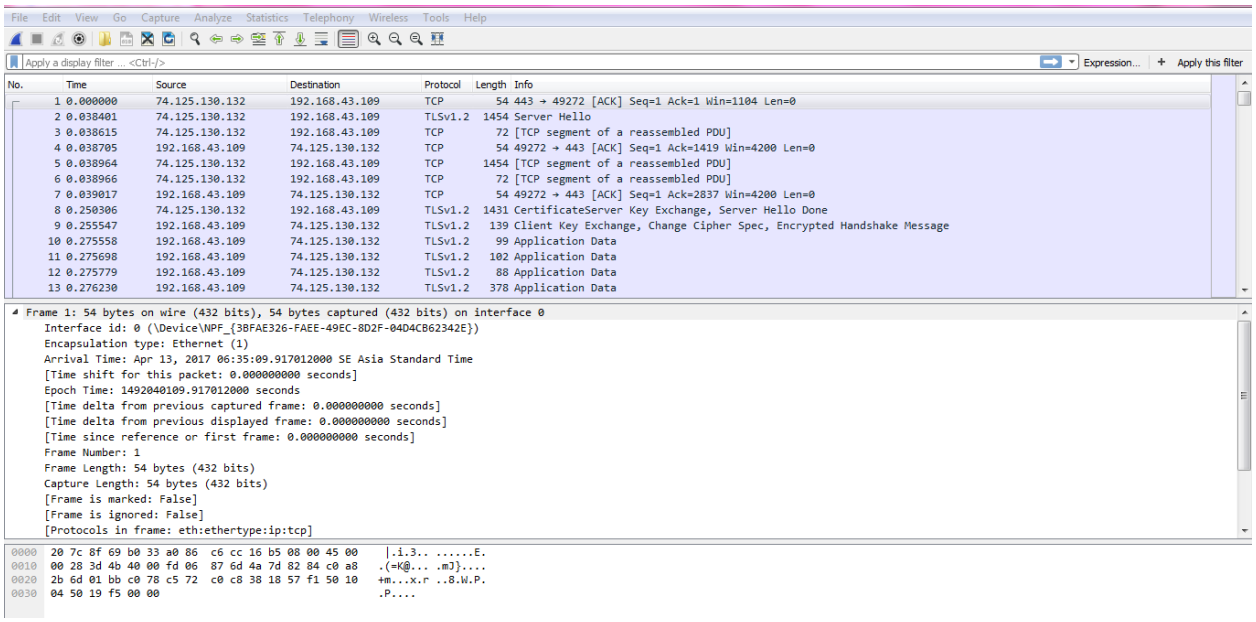
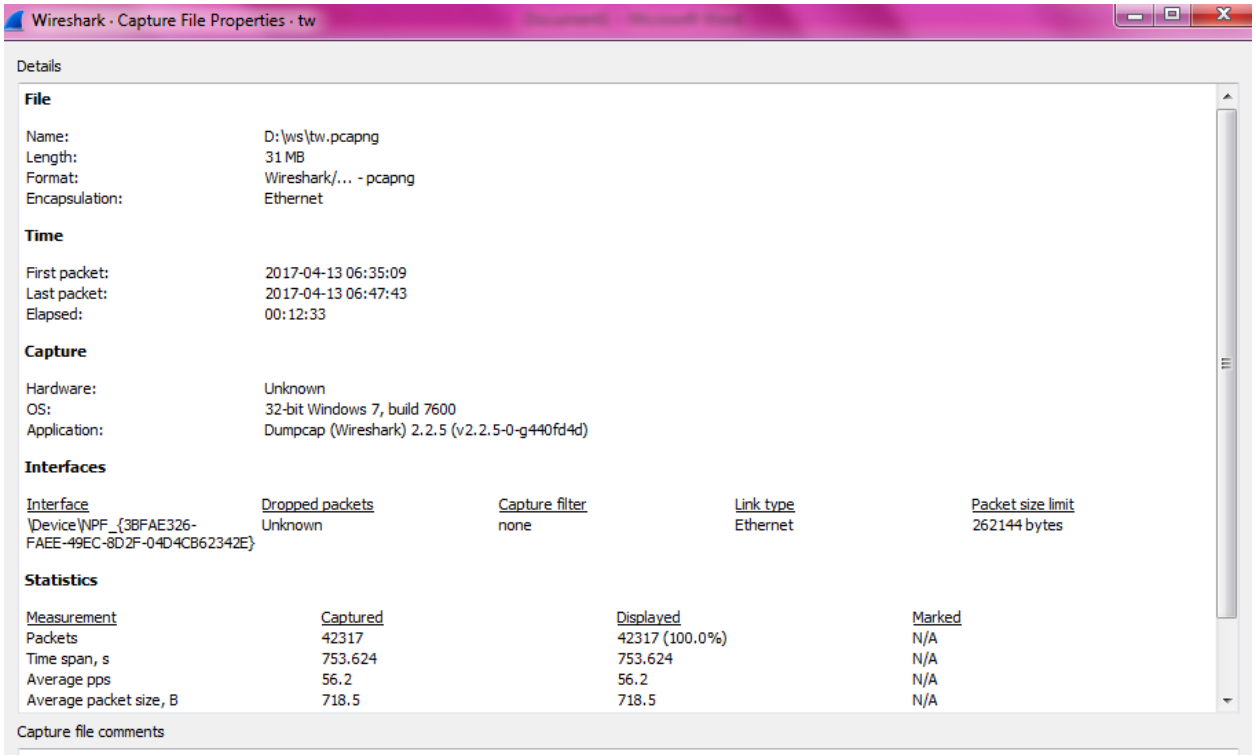
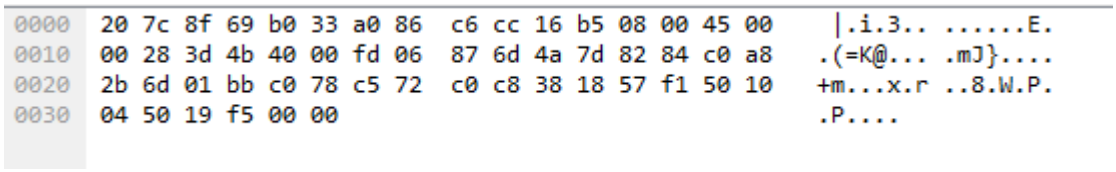
Nama : Aris Pratiwi
NIM : 09031181520121
Kelas : SI 4A

