

KOMUNIKASI DATA

Analisis jaringan menggunakan Wireshark & Visual Route



Disusun Oleh

NAMA : Ahmad Yusuf Aditama

NIM : 09011381621098

KELAS : SK4B

**UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
PRODI SISTEM KOMPUTER
2017/2018**

1) Paket data

```
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Excalibur>arp -a

Interface: 192.168.100.4 --- 0x8
Internet Address      Physical Address      Type
192.168.100.1        2c-55-d3-2e-1f-4a    dynamic
192.168.100.255     ff-ff-ff-ff-ff-ff    static
224.0.0.22          01-00-5e-00-00-16    static
224.0.0.251         01-00-5e-00-00-fb    static
224.0.0.252         01-00-5e-00-00-fc    static
224.0.0.253         01-00-5e-00-00-fd    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 --- 0xd
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
224.0.0.251         01-00-5e-00-00-fb    static
224.0.0.252         01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static

C:\Users\Excalibur>
```

Dengan menggunakan Command Prompt, ketikkan perintah “arp -a”, dengan begitu IP Address milik kita akan terlihat seperti gambar diatas.

Setelah itu, buka aplikasi Wireshark dan membuka web www.kompas.com. Lalu, akan muncul hasil seperti gambar berikut:

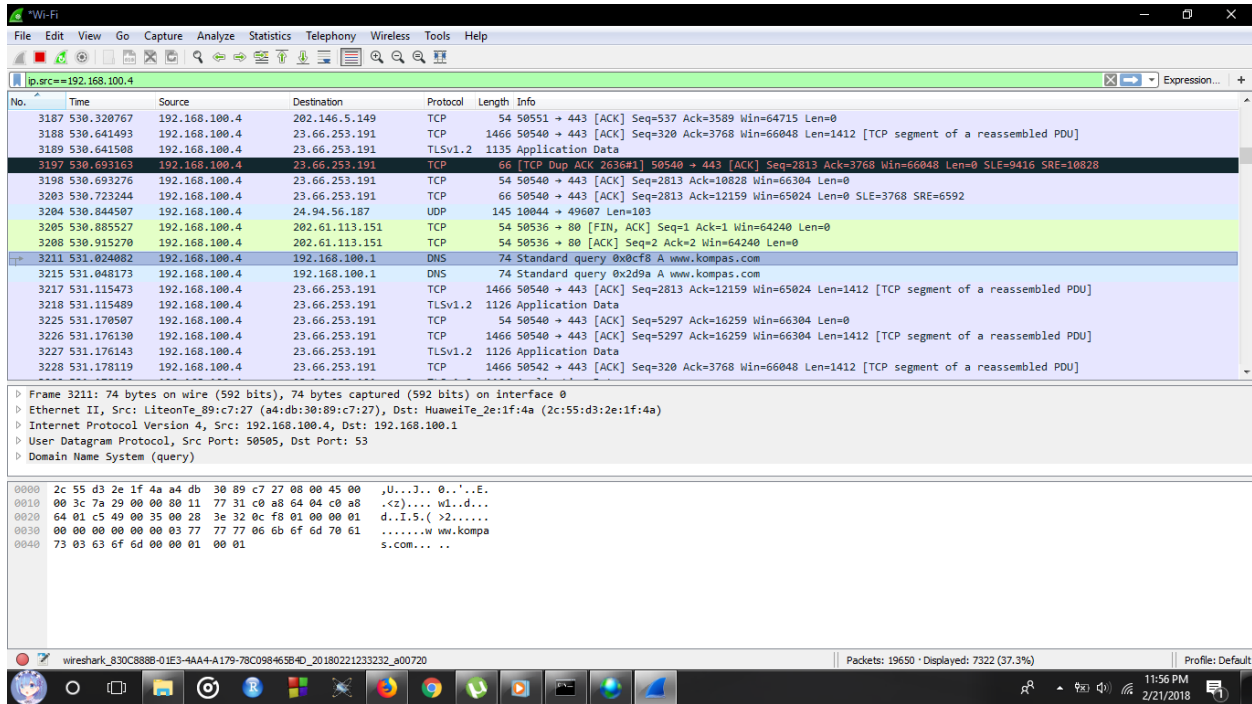
The screenshot shows a Wireshark capture of network traffic. The packet list pane shows several packets, with packet 24 selected. The details pane for packet 24 shows the following information:

- Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
- Ethernet II, Src: LiteonTe_89:c7:27 (a4:db:30:89:c7:27), Dst: HuaweiTe_2e:1f:4a (2c:55:d3:2e:1f:4a)
- Internet Protocol Version 4, Src: 192.168.100.4, Dst: 104.244.42.67
- Transmission Control Protocol, Src Port: 50123, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
- Secure Sockets Layer

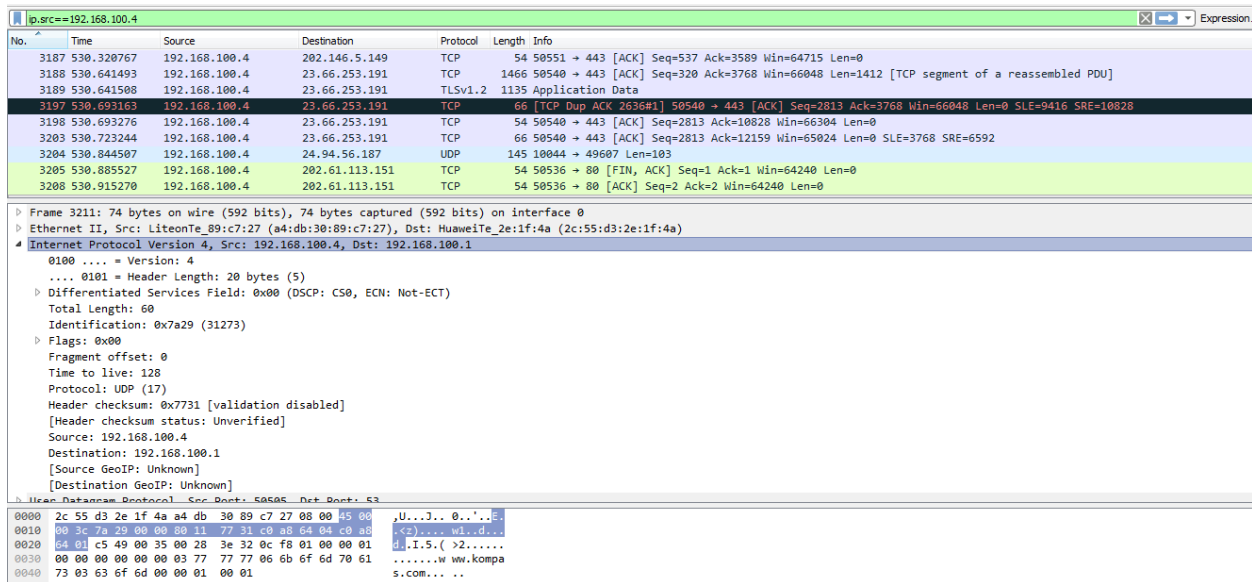
The packet bytes pane shows the raw data of the selected packet:

```
0000 2c 55 d3 2e 1f 4a a4 db 30 89 c7 27 08 00 45 00 ,U...J.. 0...'..E.
0010 00 29 56 aa 40 00 80 06 ec 40 c0 a8 64 04 68 f4 ,V@... ..@.d.h.
0020 2a 43 c3 cb 01 bb 1b 9a b6 d3 2f f0 de b0 50 10 *C..... ../...P.
0030 00 ff 50 28 00 00 00 ..P(...
```

Setelah data-data paket terlihat, ketikkan “ip.src== 192.168.100.4” pada kolom filter. Lalu, hasilnya seperti gambar berikut:



Dari gambar di atas, terlihat Source-nya adalah 192.168.100.4 dan Destination-nya adalah 202.61.113.151 dengan menggunakan protocol TCP. Setelah itu, Klik Internet Protocol Version 4, dan hasilnya sebagai berikut:



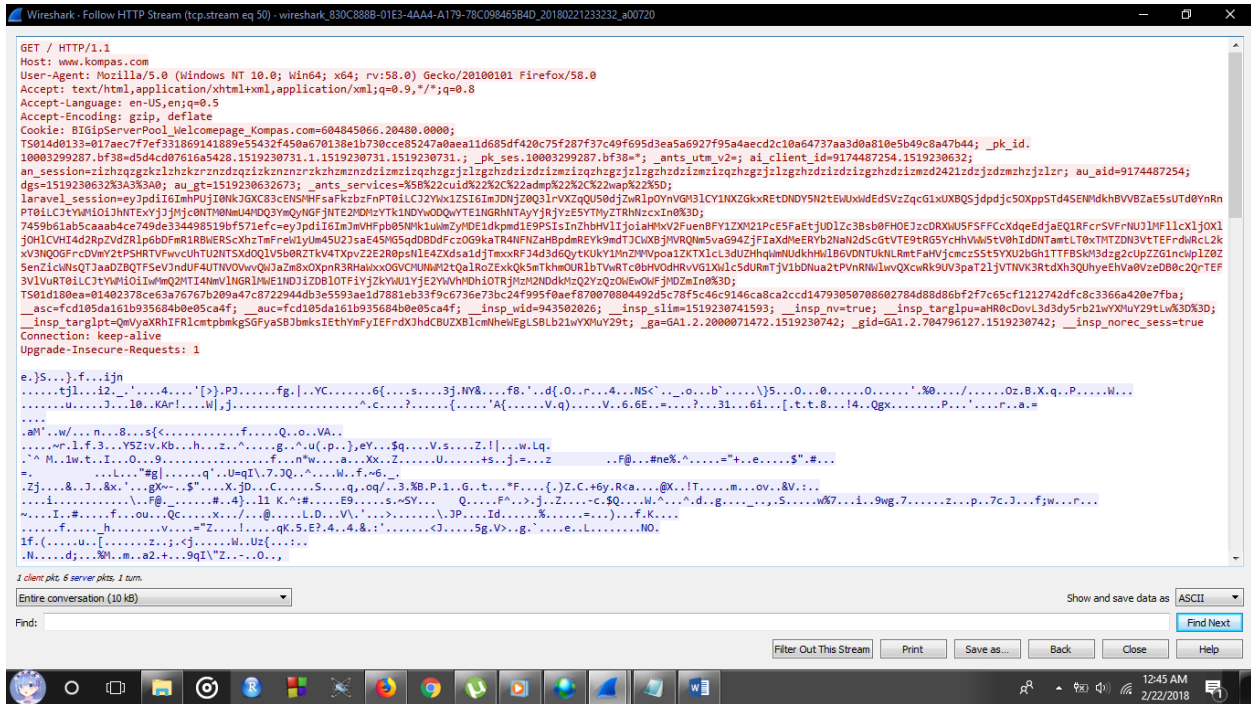
Di kolom Internet Protocol Version 4, terlihat MAC Address yang dimiliki adalah a4:db:30:89:c7:27, dan MAC Address router-nya adalah 2c:55:d3:2e:1f:4a. Terlihat juga kalau Panjangan datanya adalah 60.

