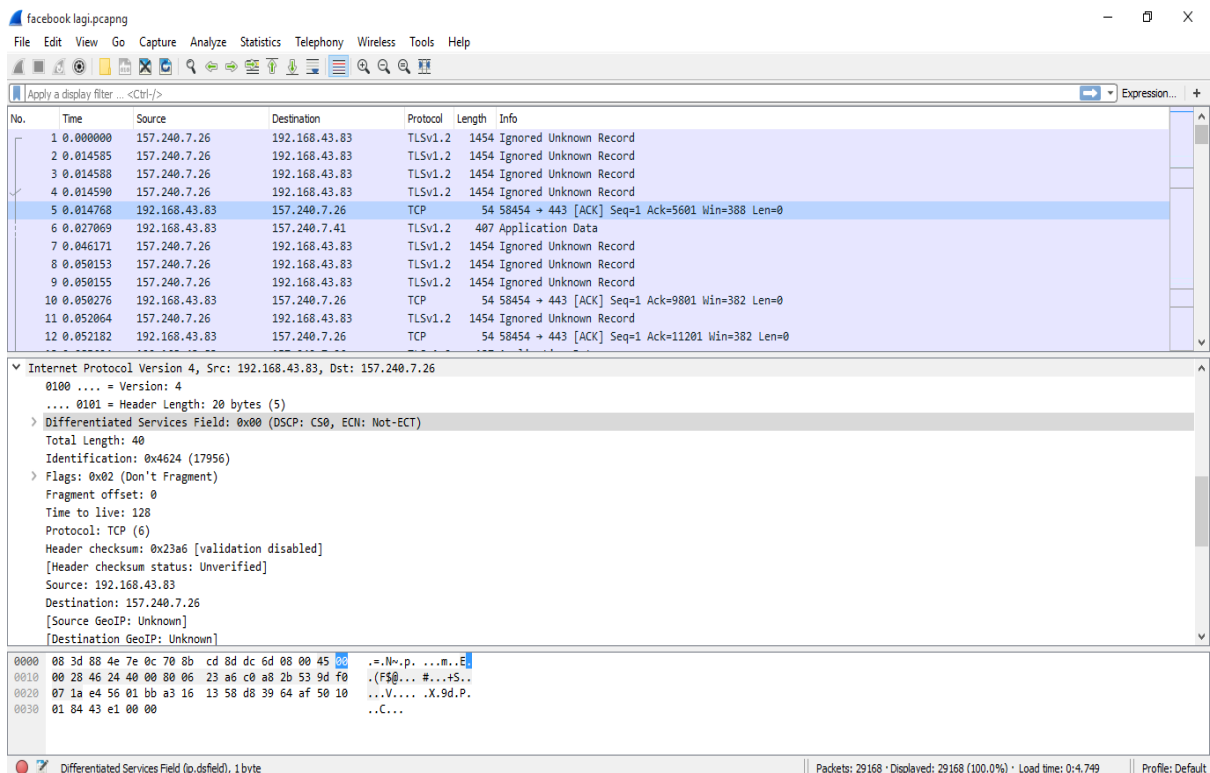


Nama : Dini Ayu Lestari  
NIM : 09031181520005  
Kelas : SI Reguler 4A  
Mata Kuliah : Komunikasi Data dan Jaringan Komputer  
Dosen Pembimbing : Deris Stiawan, Ph.D

## Analisa Paket Data Menggunakan Wireshark

Wireshark merupakan salah satu tools atau aplikasi “Network Analyzer” atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk sniffing (memperoleh informasi penting seperti password email, dll). Wireshark sendiri merupakan free tools untuk Network Analyzer yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan user karena menggunakan tampilan grafis atau GUI (Graphical User Interface).

### 1. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website [www.facebook.com](http://www.facebook.com)



Pada gambar diatas dapat diketahui bahwa **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari website yang dituju (destination)** yaitu Facebook adalah **157.240.7.26** , dikarenakan saya sudah terlebih dahulu membuka facebook dan sedang berinteraksi dihalaman tersebut, jadi pada nomor 1 sampai 4 adalah

proses ketika paket data dari facebook kembali ke PC saya, dan nomor 5 adalah request dari PC saya ke destination dengan menggunakan protocol TCP. TCP sendiri adalah suatu protokol pengiriman data yang berbasis Internet Protocol (IP) dan bersifat connection oriented.

```
▼ Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
  Interface id: 0 (\Device\NPF_{B2471995-9A2F-4AC4-BF2D-D7481A211ED9})
  Encapsulation type: Ethernet (1)
  Arrival Time: Apr 12, 2017 19:35:17.661986000 SE Asia Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1492000517.661986000 seconds
  [Time delta from previous captured frame: 0.000178000 seconds]
  [Time delta from previous displayed frame: 0.000178000 seconds]
  [Time since reference or first frame: 0.014768000 seconds]
  Frame Number: 5
  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]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
```

