

ANALISA HASIL CAPTURE, FOLLOW STREAM, DAN FOLLOW GRAPH JARINGAN  
MENGUNAKAN APLIKASI WIRESHARK,  
DAN VISUAL ROUTE



Disusun oleh :

Yoggie al hanif

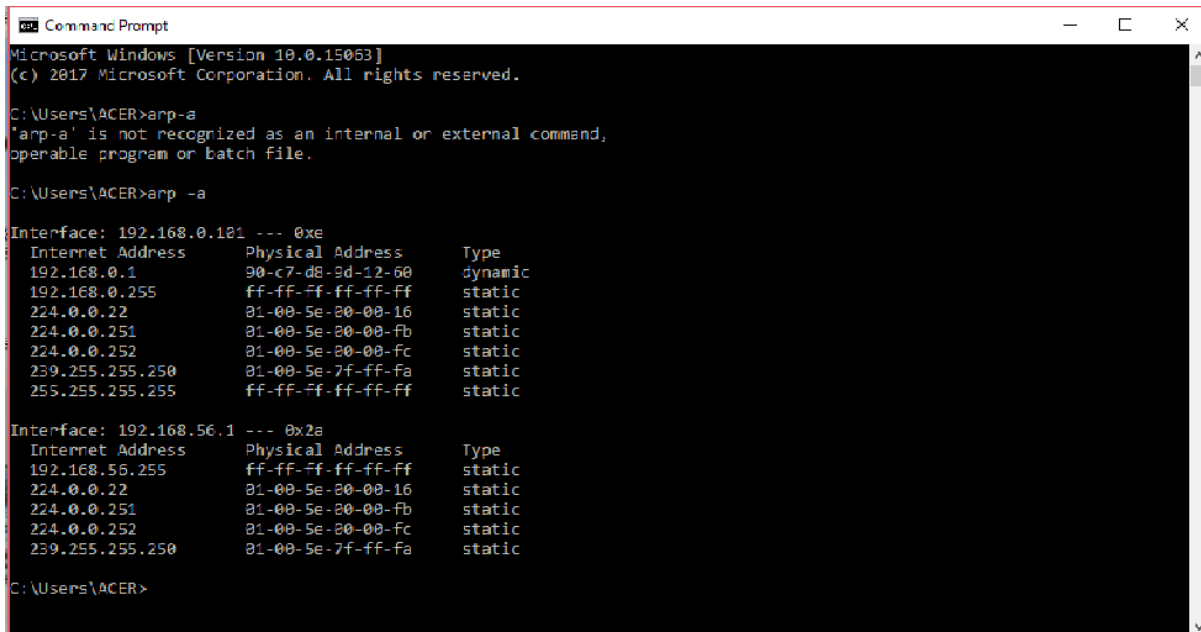
09011381621113

SK 4B

SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA

## Cara menganalisa ip jaringan kita

Sebelum melakukan menganalisa paket jaringan, terlebih dahulu mengetahui berapa adress yang sedang kita pakai. dengan cara membuka cmd dan ketik perintah "arp -a" maka adress jaringan kita akan diketahui seperti gambar dibawah ini.



```
Microsoft Windows [Version 10.0.15053]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\ACER>arp-a
'arp-a' is not recognized as an internal or external command,
operable program or batch file.

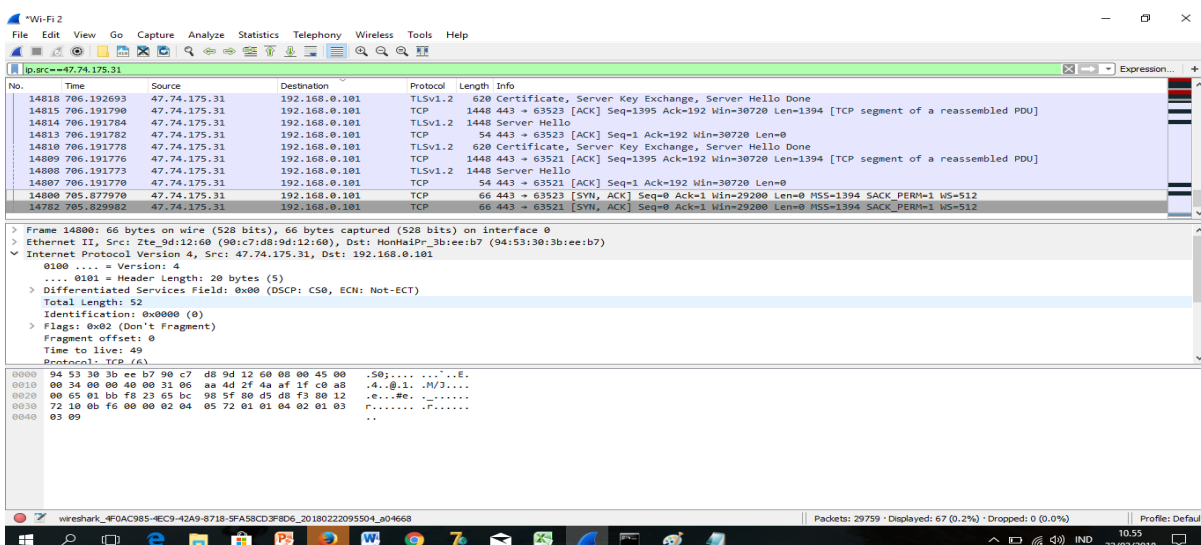
C:\Users\ACER>arp -a

Interface: 192.168.0.101 --- 0xe
Internet Address      Physical Address      Type
192.168.0.1           90-c7-d8-9d-12-60    dynamic
192.168.0.255         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
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x2a
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\ACER>
```

Selanjutnya kita dapatkan, langkah selanjutnya adalah kita membuka aplikasi WIRESHARK. Disini saya menggunakan wifi dari andromax saya Andromax-M3Z-1260.



```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src==47.74.175.31
No. Time Source Destination Protocol Length Info
14818 786.192693 47.74.175.31 192.168.0.101 TLSv1.2 608 Certificate, Server Key Exchange, Server Hello Done
14815 786.191790 47.74.175.31 192.168.0.101 TCP 1448 443 -> 63523 [ACK] Seq=1395 Ack=192 Win=30720 Len=1394 [TCP segment of a reassembled PDU]