# Analisis Packets dengan aplikasi Wireshark

Twitter.com






Pada gambar diatas merupaka ringkasan dari paket data. Untuk baris yang lainnya menunjukkan data link layer, network layer , dan transport layer. Pada dasarnya paket data yang telah dicapture terbungkus didalam frame sepeti gambar diatas. Dan bytes-bytes paket data di Wireshark diperlihatkan dalam bentuk hexadecimal

Berikut adalah hasil analisa jaringan yang ter -capture saat membuka lpmgs.unsri.ac.id
Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp, dll.

Data di atas memberikan kita informasi sebagai berikut:
Alamat IP

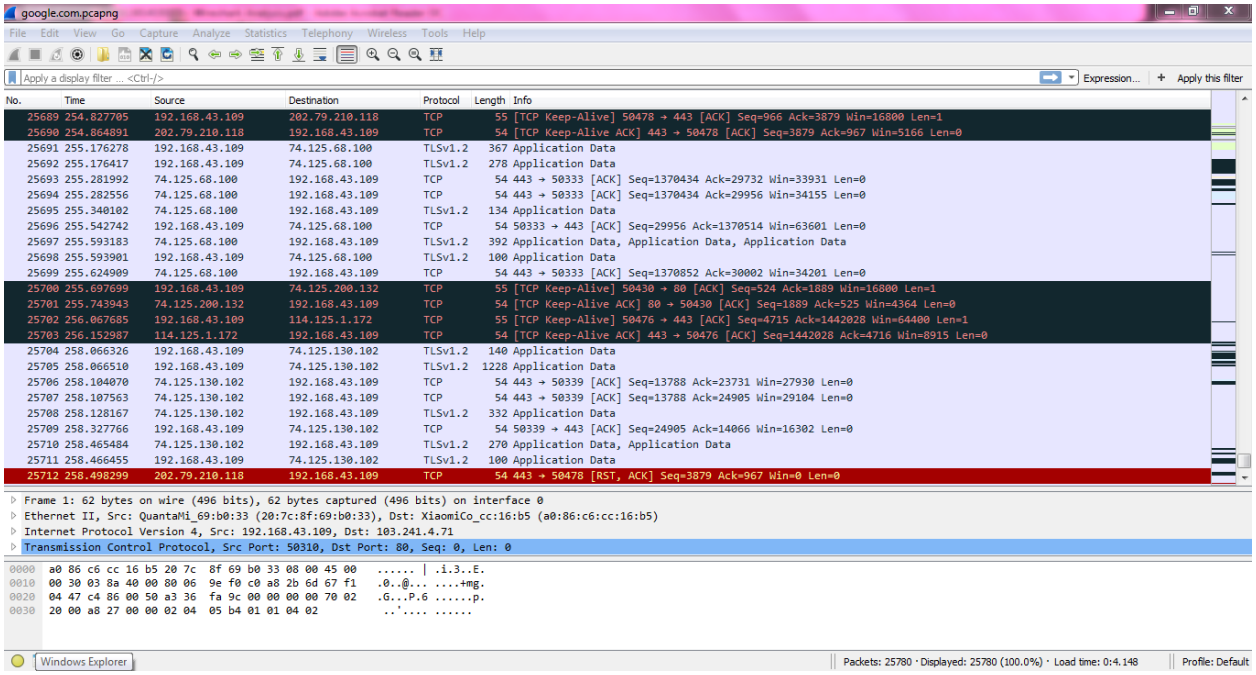
```
Src: 74.125.130.132
Dst: 192.168.43.109
```

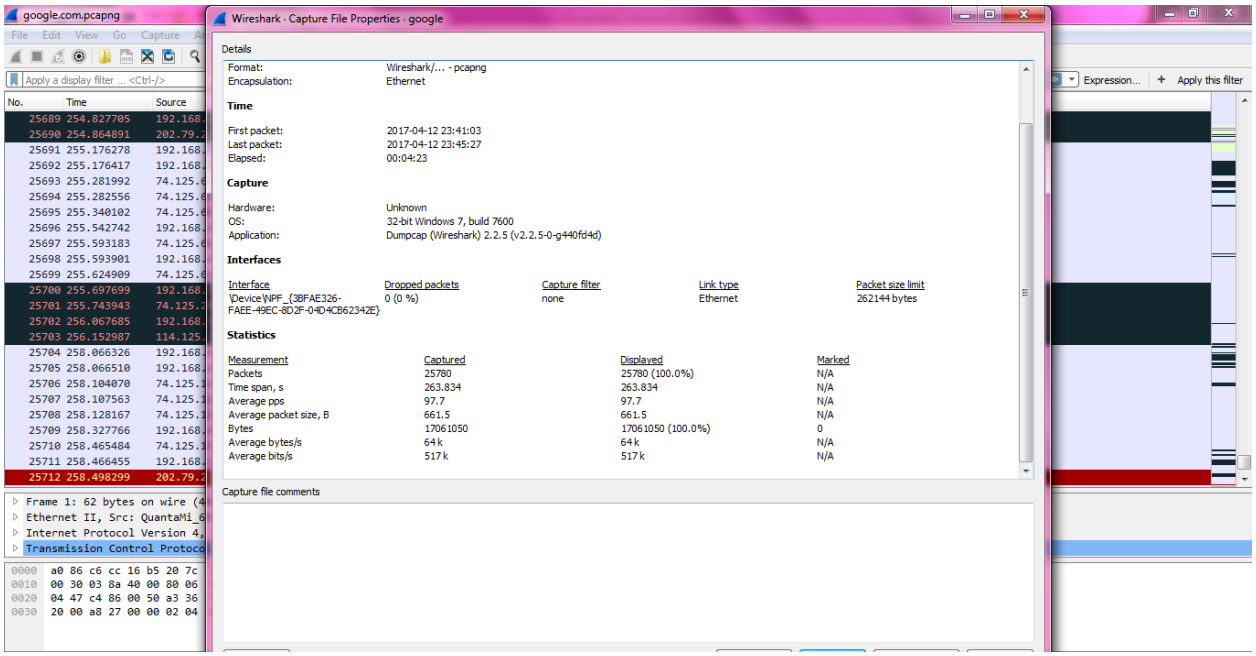
Protokol yang digunakan : TCP

```
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 253
Protocol: TCP (6)
Transmission Control Protocol, Src Port: 443, Dst Port: 49272, Seq: 1, Ack: 1, Len: 0
   Source Port: 443
   Destination Port: 49272
   [Stream index: 0]
   [TCP Segment Len: 0]
```

Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (443) dan port tujuannya (49272). Port 49272 merupakan port untuk TCP.

Google.com




Berikut adalah hasil analisa jaringan yang ter -capture saat membuka lpmgs.unsri.ac.id Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp, dll.

Data di atas memberikan kita informasi sebagai berikut:
Alamat IP

```
Src: 192.168.43.109
Dst: 103.241.4.71
```

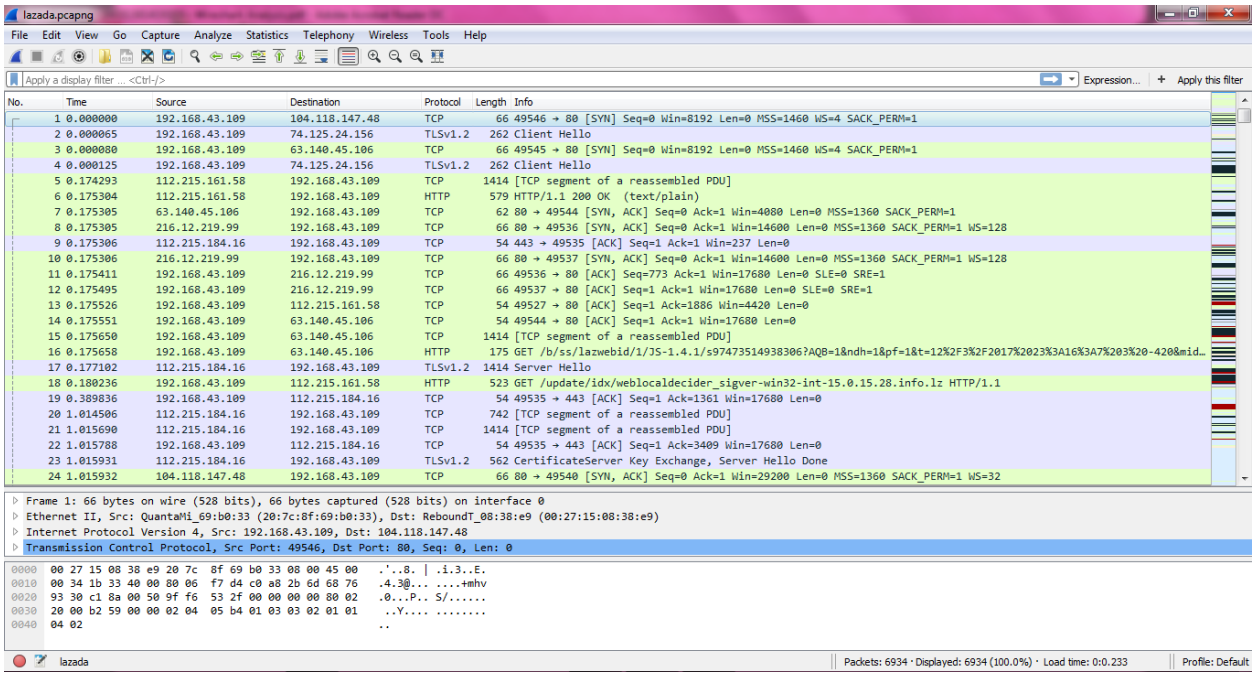
Protokol yang digunakan : TCP

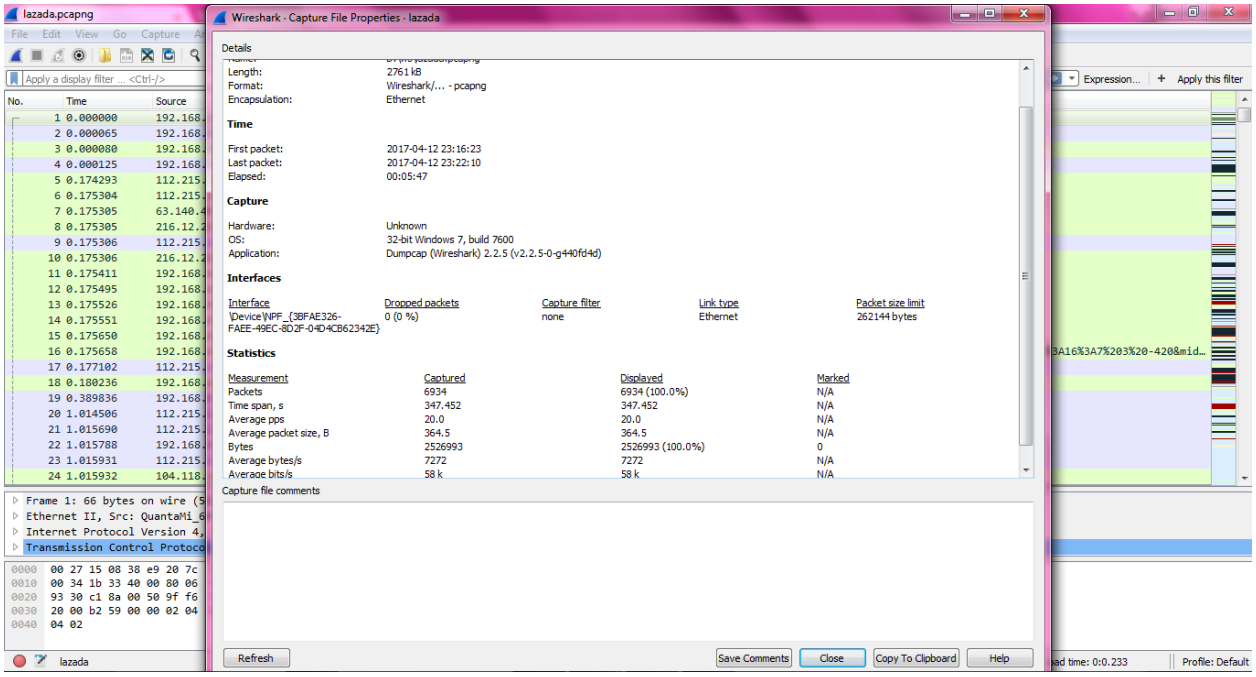
```
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)

Source Port: 50310
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
