

# **Analisis hasil capture, Follow stream, dan Flow Graph Jaringan menggunakan aplikasi Wireshark dan VisualRoute**



**Disusun Oleh:**

**NAMA : Robby Tri Putra**

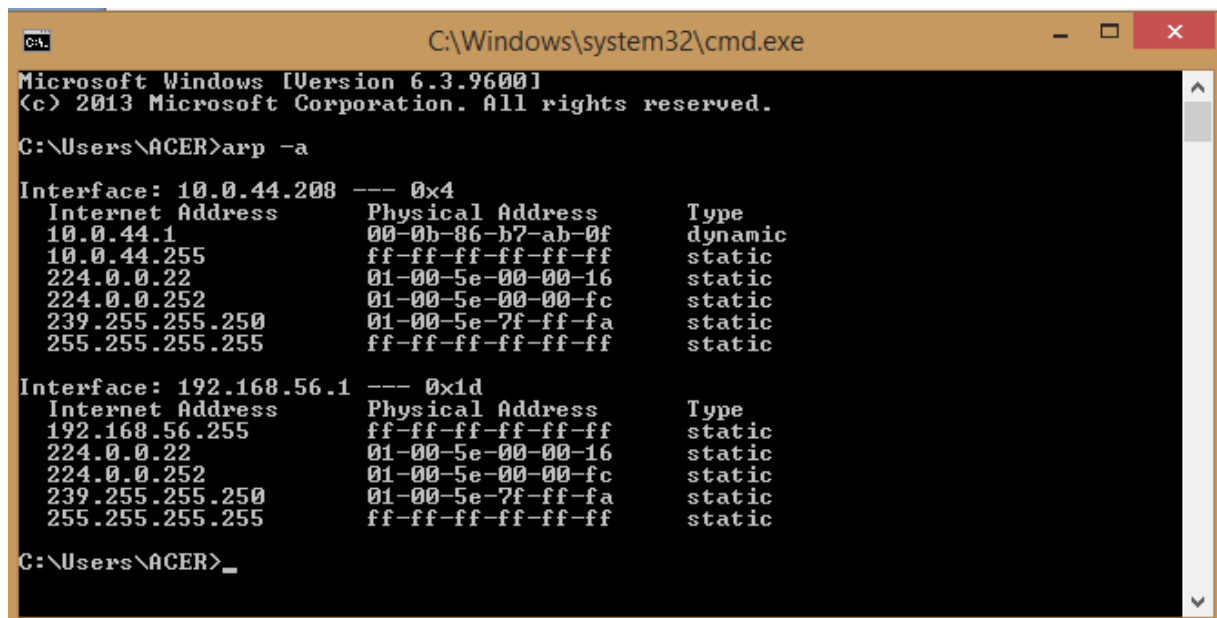
**NIM : 09011381621099**

**KELAS : SK4B**

**UNIVERSITAS SRIWIJAYA  
FAKULTAS ILMU KOMPUTER  
PRODI SISTEM KOMPUTER  
2018**