14814 786.191784 47.74.175.31 192.168.0.101 TLSv1.2 1448 Server Hello
14813 786.191782 47.74.175.31 192.168.0.101 TCP 54 443 -> 63523 [ACK] Seq=1 Ack=192 Win=30720 Len=0
14810 786.191778 47.74.175.31 192.168.0.101 TLSv1.2 608 Certificate, Server Key Exchange, Server Hello Done
14809 786.191776 47.74.175.31 192.168.0.101 TCP 1448 443 -> 63521 [ACK] Seq=1395 Ack=192 Win=30720 Len=1394 [TCP segment of a reassembled PDU]
14808 786.191773 47.74.175.31 192.168.0.101 TLSv1.2 1448 Server Hello
14807 786.191770 47.74.175.31 192.168.0.101 TCP 54 443 -> 63521 [ACK] Seq=1 Ack=192 Win=30720 Len=0
14800 785.879790 47.74.175.31 192.168.0.101 TCP 66 443 -> 63523 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512
14782 785.829982 47.74.175.31 192.168.0.101 TCP 66 443 -> 63521 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1394 SACK_PERM=1 WS=512

> Frame 14800: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Zte_9d12:12:60 (90:c7:d8:9d:12:60), Dst: HontaiPc_3b1ee:b7 (04:15:30:3b:1ee:b7)
  > Internet Protocol Version 4, Src: 47.74.175.31, Dst: 192.168.0.101
    0100 ... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 52
      Identification: 0x0000 (0)
      Flags: 0x02 (Don't Fragment)
      Fragment offset: 0
      Time to live: 49
      Protocol: TCP (6)
    0000 04 53 30 3b ee b7 90 c7 d8 9d 12 60 00 00 45 00 .S0:.....E.
    0010 00 34 00 00 40 00 31 06 aa 4d 2f 4a af 1f c0 a8 .4.@.1./J/...
    0020 00 65 01 bb f8 23 65 bc 98 5f 80 d5 d8 f3 80 12 .e...Pe.....
    0030 72 10 0b f6 00 00 02 04 05 72 01 01 04 02 01 03 P.....P.....
    0040 03 09 ..
```