```

Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (50310) dan port tujuannya (80). Port 80 merupakan port untuk TCP.

Lazada.co.id






Berikut adalah hasil analisa jaringan yang ter -capture saat membuka lpmgs.unsri.ac.id
Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp, dll.

```
6920 346.325204  192.168.43.1        192.168.43.109       DNS      132 Standard query response 0x79ee AAAA www.lazada.co.id AAAA 64:ff9b::2d74:5b01 AAAA 64:ff9c::2d74:5b01
```

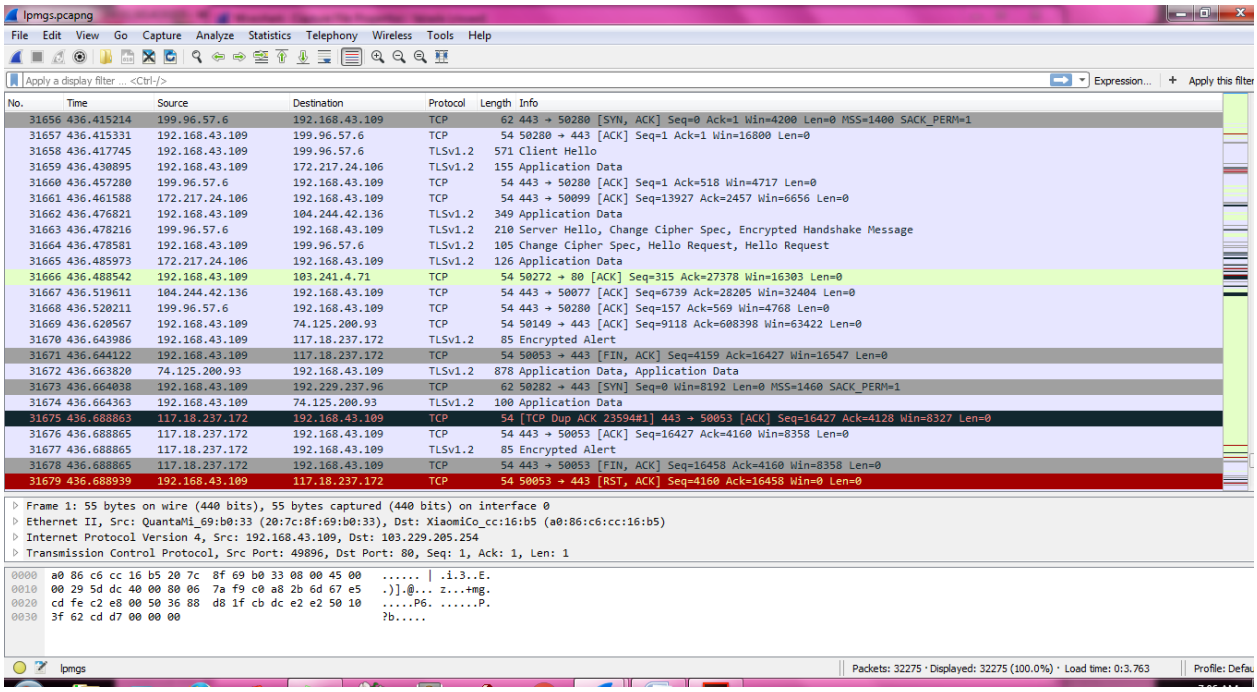
Data di atas memberikan kita informasi sebagai berikut:
Alamat IP
Src 192.168.43.1
Dst 192.168.43.109