## BAGIAN ANALISIS PERTAMA “ANALISIS PAKET DATA”.

Dalam melakukan pengecekan analisis data jaringan, Langkah pertama ialah harus mengetahui beberapa ip address yang sedang kita pakai.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ACER>arp -a

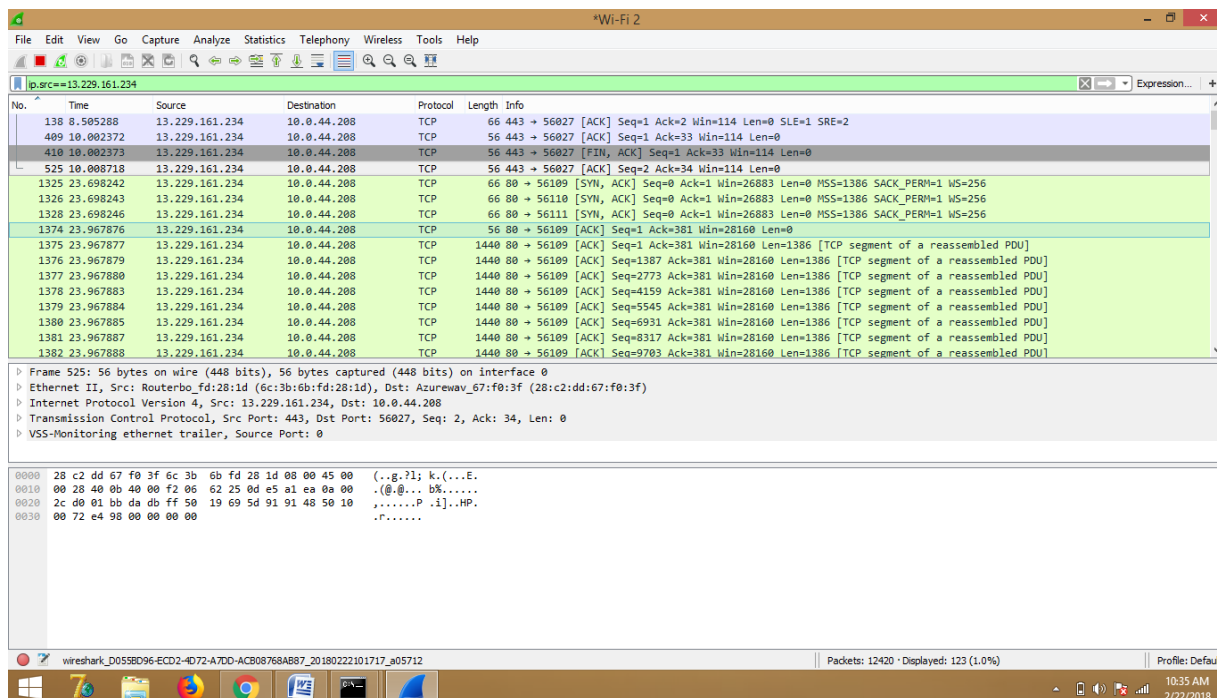
Interface: 10.0.44.208 --- 0x4
Internet Address      Physical Address      Type
