Analisis hasil Capture, Follow Stream, dan Flow Graph Jaringan menggunakan aplikasi Wireshark dan Visual Route

DISUSUN OLEH :

TIARA ANNISA DINA (09011381722124)

SK 2B

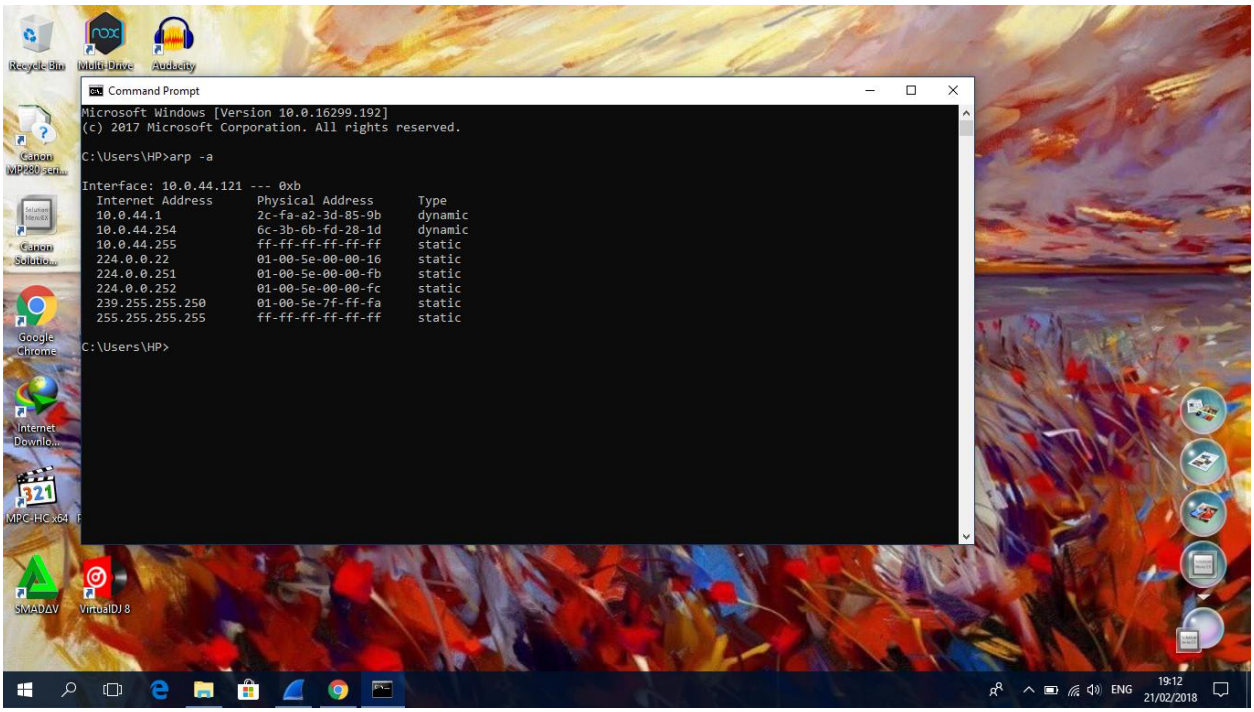
SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