Pada frame diatas dapat dilihat bahwa frame ke 5 ini diakses pada pukul 19:35:17 tanggal 12 April 2017 sesuai dengan standar waktu Asia karena website diakses dari negara yang merupakan bagian dari benua Asia.

```
▼ Transmission Control Protocol, Src Port: 58454, Dst Port: 443, Seq: 1, Ack: 5601, Len: 0
  Source Port: 58454
  Destination Port: 443
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 5601 (relative ack number)
  Header Length: 20 bytes
  > Flags: 0x010 (ACK)
  Window size value: 388
  [Calculated window size: 388]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x43e1 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
```

Pada bagian trasmission control protocol ini, dapat diketahui bahwa **Source Port nya adalah 58454** dan **Destination Portnya adalah 443**. Lalu dapat dilihat bahwa **header length nya sebesar 20 bytes**. Selain protocol TCP, terdapat juga beberapa protocol yang tercapture saat membuka website ini seperti :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record
2	0.014585	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record
3	0.014588	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record
4	0.014590	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record
5	0.014768	192.168.43.83	157.240.7.26	TCP	54	58454 → 443 [ACK] Seq=1 Ack=5601 Win=388 Len=0
6	0.027069	192.168.43.83	157.240.7.41	TLSv1.2	407	Application Data
7	0.046171	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record
8	0.050153	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record
9	0.050155	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record
10	0.050276	192.168.43.83	157.240.7.26	TCP	54	58454 → 443 [ACK] Seq=1 Ack=9801 Win=382 Len=0
11	0.052064	157.240.7.26	192.168.43.83	TLSv1.2	1454	Ignored Unknown Record

Ethernet II, Src: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d), Dst: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c)  
 Destination: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c)  
 Source: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d)  
 Type: IPv4 (0x0800)

Pada bagian ethernet terlihat bahwa source (**192.168.43.83**) memiliki mac address **70:8b:cd:8d:dc:6d** dan destinationnya (**157.240.7.26**) memiliki mac address **08:3d:88:4e:7e:0c**.

No.	Time	Source	Destination	Protocol	Length	Info
251	1.910014	157.240.7.41	192.168.43.83	TLSv1.2	628	Application Data
252	1.910164	192.168.43.83	157.240.7.41	TCP	54	58466 → 443 [ACK] Seq=4685 Ack=12606 Win=61 Len=0
253	1.917208	157.240.7.36	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
254	1.917400	157.240.7.36	192.168.43.83	TLSv1.2	135	Application Data
255	1.917484	192.168.43.83	157.240.7.36	TCP	54	58471 → 443 [ACK] Seq=1371 Ack=3827 Win=16128 Len=0
256	1.917839	192.168.43.83	157.240.7.36	TLSv1.2	92	Application Data
257	1.928504	192.168.43.83	157.240.7.20	TCP	54	58470 → 443 [ACK] Seq=5001 Ack=4395 Win=15709 Len=0
258	1.949923	157.240.7.26	192.168.43.83	TLSv1.2	1454	Application Data[TCP segment of a reassembled PDU]
259	1.949927	157.240.7.26	192.168.43.83	TLSv1.2	1454	Application DataApplication Data, Application Data, Application Data
260	1.949935	157.240.7.26	192.168.43.83	TLSv1.2	1454	Application Data[TCP segment of a reassembled PDU]
261	1.949938	157.240.7.26	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]

