

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

Analisis Packets dengan aplikasi Wireshark

Twitter.com

The screenshot shows the Wireshark interface with a packet list and details pane. The packet list shows 13 packets, with the selected packet (No. 1) being a TCP segment. The details pane shows the following information:

```

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Interface id: 0 (\Device\NPF_{38FAE326-FAEE-49EC-8D2F-04D4CB62342E})
Encapsulation type: Ethernet (1)
Arrival Time: Apr 13, 2017 06:35:09.917012000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1492040109.917012000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
  
```

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000 20 7c 0f 69 b0 33 a0 86 c6 cc 16 b5 00 00 45 00 |.i.3... ..E.
0010 00 28 3d 4b 40 00 fd 06 87 6d 4a 7d 82 84 c0 a8 |.(t@... m)|....
0020 2b 6d 01 bb c0 78 c5 72 c0 c8 38 18 57 f1 50 10 |+m...x.r ..8.W.P.
0030 04 50 19 f5 00 00 |.P....
  
```

The screenshot shows the 'Wireshark - Capture File Properties' dialog box with the following details:

File

- Name: D:\ws\tw.pcapng
- Length: 31 MB
- Format: Wireshark/... - pcapng
- Encapsulation: Ethernet

Time

- First packet: 2017-04-13 06:35:09
- Last packet: 2017-04-13 06:47:43
- Elapsed: 00:12:33

