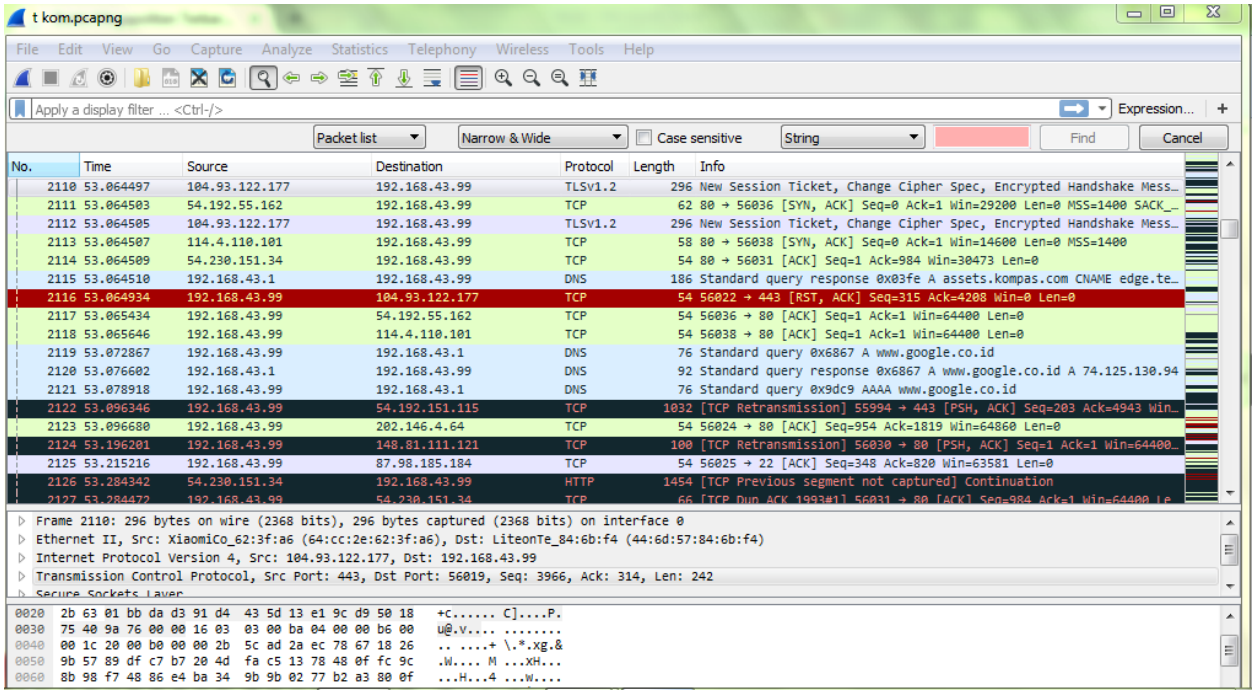
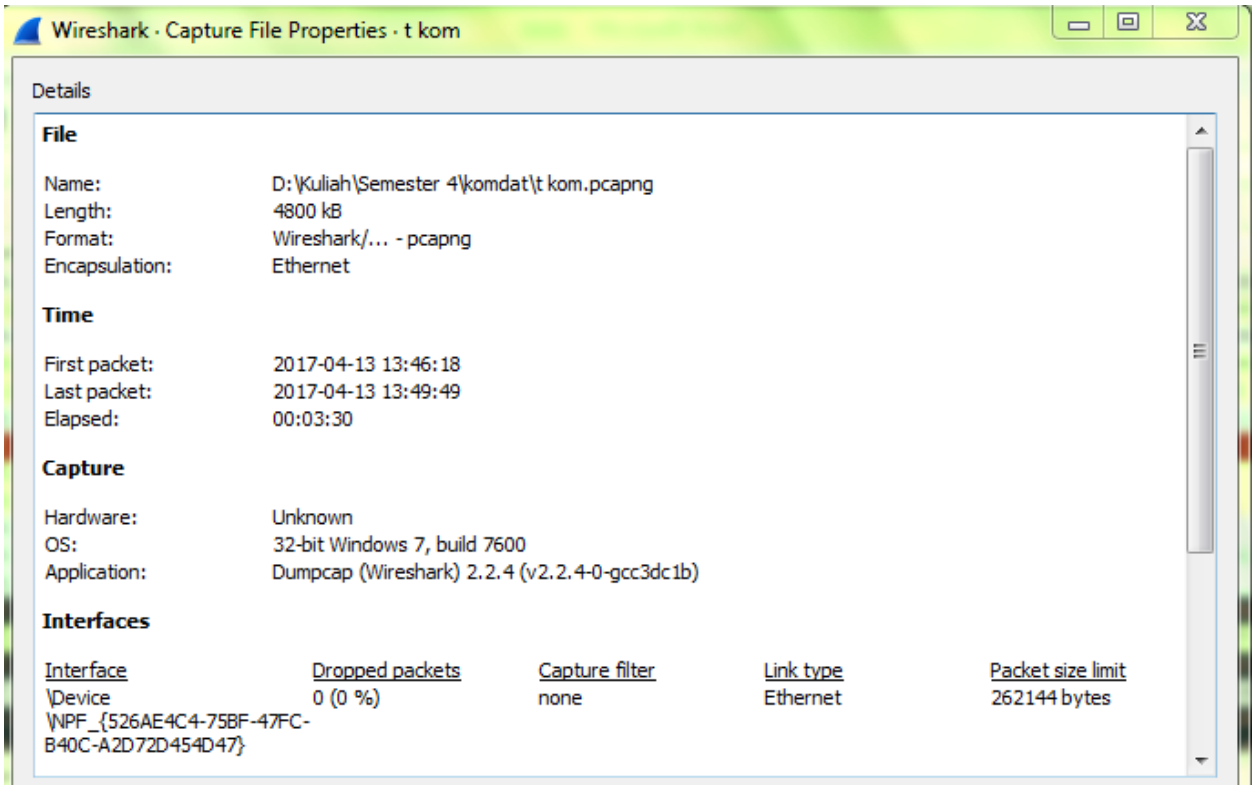
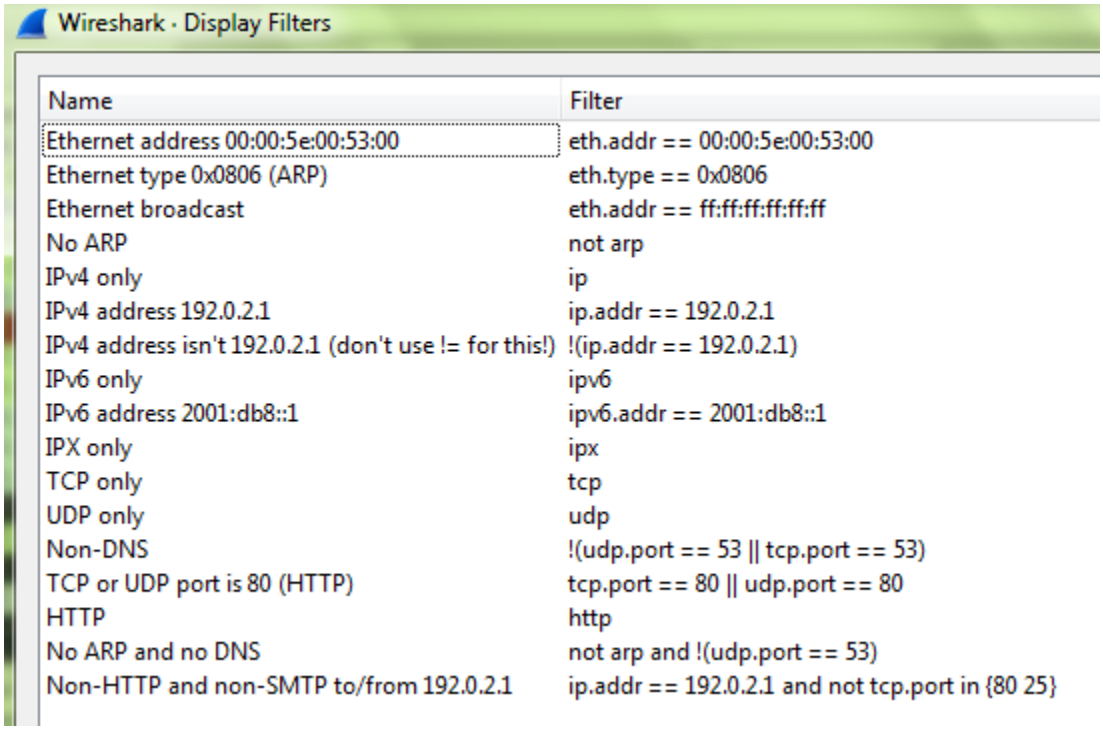
Nama : Erdo Irawan
NIM : 09031281520097
Kelas : SIREG4A
MK : Komunikasi Data dan Jaringan Komputer
Dosen Pengampuh : Deris Setiawan,Ph.D