10.0.44.1             00-0b-86-b7-ab-0f    dynamic
10.0.44.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x1d
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

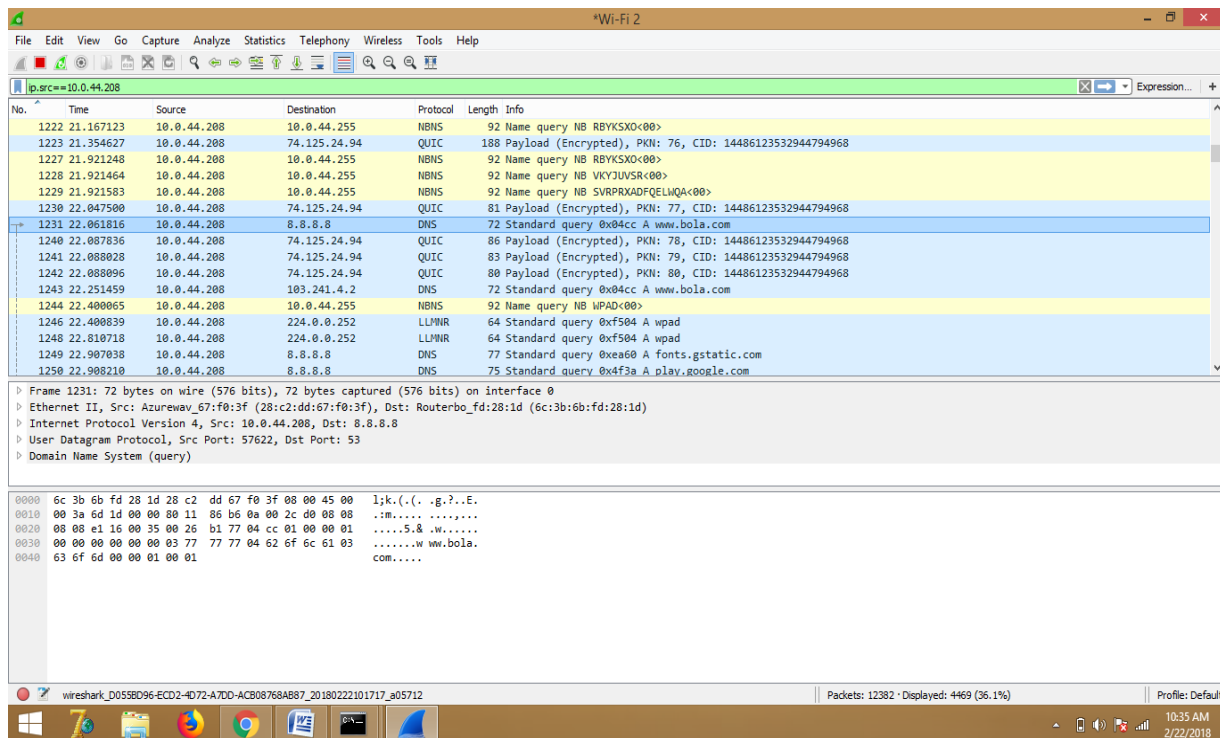
C:\Users\ACER>
```

Buka cmd lalu ketikkan perintah “arp -a”, maka secara otomatis ip address kita akan muncul seperti pada gambar diatas.

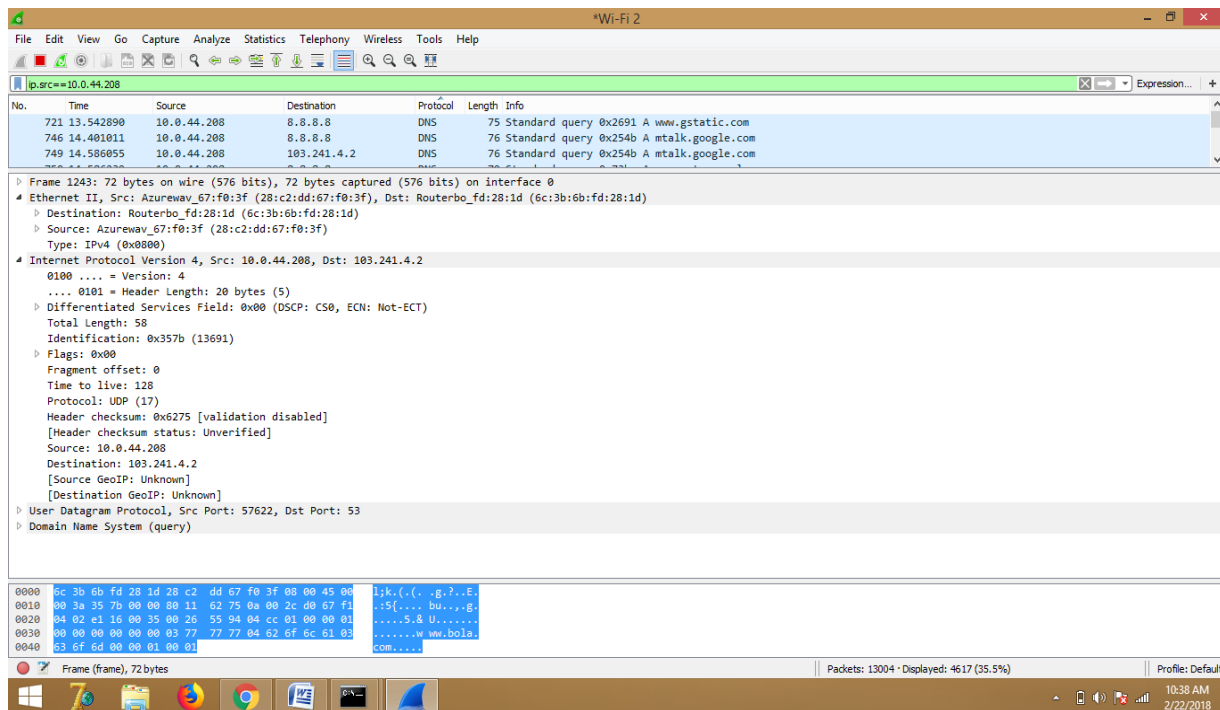