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_{38FAE326-FAEE-49EC-8D2F-04D4CB62342E}	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	42317	42317 (100.0%)	N/A
Time span, s	753.624	753.624	N/A
Average pps	56.2	56.2	N/A
Average packet size, B	718.5	718.5	N/A

Capture file comments

0000	20 7c 8f 69 b0 33 a0 86 c6 cc 16 b5 08 00 45 00	.i.3..
0010	00 28 3d 4b 40 00 fd 06 87 6d 4a 7d 82 84 c0 a8	.(=K@... .mJ})....
0020	2b 6d 01 bb c0 78 c5 72 c0 c8 38 18 57 f1 50 10	+m...x.r ..8.W.P.
0030	04 50 19 f5 00 00	.P....

Pada gambar diatas merupakan 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 seperti 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

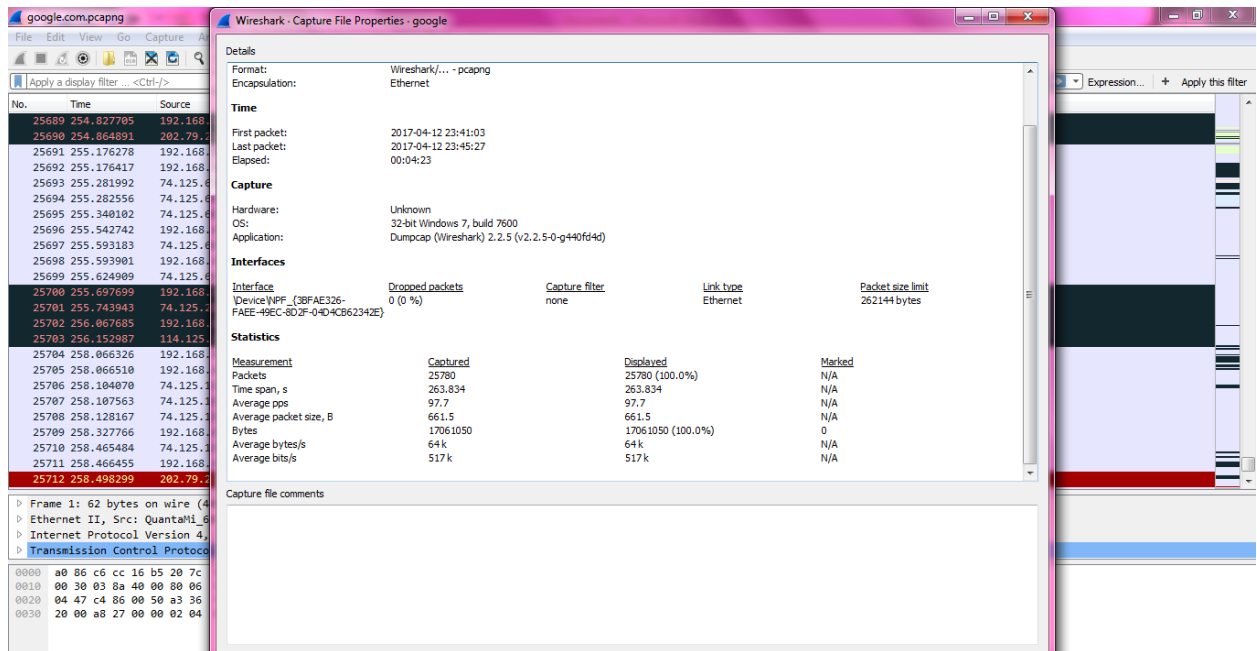
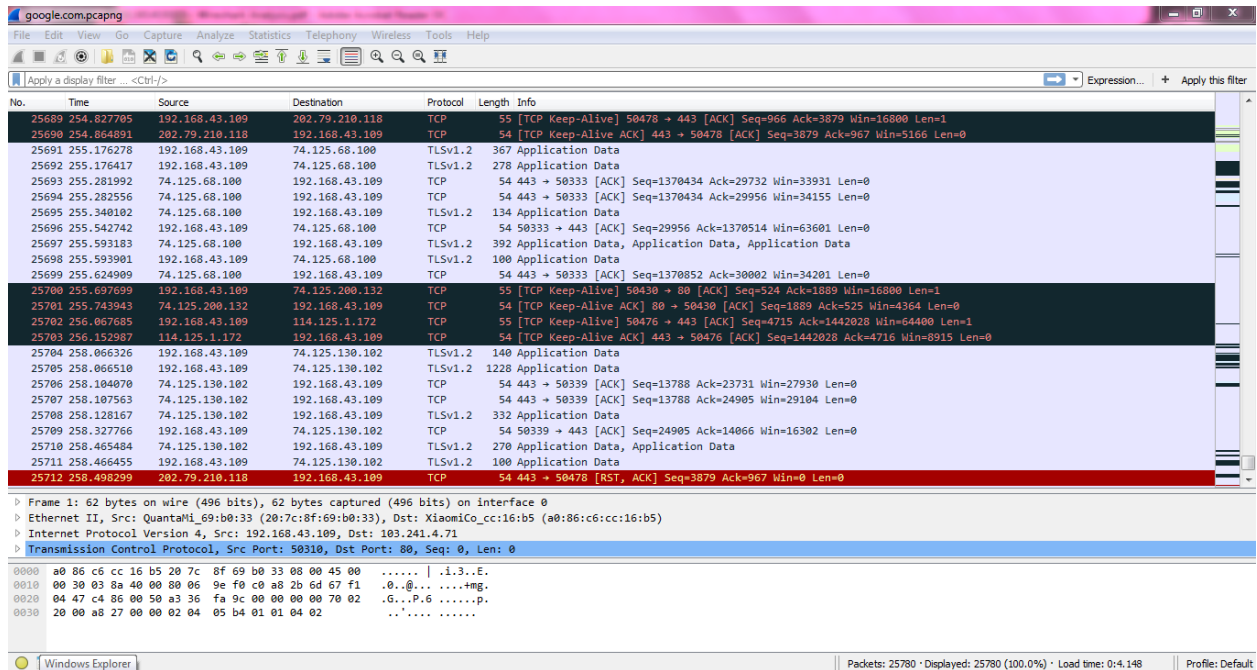
```
Src: 74.125.130.132,
Dst: 192.168.43.109
```

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]

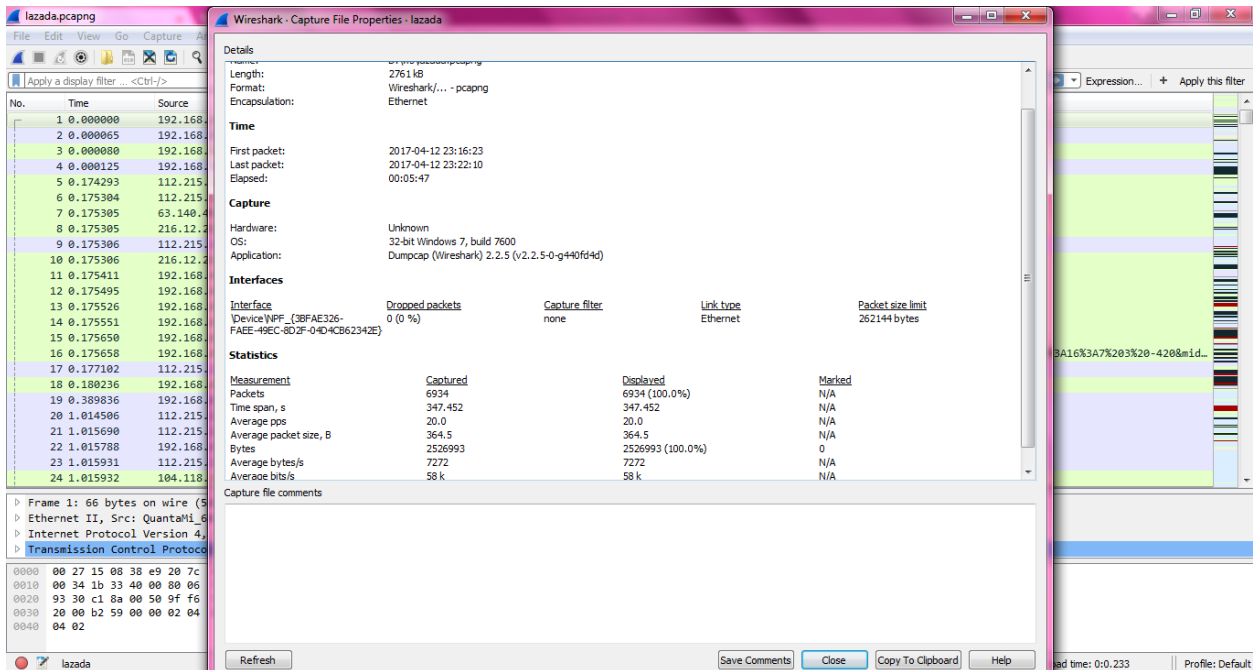
Pada gambar diatas merupakan proses komunikasi yang dilakukan melalui port. Dapat dilihat dari gambar diatas bahwa port asalnya (50310) dan port tujuannya (80). Port 80 merupakan port untuk TCP.

Lazada.co.id

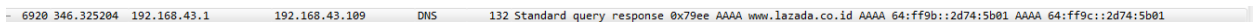
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.109	104.118.147.48	TCP	66	49546 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.000065	192.168.43.109	74.125.24.156	TLSv1.2	262	Client Hello
3	0.000080	192.168.43.109	63.140.45.106	TCP	66	49545 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.000125	192.168.43.109	74.125.24.156	TLSv1.2	262	Client Hello