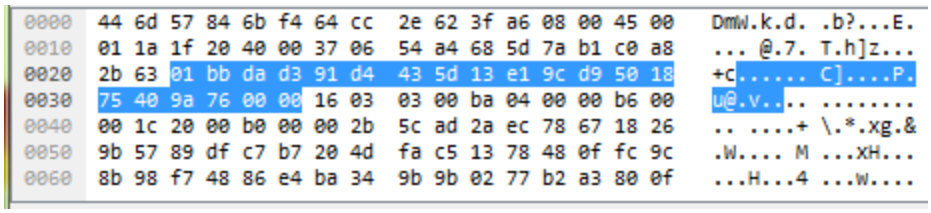
Analisis Packets Data Wireshark

1. Kompas.com




Wireshark · Capture File Properties · t kom
Details
File
Name: D:\Kuliah\Semester 4\komdat\t kom.pcapng
Length: 4800 kB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2017-04-13 13:46:18
Last packet: 2017-04-13 13:49:49
Elapsed: 00:03:30
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_{526AE4C4-75BF-47FC-B40C-A2D72D454D47}
0 (0 %)
none
Ethernet
262144 bytes


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}

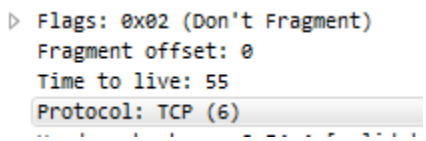


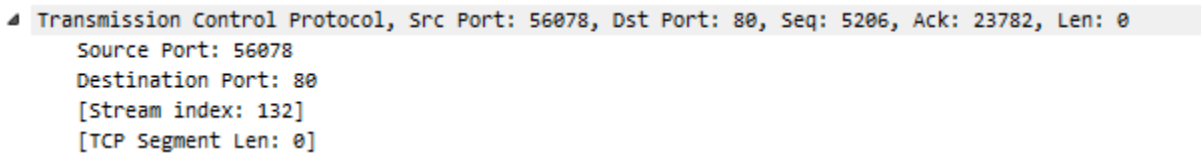
Gambar diatas merupakan ringkasan dari paket data. Untuk baris yang lainnya menunjukkan data network layer, link layer , dan transport layer. Pada dasarnya paket data yang telah dicapture terbungkus didalam frame sepeti gambar diatas. Dan bytes-bytes paket data di Wireshark diperlihatkan dalam bentuk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

Berikut adalah hasil analisa jaringan yang ter-capture dari kompas.com Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat.

