

Analisis Hasil Capture, Follow Stream, dan Flow Graph Jaringan Menggunakan  
Aplikasi Wireshark dan VisualRoute



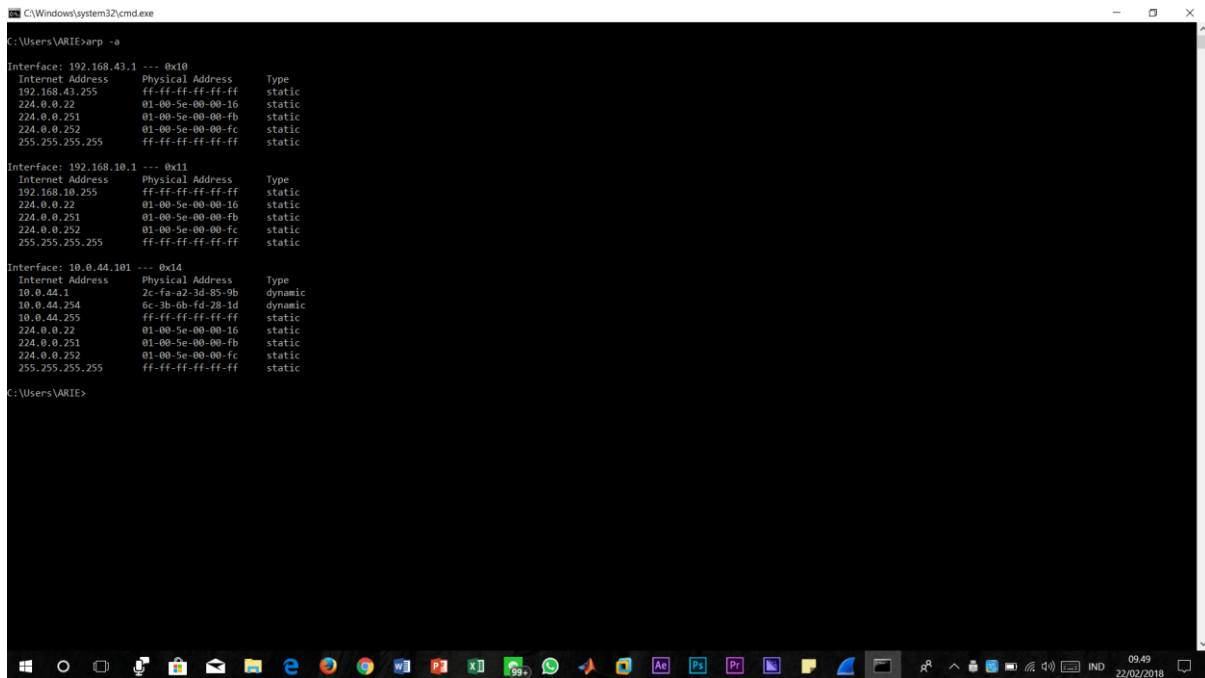
Oleh :

