

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



Disusun Oleh:

Nadhya Hassni

09011381722090

Sk4b

Sistem Komputer

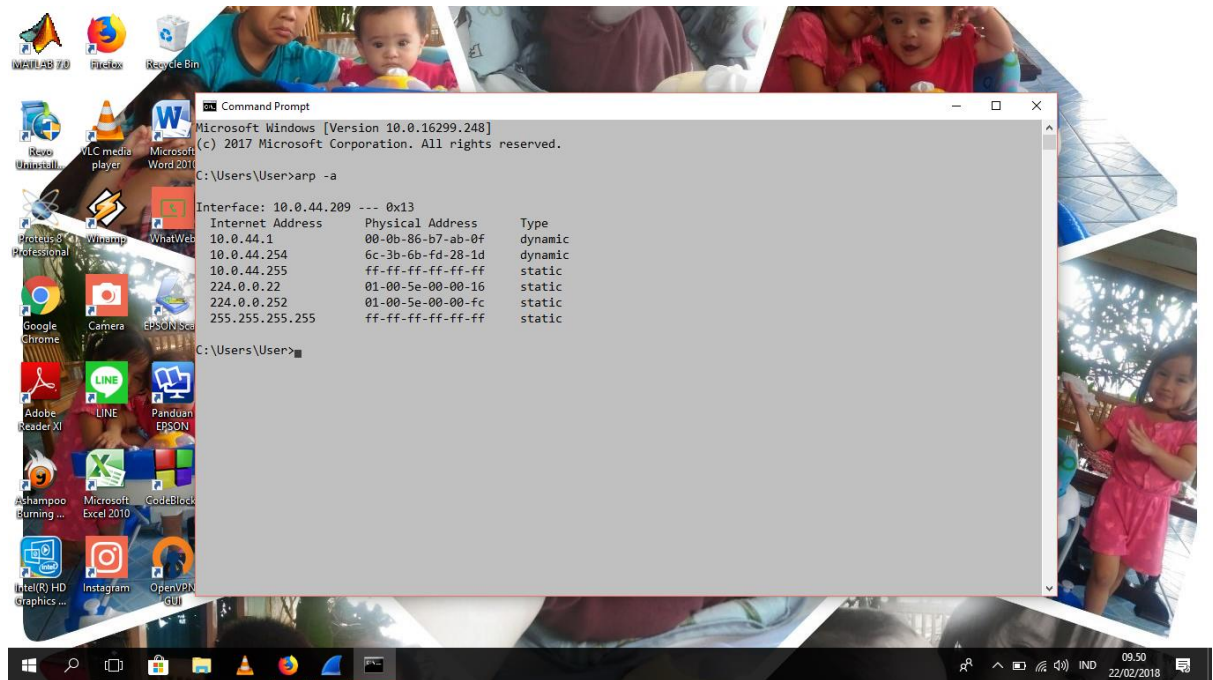
Fakultas Ilmu Komputer

Universitas Sriwijaya

2018

Bagian 1 “ANALISIS PAKET DATA”

Sebelum kita melakukan analisis paket data jaringan, terlebih dahulu kita harus mengetahui berapa IP address yang sedang kita pakai. Dengan cara membuka **Command Prompt** kemudian kita tuliskan “**arp -a**” agar IP address kita dapat ditampilkan.