Dari data diatas,dapat diperoleh infomasi sebagai berikut :
Alamat IP
Source : 192.168.43.99
Destination : 202.61.113.65

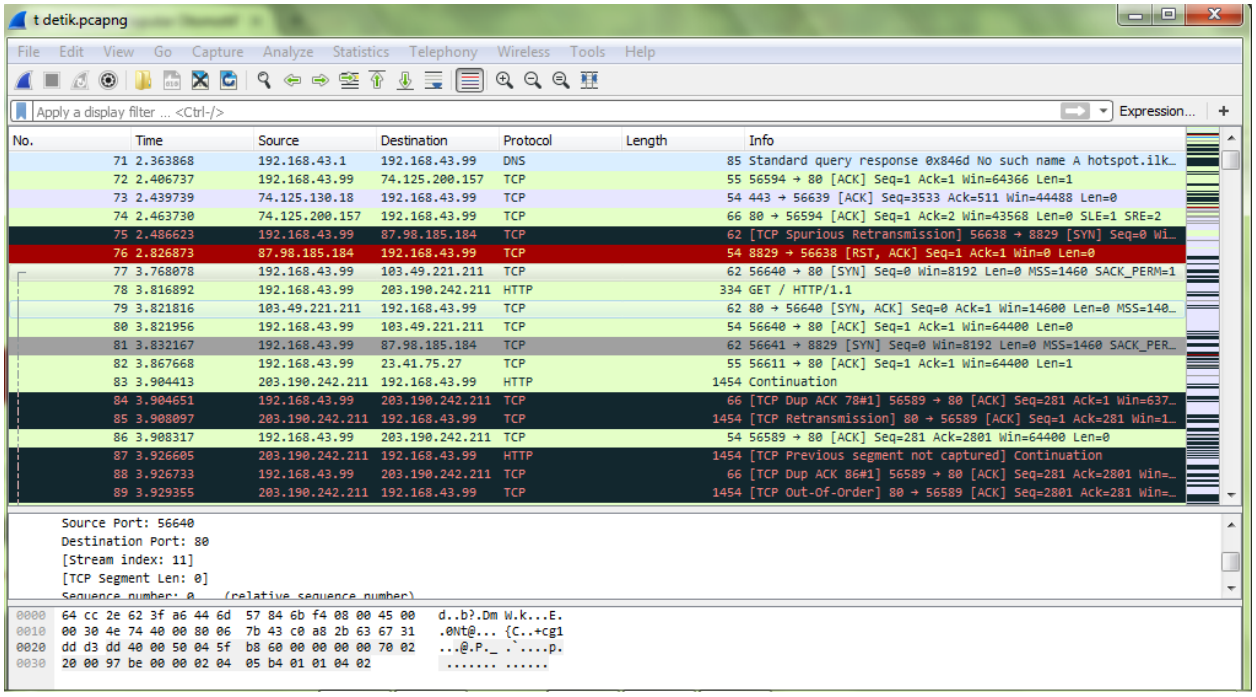
Protokol yang digunakan : TCP

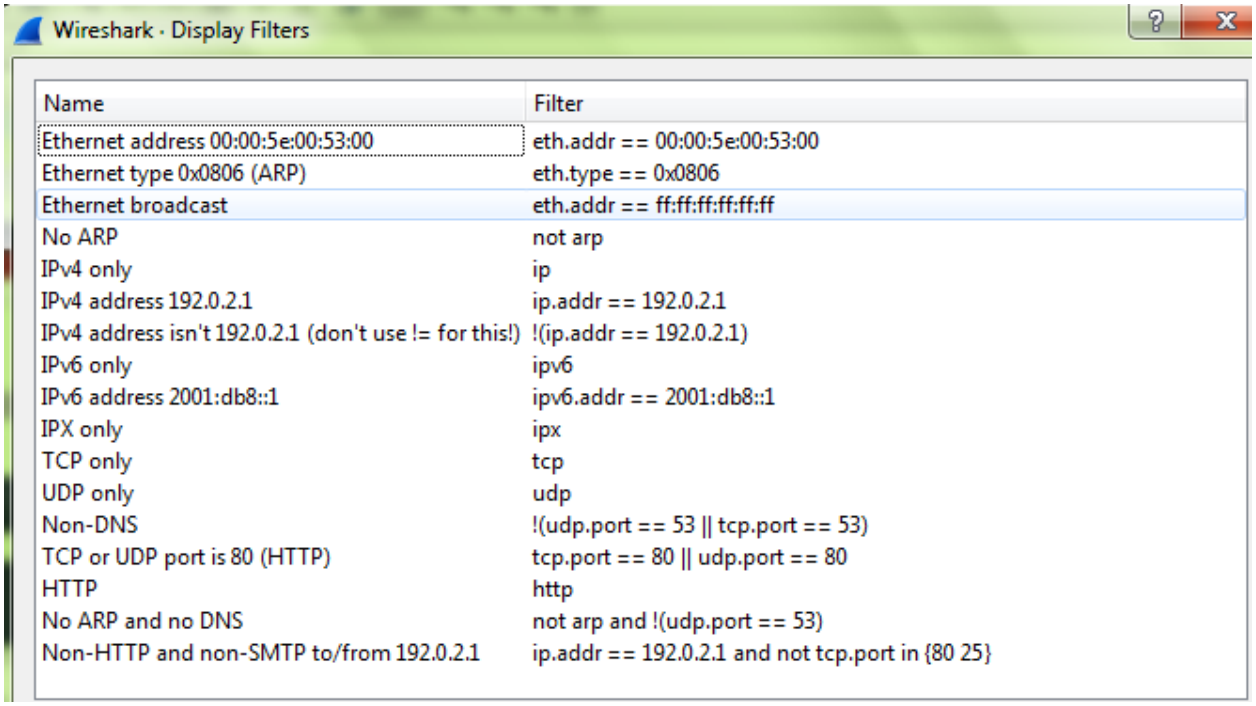




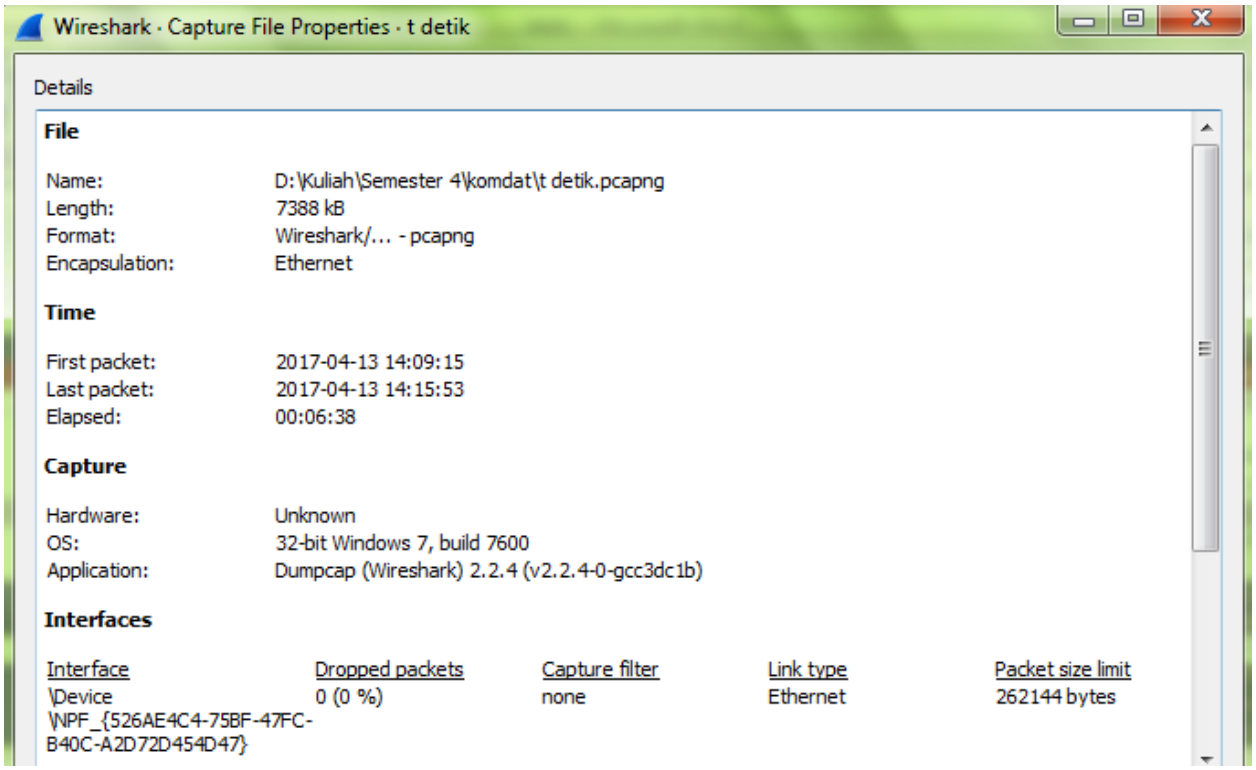
Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (56078) dan port tujuannya (80). Port 80 merupakan port untuk TCP.

2. Detik.com





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}



Berikut adalah hasil analisa jaringan yang ter -capture saat membuka detik.com Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat.

Dari data diatas,dapat diperoleh infomasi sebagai berikut :
Alamat IP
Source : 192.168.43.99
Destination : 103.49.221.211

