

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

The screenshot shows a Wireshark capture of network traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
2110	53.064497	104.93.122.177	192.168.43.99	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess...
2111	53.064503	54.192.55.162	192.168.43.99	TCP	62	80 → 56036 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_...
2112	53.064505	104.93.122.177	192.168.43.99	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess...
2113	53.064507	114.4.110.101	192.168.43.99	TCP	58	80 → 56038 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
2114	53.064509	54.230.151.34	192.168.43.99	TCP	54	80 → 56031 [ACK] Seq=1 Ack=984 Win=30473 Len=0
2115	53.064510	192.168.43.1	192.168.43.99	DNS	186	Standard query response 0x03fe A assets.kompas.com CNAME edge.te...
2116	53.064934	192.168.43.99	104.93.122.177	TCP	54	56022 → 443 [RST, ACK] Seq=315 Ack=4208 Win=0 Len=0
2117	53.065434	192.168.43.99	54.192.55.162	TCP	54	56036 → 80 [ACK] Seq=1 Ack=1 Win=64400 Len=0
2118	53.065646	192.168.43.99	114.4.110.101	TCP	54	56038 → 80 [ACK] Seq=1 Ack=1 Win=64400 Len=0
2119	53.072867	192.168.43.99	192.168.43.1	DNS	76	Standard query 0x6867 A www.google.co.id
2120	53.076602	192.168.43.1	192.168.43.99	DNS	92	Standard query response 0x6867 A www.google.co.id A 74.125.130.94
2121	53.078918	192.168.43.99	192.168.43.1	DNS	76	Standard query 0x9dc9 AAAA www.google.co.id
2122	53.096346	192.168.43.99	54.192.151.115	TCP	1032	[TCP Retransmission] 55994 → 443 [PSH, ACK] Seq=203 Ack=4943 Win...
2123	53.096680	192.168.43.99	202.146.4.64	TCP	54	56024 → 80 [ACK] Seq=954 Ack=1819 Win=64860 Len=0
2124	53.196201	192.168.43.99	148.81.111.121	TCP	100	[TCP Retransmission] 56030 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64400...
2125	53.215216	192.168.43.99	87.98.185.184	TCP	54	56025 → 22 [ACK] Seq=348 Ack=820 Win=63581 Len=0
2126	53.284342	54.230.151.34	192.168.43.99	HTTP	1454	[TCP Previous segment not captured] continuation
2127	53.284472	192.168.43.99	54.230.151.34	TCP	66	[TCP Dup ACK 1993#1] 56031 → 80 [ACK] Seq=984 Ack=1 Win=64400 Le...

The packet details pane for packet 2116 shows:

- Frame 2116: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0
- Ethernet II, Src: XiaomCo\_62:3f:a6 (64:cc:2e:62:3f:a6), Dst: LiteonTe\_84:6b:f4 (44:6d:57:84:6b:f4)
- Internet Protocol Version 4, Src: 104.93.122.177, Dst: 192.168.43.99
- Transmission Control Protocol, Src Port: 443, Dst Port: 56019, Seq: 3966, Ack: 314, Len: 242
- Secure Sockets Layer

The hex dump shows the raw bytes of the packet, including the RST flag and sequence/acknowledgment numbers.

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}

0000	44 6d 57 84 6b f4 64 cc 2e 62 3f a6 08 00 45 00	DmW.k.d. .b?...E.
0010	01 1a 1f 20 40 00 37 06 54 a4 68 5d 7a b1 c0 a8	... @.7. T.h]z...
0020	2b 63 01 bb da d3 91 d4 43 5d 13 e1 9c d9 50 18	+c..... C]....P.
0030	75 40 9a 76 00 00 16 03 03 00 ba 04 00 00 b6 00	U@.V.... .....
0040	00 1c 20 00 b0 00 00 2b 5c ad 2a ec 78 67 18 26	.. ....+ \.*.xg.&
0050	9b 57 89 df c7 b7 20 4d fa c5 13 78 48 0f fc 9c	.W.... M ...XH...
0060	8b 98 f7 48 86 e4 ba 34 9b 9b 02 77 b2 a3 80 0f	...H...4 ...W....