Nama : Arie Fatwa  
NIM : 09011381722126  
Kelas : SK2B

Sistem Komputer  
Fakultas Ilmu Komputer  
Universitas Sriwijaya  
2018

## 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.



```
C:\Windows\system32\cmd.exe
C:\Users\VARIE>arp -a

Interface: 192.168.43.1 --- 0x0
Internet Address      Physical Address      Type
192.168.43.255       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
255.255.255.255     ff-ff-ff-ff-ff-ff    static

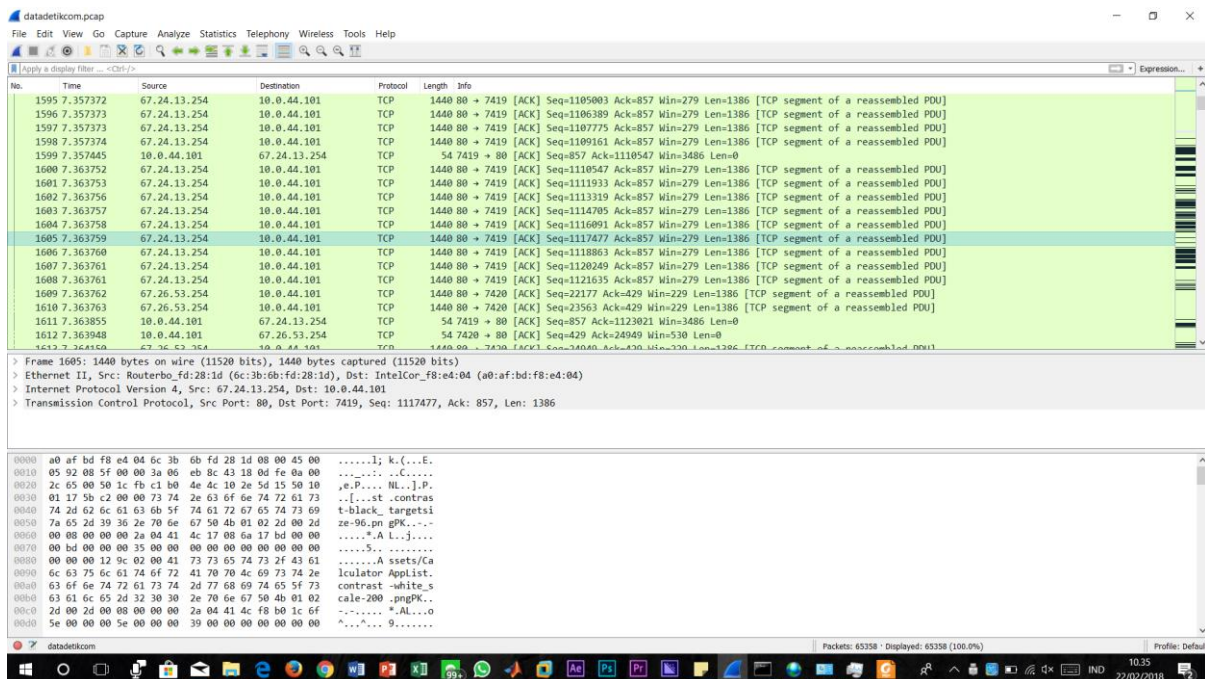
Interface: 192.168.10.1 --- 0x1
Internet Address      Physical Address      Type
192.168.10.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static

Interface: 10.0.44.101 --- 0x14
Internet Address      Physical Address      Type
10.0.44.1            2c-fa-a2-3d-85-9b    dynamic
10.0.44.254          6c-3b-0b-fd-28-1d    dynamic
10.0.44.255          ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static

C:\Users\VARIE>
```

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

Setelah kita dapatkan, langkah selanjutnya adalah kita membuka aplikasi WIRESHARK. Jaringan yang saya gunakan adalah Unsri.Net.