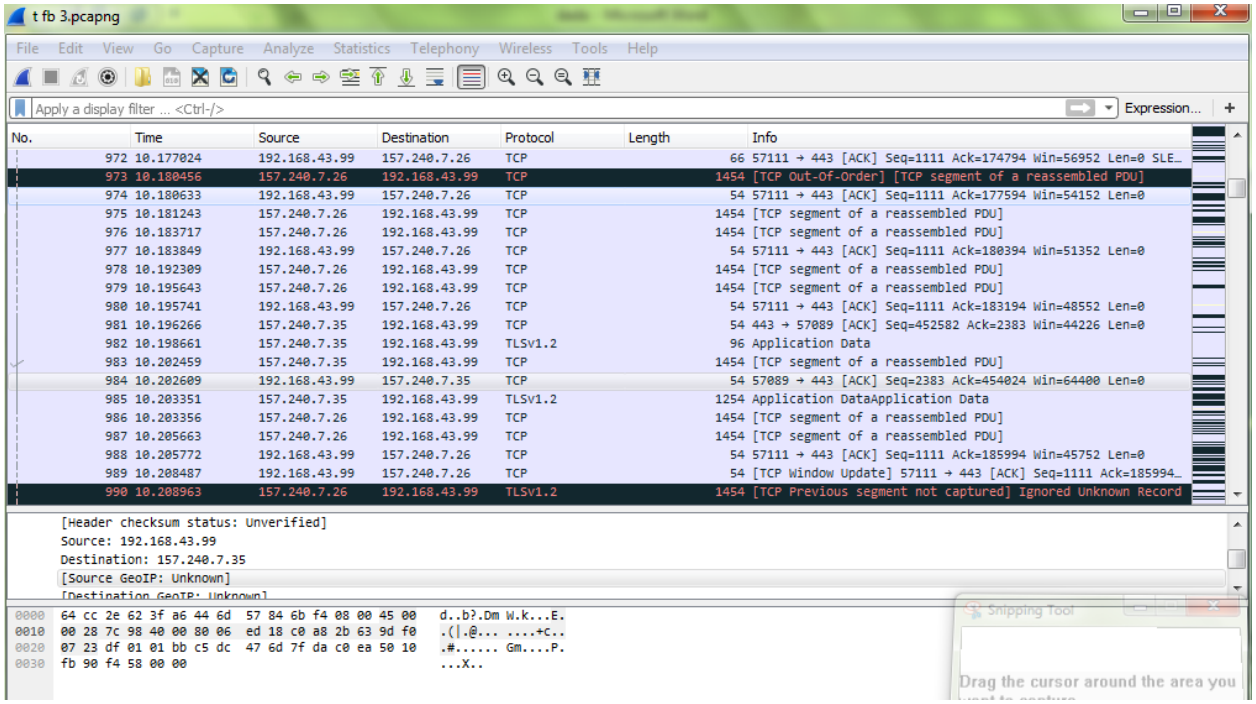
Protokol yang digunakan : TCP

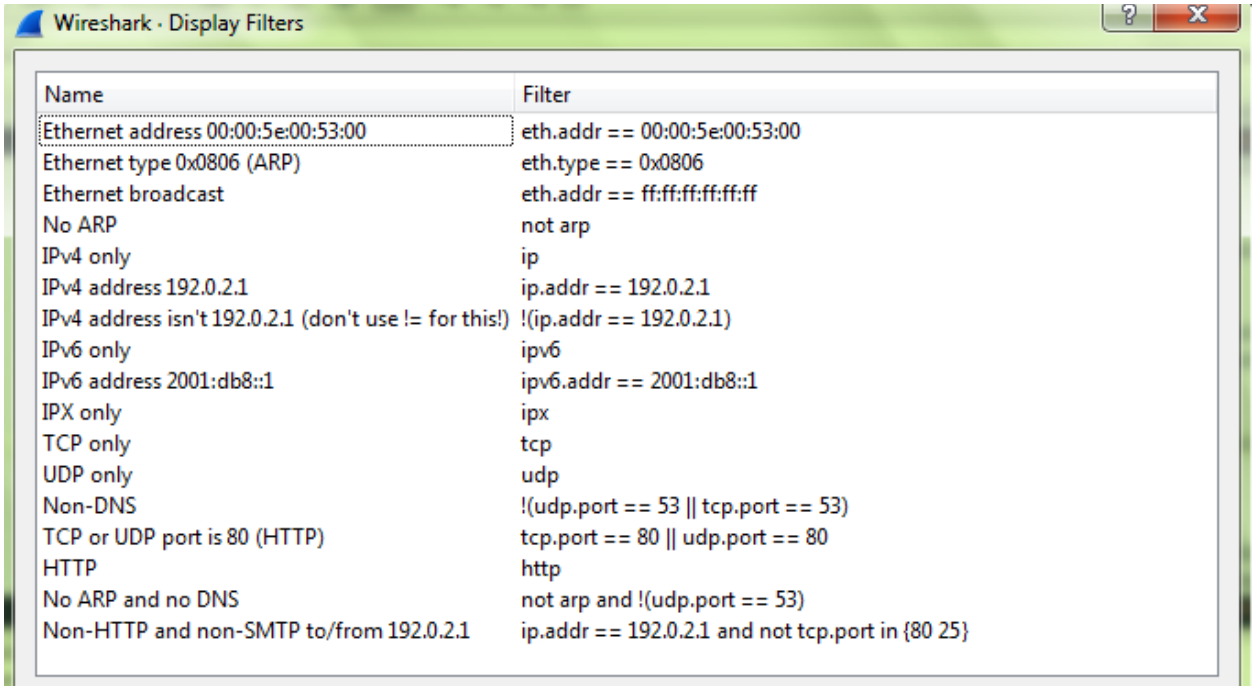
```
▷ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
```