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 seperti 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 informasi sebagai berikut :

Alamat IP

Source : 192.168.43.99

Destination : 202.61.113.65

Protokol yang digunakan : TCP

```

> Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 55
  Protocol: TCP (6)

```

```

Transmission Control Protocol, Src Port: 56078, Dst Port: 80, Seq: 5206, Ack: 23782, Len: 0
  Source Port: 56078
  Destination Port: 80
  [Stream index: 132]
  [TCP Segment Len: 0]

```

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

The image shows a Wireshark packet capture window titled "t detik.pcapng". The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 76 is highlighted in red, indicating a RST (Reset) packet. Below the packet list, the "Packet Bytes" pane shows the raw data of the selected packet, including source and destination ports, stream index, and sequence numbers.

No.	Time	Source	Destination	Protocol	Length	Info
71	2.363868	192.168.43.1	192.168.43.99	DNS	85	Standard query response 0x846d No such name A hotspot.ilk...
72	2.406737	192.168.43.99	74.125.200.157	TCP	55	56594 → 80 [ACK] Seq=1 Ack=1 Win=64366 Len=1
73	2.439739	74.125.130.18	192.168.43.99	TCP	54	443 → 56639 [ACK] Seq=3533 Ack=511 Win=44488 Len=0
74	2.463730	74.125.200.157	192.168.43.99	TCP	66	80 → 56594 [ACK] Seq=1 Ack=2 Win=43568 Len=0 SLE=1 SRE=2
75	2.486623	192.168.43.99	87.98.185.184	TCP	62	[TCP Spurious Retransmission] 56638 → 8829 [SYN] Seq=0 Wi...
76	2.826873	87.98.185.184	192.168.43.99	TCP	54	8829 → 56638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
77	3.768078	192.168.43.99	103.49.221.211	TCP	62	56640 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
78	3.816892	192.168.43.99	203.190.242.211	HTTP	334	GET / HTTP/1.1
79	3.821816	103.49.221.211	192.168.43.99	TCP	62	80 → 56640 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=140...
80	3.821956	192.168.43.99	103.49.221.211	TCP	54	56640 → 80 [ACK] Seq=1 Ack=1 Win=64400 Len=0
81	3.822167	192.168.43.99	87.98.185.184	TCP	62	56641 → 8829 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PER...
82	3.867668	192.168.43.99	23.41.75.27	TCP	55	56611 → 80 [ACK] Seq=1 Ack=1 Win=64400 Len=1
83	3.904413	203.190.242.211	192.168.43.99	HTTP	1454	Continuation
84	3.904651	192.168.43.99	203.190.242.211	TCP	66	[TCP Dup ACK 78#1] 56589 → 80 [ACK] Seq=281 Ack=1 Win=637...
85	3.908097	203.190.242.211	192.168.43.99	TCP	1454	[TCP Retransmission] 80 → 56589 [ACK] Seq=1 Ack=281 Win=1...
86	3.908317	192.168.43.99	203.190.242.211	TCP	54	56589 → 80 [ACK] Seq=281 Ack=2801 Win=64400 Len=0
87	3.926605	203.190.242.211	192.168.43.99	HTTP	1454	[TCP Previous segment not captured] Continuation
88	3.926733	192.168.43.99	203.190.242.211	TCP	66	[TCP Dup ACK 86#1] 56589 → 80 [ACK] Seq=281 Ack=2801 Win=...
89	3.929355	203.190.242.211	192.168.43.99	TCP	1454	[TCP Out-Of-Order] 80 → 56589 [ACK] Seq=2801 Ack=281 Win=...

Source Port: 56640  
Destination Port: 80  
[Stream index: 11]  
[TCP Segment Len: 0]  
Sequence number: 0 (relative sequence number)