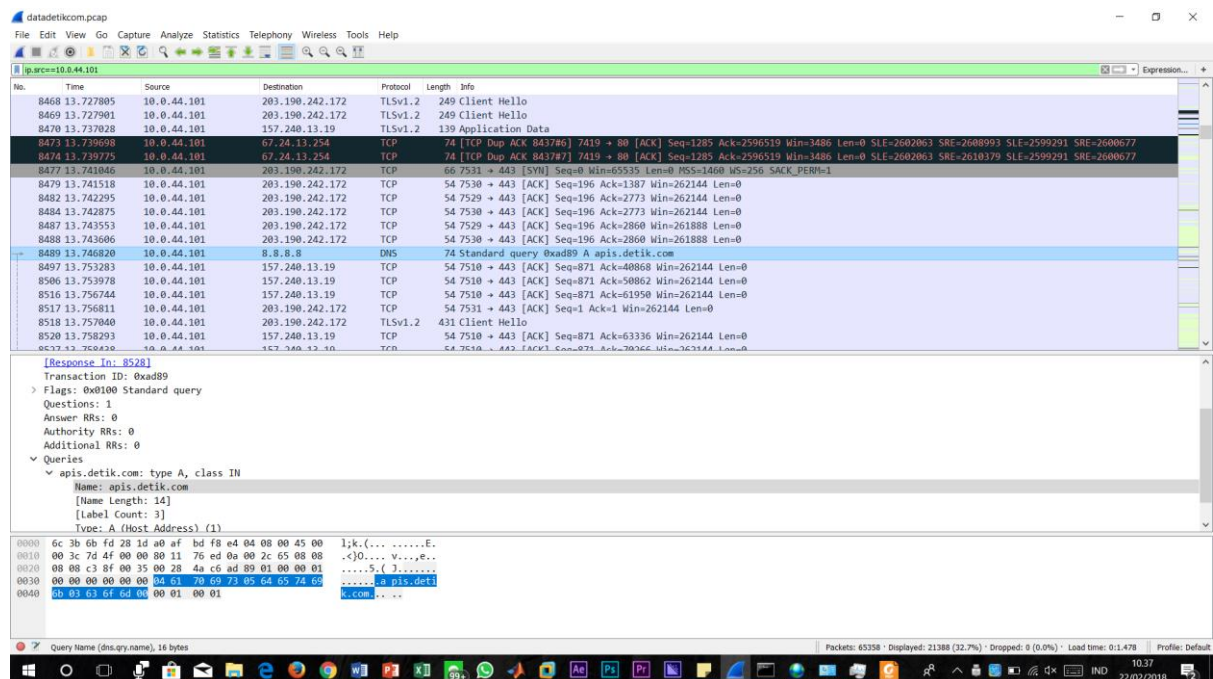
```
dataetikom.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl>+
Expression...

No. Time Source Destination Protocol Length Info
1595 7.357372 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1105003 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1596 7.357373 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1106389 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1597 7.357373 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1107775 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1598 7.357374 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1109161 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1599 7.357405 10.0.44.101 67.24.13.254 TCP 54 7419 -> 80 [ACK] Seq=857 Ack=110547 Win=3486 Len=0
1600 7.363752 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1110547 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1601 7.363753 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1111933 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1602 7.363756 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1113319 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1603 7.363757 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1114705 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1604 7.363758 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1116091 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1605 7.363759 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1117477 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1606 7.363760 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1118863 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1607 7.363761 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1120249 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1608 7.363761 67.24.13.254 10.0.44.101 TCP 1440 80 -> 7419 [ACK] Seq=1121635 Ack=857 Win=279 Len=1386 [TCP segment of a reassembled PDU]