5	0.174293	112.215.161.58	192.168.43.109	TCP	1414	[TCP segment of a reassembled PDU]
6	0.175304	112.215.161.58	192.168.43.109	HTTP	579	HTTP/1.1 200 OK (text/plain)
7	0.175305	63.140.45.106	192.168.43.109	TCP	62	80 → 49544 [SYN, ACK] Seq=0 Ack=1 Win=4080 Len=0 MSS=1360 SACK_PERM=1
8	0.175305	216.12.219.99	192.168.43.109	TCP	66	80 → 49536 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1360 SACK_PERM=1 WS=128
9	0.175306	112.215.184.16	192.168.43.109	TCP	54	443 → 49535 [ACK] Seq=1 Ack=1 Win=237 Len=0
10	0.175306	216.12.219.99	192.168.43.109	TCP	66	80 → 49537 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1360 SACK_PERM=1 WS=128
11	0.175411	192.168.43.109	216.12.219.99	TCP	66	49536 → 80 [ACK] Seq=773 Ack=1 Win=17680 Len=0 SLE=0 SRE=1
12	0.175495	192.168.43.109	216.12.219.99	TCP	66	49537 → 80 [ACK] Seq=1 Ack=1 Win=17680 Len=0 SLE=0 SRE=1
13	0.175526	192.168.43.109	112.215.161.58	TCP	54	49527 → 80 [ACK] Seq=1 Ack=1886 Win=4420 Len=0
14	0.175551	192.168.43.109	63.140.45.106	TCP	54	49544 → 80 [ACK] Seq=1 Ack=1 Win=17680 Len=0
15	0.175650	192.168.43.109	63.140.45.106	TCP	1414	[TCP segment of a reassembled PDU]
16	0.175658	192.168.43.109	63.140.45.106	HTTP	175	GET /b/ss/lazwebid/1/JS-1.4.1/s97473514938306?AQ8=i&ndh=i&pf=i&t=12%2F3%2F2017%2023%3A16%3A7%20%320-420&mid...
