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

Disusun Oleh:
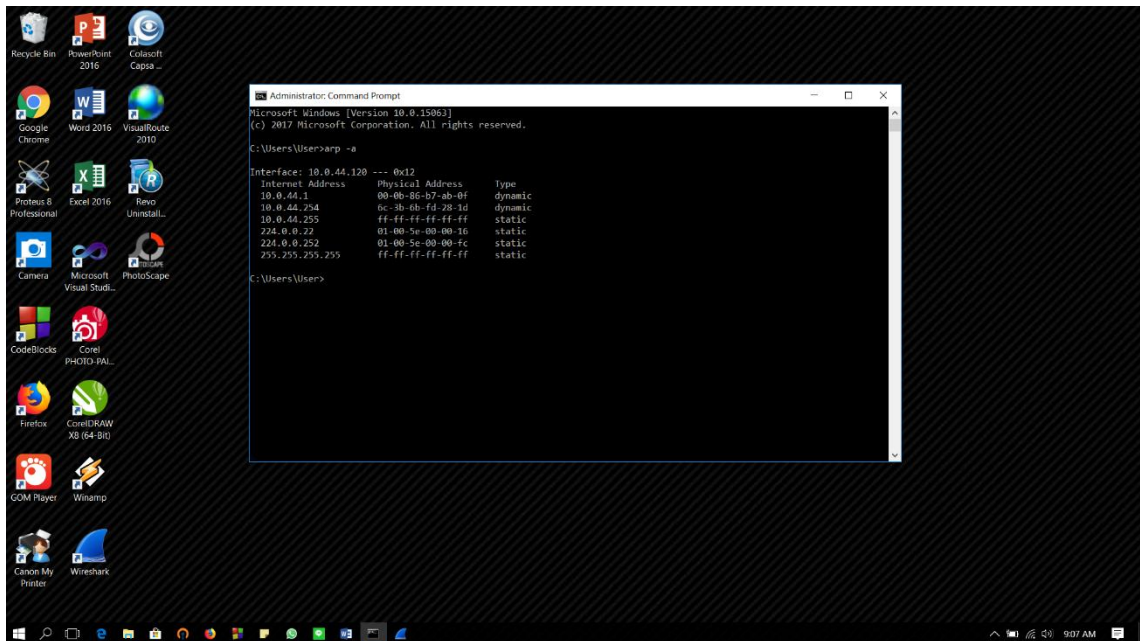
Nama   : Vanissa Wanika Siburian
NIM   : 09011381722094

Sistem Komputer
## Fakultas Ilmu Komputer
Universitas Sriwijaya
2017/2018

BAGIAN PERTAMA "Analisis Paket Data"
- ✓ Step pertama sebelum melakukan analisis paket data jaringan,kita terlebih dahulu berapa IP Address yang sedang kita pakai.


Cara mengetahui IP Address kita buka cmd lalu ketikan perintah "*arp –a*", maka secara otomatis IP Address yang kita pakai akan muncul seperti gambar diatas.