1609 7.363762 67.26.53.254 10.0.44.101 TCP 1440 80 -> 7420 [ACK] Seq=22177 Ack=429 Win=229 Len=1386 [TCP segment of a reassembled PDU]
1610 7.363763 67.26.53.254 10.0.44.101 TCP 1440 80 -> 7420 [ACK] Seq=23563 Ack=429 Win=229 Len=1386 [TCP segment of a reassembled PDU]
1611 7.363855 10.0.44.101 67.24.13.254 TCP 54 7419 -> 80 [ACK] Seq=857 Ack=1123021 Win=3486 Len=0
1612 7.363948 10.0.44.101 67.26.53.254 TCP 54 7420 -> 80 [ACK] Seq=857 Ack=24949 Win=530 Len=0

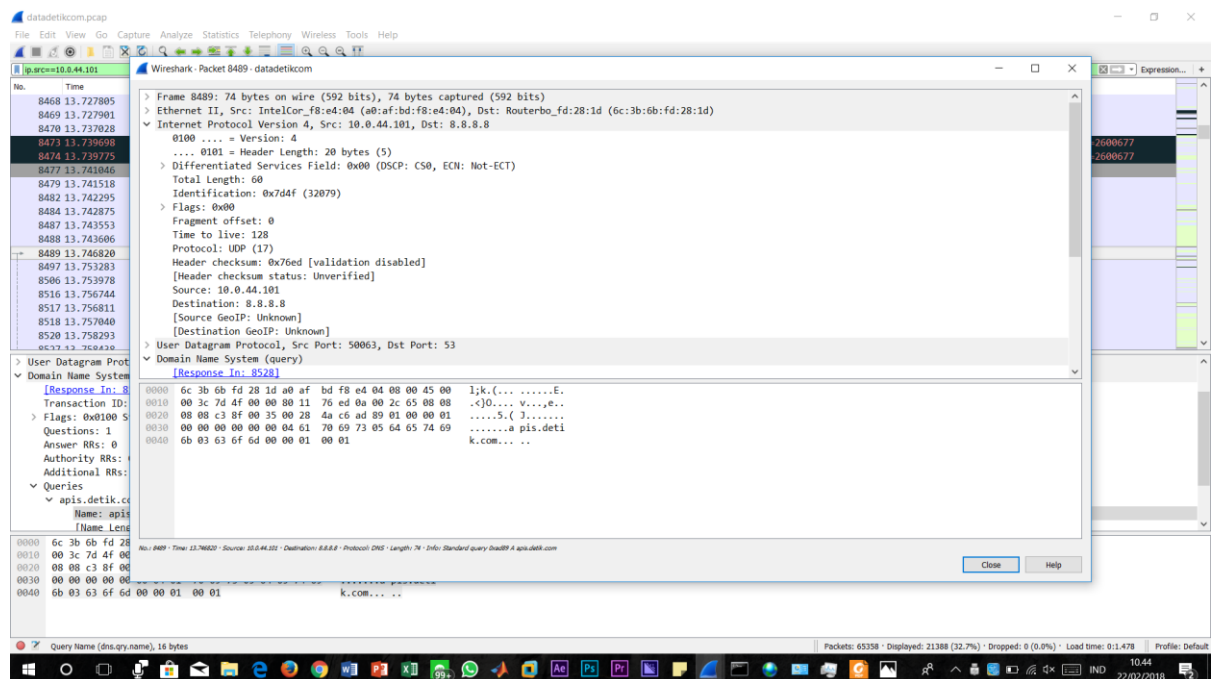
> Frame 1605: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520 bits)
> Ethernet II, Src: Routerbo_fd:28:1d (6c:3b:6b:fd:28:1d), Dst: IntelCor_f8:e4:04 (a0:af:bd:f8:e4:04)
> Internet Protocol Version 4, Src: 67.24.13.254, Dst: 10.0.44.101
> Transmission Control Protocol, Src Port: 80, Dst Port: 7419, Seq: 1117477, Ack: 857, Len: 1386

0000 a0 af bd f8 e4 04 6c 3b 6b fd 28 1d 00 00 45 00 .....; k.(...E.
0010 05 92 08 5f 00 00 3a 06 eb 8c 43 18 0d fe 0a 00 .....G.....
0020 2c 65 00 50 1c fb c1 b0 4e 4c 10 2e 5d 15 50 10 ..e.P....NL...].P.
0030 01 17 3b c2 00 00 73 74 2e 63 6f 6e 74 72 61 73 ..[...st.contras
0040 74 2d 62 6c 61 63 0b 5f 74 61 72 67 65 74 73 69 t-black_targetsi
0050 7a 65 2d 39 36 2e 70 6e 67 50 4b 01 02 2d 00 2d ze-96.pngPK...-
0060 00 08 00 00 00 2a 04 41 4c 17 08 6a 17 bd 00 00 .....*.A.L.j.....
0070 00 bd 00 00 00 35 00 00 00 00 00 00 00 00 00 00 .....5.....
0080 00 00 00 12 9c 02 00 41 73 73 65 74 73 2f 43 61 .....A ssets/Ca
0090 6c 63 75 6c 61 74 6f 72 41 70 70 4c 69 73 74 2e iculator Applist.
00a0 63 6f 6e 74 61 73 74 2d 77 68 69 74 65 5f 73 contrast_white_s
00b0 63 61 6c 65 2d 32 30 30 2e 70 6e 67 50 4b 01 02 cale-200 .pngPK..
00c0 2d 00 2d 00 08 00 00 00 2a 04 41 4c f8 b0 1c 6f .....*.AL...o
00d0 5e 00 00 00 5e 00 00 39 00 00 00 00 00 00 00 00 .....9.....
```