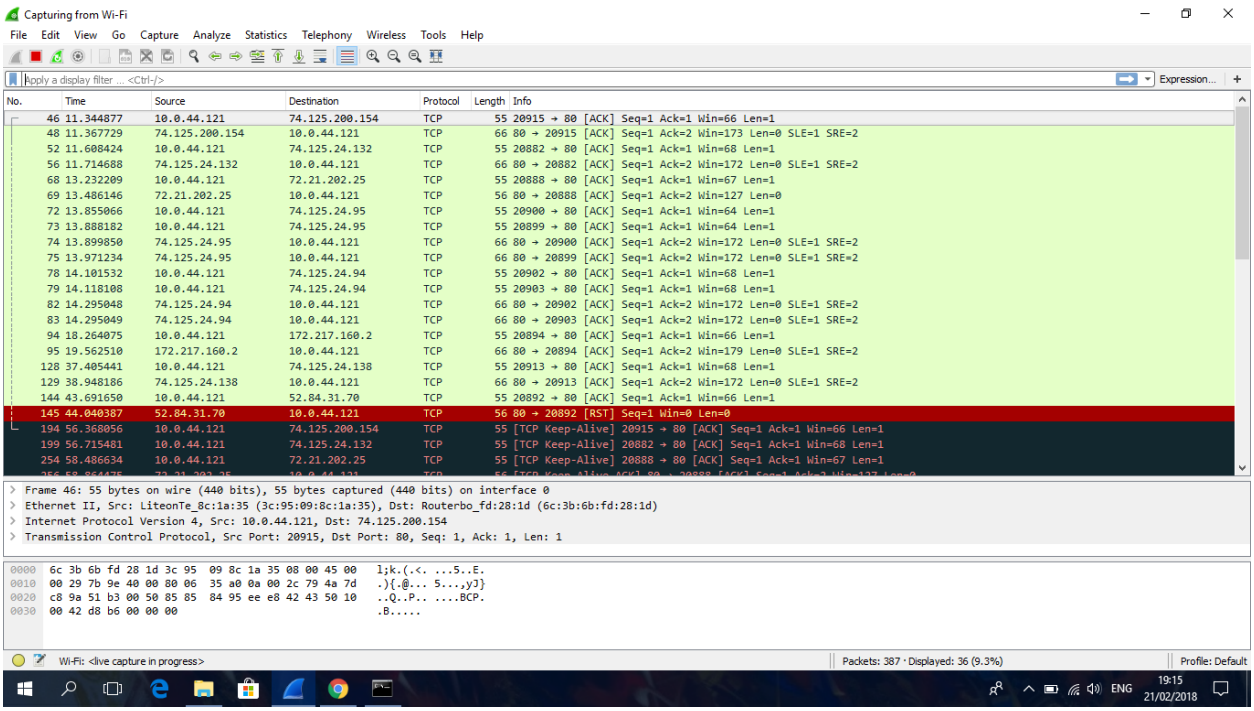
2018

1. BAGIAN PERTAMA “ANALISIS PAKET DATA”



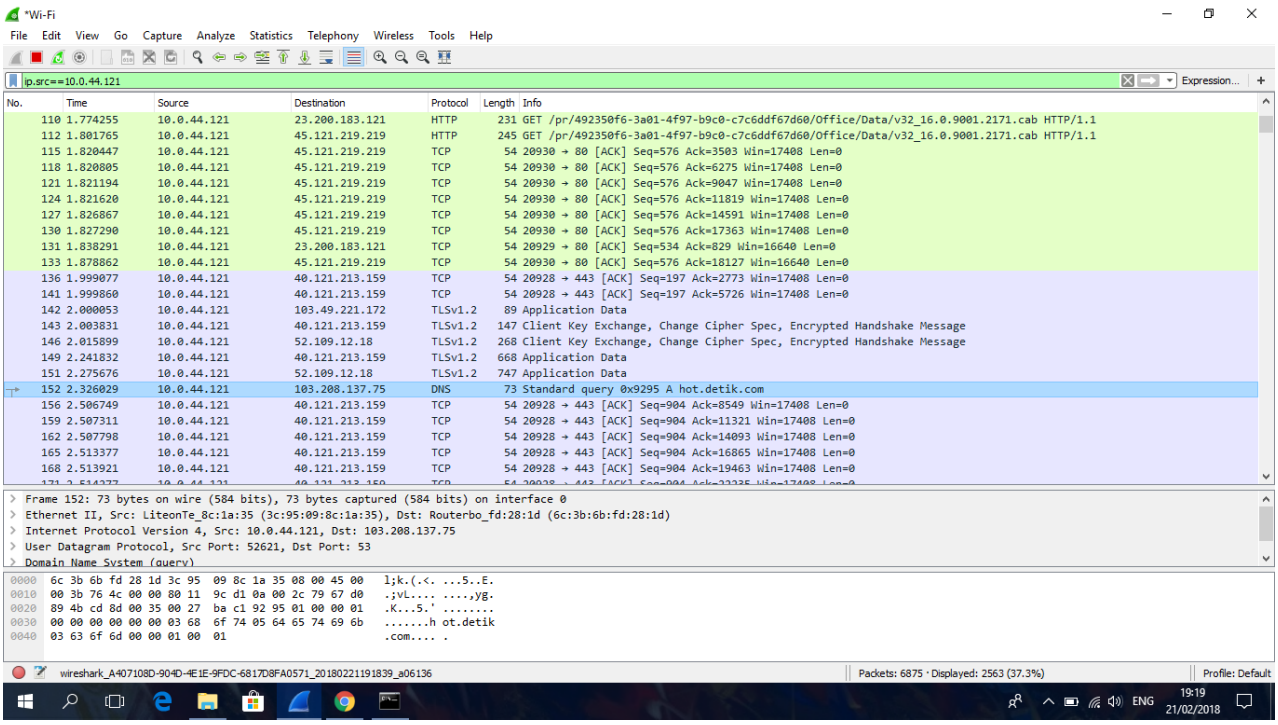
Langkah pertama sebelum kita melakukan analisis paket data jaringan, kita harus terlebih dahulu mengetahui berapa ip address yang sedang kita pakai.