[Next sequence number: 3746 (relative sequence number)]  
 Acknowledgment number: 337 (relative ack number)  
 Header Length: 20 bytes  
 Flags: 0x018 (PSH, ACK)  
 Window size value: 115  
 [Calculated window size: 29440]  
 [Window size scaling factor: 256]  
 Checksum: 0x3be8 [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 [SEQ/ACK analysis]  
 Secure Sockets Layer  
 TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket  
 TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec  
 TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

```

0000 70 8b cd 8d dc 6d 08 3d 88 4e 7e 0c 08 00 45 00  p...m.=.N...E.
0010 01 2a d0 80 40 00 57 06 c1 3d 9d f0 07 24 c0 a8  .*.@.W. ....$.
0020 2b 53 01 bb e4 67 c9 4e 58 65 47 f8 36 39 50 18  +S..g.N XeG.69P.
0030 00 73 3b e8 00 00 16 03 03 00 ca 04 00 00 c6 00  -s;.....
0040 02 a3 00 00 c0 6b f5 c2 17 ae 87 6f 1c 4f 0c b9  ....k...o.O..
0050 3e 19 2d 41 82 e9 5e 93 b9 24 bb d5 23 02 10 fe  >..A..$.#...
0060 14 e5 2e 58 2a d9 a3 ca 28 2b 10 9a 4e 5a f4 2a  ...X*...(+.NZ.*
0070 53 2c 9d 5d d2 0e bd 5b 87 8e 46 81 33 a1 db 8e  S,.U...[.F.3...
0080 e9 03 eb e7 a3 8b 29 4c 2f c0 b1 f2 e5 51 66 6c  .....L/./...Qf1

```

facebook lagi | Packets: 29168 • Displayed: 29168 (100.0%) • Load time: 0:2.151 | Profile: Default

Pada gambar diatas, yaitu pada **frame 253** terdapat **handshake** dari source **157.240.7.36** (IP address dari facebook) ke destination dengan IP address **192.168.43.83** (PC).

Selain menggunakan protokol TCP, ada juga protokol – protokol lainnya, seperti :

- **HTTP**

No.	Time	Source	Destination	Protocol	Length	Info
234.	336.163581	192.168.43.83	13.107.4.50	TCP	54	58724 → 80 [ACK] Seq=5445 Ack=563134 Win=185856 Len=0
234.	336.178193	13.107.4.50	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
234.	336.178597	13.107.4.50	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
234.	336.178682	192.168.43.83	13.107.4.50	TCP	54	58724 → 80 [ACK] Seq=5445 Ack=565934 Win=185856 Len=0
234.	336.182670	13.107.4.50	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
234.	336.183131	13.107.4.50	192.168.43.83	HTTP	604	HTTP/1.1 206 Partial Content (application/octet-stream)
234.	336.183247	192.168.43.83	13.107.4.50	TCP	54	58724 → 80 [ACK] Seq=5445 Ack=567884 Win=185856 Len=0
234.	336.902466	192.168.43.83	13.107.4.50	HTTP	380	GET /d/msdownload/update/software/defu/2017/04/am_delta_39dbd238ca98aa89565908ebefb55ab66e979d4.exe HTTP/1...
234.	337.077245	13.107.4.50	192.168.43.83	TCP	54	80 → 58724 [ACK] Seq=567884 Ack=5771 Win=130816 Len=0
234.	337.079116	13.107.4.50	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
234.	337.089287	13.107.4.50	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
234.	337.089452	192.168.43.83	13.107.4.50	TCP	54	58724 → 80 [ACK] Seq=5771 Ack=570684 Win=185856 Len=0

```

X-CCC: SG\r\n
X-MS-Edge-Ref: Ref A: 048DA341C7034F4388331099F7F0F1AE Ref B: SG1EDGE0115 Ref C: Wed Apr 12 05:40:35 2017 PST\r\n
X-MS-Edge-Ref-OriginShield: Ref A: ABAF440E1817481EBD4C4A0D18A55CC8 Ref B: SG2SCHEDG0113 Ref C: Wed Apr 12 03:08:57 2017 PST\r\n
Date: Wed, 12 Apr 2017 12:40:35 GMT\r\n
\r\n
[HTTP response 17/38]
[Time since request: 0.296206000 seconds]
[Prev request in frame: 23255]
[Prev response in frame: 23344]
[Request in frame: 23349]
[Next request in frame: 23431]
File Data: 76934 bytes
    
```

HTTP (HyperText Transfer Protocol) adalah protocol pada layer aplikasi baik TCP/IP maupun OSI yang digunakan untuk mengakses web pages dari suatu website. Secara spesifik dalam penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan yang disebut hiperteks, yang kemudian membentuk WWW (Word Wide Web).