Pada gambar diatas 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==10.0.44.101”.



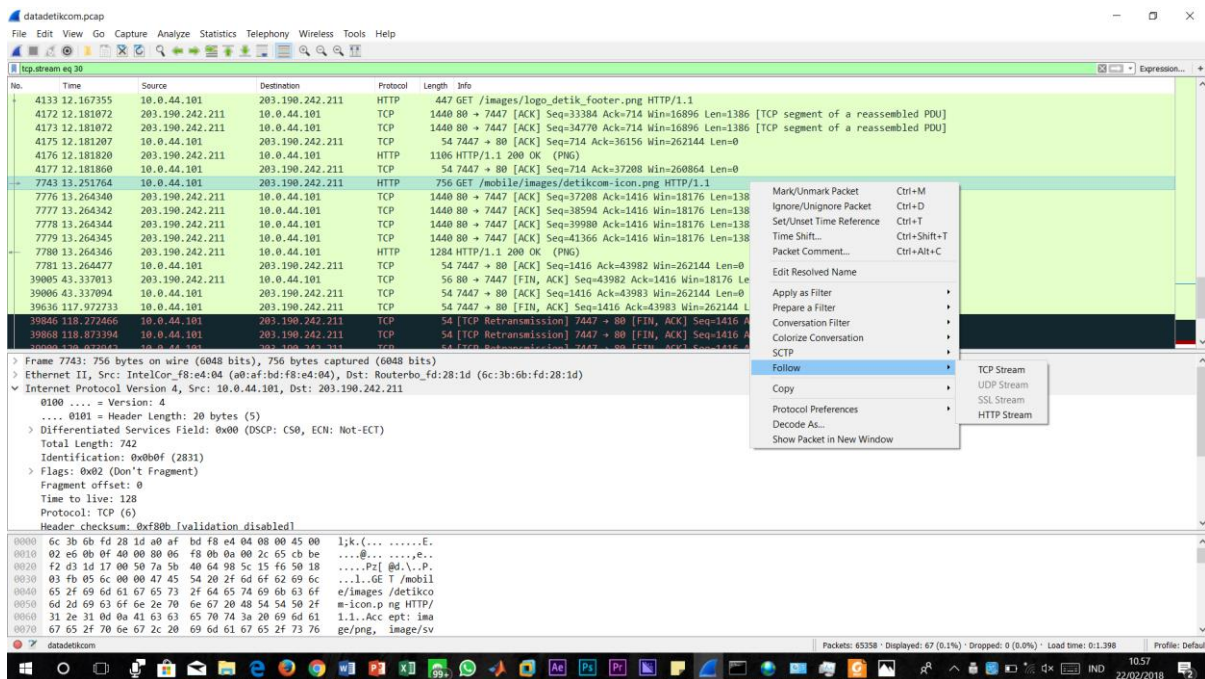
dapat dilihat sendiri bahwa dengan komputer yang beralamatkan 10.0.44.29 sedang mencoba mengakses 203.190.242.172 atau website [www.detik.com](http://www.detik.com) dengan menggunakan protokol TCP.