Setelah itu, langkah selanjutnya adalah membuka aplikasi **WIRESHARK**. Disini tersambung dengan jaringan Unsri.net



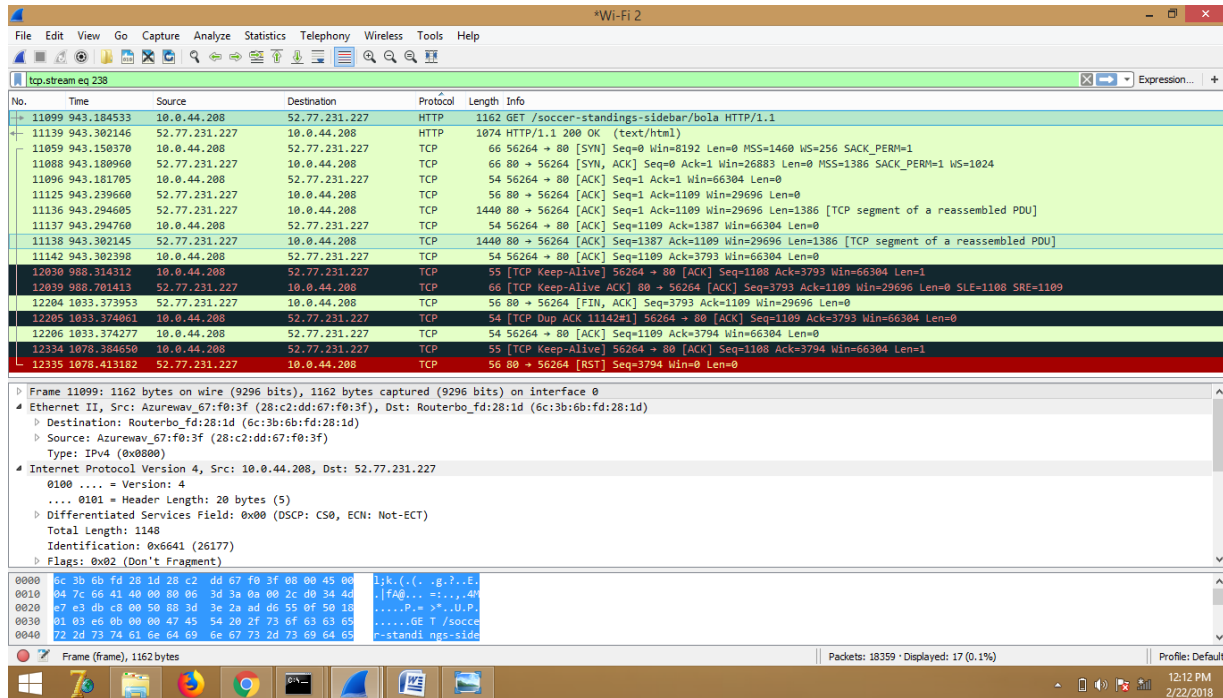
Dari gambar sebelumnya kita telah mendapatkan beberapa data dalam bentuk paket data jaringan. Karena semua paket data tersaring dengan cepat maka kita menggunakan filter terlebih dahulu menggunakan **“ip.src==10.0.44.208”**.