- **DNS**

No.	Time	Source	Destination	Protocol	Length	Info
165	1.607926	192.168.43.83	157.240.7.26	TLSv1.2	135	Application Data
166	1.636855	192.168.43.83	157.240.7.41	TCP	54	58466 → 443 [ACK] Seq=4685 Ack=11641 Win=59 Len=0
167	1.653242	203.104.174.12	192.168.43.83	TCP	54	443 → 58248 [ACK] Seq=236 Ack=28 Win=105 Len=0
168	1.653244	192.168.43.1	192.168.43.83	DNS	117	Standard query response 0x55ce A pixel.facebook.com CNAME z-m.c10r.facebook.com A 157.240.7.36
169	1.653244	157.240.7.41	192.168.43.83	TCP	54	443 → 58466 [ACK] Seq=11641 Ack=4615 Win=263 Len=0
170	1.653367	192.168.43.83	203.104.174.12	SSL	114	Continuation Data
171	1.655046	157.240.7.26	192.168.43.83	TCP	54	443 → 58454 [ACK] Seq=25456 Ack=680 Win=119 Len=0
172	1.655048	157.240.7.26	192.168.43.83	TCP	54	443 → 58454 [ACK] Seq=25456 Ack=1219 Win=119 Len=0
173	1.656245	192.168.43.83	157.240.7.36	TCP	66	58471 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
174	1.657607	157.240.7.26	192.168.43.83	TLSv1.2	96	Application Data
175	1.657906	157.240.7.26	192.168.43.83	TLSv1.2	849	Application Data
176	1.657979	192.168.43.83	157.240.7.26	TCP	54	58469 → 443 [ACK] Seq=443 Ack=12279 Win=61 Len=0

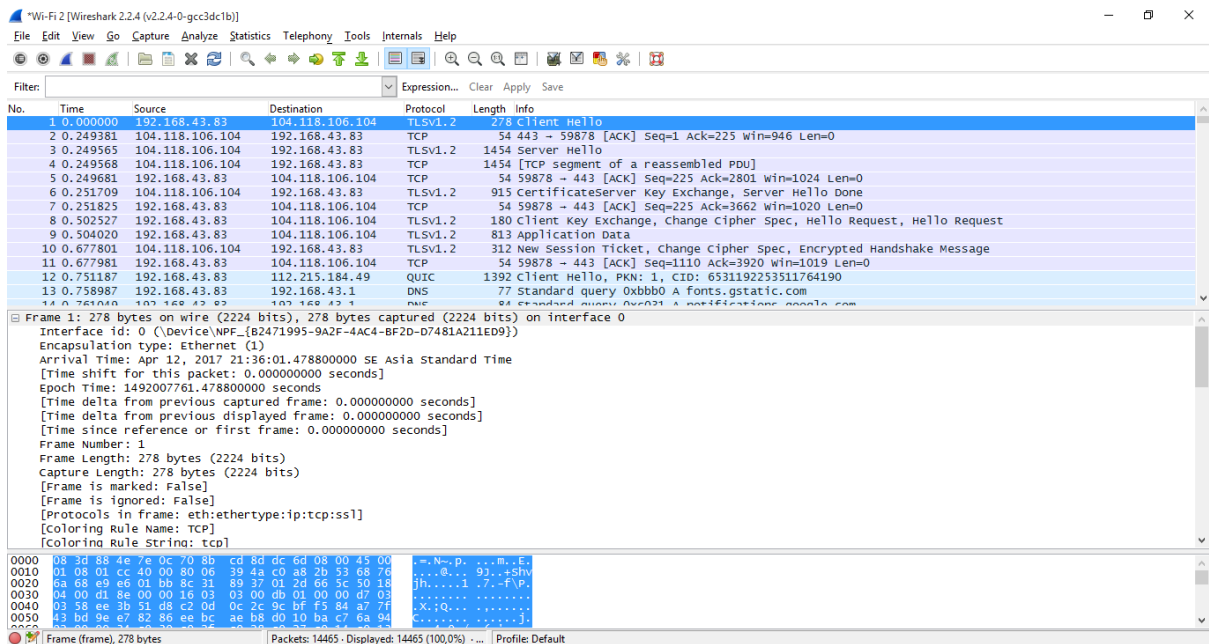
```

Capture Length: 117 bytes (936 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
▼ Ethernet II, Src: SamsungE_4e:7e:0c (08:3d:88:4e:7e:0c), Dst: AsustekC_8d:dc:6d (70:8b:cd:8d:dc:6d)
  > Destination: AsustekC_8d:dc:6d (70:8b:cd:8d:dc:6d)
  > Source: SamsungE_4e:7e:0c (08:3d:88:4e:7e:0c)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.83
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 103
  Identification: 0xf400 (62672)
0000 70 8b cd 8d dc 6d 08 3d 88 4e 7e 0c 08 00 45 00  p.....N....E.
    
```