17	0.177102	112.215.184.16	192.168.43.109	TLSv1.2	1414	Server Hello
18	0.180236	192.168.43.109	112.215.161.58	HTTP	523	GET /update/idx/weblocaldecider_sigver-win32-int-15.0.15.28.info.1z HTTP/1.1
19	0.389836	192.168.43.109	112.215.184.16	TCP	54	49535 → 443 [ACK] Seq=1 Ack=1361 Win=17680 Len=0
20	1.014506	112.215.184.16	192.168.43.109	TCP	742	[TCP segment of a reassembled PDU]
21	1.015690	112.215.184.16	192.168.43.109	TCP	1414	[TCP segment of a reassembled PDU]
22	1.015788	192.168.43.109	112.215.184.16	TCP	54	49535 → 443 [ACK] Seq=1 Ack=3409 Win=17680 Len=0
23	1.015931	112.215.184.16	192.168.43.109	TLSv1.2	562	CertificateServer Key Exchange, Server Hello Done
24	1.015932	104.118.147.48	192.168.43.109	TCP	66	80 → 49540 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=32

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: QuantaML69:b0:33 (20:7c:8f:69:b0:33), Dst: ReboundT_08:38:e9 (00:27:15:08:38:e9)
Internet Protocol Version 4, Src: 192.168.43.109, Dst: 104.118.147.48
Transmission Control Protocol, Src Port: 49546, Dst Port: 80, Seq: 0, Len: 0

```
0000  00 27 15 08 38 e9 20 7c 8f 69 b0 33 00 00 45 00  .'.8. |.i..E.  
0010  00 34 1b 33 40 00 80 06 f7 d4 c0 a8 2b 6d 68 76  .4.30...+mhv  
0020  93 30 c1 8a 00 50 9f f6 53 2f 00 00 00 80 02    .0...P.. S/.....  
0030  20 00 b2 59 00 00 02 04 05 b4 01 03 03 02 01 01  ..Y.....  
0040  04 02
```



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 192.168.43.1
 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-F> 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: QuantaML_69:b0:33 (20:7c:8f:69:b0:33), Dst: XiaomiCo_cc:16:b5 (08:06: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 e5 10  ....P6. ....P.
0030  3f 62 cd d7 00 00 00  ?b.....
  
```

Packets: 32275 · Displayed: 32275 (100.0%) · Load time: 0:3.763 Profile: Defau

lpmgs-pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> 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: QuantaML_69:b0:33 (20:7c:8f:69:b0:33), Dst: XiaomiCo_cc:16:b5 (08:06: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 e5 10  ....P6. ....P.
0030  3f 62 cd d7 00 00 00  ?b.....