- ✓ Setelah itu,langkah selanjutnya kita membuka aplikasi **WireShark**. Disini saya tersambung dengan Wi-Fi Unsri.Net.
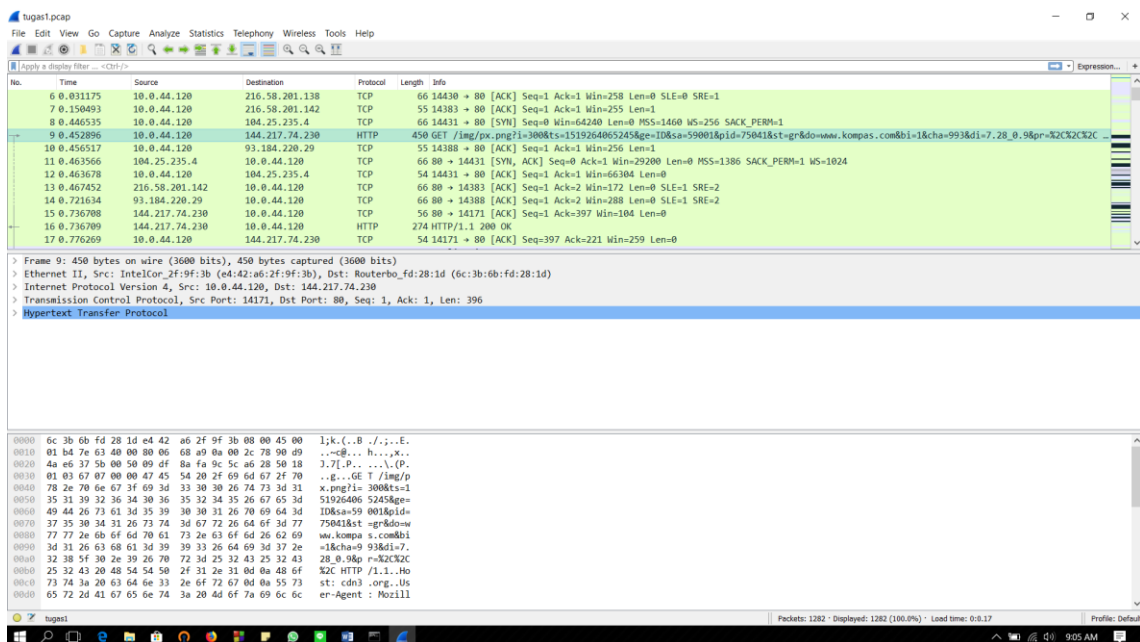

Pada gambar diatas telah didapatkan beberapa data dalam bentuk paket-paket data jaringan .Dikarenakan semua paket tersaring dengan cepat, maka kita akan filter terlebih dahulu dengan menggunakan sintaks "*ipc.rc==10.0.44.29*".

Setelah di filter maka akan terdapat data sebagai berikut:
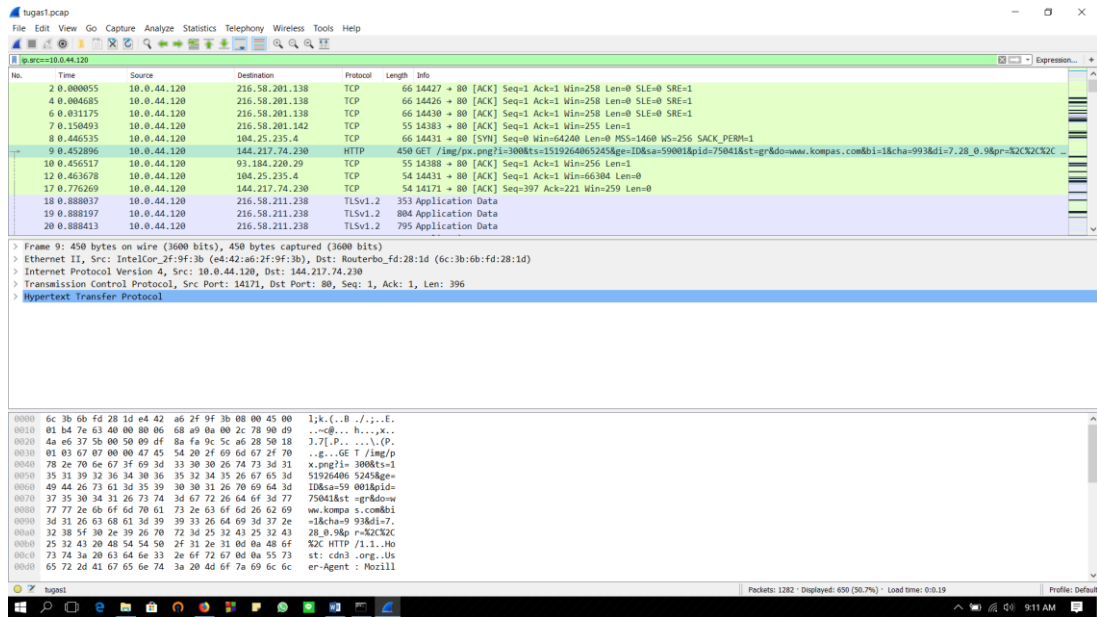
dapat dilihat sendiri bahwa dengan komputer yang beralamatkan 10.0.44.29 sedang mencoba mengakses 144.217.74.20 atau website www.kompas.com dengan menggunakan protokol TCP. Setelah itu jika kita mengklik bagian kotak tengah di menu Internet Protocol.