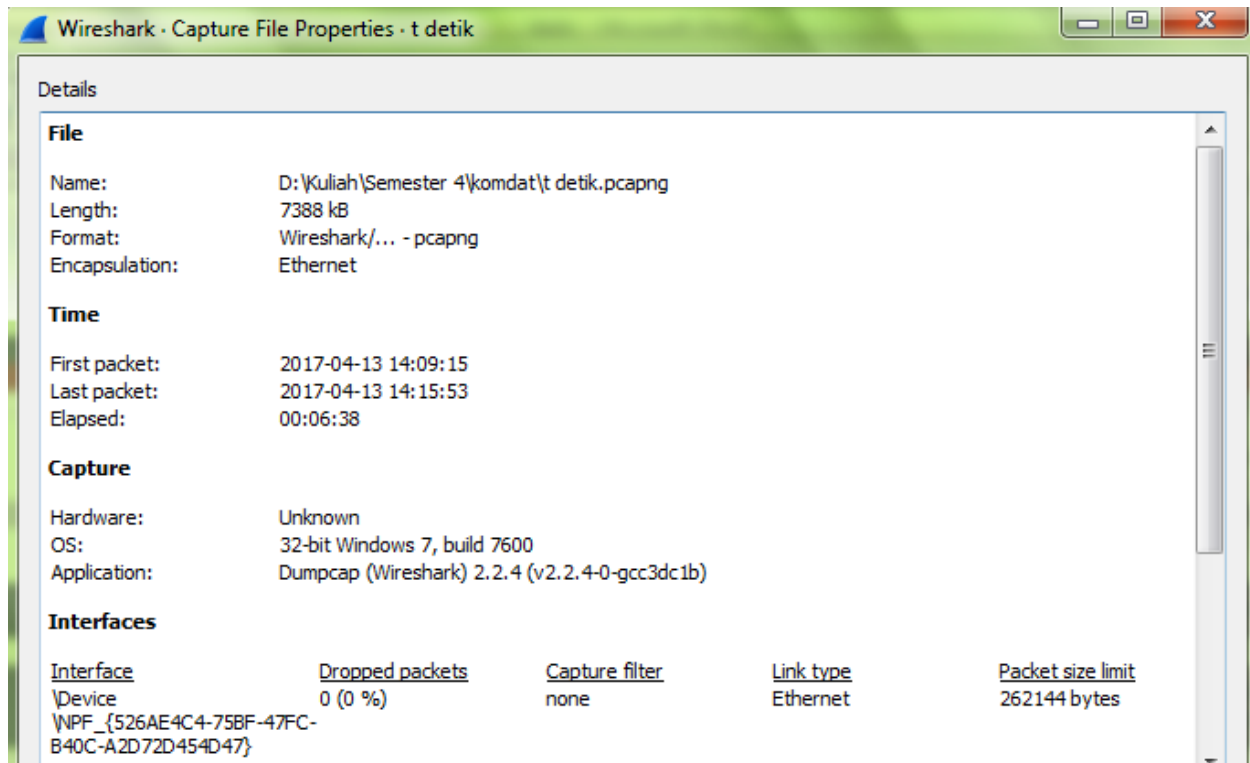
```

0000 64 cc 2e 62 3f a6 44 6d 57 84 eb f4 08 00 45 00 d..b?.Dm W.k...E.
0010 00 30 4e 74 40 00 80 06 7b 43 c0 a8 2b 63 67 31 .0nt@...{C...cgl
0020 dd d3 dd 40 00 50 04 5f b8 60 00 00 00 70 02 ...@.P_.....p.
0030 20 00 97 be 00 00 02 04 05 b4 01 01 04 02 .....

```

The image shows the "Wireshark · Display Filters" window. It contains a list of filter rules that can be applied to the packet capture. The filters are organized into a table with columns for Name and Filter.

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.

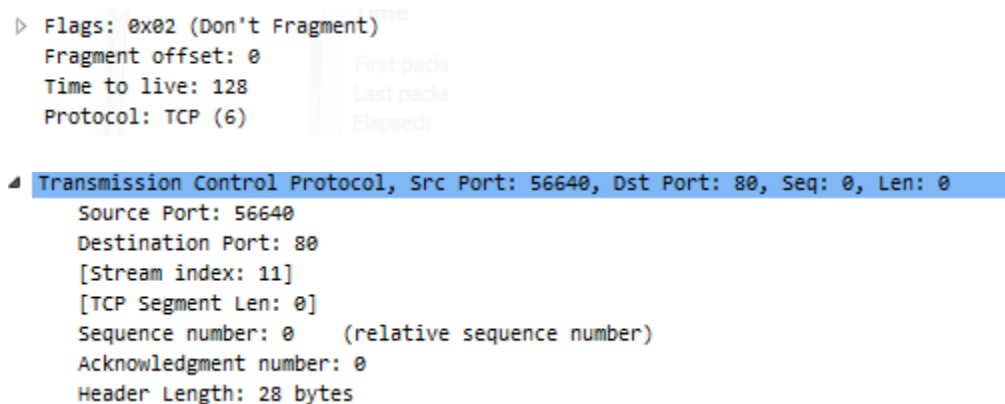
Dari data diatas,dapat diperoleh informasi sebagai berikut :