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

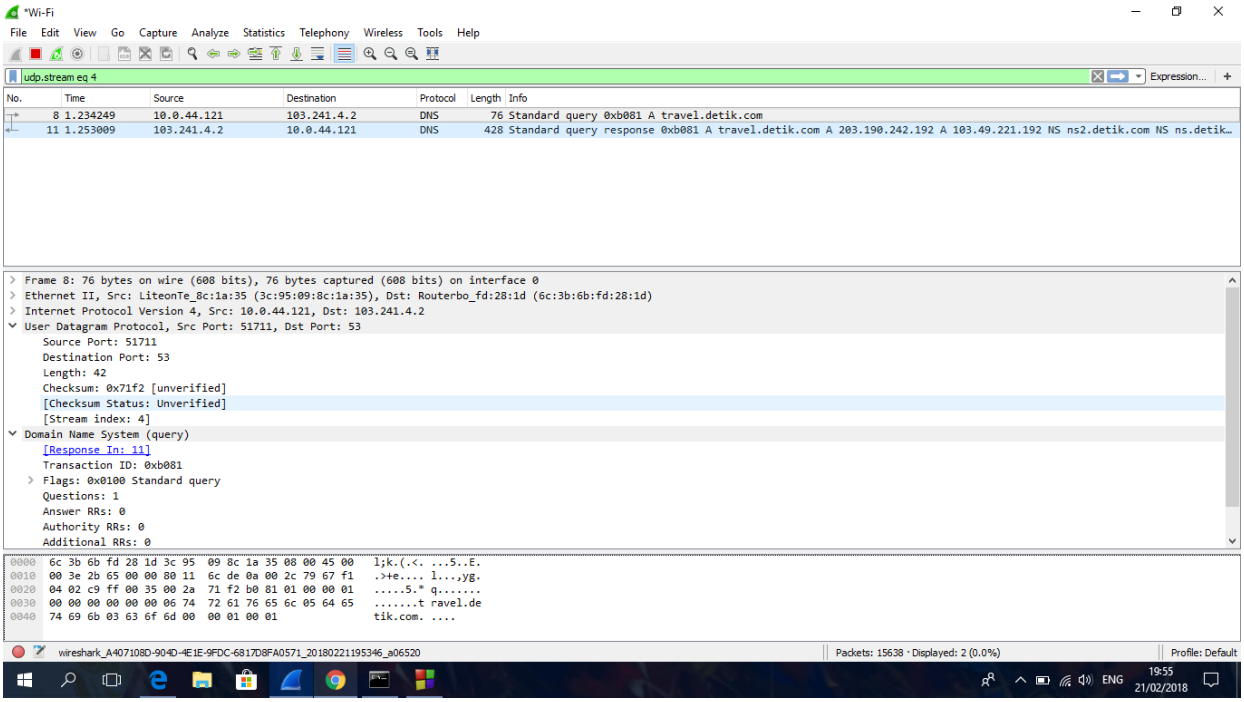


Setelah didapatkan, langkah selanjutnya adalah kita membuka aplikasi **WIRESHARK**. Saya menggunakan jaringan **Unsri.Net**.