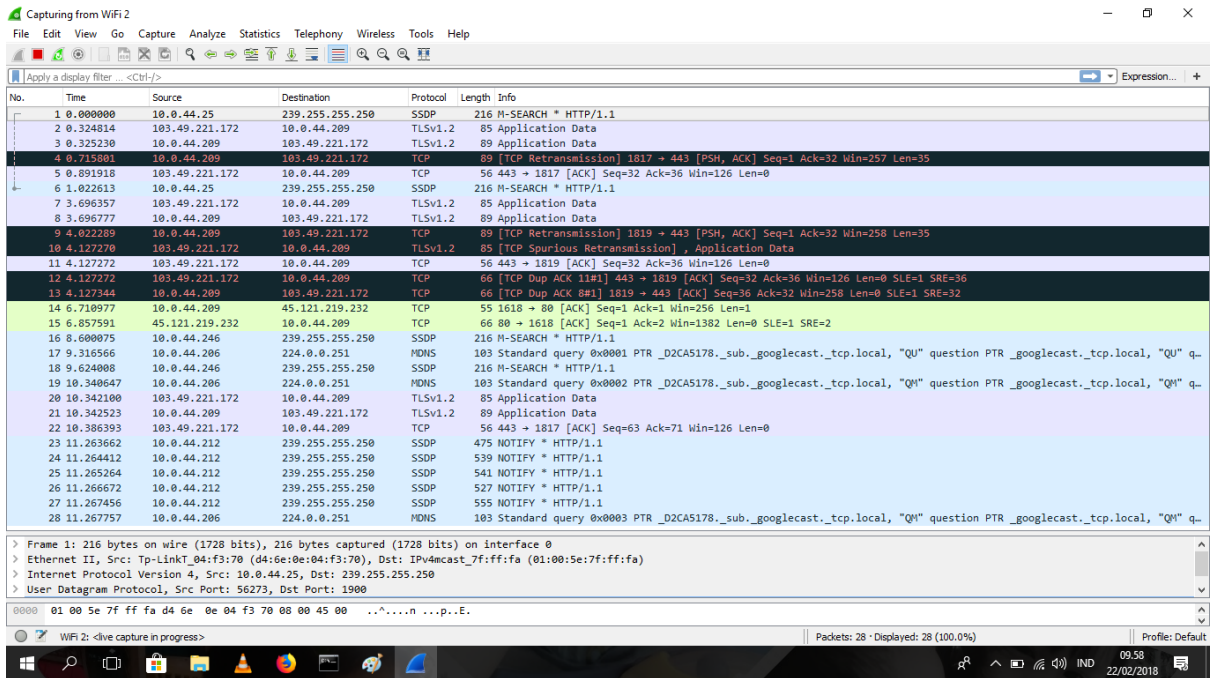
```
Microsoft Windows [Version 10.0.16299.248]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\User>arp -a

Interface: 10.0.44.209 --- 0x13
Internet Address      Physical Address      Type
10.0.44.1             00-0b-86-b7-ab-0f    dynamic
10.0.44.254          6c-3b-6b-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
224.0.0.252          01-00-5e-00-00-fc    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

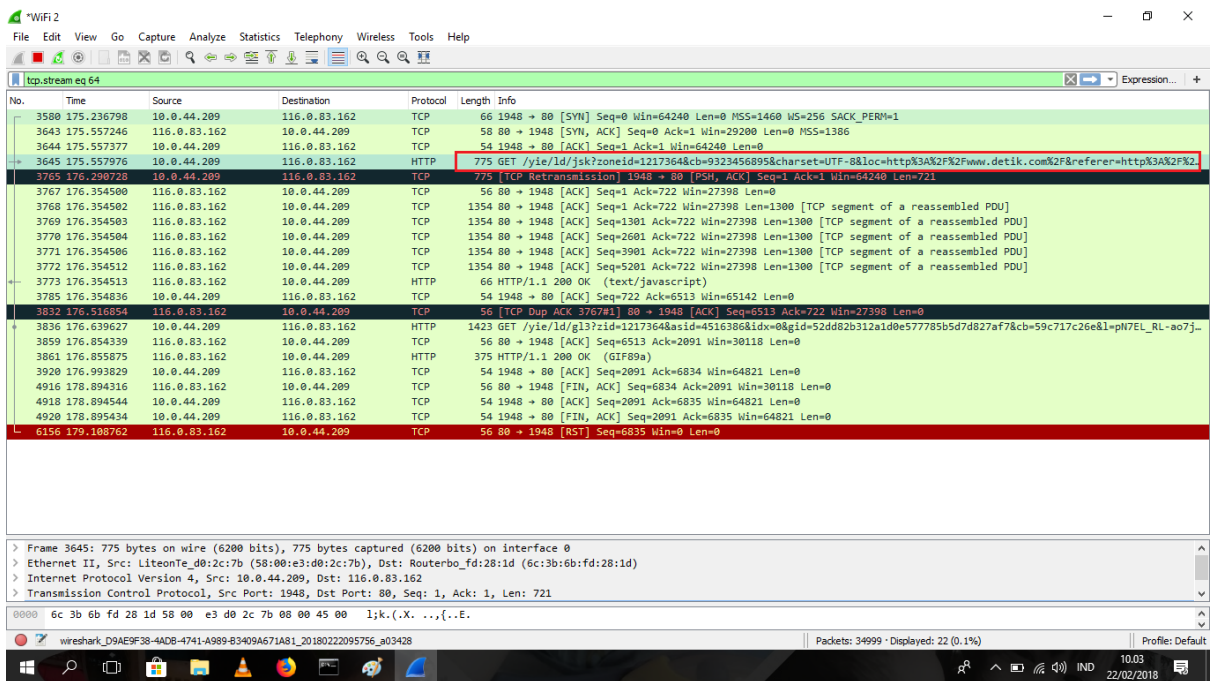
C:\Users\User>
```