BAGIAN KEDUA "Dengan Menggunakan Menu Follow Stream"
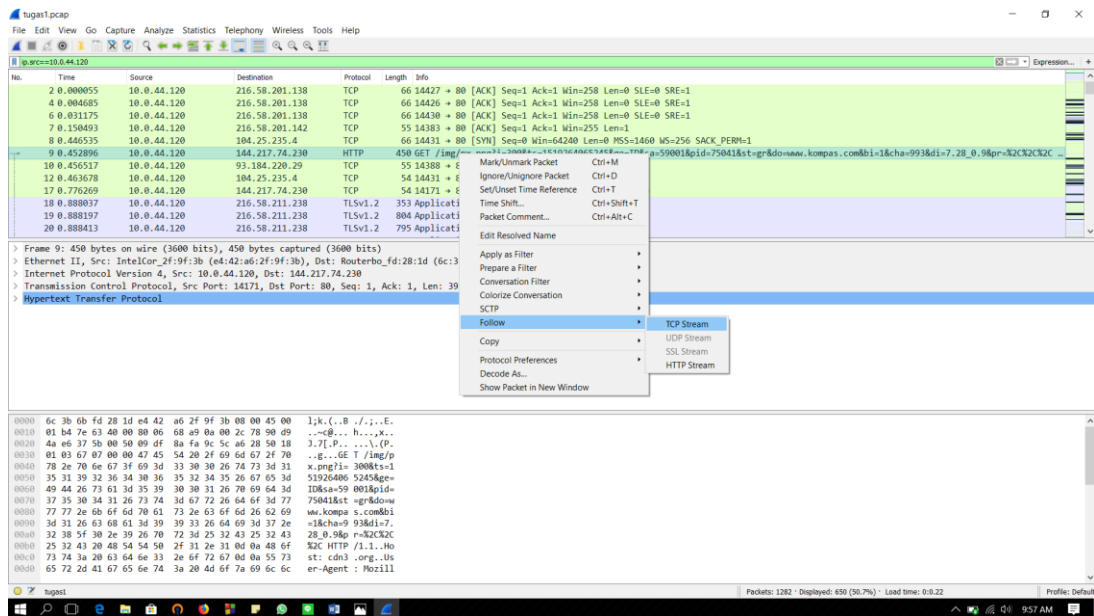
Seperti yang terlihat di gambar atas,pilih paket yang memiliki bentuk protokol http,dan langsung klik **analyze** => pilih **follow** => pilih **TCP Stream** atau bias klik kanan pada mouse => pilih **follow** => pilih **TCP Stream**.
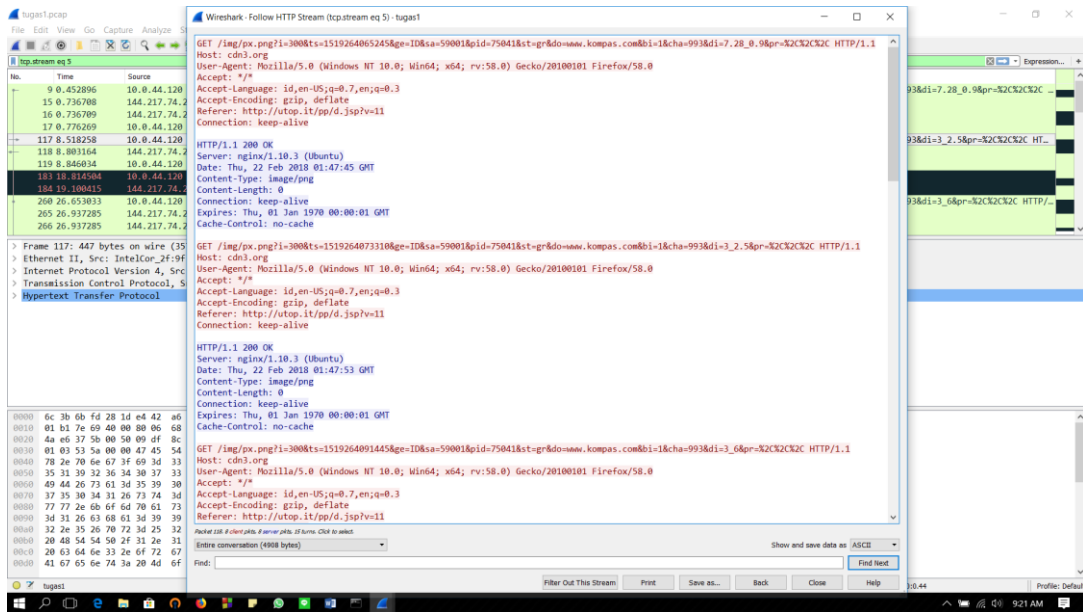
Bisa kita lihat pada gambar diatas info apa saja yang telah dapat kita baca yakni :