Pada gambar diatas tadi telah kita dapatkan beberapa data dalam bentuk paket-paket data jaringan, dikarenakan semua paket tersaring dengan sangat cepat, maka ada baiknya kita filter terlebih dahulu dengan menggunakan sintaks "**ip.src==10.0.44.121**". Dan setelah kita filter maka akan terdapat lagi data yakni berupa :

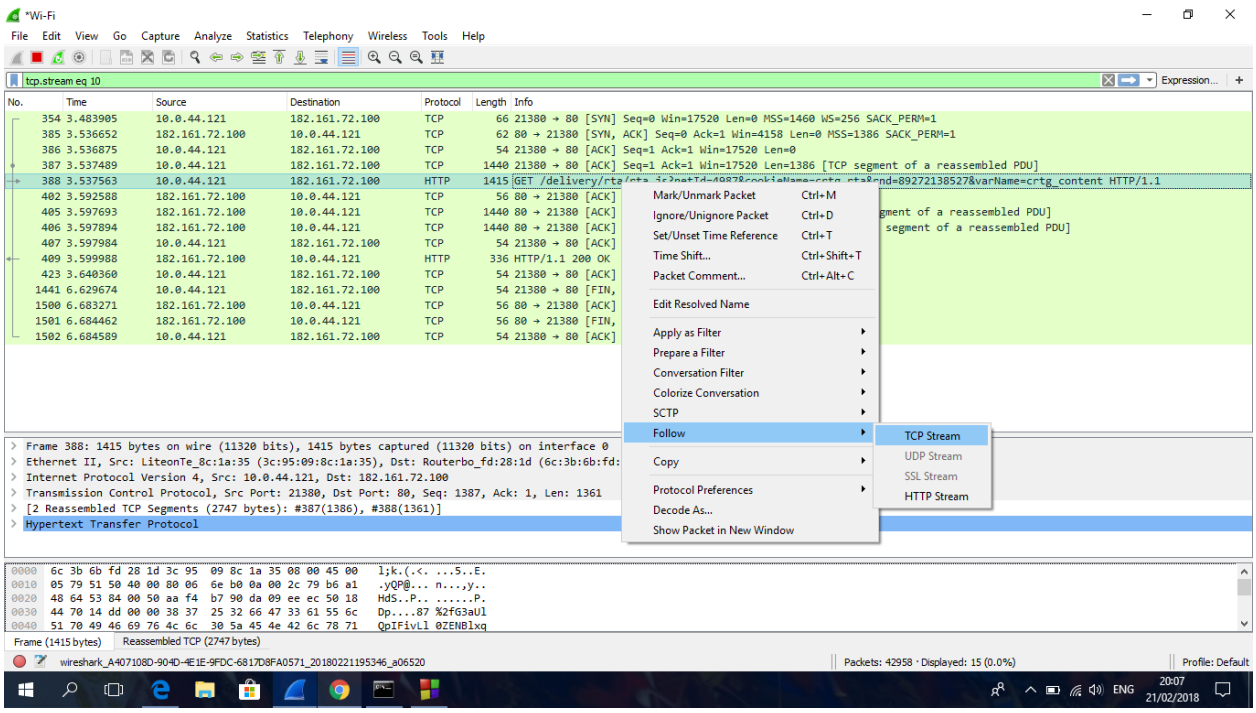


Dapat dilihat sendiri bahwa dengan komputer yang beralamatkan 10.0.44.121 sedang mencoba mengakses 168.235.193.143 atau website www.detik.com dengan menggunakan protokol TCP. setelah itu jika kita mengklik bagian kotak tengah di menu Internet Protocol Version 4.