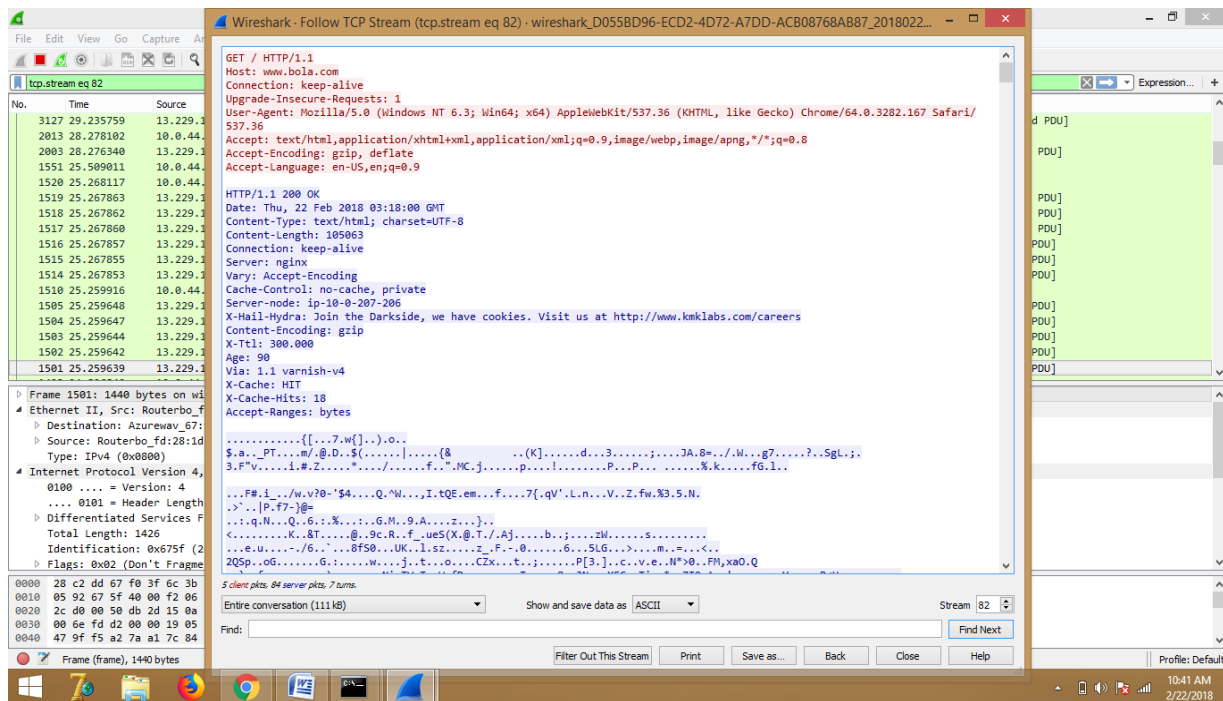
Dapat dilihat bahwa dengan computer yang beralamatkan ip 10.0.44.208 yang sedang mencoba mengakses website [www.bola.com](http://www.bola.com) atau beralamatkan ip 13.229.161.234 dengan menggunakan TCP protocol. Setelah itu jika kita mengklik bagian kotak tengah di menu Internet Protocol Version 4, maka akan menampilkan jika computer sedang mengakses web tersebut.