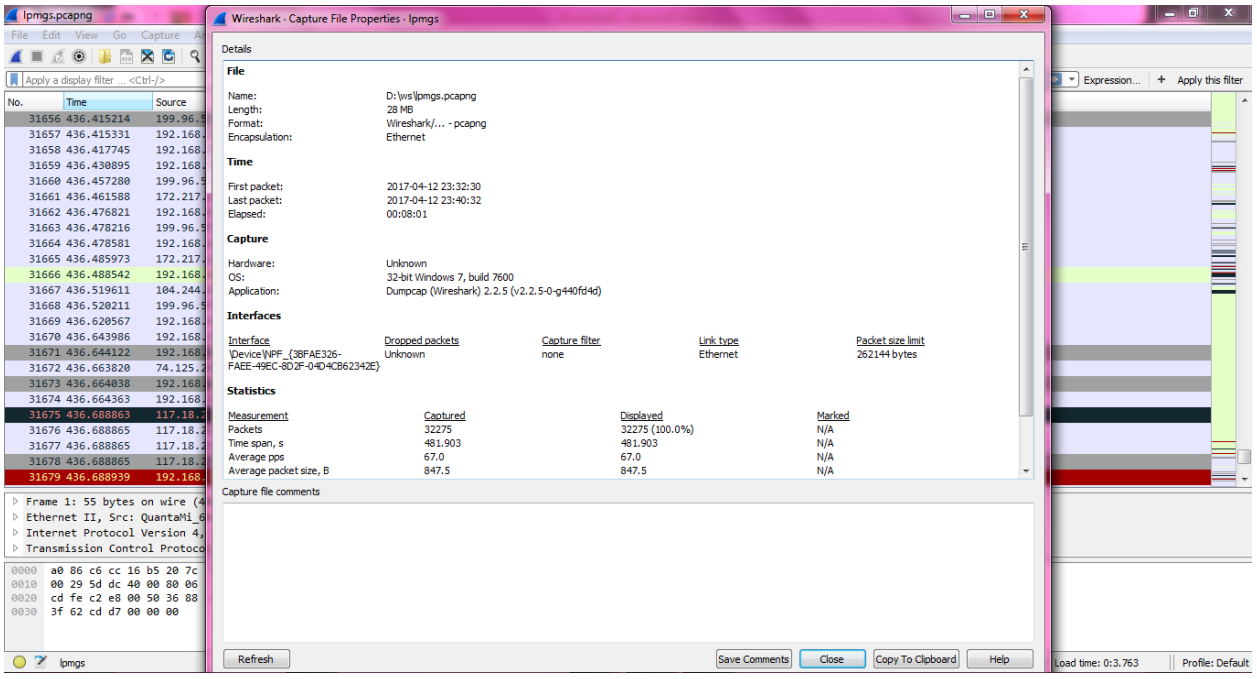
Protokol yang digunakan : DNS

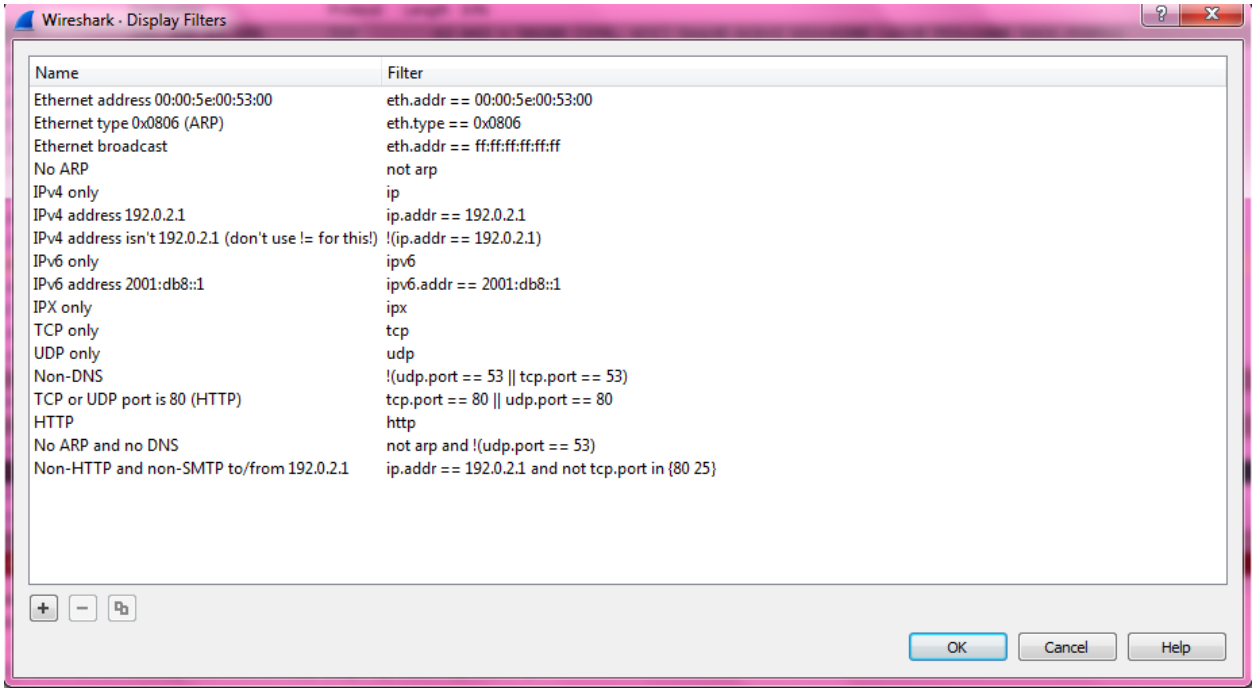
```
Source Port: 50310
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
```

Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (50310) dan port tujuannya (80). Port 80 merupakan port untuk TCP.