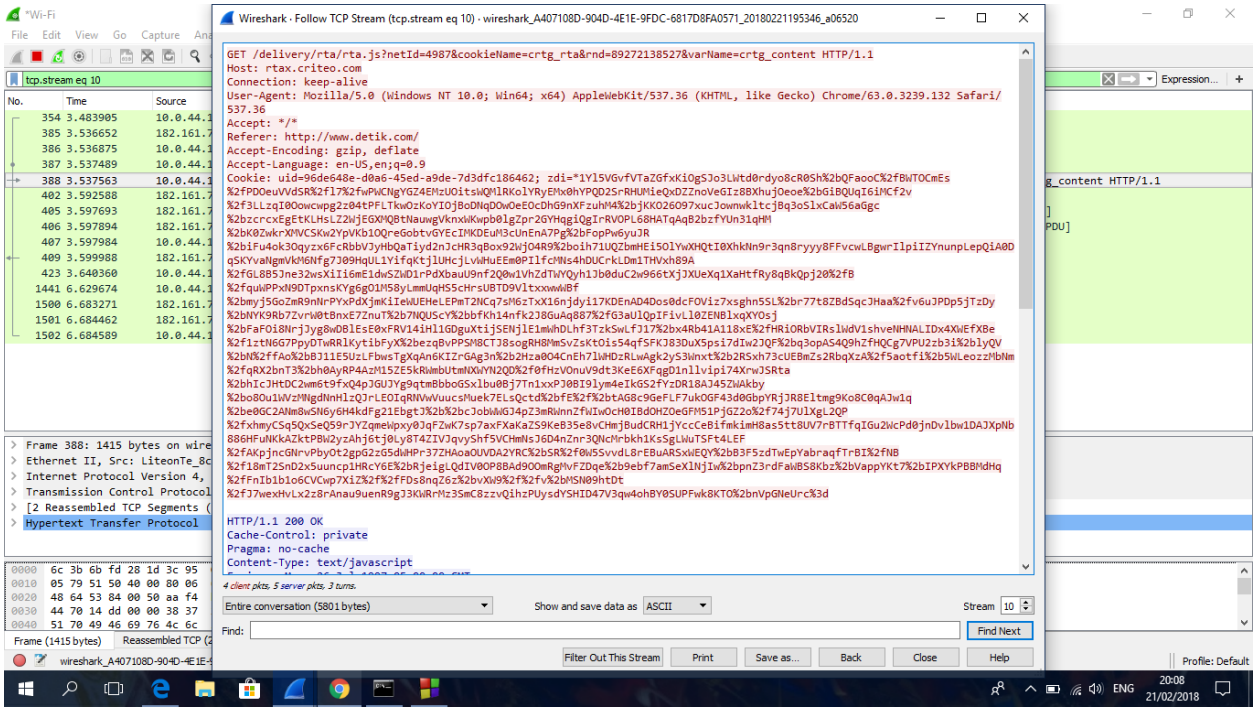


maka akan jelas jika komputer yang sedang mengakses web tersebut memiliki mac addres yakni 3c:95:89:8c:1a:35,sedangkan mac address dari routernya sendiri adalah 6c:3b:6b:fd:28:1d. Selain mendapatkan info mengenai mac addressnya kita disini juga dapat mengetahui bahwa panjang data yang terbaca yaitu sepanjang 53,dan menggunakan port yaitu 8.8.8.8