Dari gambar di atas kita telah mendapatkan bentuk pakeet jaringan karena semua paket tersaing dengan cepat, maka lebih baik di filter terlebih dahulu dengan menggunakan sintak "ip.src==192.168.0.101".

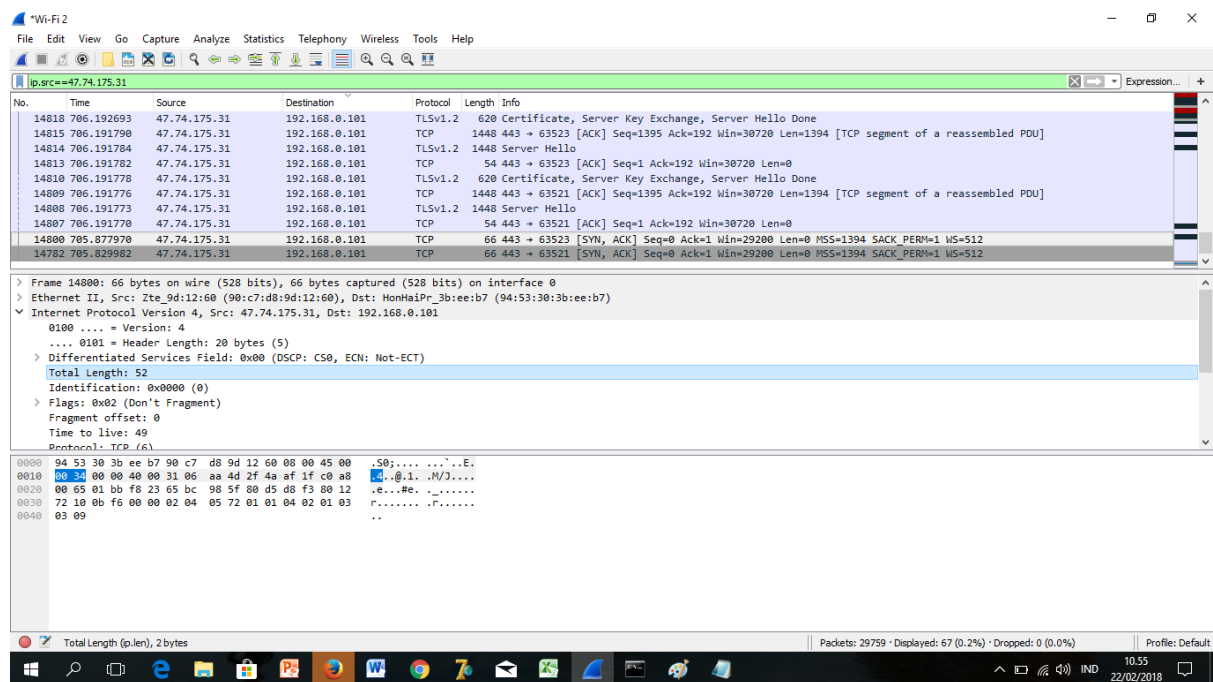
Dan setelah di filter maka akan terdapat lagi data yang berupa yakni:

The screenshot shows a Wireshark capture with the filter `ip.src==192.168.0.101`. The packet list shows several DNS queries from 192.168.0.101 to 192.168.0.1. The selected packet (No. 14753) is a DNS query for `www.tokopedia.com`. The packet details pane shows the Internet Protocol Version 4 and User Datagram Protocol sections. The packet bytes pane shows the raw data of the DNS query.