## BAGIAN KEDUA “DENGAN MENGGUNAKAN MENU FOLLOW STREAM”



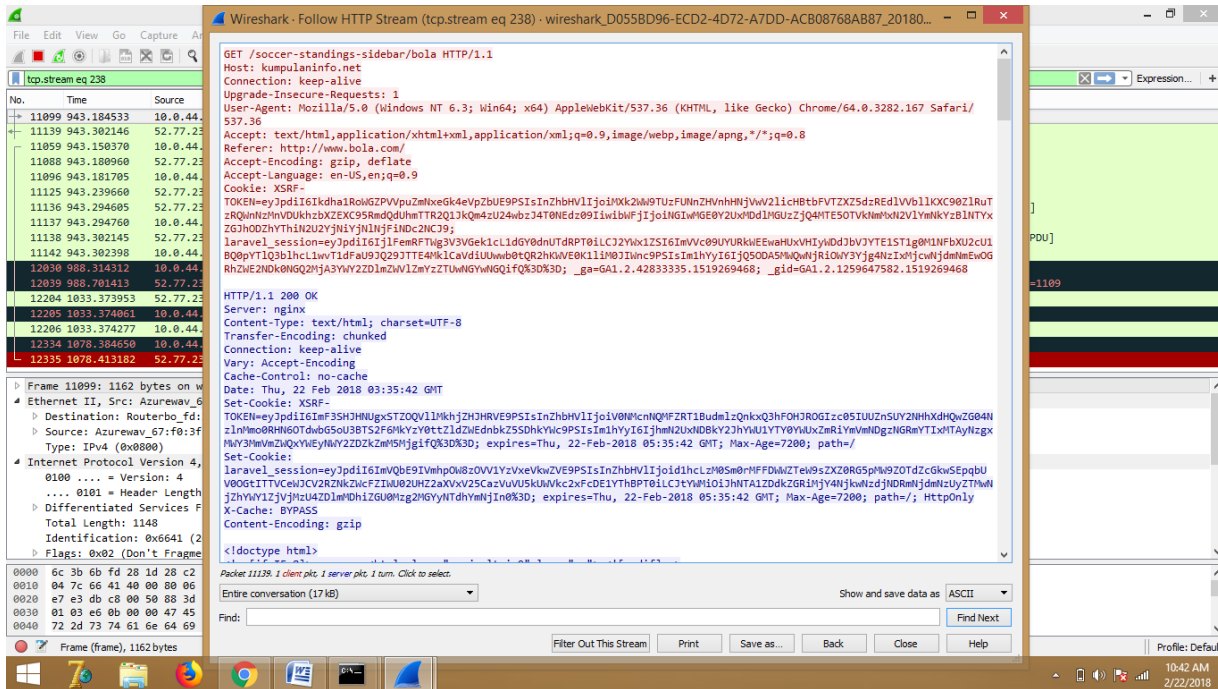
Seperti gambar di atas, pilih paket yang memiliki bentuk protocol http, dan klik **analyze=> pilih follow** dan => untuk pertama pilih bagian **TCP Stream** :



Bisa dilihat gambar di atas info apa saja yang dapat kita baca yaitu :

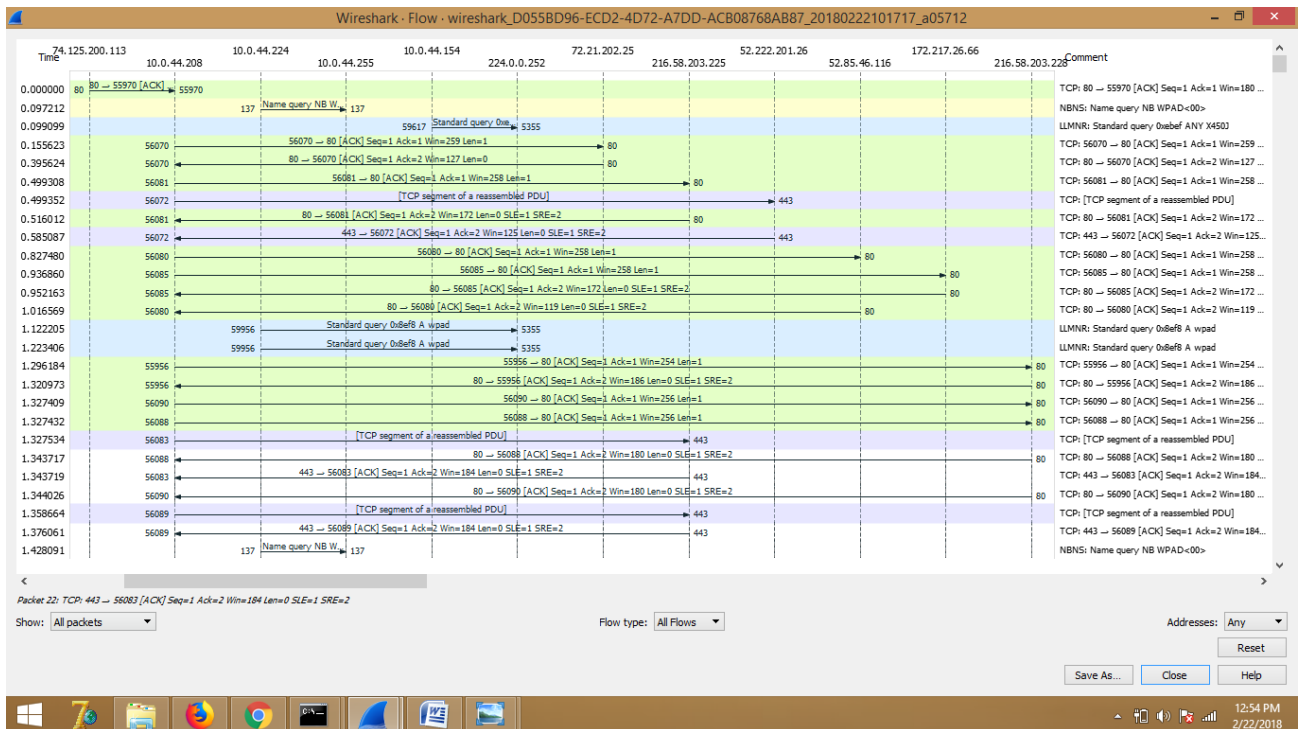
1. Sang pengguna yang sedang mengakses website [www.bola.com](http://www.bola.com) menggunakan aplikasi browser.
2. Waktu user mengakses web tersebut
3. Tipe data yang sedang diakses itu berupa text/html.

Untuk bagian keduanya kita gunakan kembali suatu pilihan yakni TCP Http :



### BAGIAN KETIGA “dan Flow Graph jaringan menggunakan aplikasi Wireshark dan visual route”

Kita mengklik menu statistics dan kita pilih flow graph maka data yang akan muncul akan seperti dibawah ini :

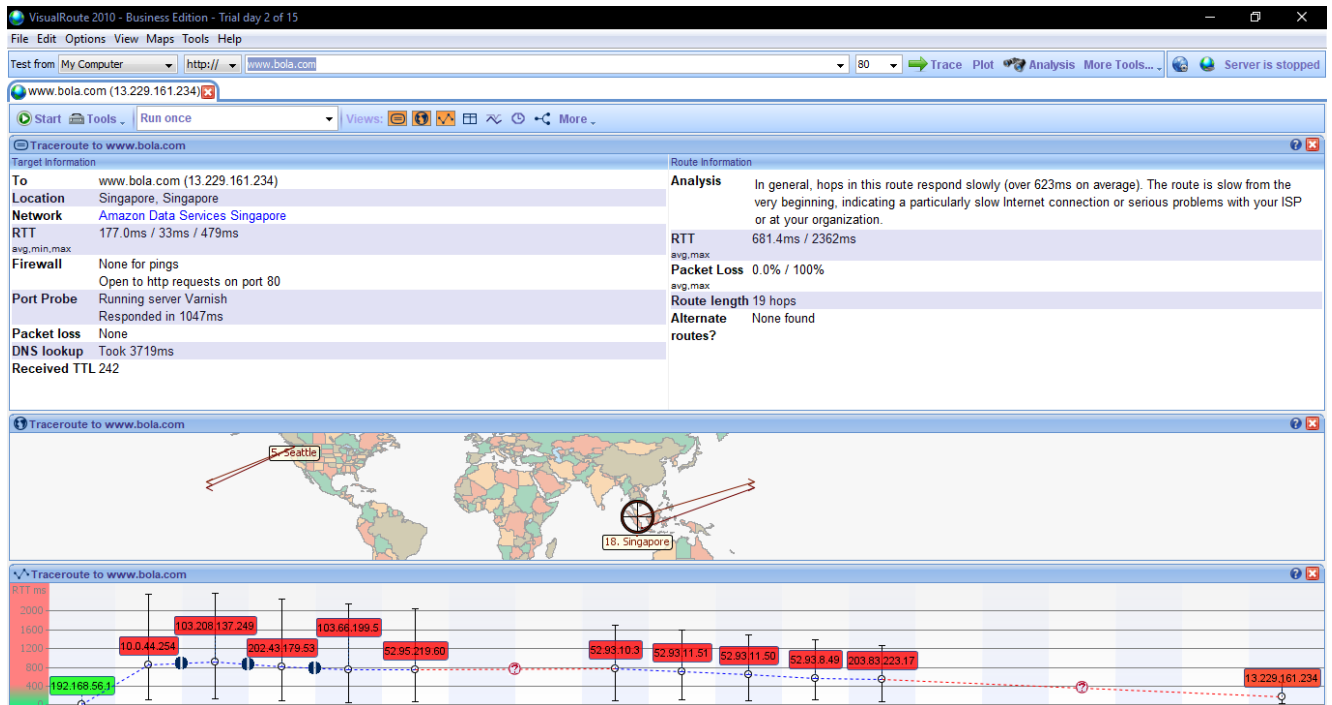


Lalu lintas berjalannya ekspedisi informasi dapat divisualisasikan menggunakan FlowGraph seperti gambar diatas. Berikut adalah penjelasan terhadap panah pada FlowGraph:

1. → 1 – computer user mengirim informasi address atau link ke router jaringan.