2. BAGIAN KEDUA “DENGAN MENGGUNAKAN MENU FOLLOW STREAM”



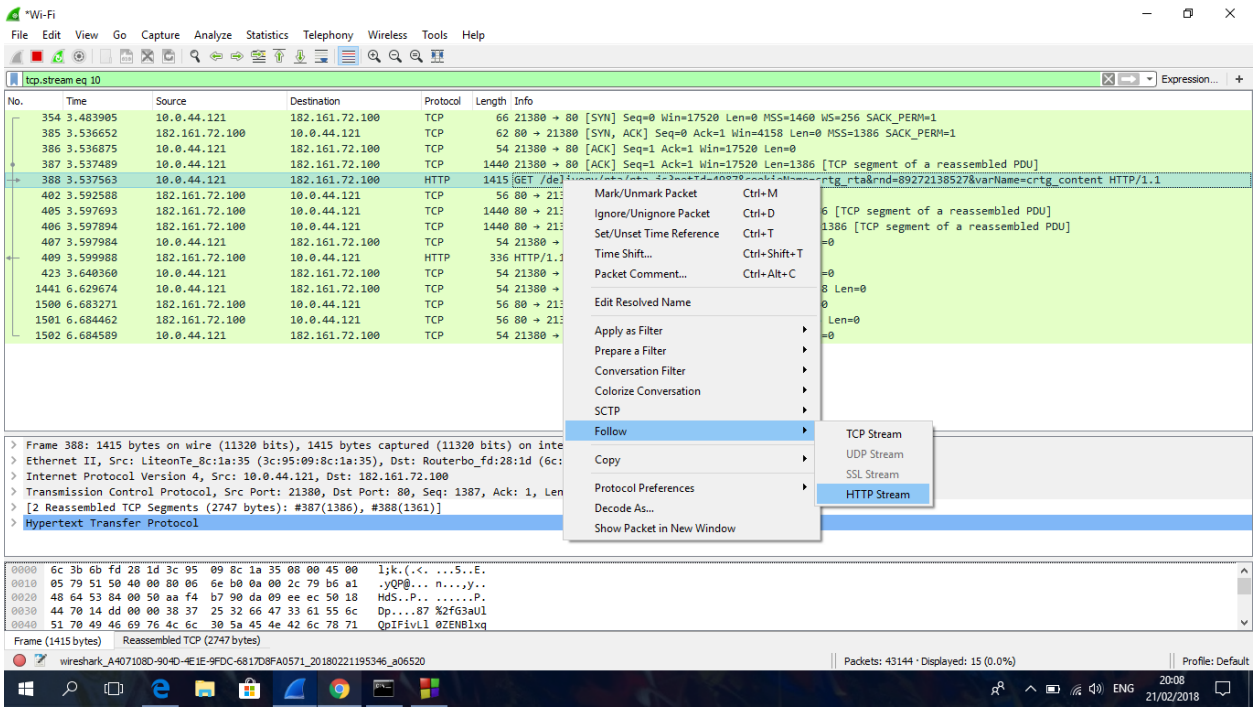
Seperti yang terlihat di gambar atas, pilih paket yang memiliki bentuk protokol http dan langsung klik **analyze** => pilih **follow** dan =>untuk pertama pilih bagian **TCP Stream** :



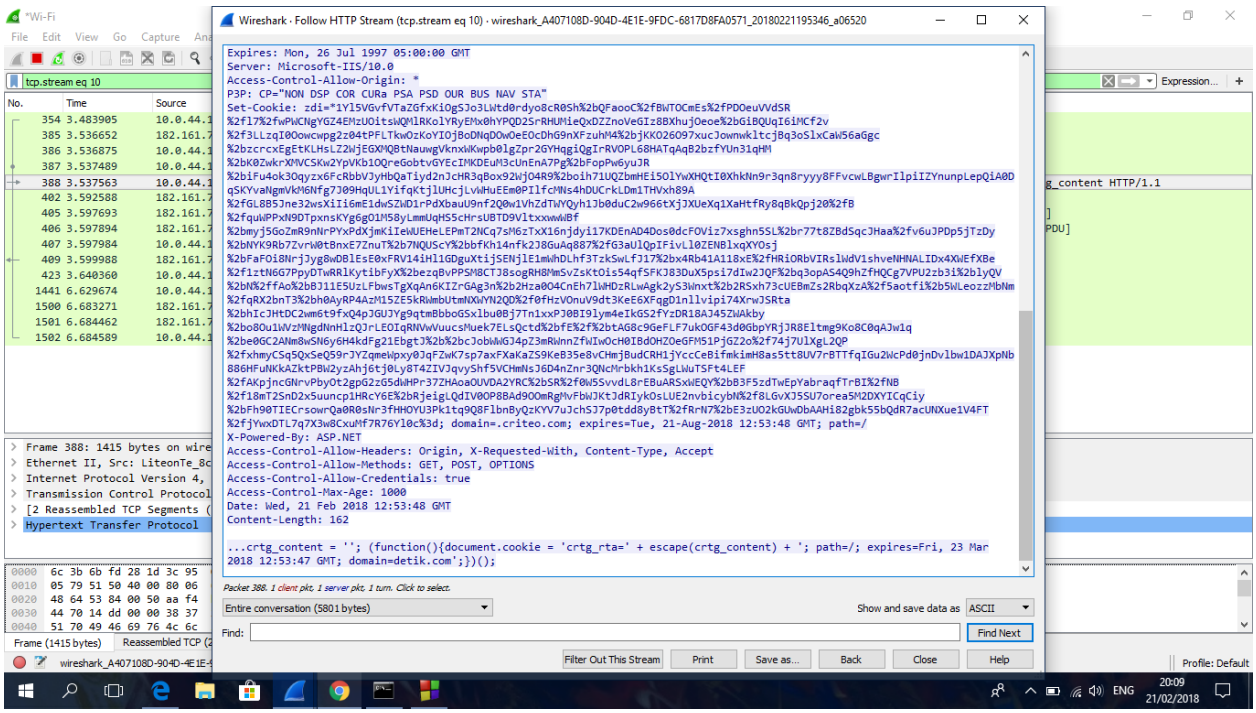
Bisa kita lihat diatas info apa saja yang telah dapat kita baca yakni :