Alamat IP

Source : 192.168.43.99

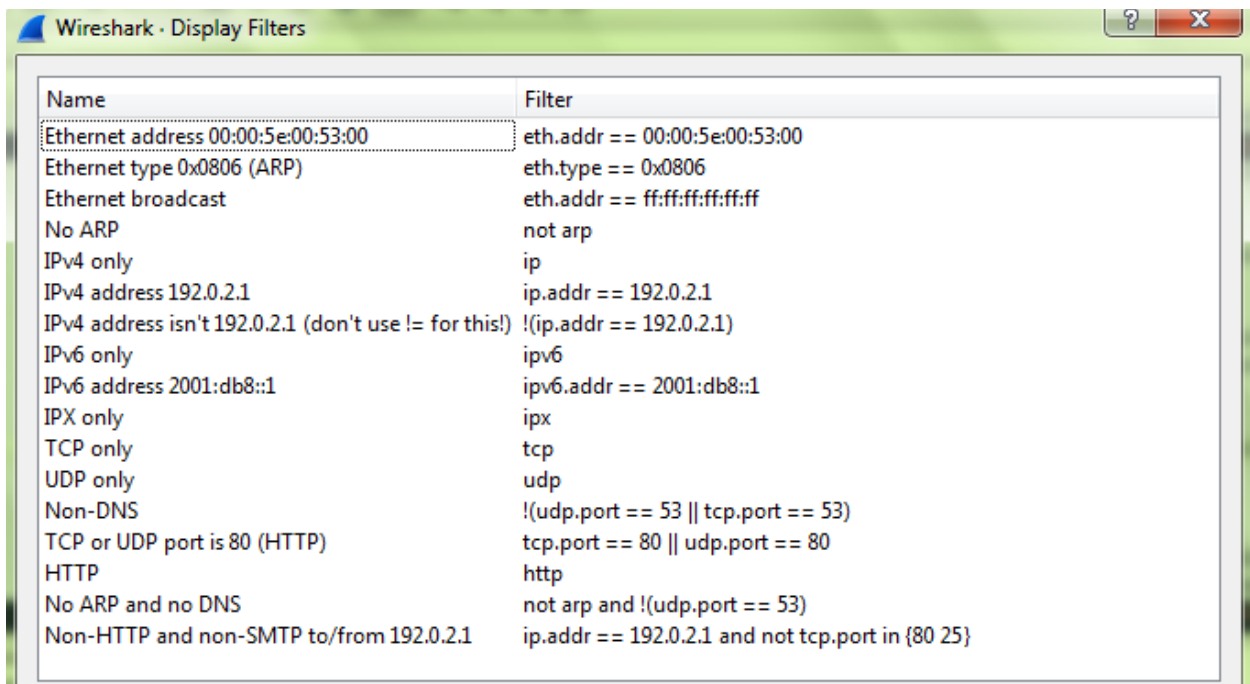
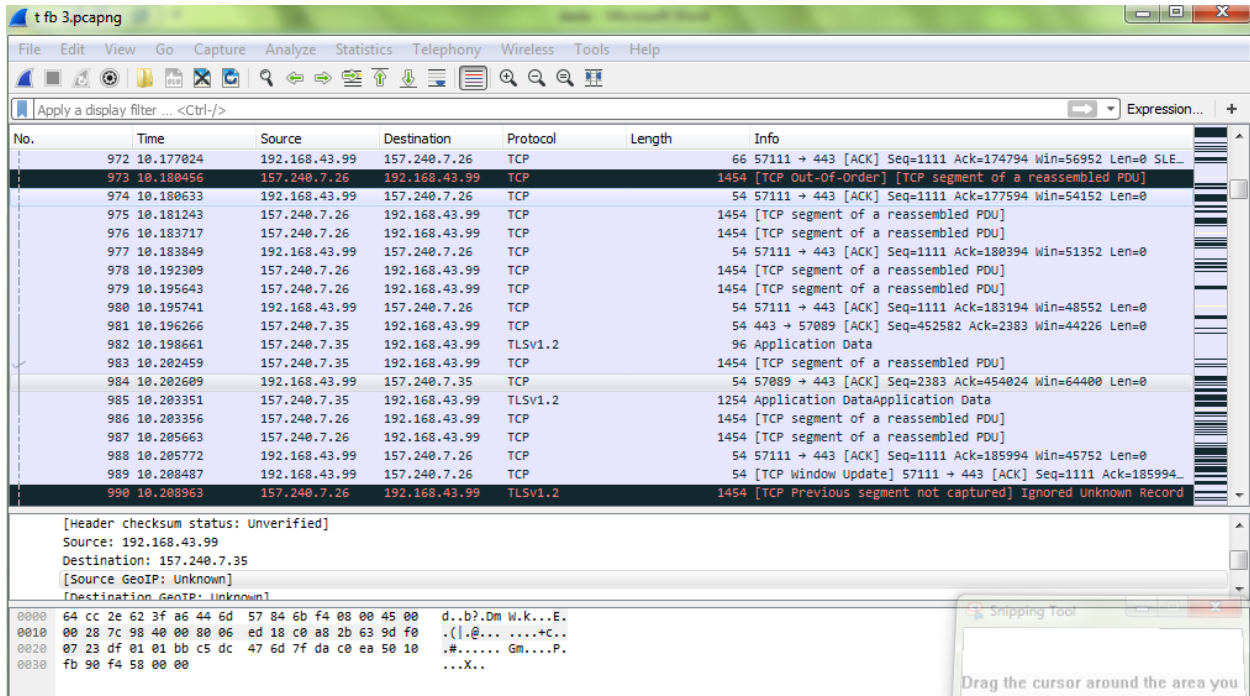
Destination : 103.49.221.211