2. → 2 – ketika router menerima informasi, maka ia akan mengkasihkan alamat data tersebut.
3. → 3 – isp akan menanggapi permintaan user tersebut, apakah alamat yang dituju.
4. → 4 – apabila alamat tersedia, maka isp akan mengarahkan informasi tersebut ke isp pusat
5. → 5 – isp pusat pun akan menanggapi permintaan tersebut, dan informasi tanggapan akan dikirim kembali ke user.
6. → 6 – ketika informasi tersebut tidak valid atau address tersebut tidak ditemukan, maka user diharuskan mengirim ulang informasi yang valid. Dimana data tersebut akan kembali diperiksa oleh isp terdekat.
7. → 7 – jika informasi tersebut valid, isp akan kembali mengirimkan tanggapan dan mengarahkannya ke isp pusat.
8. → 8 – apabila isp pusat menanggapi informasi tersebut valid, maka kita akan diarahkan ke server perusahaan yang memberi isp bandwidth. Yang mana disini kita akan di arahkan ke link server cloud berikutnya.
9. → 9 – disini situs yang diakses adalah www.detik.com dengan mengambil berita International dan nasional
10. → 10 – seperti pada isp tadi, server pun akan mengirimkan informasi kepada user apakah address yang dituju tersebut valid atau tidak.

Di Bawah ini adalah tampilan dari aplikasi Visual Route :



