.net.id [27.50.30.185]
  7    32 ms    31 ms    32 ms  lazada.openixp.net [218.100.36.53]
  8     *        *        *     Request timed out.
  9    32 ms    33 ms    32 ms  45.116.90.1

Trace complete.
```

Gambar 3

Pada gambar 3 dilakukan percobaan tracert pada lazada.co.id untuk mengetahui jumlah loncatan (Hops) yang terjadi, dan pada gambar tersebut dapat terlihat bahwa terjadi 9 Hops. Koneksi yang digunakanpun cukup stabil. Waktu dalam satuan ms (millisecond) sama seperti halnya Hops, semakin kecil waktu perpindahan data maka kecepatan anda semakin baik dan cepat dalam mengakses situs yanf anda traceroute.

Tetapi jika anda melihat pada hasil tracert ada tanda * atau pesan “request timed out” pada hasil tracert anda, maka disitulah masalah yang ada pada koneksi internet anda.

Bagian Kedua



Gambar 4

Pada gambar 4, dapat diketahui bahwa sebuah komputer dengan IP address source 192.168.100.10 mengirim paket data yang akan menuju IP address destination 202.158.55.18. IP address tersebut merupak IP milik website kedua yang telah dibuka yaitu www.jasaraharja.co.id .

Wireshark menunjukan bahwa IP address yang muncul pertama kali adalah IP dari website yang pertama kali di request di browser yaitu www.lazada.co.id dan setelah itu baru muncul IP address dari website kedua yaitu www.jasaraharja.co.id .

```
C:\Users\Acer>tracert jasaraharja.co.id

Tracing route to jasaraharja.co.id [202.158.55.18]
over a maximum of 30 hops:

  1     6 ms     6 ms     5 ms  192.168.100.1
  2     8 ms     8 ms     8 ms  10.37.0.1
  3    31 ms    29 ms    31 ms  172.16.2.94
  4     *        *        *     Request timed out.
  5    16 ms     *       18 ms  11.1.1.1
  6    19 ms    25 ms    20 ms  ip-27-50-30-185.cepat.net.id [27.50.30.185]
  7    23 ms    22 ms    25 ms  cbn.openixp.net [218.100.36.36]
  8    29 ms    29 ms    39 ms  210.210.161.177.cbn.net.id [210.210.161.177]
  9    20 ms    20 ms    33 ms  210.210.161.20.cbn.net.id [210.210.161.20]
 10    24 ms    53 ms    80 ms  ip55-18.cbn.net.id [202.158.55.18]

Trace complete.
```

Gambar 5

Percobaan tracert pada website Jasaraharja.co.id menunjukan koneksi yang digunakan kurang stabil. Kita dapat melihat bahwa terjadi 10 Hops (loncatan). Waktu dalam satuan ms (millisecond) sama seperti halnya Hops, semakin kecil waktu perpindahan data maka kecepatan anda semakin baik dan cepat dalam mengakses situs yanf anda traceroute.

Tetapi jika anda melihat pada hasil tracert ada tanda * atau pesan “request timed out” pada hasil tracert anda, maka disitulah masalah yang ada pada koneksi internet anda.