Setelah kita mengetahui berapa IP address kita, kemudian kita harus tersambung ke internet sebelum kita bisa menggunakan aplikasi **WIRESHARK**. Disini saya menggunakan jaringan **unsri.net**.

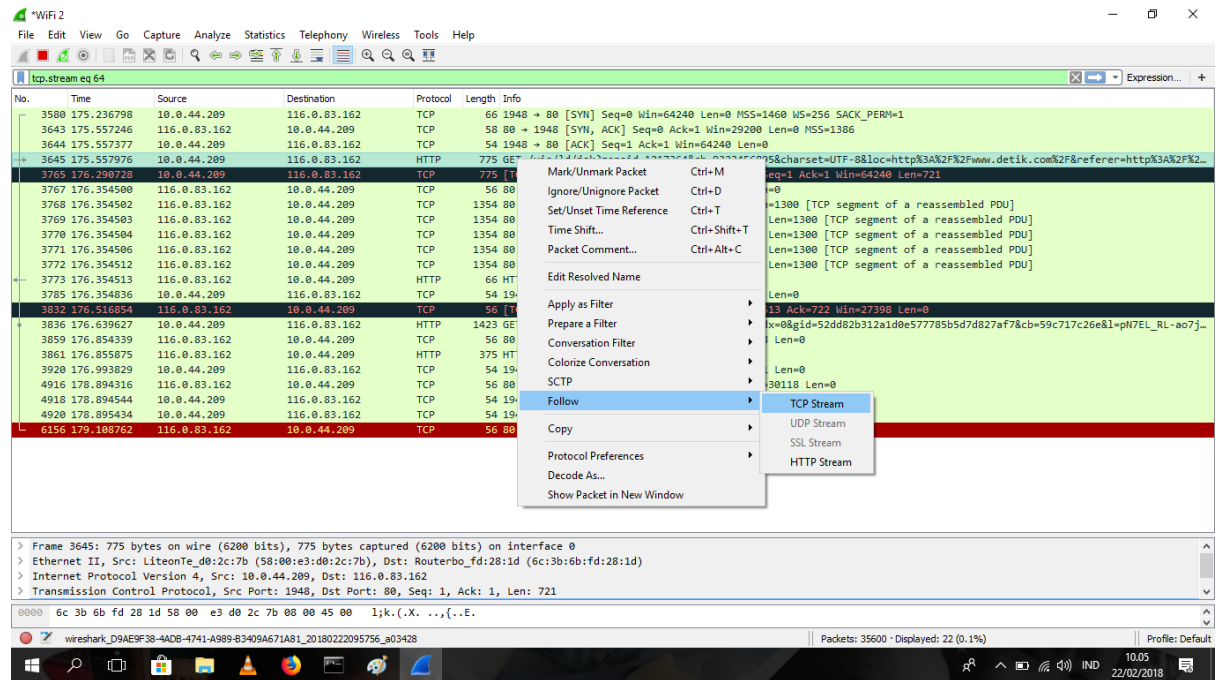


Pada gambar diatas terdapat banyak data dalam bentuk paket data jaringan. Dikarenakan banyaknya paket data yang terjangkau agar kita bisa lebih cepat mendapatkan ip yang ingin kita analisis maka kita kerikan dengan sintaks **“ip.src= =10.0.44.209”**.