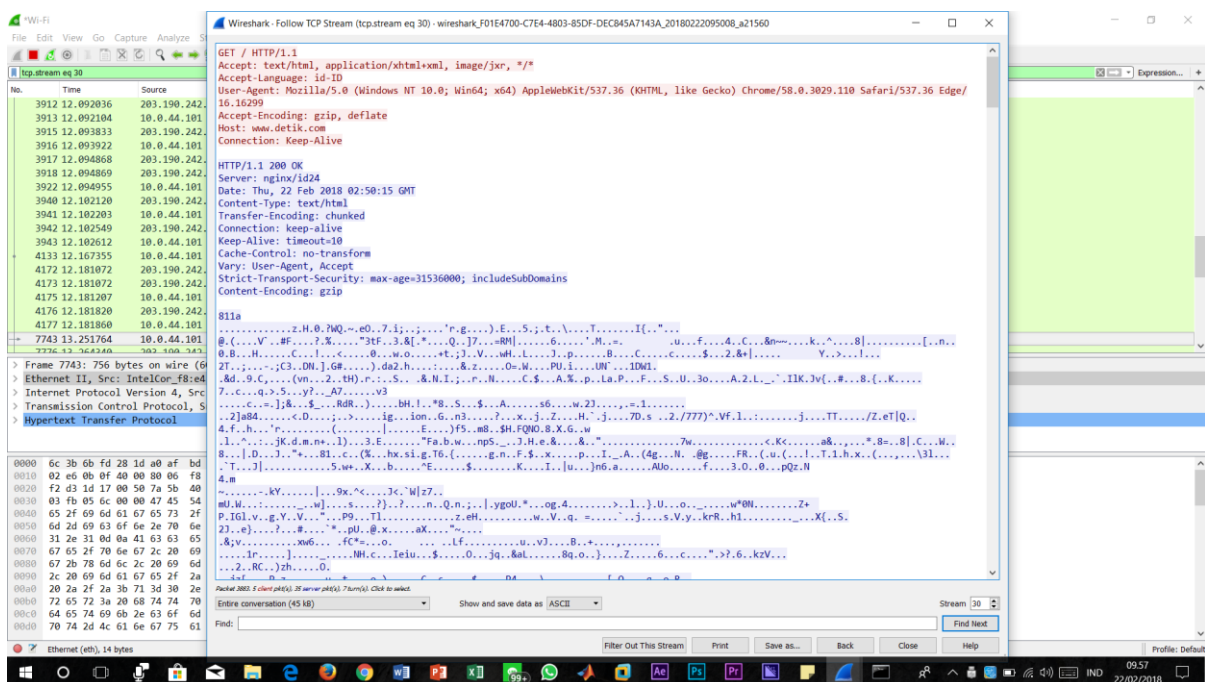
Setelah itu jika kita mengkliknya dan mengklik bagian menu Internet Protocol Version 4, maka akan jelas jika komputer yang sedang mengakses web tersebut memiliki mac address yakni

a0:af:bd:f8:e4:04, sedangkan mac address dari routernya sendiri adalah 6c:3b:6b:fd:28:1d. Selain kita mendapatkan info mengenai mac addressnya kita juga dapat mengetahui bahwa panjang data yang terbaca yaitu sepanjang 74 bytes atau 592 bits yang menggunakan port yaitu 8.8.8.8.

## BAGIAN KEDUA “DENGAN MENGGUNAKAN MENU FOLLOW STREAM”



Seperti yang terlihat di gambar atas, pilih paket yang memiliki bentuk protokol http dan langsung klik kanan lalu pilih follow dan klik untuk pertama pilih bagian TCP Stream :





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

1. Sang pengguna yang sedang mengakses website [www.detik.com](http://www.detik.com) menggunakan aplikasi browser microsoft edge.
2. Waktu sang user mengakses web tersebut pada tanggal 22 Februari 2018 pada hari Kamis.
3. Type data yang sedang diakses itu berupa text atau html.

Untuk bagian keduanya kita gunakan kembali suatu pilihan yakni HTTP Stream, 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 yang datanya sendiri berupa teks atau html.