  
```

WireShark - Capture File Properties - lpmgs

File

Name: D:\lws\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-g40fdd4)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{38FAE326-FAEE-49EC-8D2F-0404C862342E}	Unknown	none	Ethernet	262144 bytes

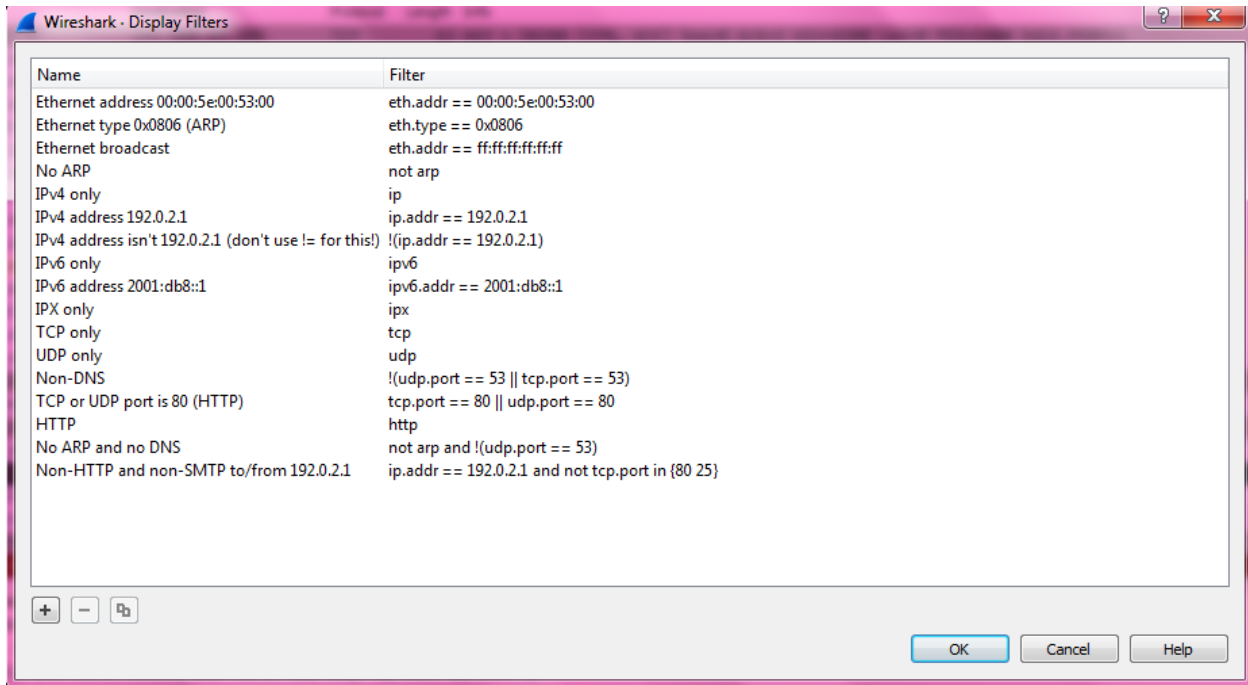
Statistics

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.

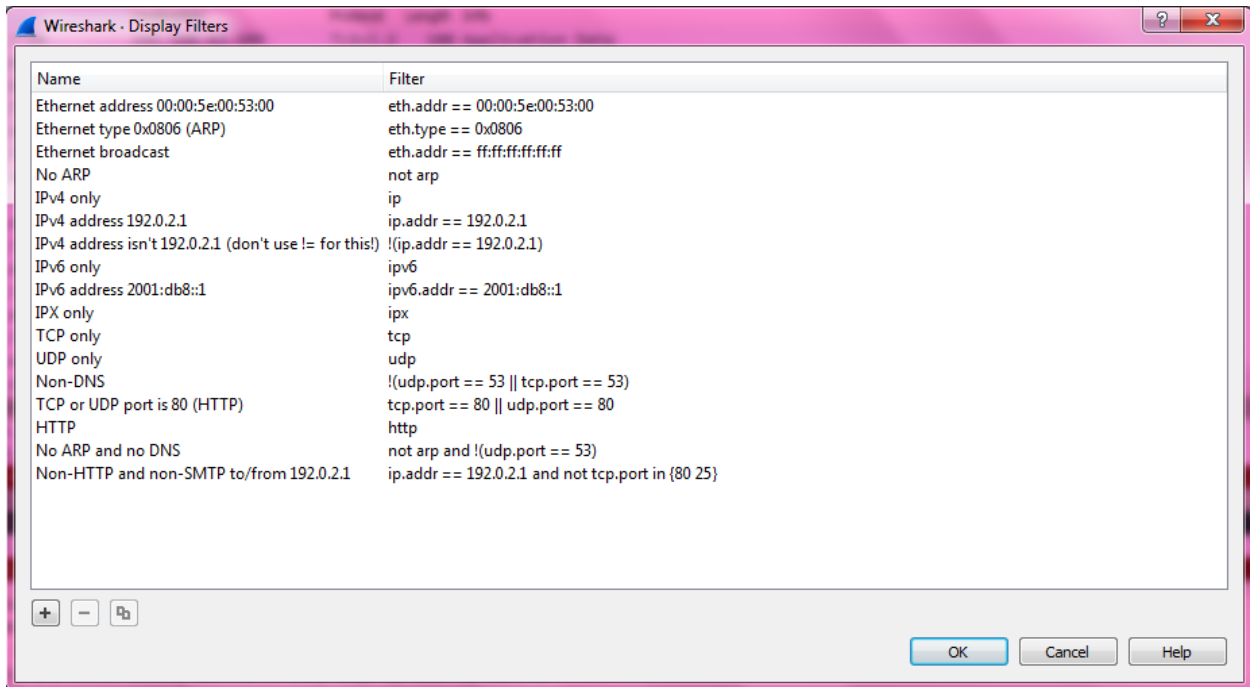
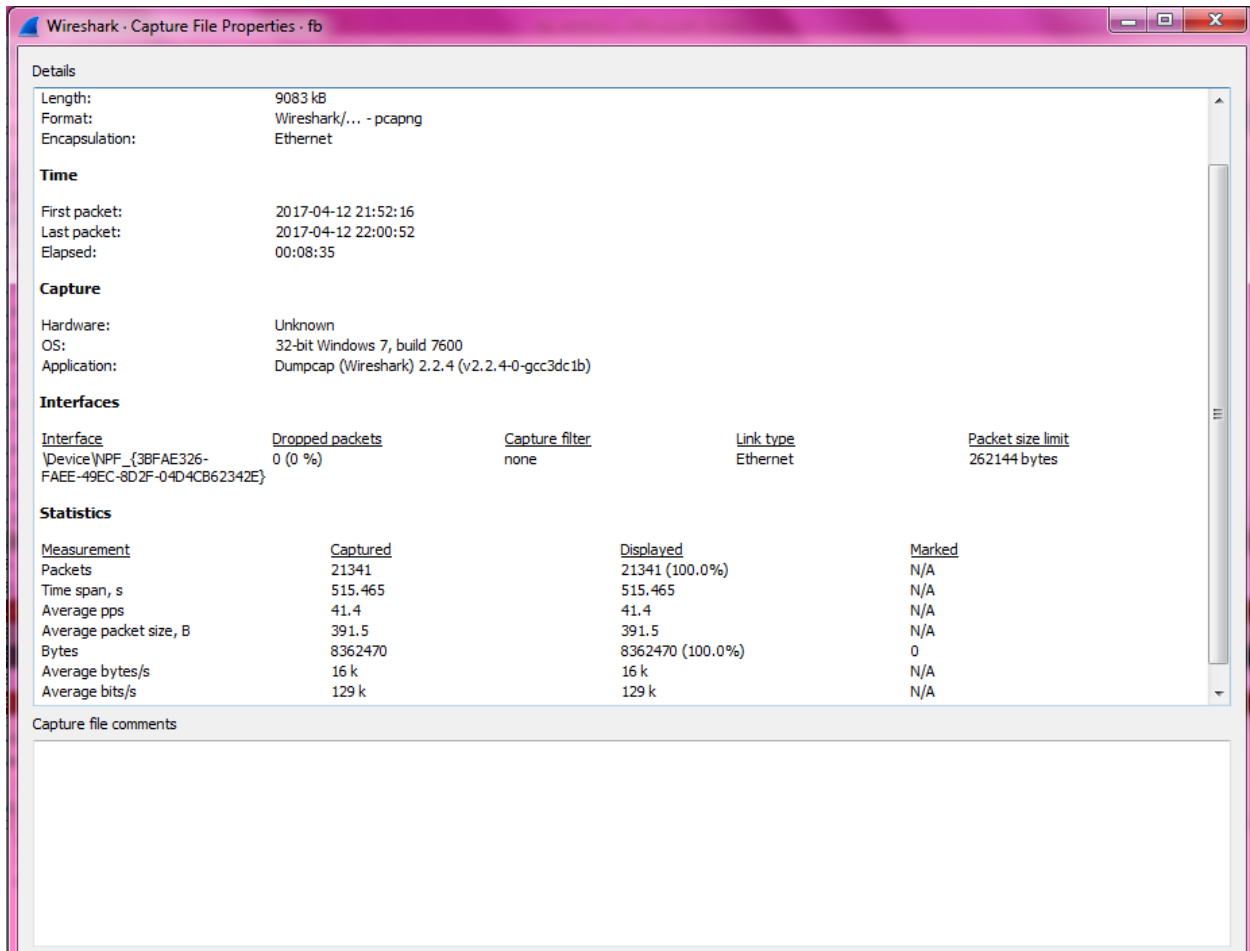
Facebook.com

No.	Time	Source	Destination	Protocol	Length	Info
21227	510.597501	157.240.7.26	192.168.43.109	TLSv1.2	100	Application Data
21228	510.793051	192.168.43.109	157.240.7.26	TCP	54	56078 → 443 [ACK] Seq=201197 Ack=47387 Win=60 Len=0
21229	510.801047	192.168.43.109	157.240.7.26	TCP	54	56153 → 443 [ACK] Seq=877 Ack=4985 Win=15872 Len=0
21230	510.890946	157.240.7.26	192.168.43.109	TCP	114	[TCP segment of a reassembled PDU]
21231	511.093051	192.168.43.109	157.240.7.26	TCP	54	56078 → 443 [ACK] Seq=201197 Ack=47447 Win=60 Len=0
21232	511.131028	157.240.7.26	192.168.43.109	TCP	114	[TCP segment of a reassembled PDU]