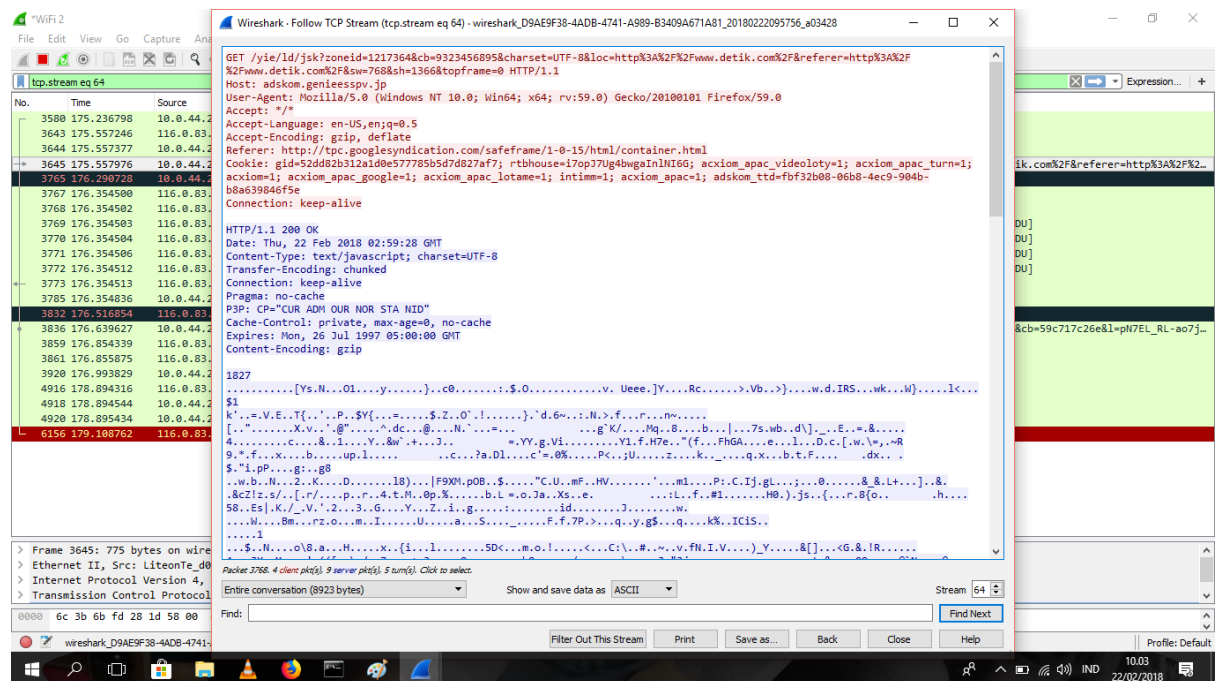
Dan filter data hanya akan mengumpulkan paket data dengan **ip 10.0.44.209**.



Bagian 2 “MENGUNAKAN MENU FOLLOW STREAM”.



Maka kita cari paket yang memiliki bentuk protokol http dan klik. Analyze → follow → tcp stream. Setelah itu akan muncul tampilan :



Informasi – informasi yang dapat kita lihat adalah :

1. User sedang mengakses ww.detik.com menggunakan aplikasi mozilla firefox.
2. User mengakses pada hari rabu tanggal 22 februari 2018.

Selanjutnya kina gunakan pilihan TCP Http :

The screenshot shows the Wireshark interface with a list of network packets. The selected packet (No. 6156) is a TCP segment from 179.188.762 to 116.0.83.162, port 80. A context menu is open over this packet, and the 'Follow' option is selected, leading to a sub-menu where 'HTTP Stream' is chosen. The interface also shows packet details for the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields.