2) TCP Stream & HTTP Stream

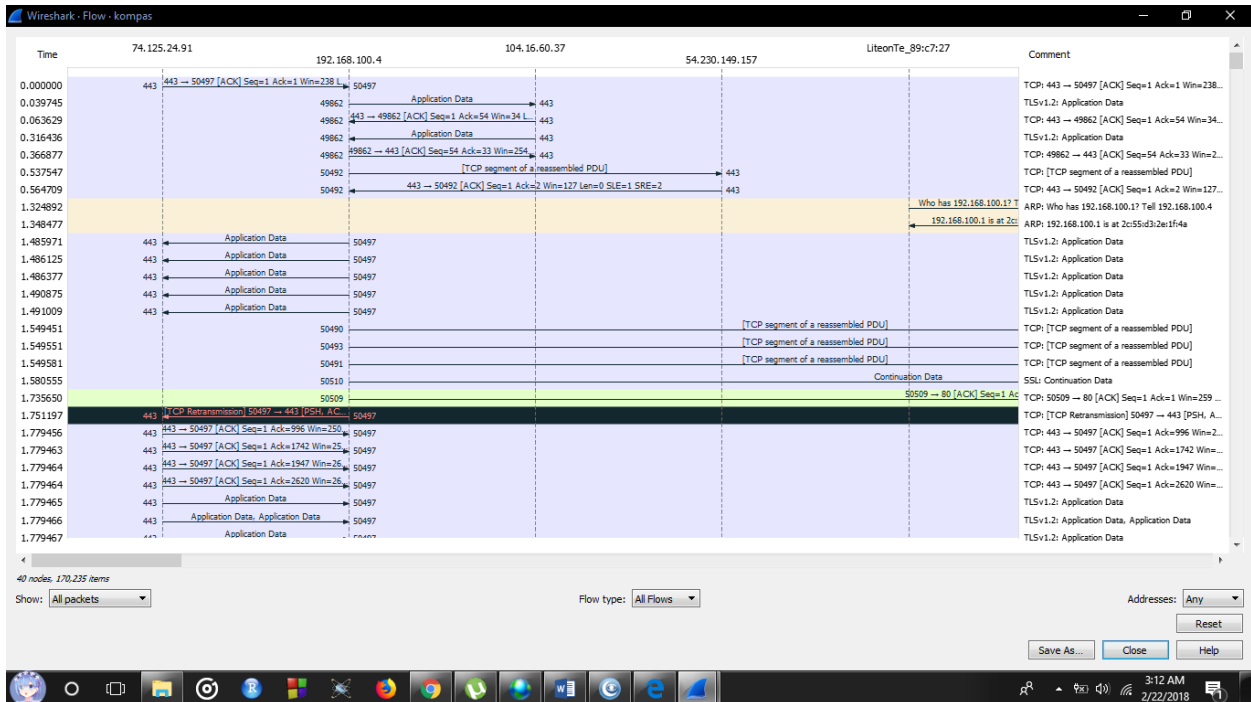
Untuk membuka TCP Stream, klik Analyze -> Follow -> TCP Stream. Web yang sedang diakses saat ini adalah www.kompas.com disini Browser yang digunakan adalah Mozilla Firefox. Diakses pada Rabu, 21 Februari 2018.

The screenshot shows a Wireshark window titled "Wireshark - Follow TCP Stream (tcp.stream eq 50) - wireshark_830C888B-01E3-4AAA-A179-78C09846584D_201802212332_a00720". The main pane displays the raw data of the HTTP request and response. The request is a GET request to `http://www.kompas.com`. The response is an `HTTP/1.1 200 OK` with a `Content-Type: text/html; charset=UTF-8`. The response body contains a large block of HTML code, including a `<script>` tag with a long alphanumeric string. The status bar at the bottom indicates "4 client pkts, 22 server pkts, 3 turns".

Pada menu tersebut data TCP Stream yang tak bisa terbaca, akan terbaca di menu TCP johon seperti gambar berikut ini:

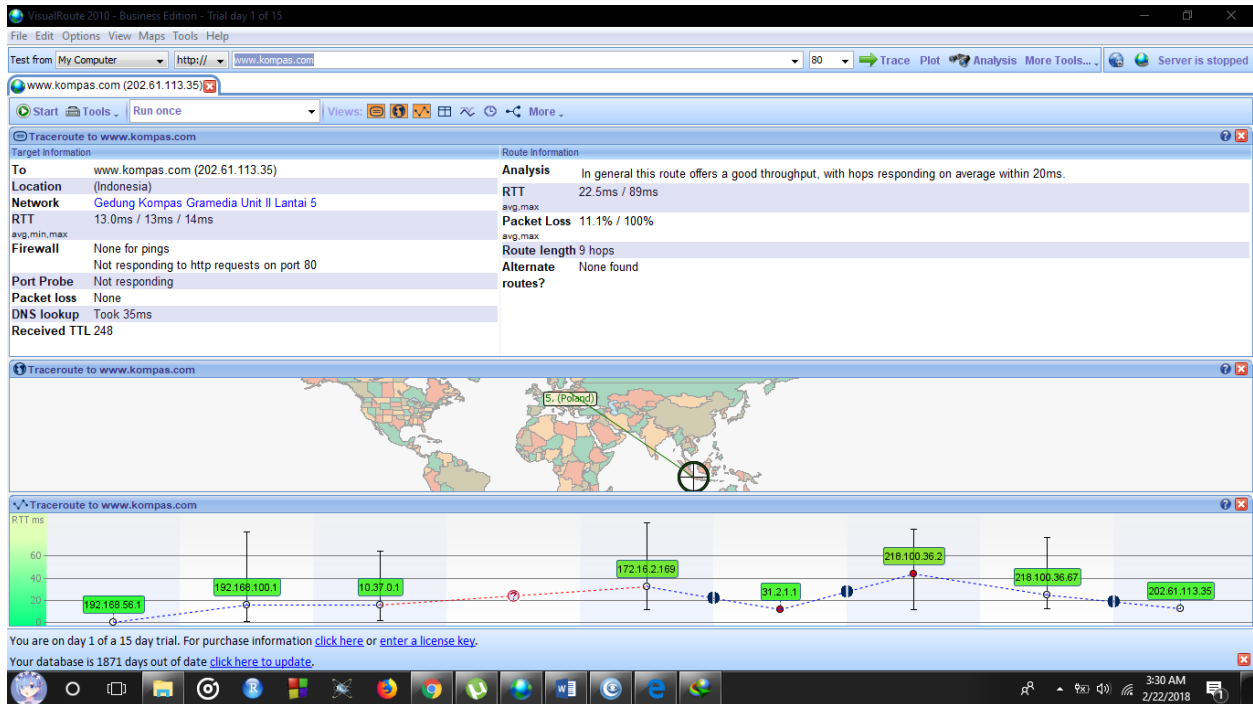


3) Flow Graph dengan menggunakan Wireshark



1. Komputer mengirim informasi address ke router.
2. Router menerima informasi, dan akan menyampaikan data ke ISP terdekat.
3. ISP akan menanggapi permintaan user tersebut, apakah address yang dituju itu tersedia atau tidak.
4. Apabila address tersedia, maka ISP akan mengarahkan informasi tersebut ke ISP pusat.
5. ISP pusat akan menanggapi permintaan tersebut, dan informasi tanggapan akan dikirim kembali ke user.
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. Jika informasi tersebut valid, isp akan kembali mengirimkan tanggapan dan mengarahkannya ke isp pusat.
8. Jika ISP pusat menganggap informasi tersebut benar, maka akan diarahkan ke server perusahaan yang memberi ISP bandwidth. Yang mana akan di arahkan ke link server cloud berikutnya.
9. Disini situs yang diakses adalah www.kompas.com.
10. Seperti pada isp tadi, server pun akan mengirimkan informasi kepada user apakah address yang dituju tersebut benar atau tidak.

4) Perbandingan Visual Route dengan Wireshark



Gambar diatas merupakan hasil dengan menggunakan Visual Route. Aplikasi ini memiliki tampilan yang lebih sederhana disbanding Wireshark, sehingga sangat mudah untuk digunakan. Dari tes menggunakan www.kompas.com, terlihat jika memiliki 9 hops dan juga ditampilkan dengan grafik agar mudah dipahami.

Visualisai penggunaan Source to Destination disini sangat jelas, yaitu dari IP 192.168.56.1 sampai 202.61.113.35 . Rata-rata kecepatan akses-nya dalah 13 ms. Dan juga, web www.kompas.com berlokasi di Indonesia.