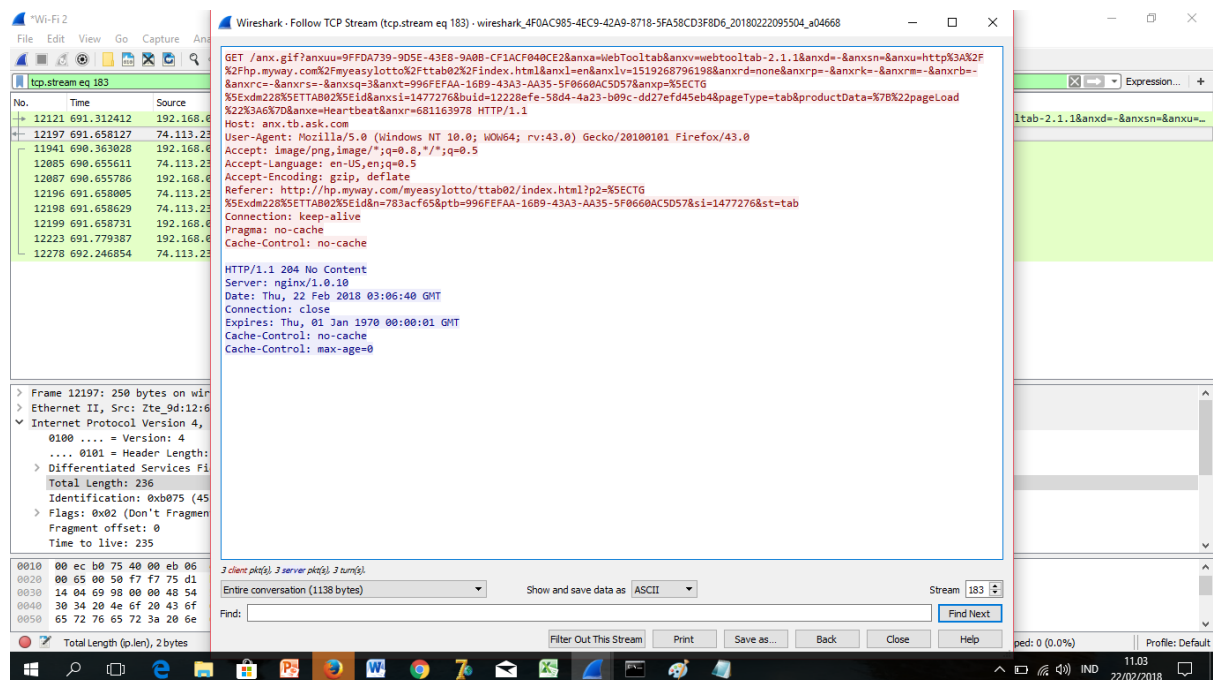
Dapat dilihat sendiri bahwa dengan komputer yang ber alamatkan 192.168.0.101 sedang mengakses 47.74.175.31 atau website [www.tokopedia.com](http://www.tokopedia.com) dengan menggunakan protocol TCP, setelah itu klik dibagian kotak tengah di menu internet protocol version 4,

The screenshot shows a Wireshark capture with the filter `ip.src==47.74.175.31`. The packet list shows several TCP segments from 47.74.175.31 to 192.168.0.101. The selected packet (No. 14800) is a SYN-ACK response. The packet details pane shows the Internet Protocol Version 4 and Transmission Control Protocol sections. The packet bytes pane shows the raw data of the TCP segment.

Dari gambar di atas di jelaskan komputer tersebut mengakses web tersebut memiliki web adress,selain itu kita mendapatkan info mengenai mac adressnya kita desaiain juga dapat mengetahui bahwa panjang yang terbaca dan mendapatkan info mengetahui tentang port.