1. Pengguna yang sedang mengakses website www.detik.com menggunakan aplikasi search engine Chrome.
2. Waktu user mengakses web tersebut pada tanggal 21 februari 2018 pada hari rabu.
3. Type data yang sedang diakses itu berupa text /html.

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



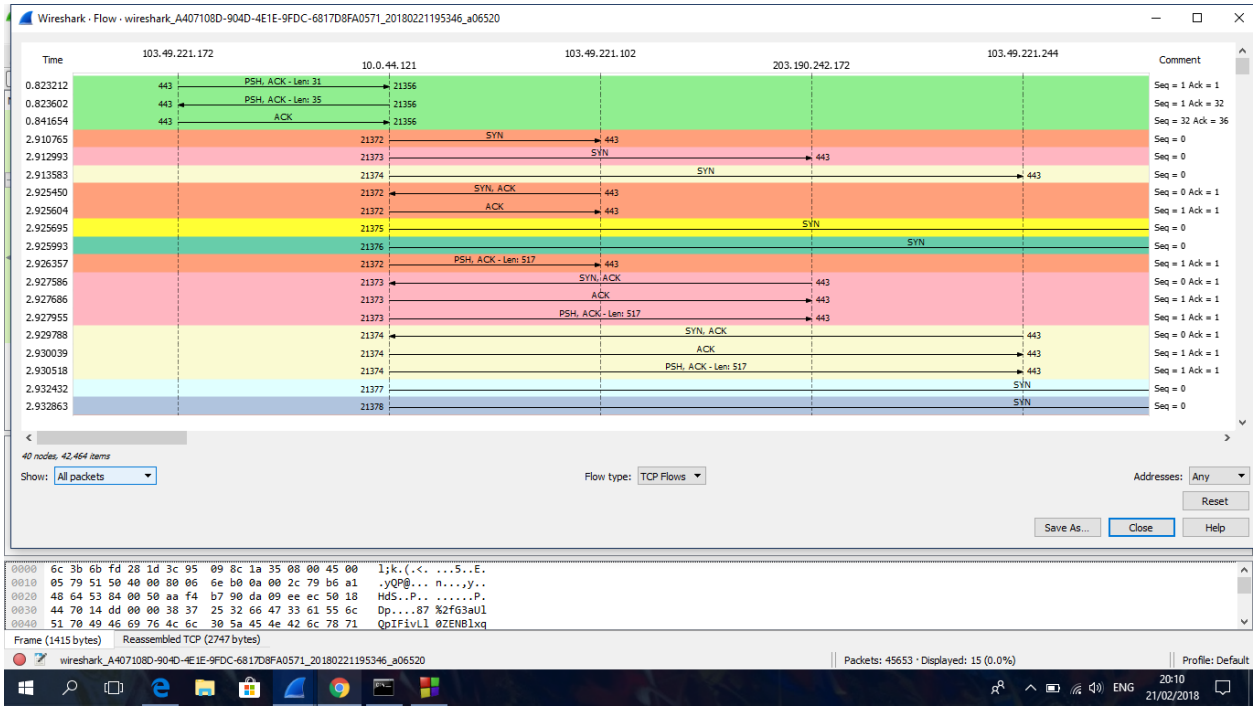
Dan saat kita memilih menu tersebut maka data yang di menu tcp stream tidak bisa terbaca akan terbaca di menu tcp http seperti berikut ini :



Datanya berupa teks atau html.