21233	511.331028	192.168.43.109	157.240.7.26	TCP	54	56078 → 443 [ACK] Seq=201197 Ack=47507 Win=60 Len=0
21234	511.417267	157.240.7.26	192.168.43.109	TCP	114	[TCP segment of a reassembled PDU]
21235	511.621064	192.168.43.109	157.240.7.26	TCP	54	56078 → 443 [ACK] Seq=201197 Ack=47567 Win=60 Len=0
21236	511.661648	157.240.7.26	192.168.43.109	TCP	114	[TCP segment of a reassembled PDU]
21237	511.861069	192.168.43.109	157.240.7.26	TCP	54	56078 → 443 [ACK] Seq=201197 Ack=47627 Win=65 Len=0
21238	512.159087	157.240.7.26	192.168.43.109	TCP	119	[TCP segment of a reassembled PDU]
21239	512.358988	192.168.43.109	157.240.7.26	TCP	54	56078 → 443 [ACK] Seq=201197 Ack=47692 Win=65 Len=0
21240	512.402291	157.240.7.26	192.168.43.109	TCP	119	[TCP segment of a reassembled PDU]
21241	512.461747	192.168.43.109	31.13.78.17	TLSv1.2	100	Application Data
21242	512.496622	192.168.43.109	31.13.78.17	TLSv1.2	85	Encrypted Alert
21243	512.497094	192.168.43.109	31.13.78.17	TCP	54	56131 → 443 [FIN, ACK] Seq=32790 Ack=3847061 Win=64262 Len=0
21244	512.510508	31.13.78.17	192.168.43.109	TCP	54	443 → 56131 [ACK] Seq=3847061 Ack=32759 Win=34366 Len=0