lpmgs.unsri.ac.id


lpmgs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression... Apply this filter
No. Time Source Destination Protocol Length Info
31656 436.415214 199.96.57.6 192.168.43.109 TCP 62 443 → 50280 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 SACK_PERM=1
31657 436.415331 192.168.43.109 199.96.57.6 TCP 54 50280 → 443 [ACK] Seq=1 Ack=1 Win=16800 Len=0
31658 436.417745 192.168.43.109 199.96.57.6 TLSv1.2 571 Client Hello
31659 436.430895 192.168.43.109 172.217.24.106 TLSv1.2 155 Application Data
31660 436.457280 199.96.57.6 192.168.43.109 TCP 54 443 → 50280 [ACK] Seq=1 Ack=518 Win=4717 Len=0
31661 436.461588 172.217.24.106 192.168.43.109 TCP 54 443 → 50099 [ACK] Seq=13927 Ack=2457 Win=6656 Len=0
31662 436.476821 192.168.43.109 104.244.42.136 TLSv1.2 349 Application Data
31663 436.478216 199.96.57.6 192.168.43.109 TLSv1.2 210 Server Hello, Change Cipher Spec, Encrypted Handshake Message
31664 436.478581 192.168.43.109 199.96.57.6 TLSv1.2 105 Change Cipher Spec, Hello Request, Hello Request
31665 436.485973 172.217.24.106 192.168.43.109 TLSv1.2 126 Application Data
31666 436.488542 192.168.43.109 103.241.4.71 TCP 54 50272 → 80 [ACK] Seq=315 Ack=27378 Win=16303 Len=0
31667 436.519611 104.244.42.136 192.168.43.109 TCP 54 443 → 50077 [ACK] Seq=6739 Ack=28205 Win=32404 Len=0
31668 436.520211 199.96.57.6 192.168.43.109 TCP 54 443 → 50280 [ACK] Seq=157 Ack=569 Win=4768 Len=0
31669 436.620567 192.168.43.109 74.125.200.93 TCP 54 50149 → 443 [ACK] Seq=9118 Ack=608398 Win=63422 Len=0
31670 436.643986 192.168.43.109 117.18.237.172 TLSv1.2 85 Encrypted Alert
31671 436.644122 192.168.43.109 117.18.237.172 TCP 54 50053 → 443 [FIN, ACK] Seq=4159 Ack=16427 Win=16547 Len=0
31672 436.663820 74.125.200.93 192.168.43.109 TLSv1.2 878 Application Data, Application Data
31673 436.664038 192.168.43.109 192.229.237.96 TCP 62 50282 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
31674 436.664363 192.168.43.109 74.125.200.93 TLSv1.2 100 Application Data
31675 436.688863 117.18.237.172 192.168.43.109 TCP 54 [TCP Dup ACK 23594#1] 443 → 50053 [ACK] Seq=16427 Ack=4128 Win=8327 Len=0
31676 436.688865 117.18.237.172 192.168.43.109 TCP 54 443 → 50053 [ACK] Seq=16427 Ack=4160 Win=8358 Len=0
31677 436.688865 117.18.237.172 192.168.43.109 TLSv1.2 85 Encrypted Alert
31678 436.688865 117.18.237.172 192.168.43.109 TCP 54 443 → 50053 [FIN, ACK] Seq=16458 Ack=4160 Win=8358 Len=0
31679 436.688939 192.168.43.109 117.18.237.172 TCP 54 50053 → 443 [RST, ACK] Seq=4160 Ack=16458 Win=0 Len=0
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
Ethernet II, Src: QuantaMi_69:b0:33 (20:7c:8f:69:b0:33), Dst: XiaomiCo_cc:16:b5 (a0:86:c6:cc:16:b5)
Internet Protocol Version 4, Src: 192.168.43.109, Dst: 103.229.205.254
Transmission Control Protocol, Src Port: 49896, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
0000 a0 86 c6 cc 16 b5 20 7c 8f 69 b0 33 08 00 45 00 ..... | .i.3..E.
0010 00 29 5d dc 40 00 80 06 7a f9 c0 a8 2b 6d 67 e5 .)].@... z...+mg.
0020 cd fe c2 e8 00 50 36 88 d8 1f cb dc e2 e2 50 10 .....P6. ......P.
0030 3f 62 cd d7 00 00 00 ?b.....
lpmgs
Packets: 32275 · Displayed: 32275 (100.0%) · Load time: 0:3.763
Profile: Defau


lpmgs.pcapng
Wireshark · Capture File Properties · lpmgs
Details
File
Name: D:\ws\lpmgs.pcapng
Length: 28 MB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2017-04-12 23:32:30
Last packet: 2017-04-12 23:40:32
Elapsed: 00:08:01
Capture
Hardware: Unknown
OS: 32-bit Windows 7, build 7600
Application: Dumpcap (Wireshark) 2.2.5 (v2.2.5-0-g440fd4d)
Interfaces
Interface Dropped packets Capture filter Link type Packet size limit
\Device\NPF_{3BFAE326-FAEE-49EC-8D2F-04D4CB62342E} Unknown none Ethernet 262144 bytes
Statistics
Measurement Captured Displayed Marked
Packets 32275 32275 (100.0%) N/A
Time span, s 481.903 481.903 N/A
Average pps 67.0 67.0 N/A
Average packet size, B 847.5 847.5 N/A
Capture file comments
Refresh
Save Comments
Close
Copy To Clipboard
Help
Load time: 0:3.763
Profile: Default




Berikut adalah hasil analisa jaringan yang ter -capture saat membuka lpmgs.unsri.ac.id Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp, dll.

Data di atas memberikan kita informasi sebagai berikut:
Alamat IP

```
Src: 192.168.43.109
Dst: 103.229.205.254
```