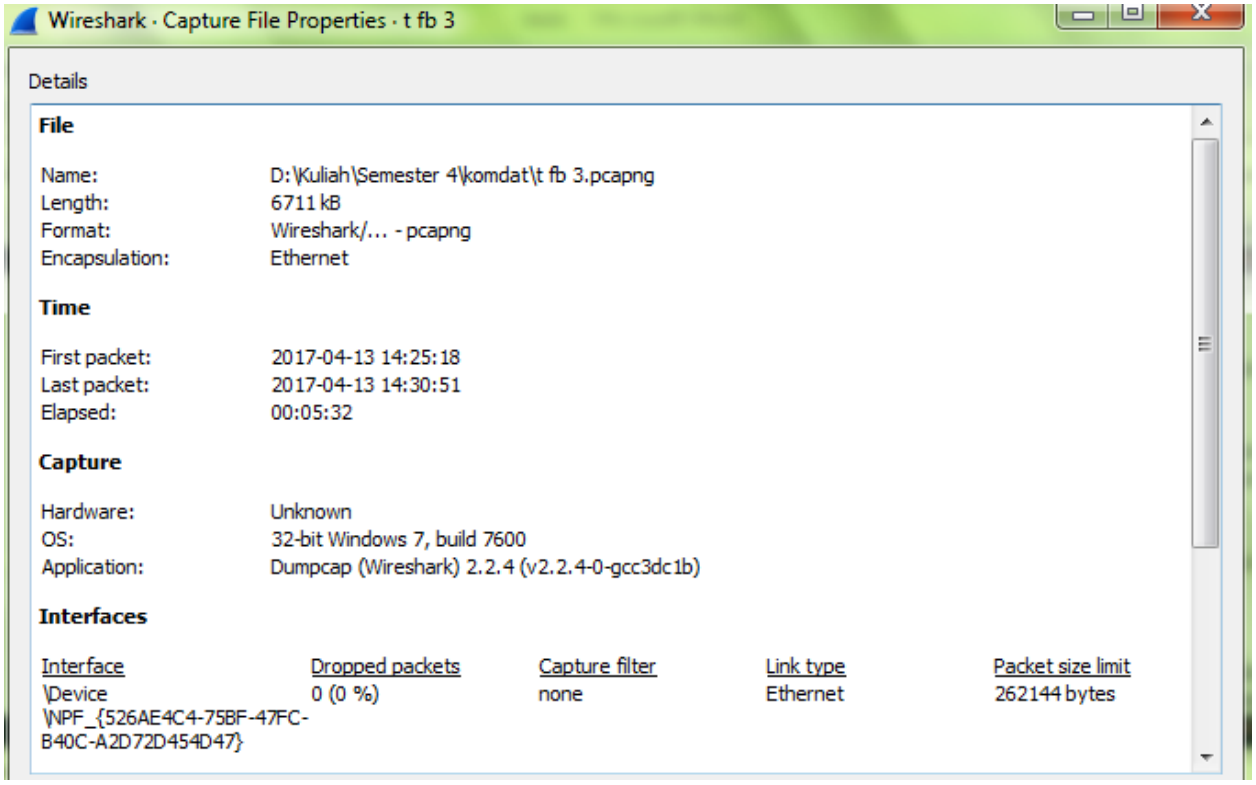
```
◢ Transmission Control Protocol, Src Port: 56640, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 56640
    Destination Port: 80
    [Stream index: 11]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 28 bytes
```

Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (56640) dan port tujuannya (80). Port 80 merupakan port untuk TCP.

3. Facebook.com



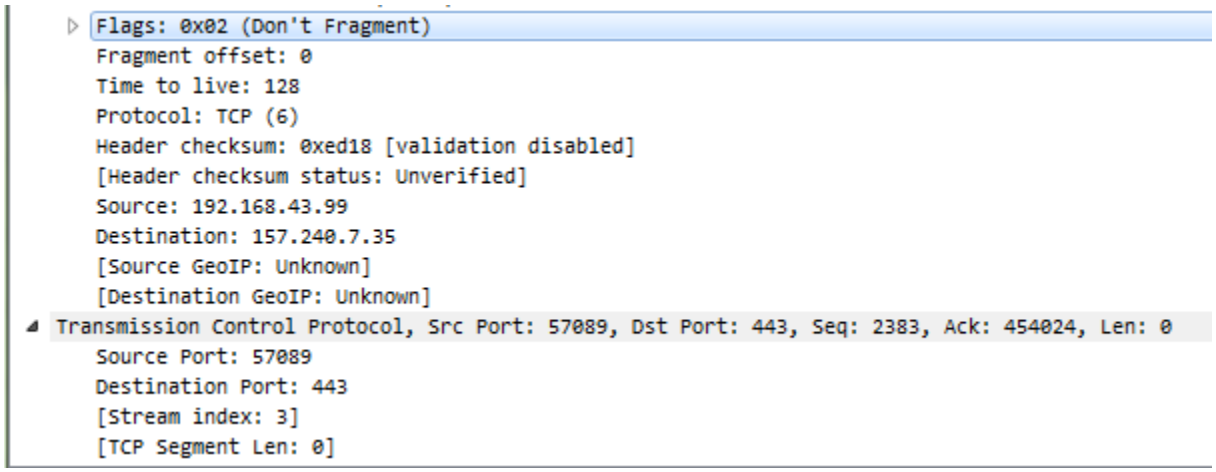




Berikut adalah hasil analisa jaringan yang ter -capture saat membuka facebook.com
Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp, dll.