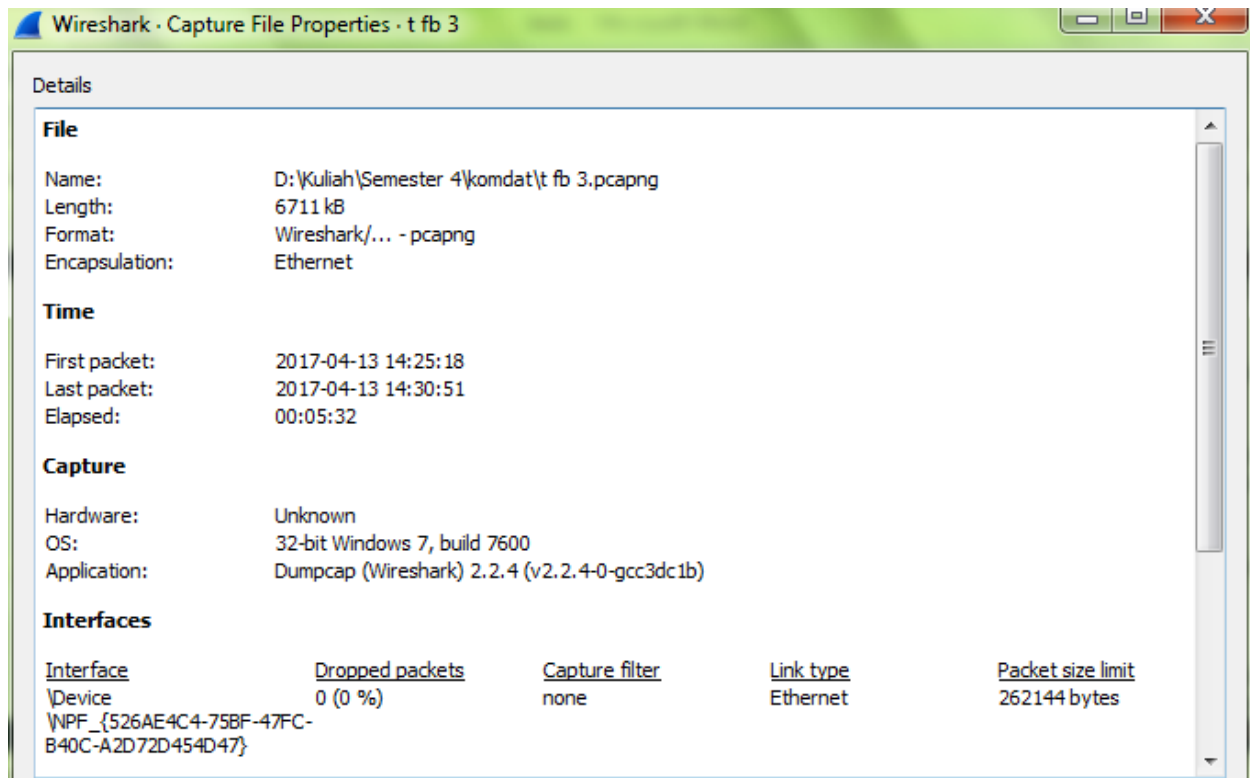
Protokol yang digunakan : TCP



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.