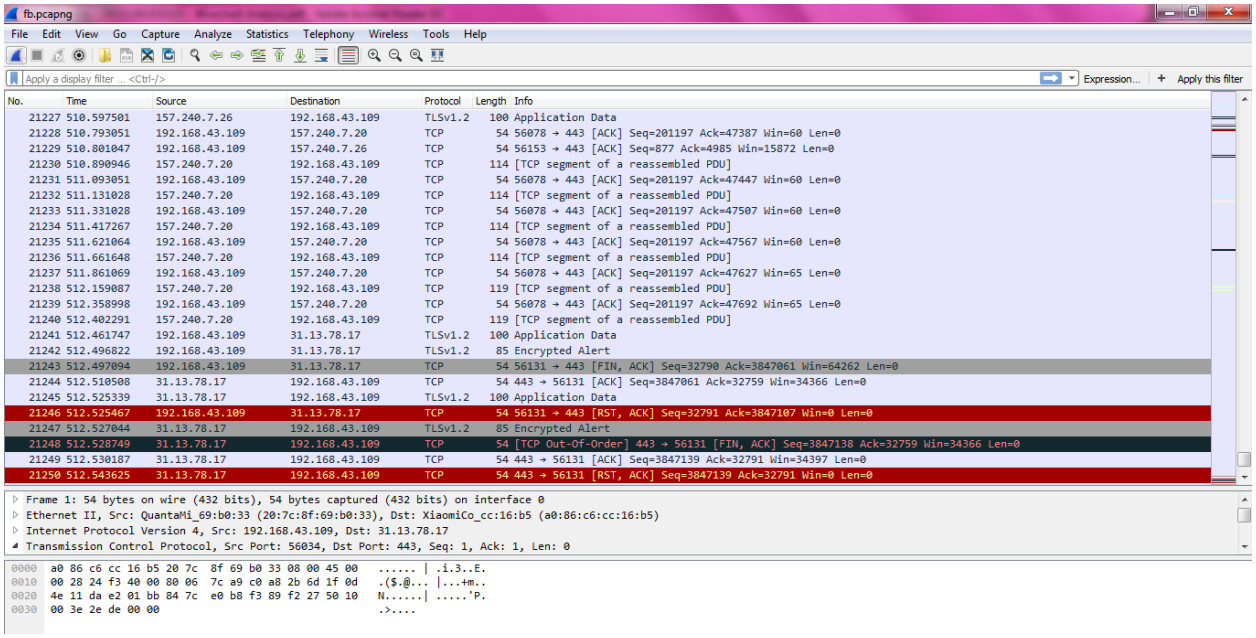
Protokol yang digunakan : TCP

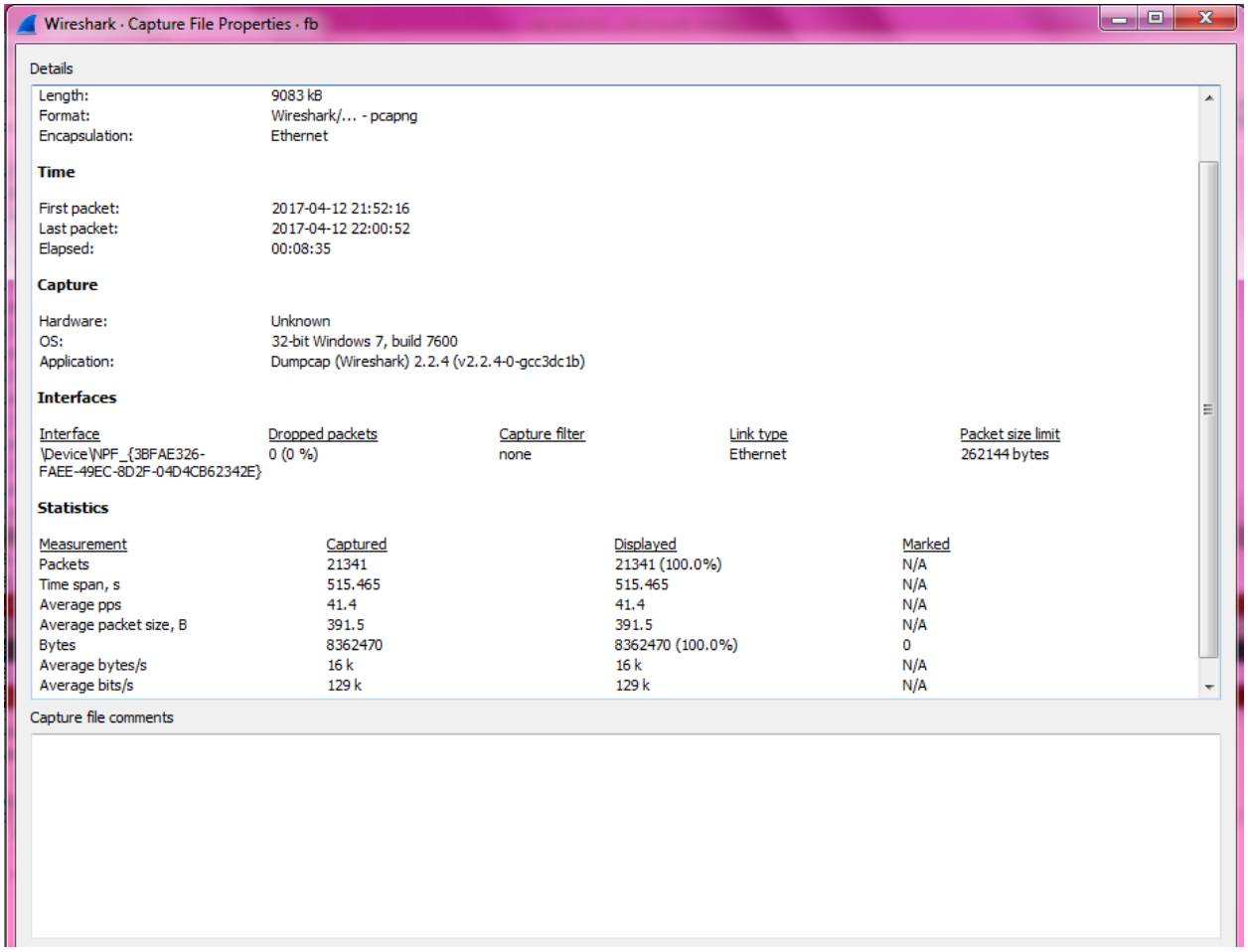
```
Flags: 0x02 (Don't Fragment)
   0... .... = Reserved bit: Not set
   .1.. .... = Don't fragment: Set
   ..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
```