Disini kita bias lihat sendiri perbedaan data yang diperoleh dari aplikasi wireshark dan aplikasi visualroute ini:

1. Pada aplikasi wireshark setiap lalu lintas perjalanan data dapat dilihat serta dianalis kemana dan apakah data tersebut memberi timbal balik kepada user, tentu saja dapat diambil satu point untuk

aplikasi ini yaitu sangat berguna bagi operator server atau server manager yang memiliki kemampuan expert dan para peneliti jaringan untuk mendapatkan data yang sangat mendetail, karena setiap hop terstruktur dengan rapi. Selain itu, aplikasi wireshark dapat memberikan fasilitas filter protocol sehingga dalam menganalisis data lebih effective dan akurat.

2. Sedangkan pada aplikasi visualroute akan dibagi menjadi:

Kelemahan :

- a. Kurang mendetailnya aliran data dari awal sesi hingga sampai ke destination atau tidak tersedianya fasilitas flow graph seperti wireshark.
- b. Tidak adanya filter protocol.
- c. Kurang mumpuni dalam mencapture data pada sebuah ip.

Kelebihan :

- a. Penggunaan yang mudah.
- b. Visualisasi tempat source dan destination terlihat jelas.
- c. Setiap hop ditampilkan semua dan panjang hopnya sudah ada di layar tampilan.