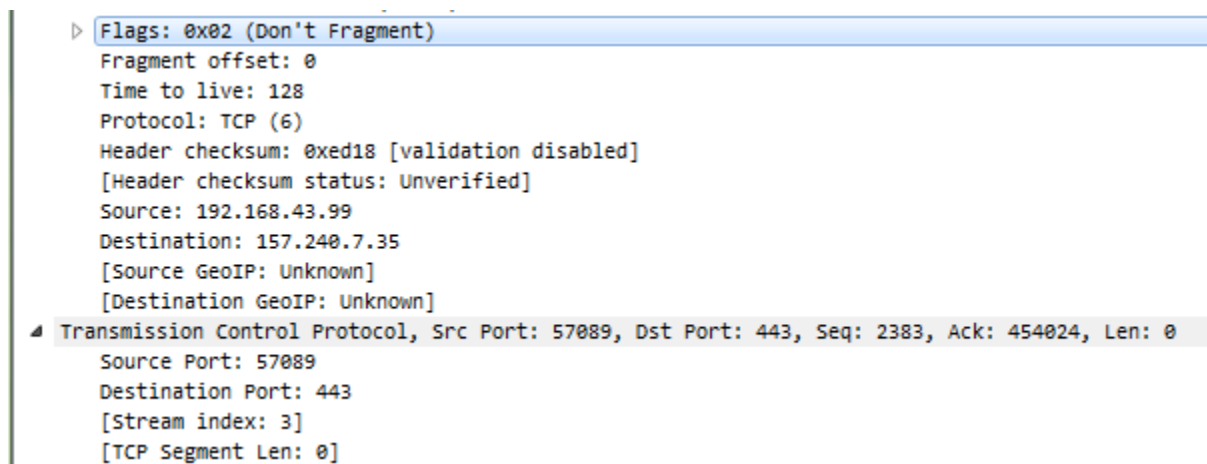
Dari data diatas,dapat diperoleh infomasi sebagai berikut :

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

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. Packet 556 is highlighted, showing a TCP segment from source 74.125.130.120 to destination 192.168.43.99 on port 443. The info pane below shows the details of this packet, including the Internet Protocol Version 4 header and the application data payload.

No.	Time	Source	Destination	Protocol	Length	Info
551	8.831928	192.168.43.99	192.168.43.1	DNS	77	Standard query 0xcd95 AAAA plus.l.google.com
552	8.924774	192.168.43.99	192.168.43.1	DNS	90	Standard query 0x45b8 A nexusrules.officeapps.live.com
553	8.990151	192.168.43.1	192.168.43.99	DNS	155	Standard query response 0x45b8 A nexusrules.officeapps.li...
554	9.012632	192.168.43.99	74.125.130.106	TLSv1.2	369	Application Data
555	9.013530	192.168.43.99	74.125.130.106	TLSv1.2	92	Application Data
556	9.101264	74.125.130.120	192.168.43.99	TCP	74	[TCP Dup ACK 488#2] 443 → 57544 [ACK] Seq=4053 Ack=190 Wi...
557	9.102977	192.168.43.99	40.113.14.159	TCP	62	57550 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERML...
558	9.112170	192.168.43.99	74.125.130.120	TLSv1.2	100	Application Data
559	9.118372	192.168.43.1	192.168.43.99	DNS	138	Standard query response 0x8e85 A www.googleadservices.com...
560	9.130627	192.168.43.99	192.168.43.1	DNS	84	Standard query 0x576d A pagead.doubleclick.net
561	9.134860	192.168.43.1	192.168.43.99	DNS	100	Standard query response 0x576d A pagead.doubleclick.net...
562	9.136425	192.168.43.99	74.125.130.120	TCP	54	57545 → 443 [FIN, ACK] Seq=519 Ack=4054 Win=63607 Len=0
563	9.138826	192.168.43.99	172.217.26.66	TCP	62	57551 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERML...
564	9.138826	192.168.43.99	192.168.43.1	DNS	84	Standard query 0xea8d AAAA pagead.doubleclick.net
565	9.158152	192.168.43.1	192.168.43.99	DNS	103	Standard query response 0x0431 A twitter.com A 104.244.42...
566	9.160183	192.168.43.99	104.244.42.1	TCP	62	57552 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERML...
567	9.190772	172.217.25.99	192.168.43.99	TCP	54	443 → 57530 [ACK] Seq=5078 Ack=1259 Win=46252 Len=0