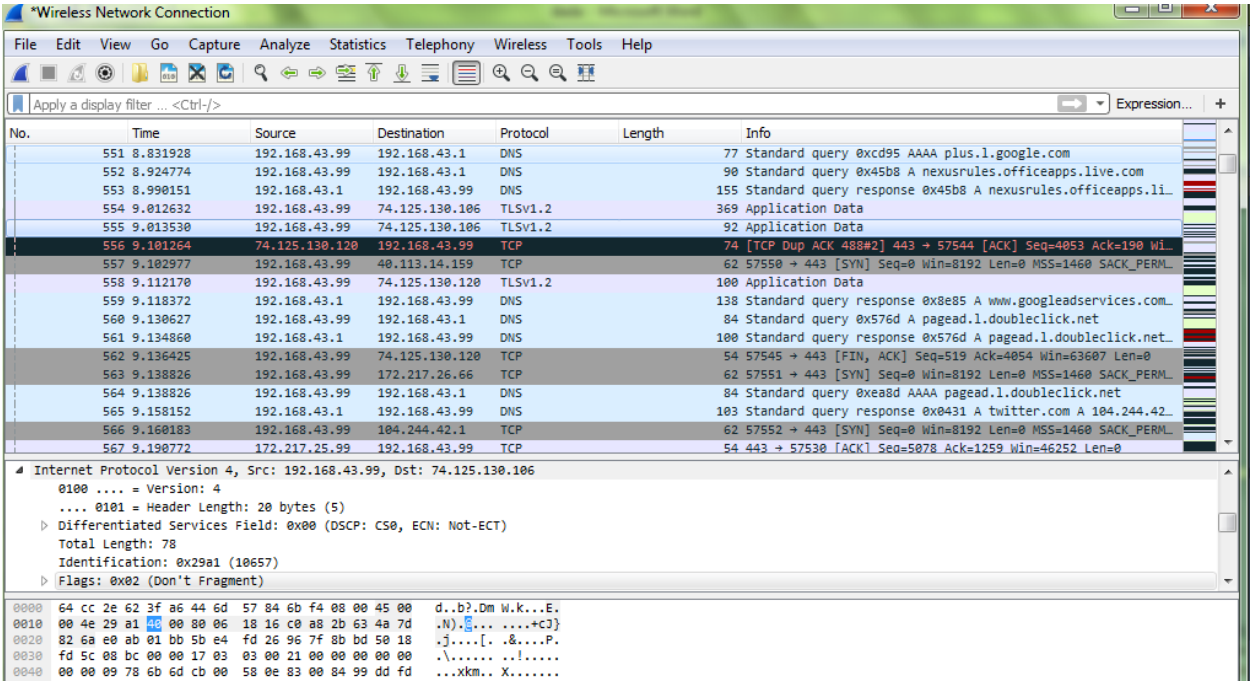
Dari data diatas,dapat diperoleh infomasi sebagai berikut :
Alamat IP
Source : 192.168.43.99
Destination : 157.240.7.35