3. BAGIAN KETIGA “Flow Graph Jaringan menggunakan aplikasi Wireshark dan VisualRoute

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



Lalu lintas berjalannya ekspedisi informasi dapat divisualisasikan menggunakan Flow Graph seperti gambar diatas. Berikut adalah penjelasan terhadap panah pada flow graph:

1. Panah 1 – komputer user mengirim informasi address atau link ke router jaringan.
2. Panah 2 – ketika router menerima informasi, maka ia akan mengalamatkan data tersebut ke isp sumber terdekat (palembang).
3. Panah 3 – isp akan menanggapi permintaan user tersebut, apakah address yang dituju itu tersedia atau tidak.
4. Panah 4 – apabila address tesedia, maka isp akan mengarahkan informasi tersebut ke isp pusat (mis. Jakarta).
5. Panah 5 – isp pusat pun akan menanggapi permintaan tersebut, dan informasi tanggapan akan dikirim kembali ke user.
6. Panah 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.

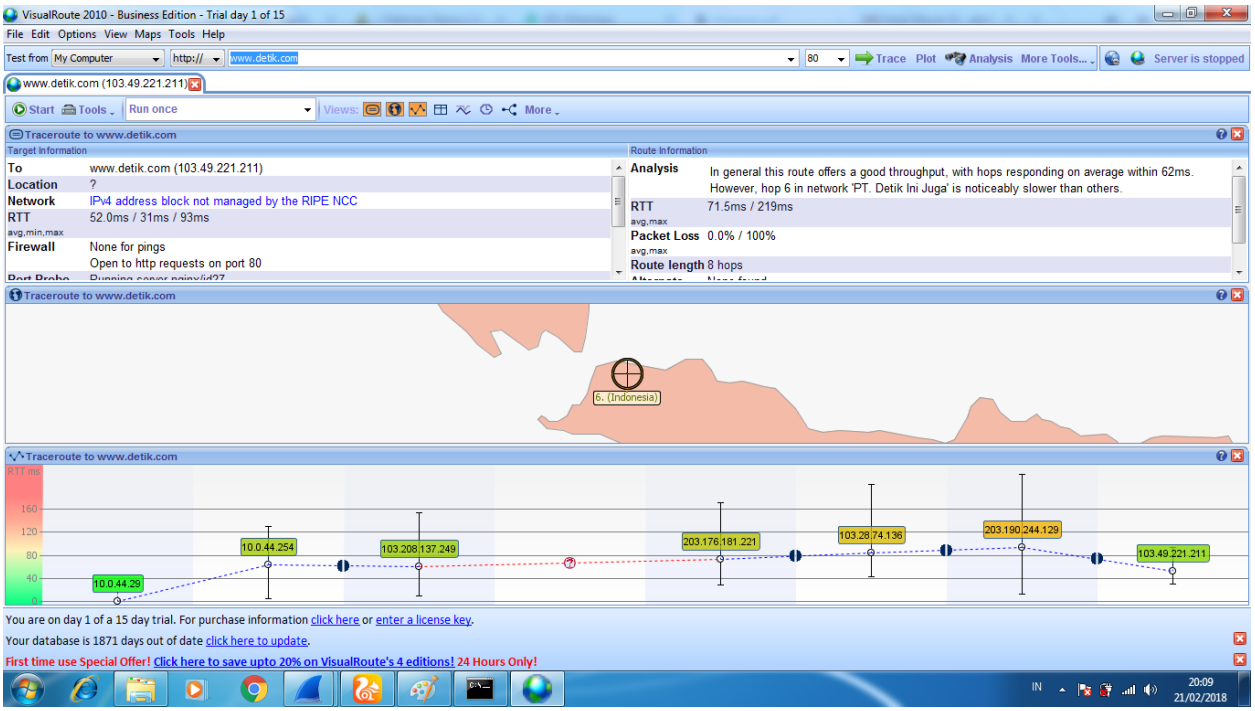
7. Panah 7 – jika informasi tersebut valid, isp akan kembali mengirimkan tanggapan dan mengarahkannya ke isp pusat.

8. Panah 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. Panah 9 – disini situs yang diakses adalah www.detik.com dengan mengambil berita International dan nasional

10. Panah 10 – seperti pada isp tadi, server pun akan mengirimkan informasi kepada user apakah address yang dituju tersebut valid atau tidak.

Dan berikut adalah tampilan dari aplikasi visualroute :



Dapat kita 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 menganalis 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. Dapat dimengerti oleh pengguna pemula.

c. Visualisasi tempat source dan destination terlihat jelas.

d. Setiap hope ditampilkan semua.