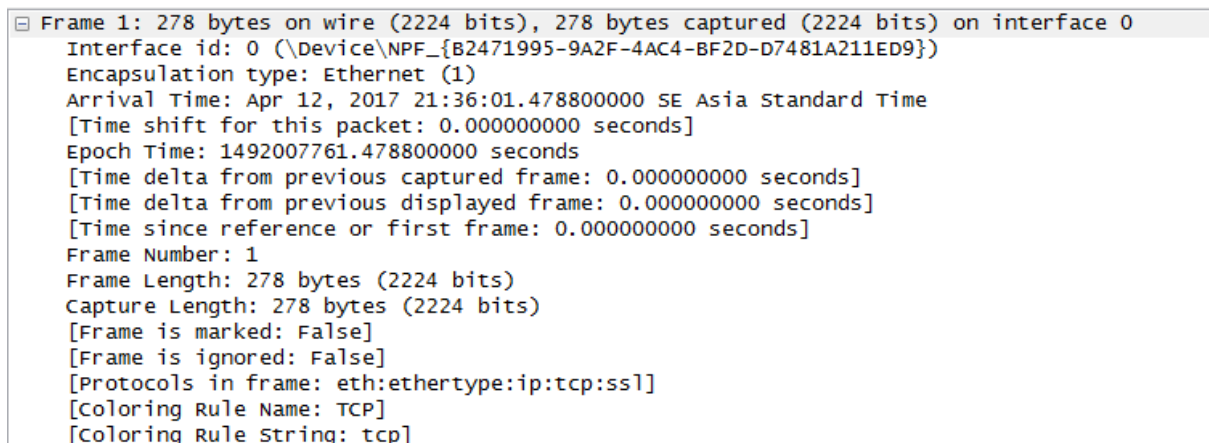
DNS (Domain Name System) adalah protocol yang digunakan untuk mentranslate hostname ke IP address dan sebaliknya. Karena di dunia manusia ini, lebih susah menghafalkan IP dibanding dengan deretan tulisan yang membentuk nama host.

Pada setiap paket data yang tercapture memiliki data – data yang berbeda mulai dari frame, ethernet, internet protocol dan lainnya.

## 2. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website [www.twitter.com](http://www.twitter.com)



Pada gambar diatas dapat diketahui bahwa frame pertama memiliki **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari halaman yang dituju (destination)** yaitu Twitter adalah **104.118.106.104** . Pada frame 1 adalah request dari PC saya ke destination dan pada frame 2,3 dan 4 adalah respon dari website yang dituju tadi kembali ke PC yang saya gunakan.



Pada frame diatas dapat dilihat bahwa frame ke 1 ini diakses pada pukul 21:36:01 tanggal 12 April 2017 sesuai dengan standar waktu Asia karena website diakses dari negara yang merupakan bagian dari benua Asia.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.83	104.118.106.104	TLSv1.2	278	Client Hello
2	0.249381	104.118.106.104	192.168.43.83	TCP	54	443 → 59878 [ACK] Seq=1 Ack=225 win=946 Len=0
3	0.249565	104.118.106.104	192.168.43.83	TLSv1.2	1454	Server Hello
4	0.249568	104.118.106.104	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
5	0.249681	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=225 Ack=2801 win=1024 Len=0
6	0.251709	104.118.106.104	192.168.43.83	TLSv1.2	915	CertificateServer Key Exchange, Server Hello Done
7	0.251825	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=225 Ack=3662 win=1020 Len=0
8	0.502527	192.168.43.83	104.118.106.104	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
9	0.504020	192.168.43.83	104.118.106.104	TLSv1.2	813	Application Data
10	0.677801	104.118.106.104	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	0.677981	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=1110 Ack=3920 win=1019 Len=0
12	0.751187	192.168.43.83	112.215.184.49	QUIC	1392	Client Hello, PKN: 1, CID: 6531192253511764190
13	0.758987	192.168.43.83	192.168.43.1	DNS	77	Standard query 0xbbb0 A fonts.gstatic.com
14	0.761040	192.168.43.83	192.168.43.1	DNS	84	Standard query 0xc021 A notifications.google.com

Transmission Control Protocol, Src Port: 443, Dst Port: 59878, Seq: 1, Ack: 225, Len: 0