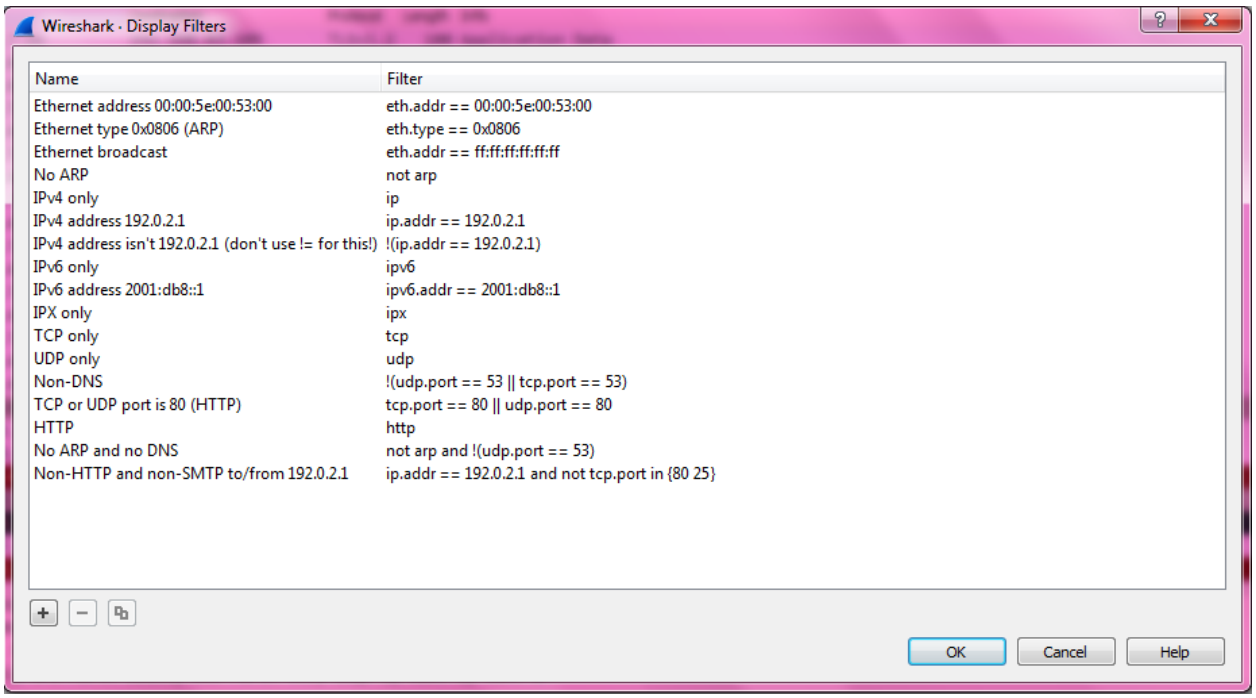
```
Transmission Control Protocol, Src Port: 49896, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
   Source Port: 49896
   Destination Port: 80
   [Stream index: 0]
   [TCP Segment Len: 1]
   Sequence number: 1    (relative sequence number)
   [Next sequence number: 2    (relative sequence number)]
   Acknowledgment number: 1    (relative ack number)
   Header Length: 20 bytes
```

Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (49896) dan port tujuannya (80). Port 80 merupakan port untuk TCP.

Facebook.com




Wireshark · Capture File Properties · fb
Details
Length: 9083 kB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2017-04-12 21:52:16
Last packet: 2017-04-12 22:00:52
Elapsed: 00:08:35
Capture
Hardware: Unknown
OS: 32-bit Windows 7, build 7600
Application: Dumpcap (Wireshark) 2.2.4 (v2.2.4-0-gcc3dc1b)
Interfaces
Interface
Dropped packets
Capture filter
Link type
Packet size limit
\Device\NPF_{3BFAE326-FAEE-49EC-8D2F-04D4CB62342E}
0 (0 %)
none
Ethernet
262144 bytes
Statistics
Measurement
Captured
Displayed
Marked
Packets 21341 21341 (100.0%) N/A
Time span, s 515.465 515.465 N/A
Average pps 41.4 41.4 N/A
Average packet size, B 391.5 391.5 N/A
Bytes 8362470 8362470 (100.0%) 0
Average bytes/s 16 k 16 k N/A
Average bits/s 129 k 129 k N/A
Capture file comments


Wireshark · Display Filters
Name
Filter
Ethernet address 00:00:5e:00:53:00 eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP) eth.type == 0x0806
Ethernet broadcast eth.addr == ff:ff:ff:ff:ff:ff
No ARP not arp
IPv4 only ip
IPv4 address 192.0.2.1 ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!) !(ip.addr == 192.0.2.1)
IPv6 only ipv6
IPv6 address 2001:db8::1 ipv6.addr == 2001:db8::1
IPX only ipx
TCP only tcp
UDP only udp
Non-DNS !(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP) tcp.port == 80 || udp.port == 80
HTTP http
No ARP and no DNS not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1 ip.addr == 192.0.2.1 and not tcp.port in {80 25}
OK
Cancel
Help

Berikut adalah hasil analisa jaringan yang ter -capture saat membuka facebook.com. Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp, dll.

Data di atas memberikan kita informasi sebagai berikut:

Alamat IP

```
Source: 192.168.43.109
Destination: 31.13.78.17
```

Protokol yang digunakan : TCP

```
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x7ca9 [validation disabled]
[Header checksum status: Unverified]
Transmission Control Protocol, Src Port: 56034, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
   Source Port: 56034
   Destination Port: 443
   [Stream index: 0]
   [TCP Segment Len: 0]
   Sequence number: 1    (relative sequence number)
   Acknowledgment number: 1    (relative ack number)
   Header Length: 20 bytes
```

Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (56034) dan port tujuannya (443). Port 443 merupakan port untuk TCP.