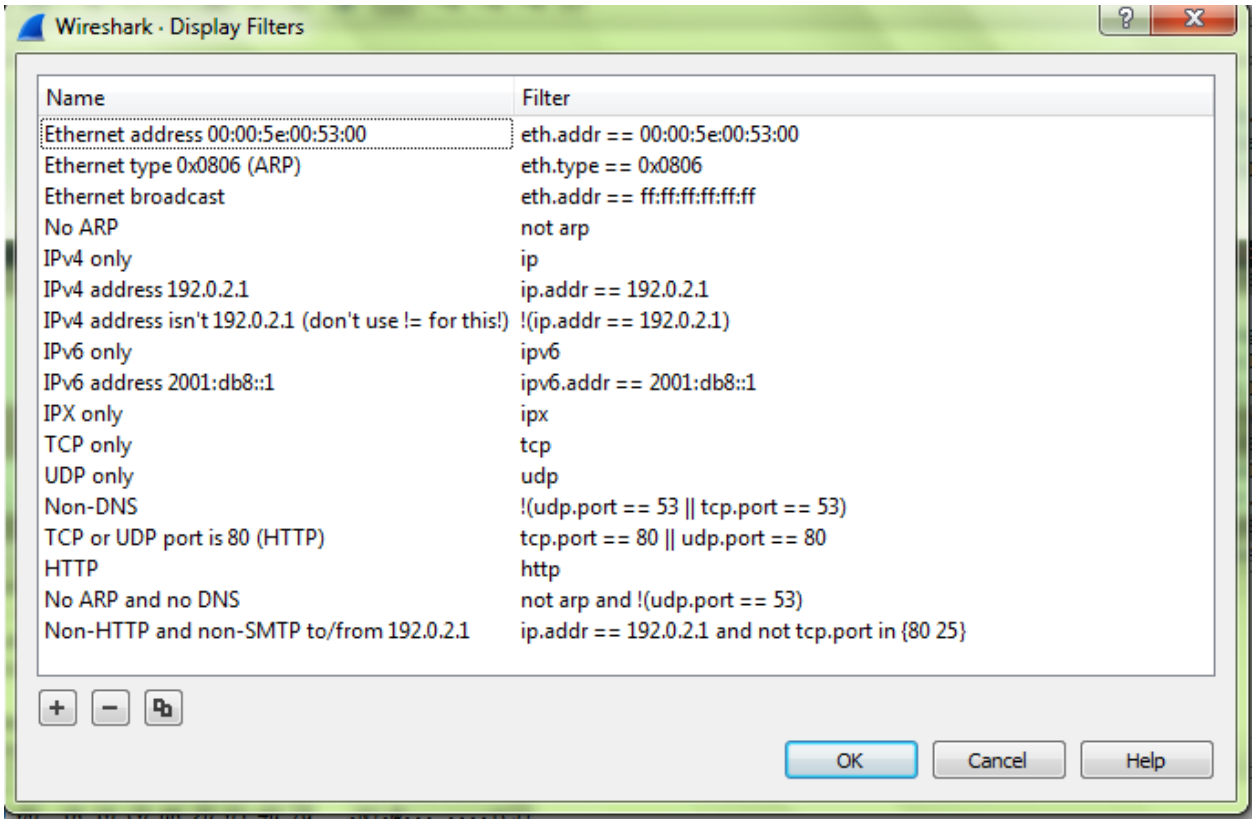
Protokol yang digunakan : TCP

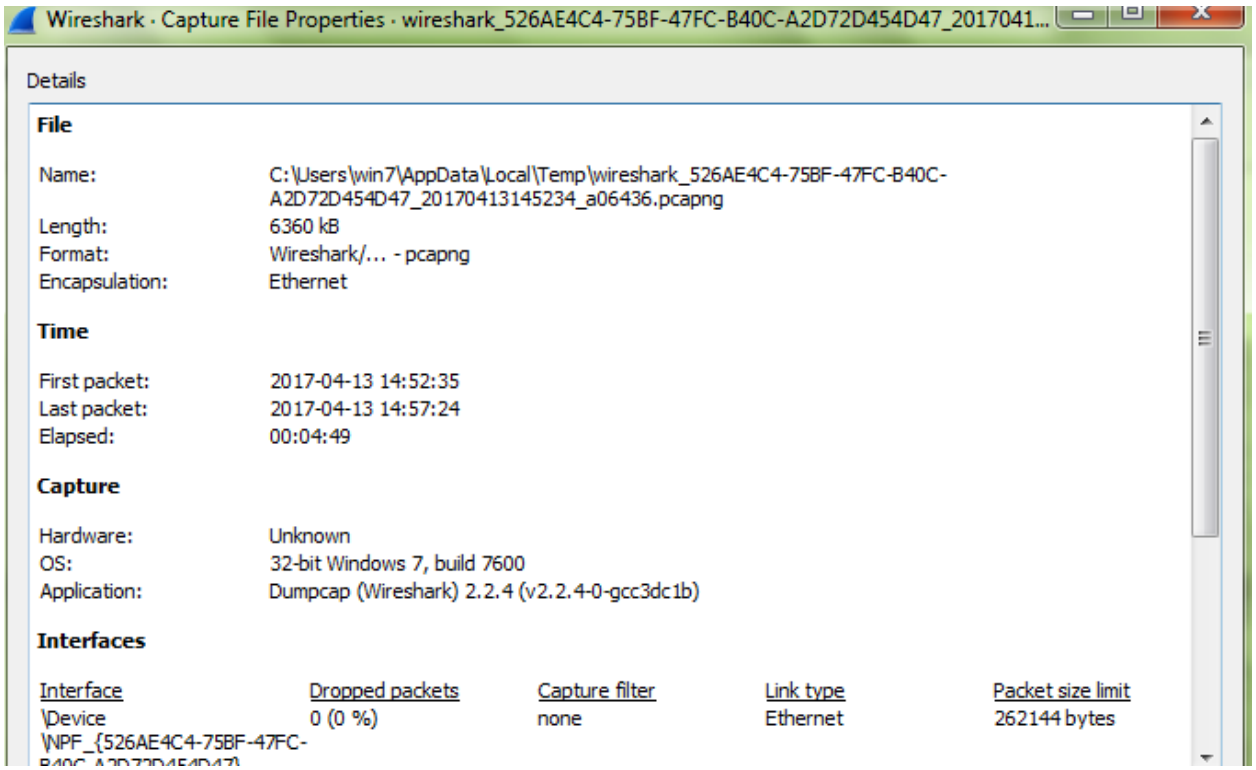


Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (57089) dan port tujuannya (443). Port 443 merupakan port untuk TCP.

4. twitter.com



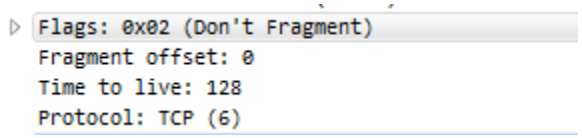

Wireshark · Display Filters
Name
Filter
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
IPv4 only
ip
IPv4 address 192.0.2.1
ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (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

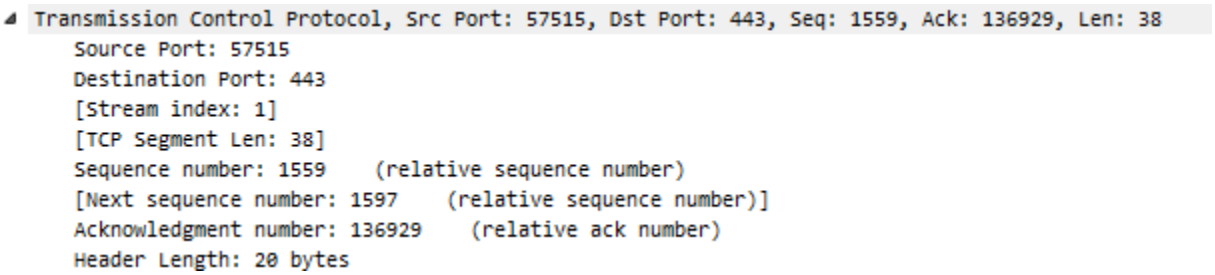

Wireshark · Capture File Properties · wireshark_526AE4C4-75BF-47FC-B40C-A2D72D454D47_2017041...
Details
File
Name:
C:\Users\win7\AppData\Local\Temp\wireshark_526AE4C4-75BF-47FC-B40C-A2D72D454D47_20170413145234_a06436.pcapng
Length:
6360 kB
Format:
Wireshark/... - pcapng
Encapsulation:
Ethernet
Time
First packet:
2017-04-13 14:52:35
Last packet:
2017-04-13 14:57:24
Elapsed:
00:04:49
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_{526AE4C4-75BF-47FC-
0 (0 %)
none
Ethernet
262144 bytes

Berikut adalah hasil analisa jaringan yang ter -capture saat membuka twitter.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.

Dari data diatas,dapat diperoleh infomasi sebagai berikut :
Alamat IP
Source : 192.168.43.99
Destination : 104.244.42.1

Protokol yang digunakan : TCP





Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (57515) dan port tujuannya (1559). Port 1559 merupakan port untuk TCP.