1. Sang pengguna yang sedang mengakses website www.kompas.com menggunakan aplikasi Mozila.
2. Waktu mengakses web tersebut pada tanggal 22 februari 2018 pada hari kamis.
3. Type data yang sedang diakses itu berupa image/png.

BAGIAN KETIGA "Flow Graph Jaringan Menggunakan Aplikasi WireShark dan Visual Route"

Untuk melihat FlowGraph, kita mengklik menu "Statistics" lalu pilih "Flowgraph" maka data yang akan muncul adalah 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 :
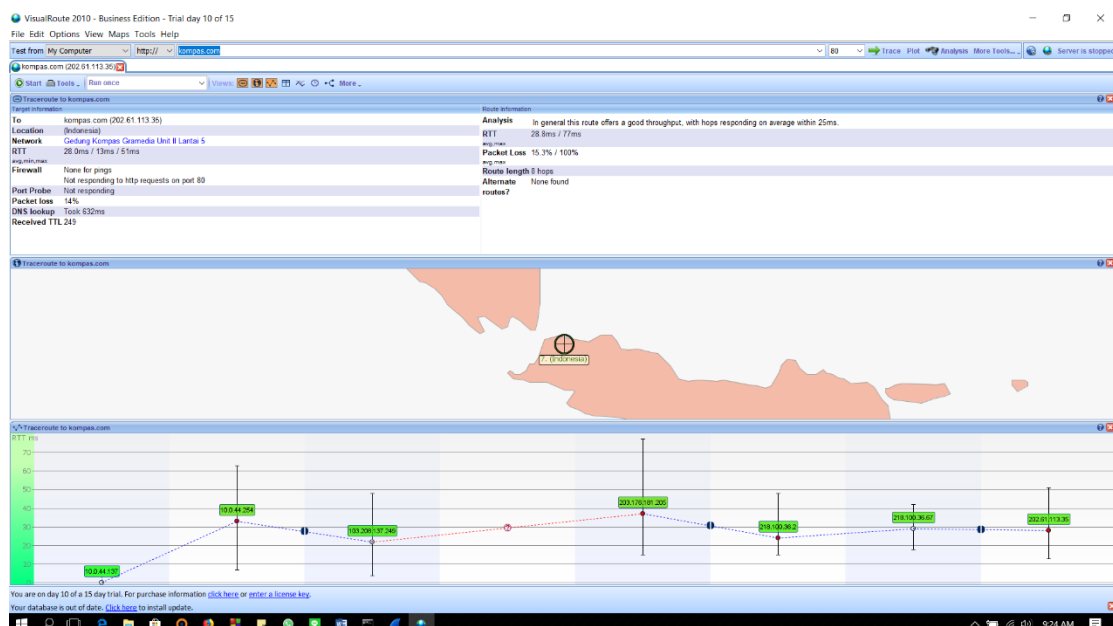
Dapat kita lohat sendiri perbedaan data yang diperoleh dari aplikasi wireshark dan aplikasi visualroute ini:

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.