Setelah itu akan muncul menu seperti dibawah ini :

The screenshot shows the 'Follow HTTP Stream' dialog box in Wireshark. The dialog displays the raw HTTP request data, including headers like Host, User-Agent, and Cookie, and the body content. The body content is a JavaScript function call, likely for tracking or analytics. The dialog also shows the 'Find' field and 'Find Next' button.

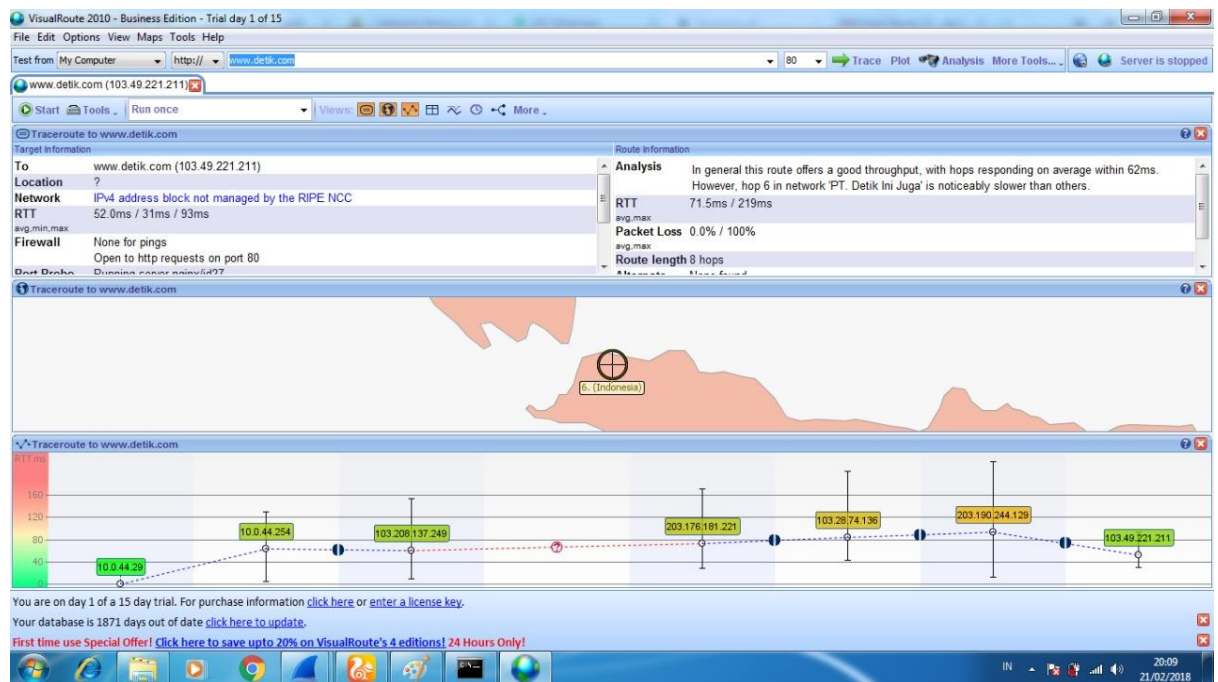
Bagian 3 “FLOW GRAPH JARINGAN MENGGUNAKAN APLIKASI WIRWSHARK DAN VISUAL ROUTE”

Didata yang sama kita flow graph data tersebut, maka akan muncul tampilan

WIRESHARK



VISUALROUTE



Dapat kita lihat langsung bagaimana perbedaan aplikasi wireshark dengan visualroute

1. Pada aplikasi wireshark kita bisa melihat langsung bagai mana laju lalu lintas perjalanan data apakah data itu mentap atau kembali atau tidak kepada user. Data yang diberikan juga sangat spesifik dan mendetail karena setiap hop terstruktur dengan rapi.
2. Aplikasi visual route sangat mudah dipakai dan dipahami oleh pemula, penampakan daerah hop terlihat jelas, visualisasi source dan destination terlihat jelas tetapi detail aliran data tidak ditampilkan tidak ada flowgraph yang menunjukkan timbal balik antar data.