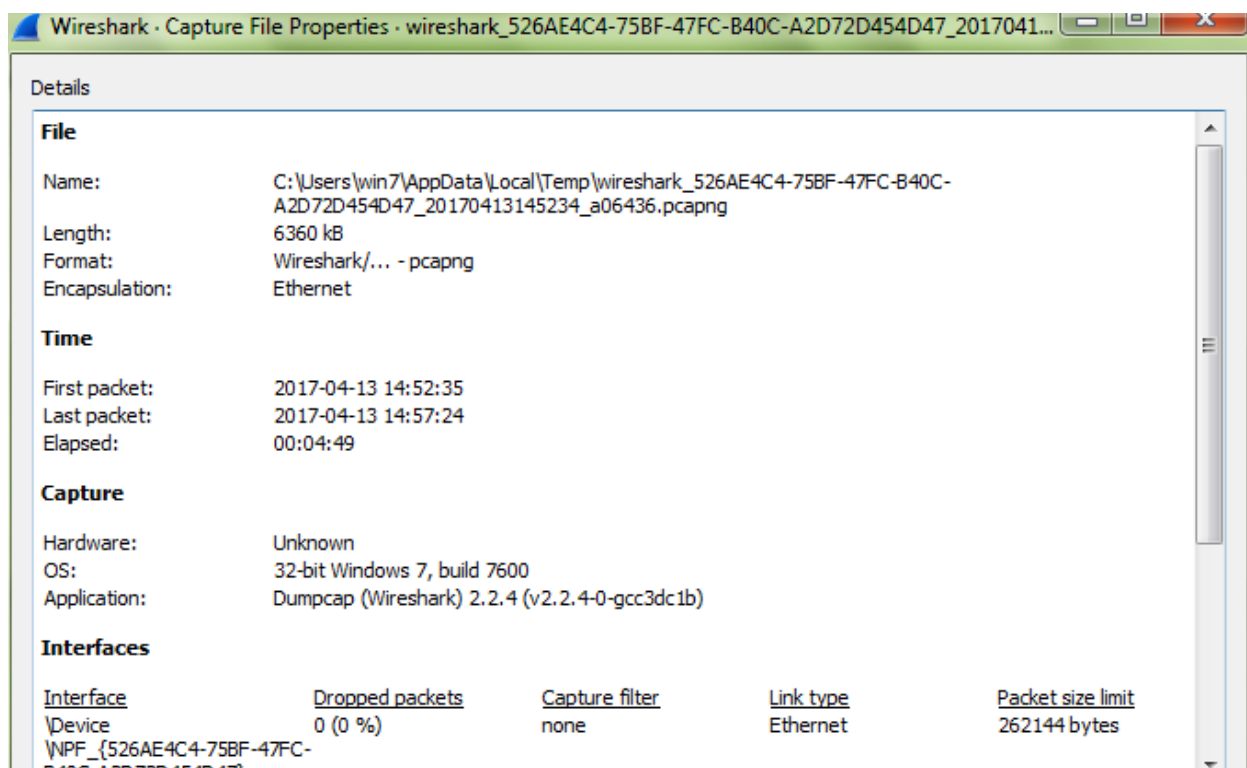
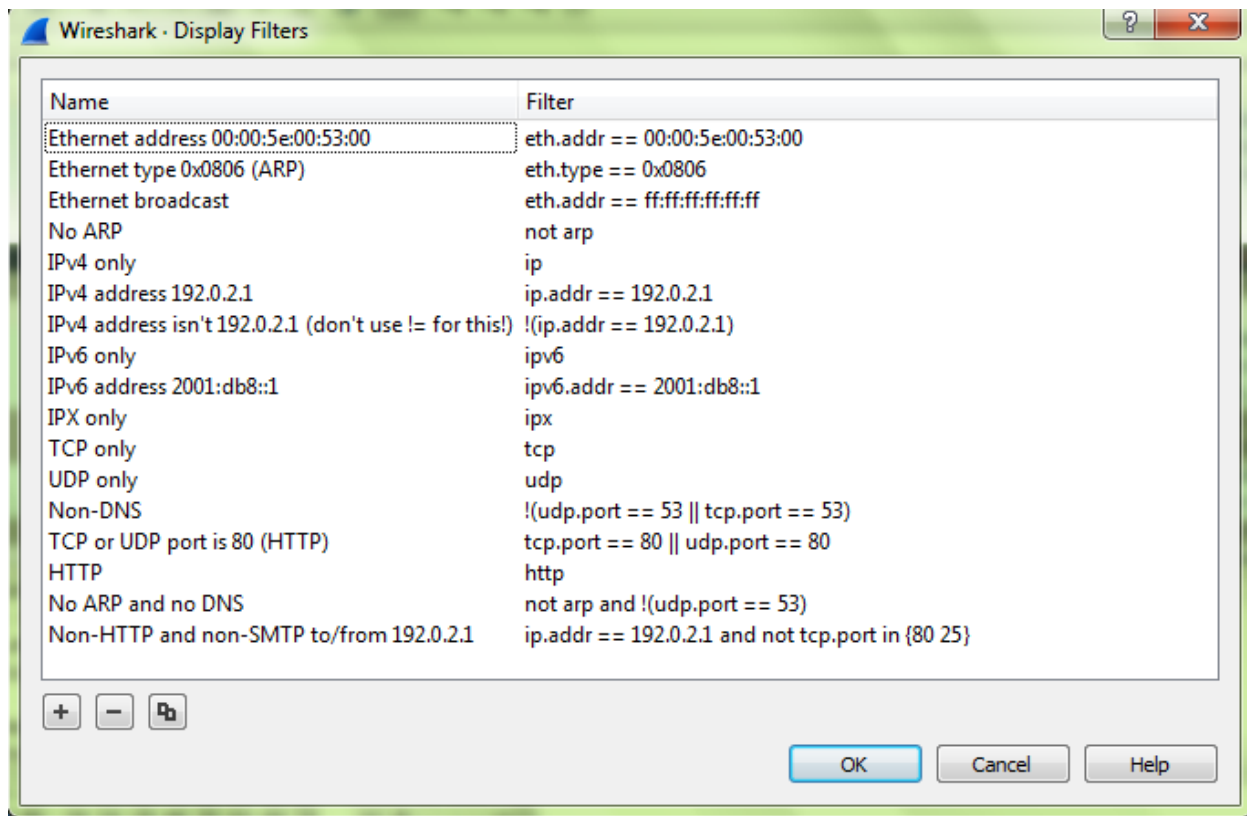
Internet Protocol Version 4, Src: 192.168.43.99, Dst: 74.125.130.106

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 78
- Identification: 0x29a1 (10657)
- Flags: 0x02 (Don't Fragment)

```

0000 64 cc 2e 62 3f a6 44 6d 57 84 6b f4 08 00 45 00  d..b?.Dm W.k...E.
0010 00 4e 29 a1 40 00 00 06 18 16 c0 a8 2b 63 4a 7d  .N).[... ..+CJ}
0020 82 6a e0 ab 01 bb 5b e4 fd 26 96 7f 0b bd 50 18  .j...[. .&....P.
0030 fd 5c 08 bc 00 00 17 03 03 00 21 00 00 00 00 00  \..... !!.....
0040 00 00 09 78 6b 6d cb 00 58 0e 83 00 84 99 dd fd  ...xkm.. X.....
  
```





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

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

  ▲ Transmission Control Protocol, Src Port: 57515, Dst Port: 443, Seq: 1559, Ack: 136929, Len: 38
    Source Port: 57515
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 38]
    Sequence number: 1559 (relative sequence number)
    [Next sequence number: 1597 (relative sequence number)]
    Acknowledgment number: 136929 (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 (57515) dan port tujuannya (1559). Port 1559 merupakan port untuk TCP.