Lalu klik analyze=> pilih follow dan => untuk pertama pilih bagian TCP stream seperti dibawah ini :

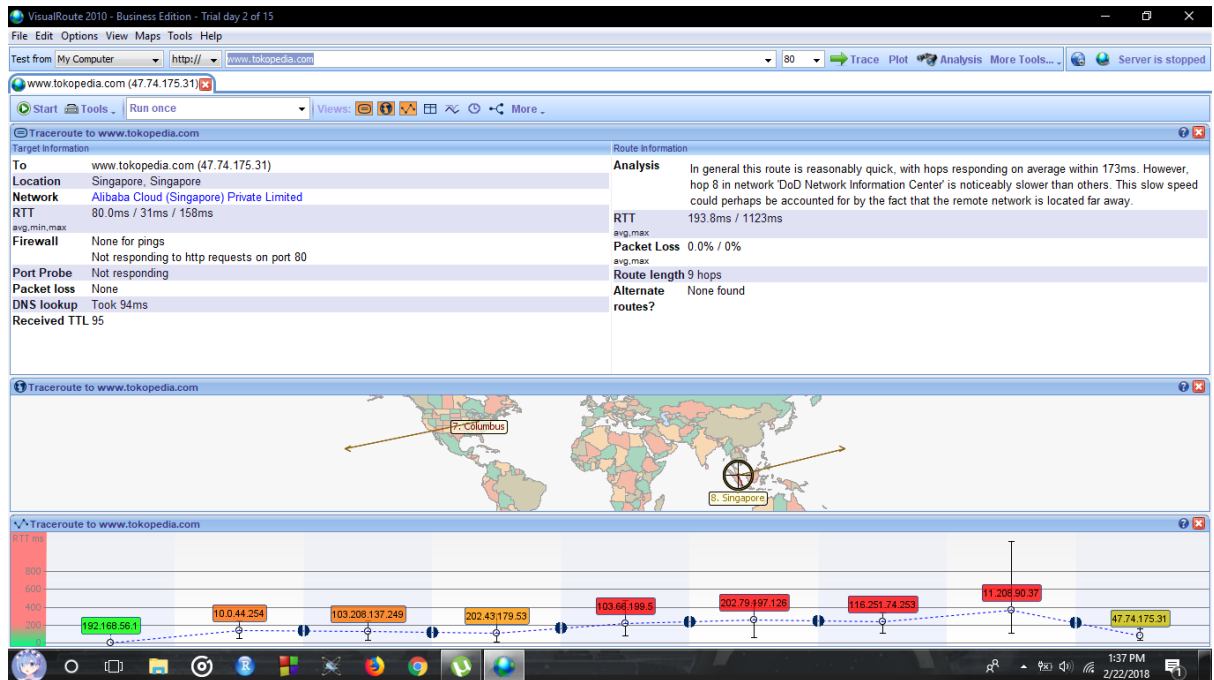


1. Pengguna yang sedang mengakses website [www.tokopedia.com](http://www.tokopedia.com) menggunakan aplikasi mozilla.



- Panah 9, yang diakses adalah [www.tokopedia.com](http://www.tokopedia.com) dengan mengambil berita internasional dan nasional.
- Panah 10, seperti pada isp tadi, server pun akan mengirim informasi ke user apakah yang dituju valid atau tidak

*BERIKUT INI TAMPILAN DARI APLIKASI VISUALROUTE :*



Perbedaan antara wireshark dan visualroute:

1. Aplikasi wireshark, dapat di analisa dan ada timbal balik kepada user, sangat berguna bagi operator server atau server manager yang memiliki kemampuan expert dan dapat meneliti data dengan detail. lebih akurat dan efektif.
2. Visual route, penggunaan aplikasi ini mudah dan mudah di mengerti oleh pengguna, dan destinasi terlihat jelas dan setiap hop ditampilkan semua tetapi kurang mumpuni dan mencapture data pada sebuah ip. dan tidak adanya filter protocol.