21245	512.525339	31.13.78.17	192.168.43.109	TLSv1.2	100	Application Data
21246	512.525467	192.168.43.109	31.13.78.17	TCP	54	56131 → 443 [RST, ACK] Seq=32791 Ack=3847107 Win=0 Len=0
21247	512.527044	31.13.78.17	192.168.43.109	TLSv1.2	85	Encrypted Alert
21248	512.529749	31.13.78.17	192.168.43.109	TCP	54	[TCP Out-Of-Order] 443 → 56131 [FIN, ACK] Seq=3847138 Ack=32759 Win=34366 Len=0
21249	512.530187	31.13.78.17	192.168.43.109	TCP	54	443 → 56131 [ACK] Seq=3847139 Ack=32791 Win=34397 Len=0
21250	512.543625	31.13.78.17	192.168.43.109	TCP	54	443 → 56131 [RST, ACK] Seq=3847139 Ack=32791 Win=0 Len=0

```

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: QuantaML 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: 31.13.78.17
Transmission Control Protocol, Src Port: 56034, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000  a0 86 c6 cc 16 b5 20 7c 8f 69 b0 33 08 00 45 00  .... |.i.3.E.
0010  00 28 24 f3 40 00 00 06 7c a9 c0 a8 2b 6d 1f 0d  .(.$@... |...+m..
0020  4e 11 da e2 01 bb 84 7c e0 b8 f3 89 f2 27 50 10  N.....| .....P.
0030  00 3e 2e de 00 00  .>....
  
```

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.