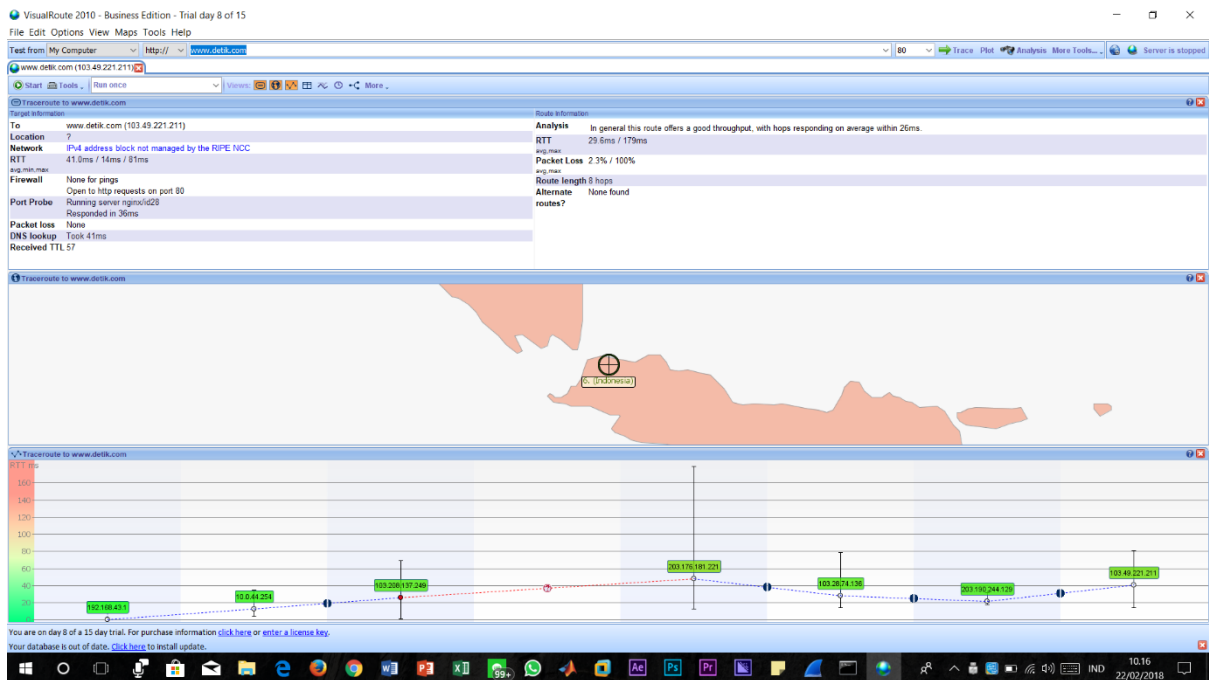
The screenshot displays the Wireshark interface with the following details:

- Packet List:** Shows a GET request from 10.0.44.101 to 203.190.242 at 12:09:20:36.
- Packet Details:**
  - GET / HTTP/1.1
  - Accept: text/html, application/xhtml+xml, image/jxr, \*/\*
  - Accept-Language: id-ID
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36 Edge/16.16299
  - Accept-Encoding: gzip, deflate
  - Host: www.detik.com
  - Connection: Keep-Alive
  - HTTP/1.1 200 OK
  - Server: nginx/id24
  - Date: Thu, 22 Feb 2018 02:50:15 GMT
  - Content-Type: text/html
  - Transfer-Encoding: chunked
  - Connection: keep-alive
  - Keep-Alive: timeout=10
  - Cache-Control: no-transform
  - Vary: User-Agent, Accept
  - Strict-Transport-Security: max-age=31536000; includeSubDomains
  - Content-Encoding: gzip
  - <doctype html>
  - <html>
  - <head>
  - <script>
  - if (typeof console.log == 'undefined') {
  - this.console = (log: function() {}, info: function() {});
  - }
  - var \_\_cmonErrorLog = [];
  - window.onerror = function (errorMsg, url, lineNumber, column, errorObj) {
  - \_\_cmonErrorLog.push('Error: ' + errorMsg + ' Script: ' + url + ' Line: ' + lineNumber
  - + ' Column: ' + column + ' StackTrace: ' + errorObj);
  - return true;
  - }
  - </script>
  - <title>detikcom - Informasi Berita Terupdate Hari Ini</title>
  - <meta name="description" content="Indeks berita terbaru hari ini dari peristiwa, kecelakaan, kriminal, hukum, berita unik, Politik, dan liputan khusus di Indonesia dan Internasional" itemprop="description" />
  - <meta charset="utf-8">
  - <meta http-equiv="X-UA-Compatible" content="text/html; charset=UTF-8" />
  - <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  - <link href="https://plus.google.com/+detikcom" rel="publisher" />

- Packet Bytes:** Shows the raw data of the request, including the status bar: "Entire conversation (251 KB)".

## BAGIAN KETIGA “Flow Graph Jaringan menggunakan aplikasi Wireshark dan VisualRoute”

Pertama kali kita search [www.detik.com](http://www.detik.com) kemudian tunggu hingga proses selesai.



Kemudian kita mengklik menu statistics dan kita 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 tersedia, 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](http://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.

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 dianalisis 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 hops terstruktur dengan rapi. Selain itu, aplikasi wireshark dapat memberikan fasilitas filter protocol sehingga dalam menganalisis data lebih efektif 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 hops ditampilkan semua.