Source Port: 443  
Destination Port: 59878  
[Stream index: 0]  
[TCP Segment Len: 0]  
Sequence number: 1 (relative sequence number)  
Acknowledgment number: 225 (relative ack number)  
Header Length: 20 bytes

Untuk frame kedua ini, **IP address dari source nya adalah 104.118.106.104 (twitter)** dan **IP address destination nya adalah 192.168.43.83 (PC)**, frame kedua ini merupakan respon dari frame 1 yang mana frame 1 adalah request ketika PC mengirimkan paket ke destination. Frame kedua ini menggunakan protokol TCP yang mana **Source Portnya adalah 443 dan Destination Port nya 59878.**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.83	104.118.106.104	TLSv1.2	278	Client Hello
2	0.249381	104.118.106.104	192.168.43.83	TCP	54	443 → 59878 [ACK] Seq=1 Ack=225 win=946 Len=0
3	0.249565	104.118.106.104	192.168.43.83	TLSv1.2	1454	Server Hello
4	0.249568	104.118.106.104	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
5	0.249681	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=225 Ack=2801 win=1024 Len=0
6	0.251709	104.118.106.104	192.168.43.83	TLSv1.2	915	CertificateServer Key Exchange, Server Hello Done
7	0.251825	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=225 Ack=3662 win=1020 Len=0
8	0.502527	192.168.43.83	104.118.106.104	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
9	0.504020	192.168.43.83	104.118.106.104	TLSv1.2	813	Application Data
10	0.677801	104.118.106.104	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	0.677981	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=1110 Ack=3920 win=1019 Len=0
12	0.751187	192.168.43.83	112.215.184.49	QUIC	1392	Client Hello, PKN: 1, CID: 6531192253511764190
13	0.758987	192.168.43.83	192.168.43.1	DNS	77	Standard query 0xbbb0 A fonts.gstatic.com
14	0.761040	192.168.43.83	192.168.43.1	DNS	84	Standard query 0xc021 A notifications.google.com

[coloring Rule String: tcp]

Ethernet II, Src: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c), Dst: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d)

Destination: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d)  
Source: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c)  
Type: IPv4 (0x0800)

Pada bagian ethernet terlihat bahwa source (**104.118.106.104**) memiliki mac address **08:3d:88:4e:7e:0c** dan destinationnya (**192.168.43.83**) memiliki mac address **70:8b:cd:8d:dc:6d**.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.83	104.118.106.104	TLSv1.2	278	Client Hello
2	0.249381	104.118.106.104	192.168.43.83	TCP	54	443 → 59878 [ACK] Seq=1 Ack=225 Win=946 Len=0
3	0.249565	104.118.106.104	192.168.43.83	TLSv1.2	1454	Server Hello
4	0.249568	104.118.106.104	192.168.43.83	TCP	1454	[TCP segment of a reassembled PDU]
5	0.249681	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=225 Ack=2801 Win=1024 Len=0
6	0.251709	104.118.106.104	192.168.43.83	TLSv1.2	915	CertificateServer Key Exchange, Server Hello Done
7	0.251825	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=225 Ack=3662 Win=1020 Len=0
8	0.502527	192.168.43.83	104.118.106.104	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
9	0.504020	192.168.43.83	104.118.106.104	TLSv1.2	813	Application Data
10	0.677801	104.118.106.104	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	0.677981	192.168.43.83	104.118.106.104	TCP	54	59878 → 443 [ACK] Seq=1110 Ack=3920 Win=1019 Len=0

```

Frame Length: 312 bytes (2496 bits)
Capture Length: 312 bytes (2496 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:ssl]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
> Ethernet II, Src: SamsungE_4e:7e:0c (08:3d:88:4e:7e:0c), Dst: AsustekC_8d:cd:6d (78:7b:cd:8d:dc:6d)
> Internet Protocol Version 4, Src: 104.118.106.104, Dst: 192.168.43.83
> Transmission Control Protocol, Src Port: 443, Dst Port: 59878, Seq: 3662, Ack: 351, Len: 258
▼ Secure Sockets Layer
  > TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
  > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
  
```

```

0000  70 8b cd 8d dc 6d 08 3d 88 4e 7e 0c 08 00 45 00  p...m.=.N...E.
0010  01 2a 61 16 40 00 3b 06 1e de 68 76 6a 68 c0 a8  .*a. @;. .hvjh..
0020  2b 53 01 bb e9 e6 01 2d 74 a9 8c 31 8a 95 50 18  +S....- t..1..P.
0030  03 b2 50 2e 00 00 16 03 03 00 ca 04 00 00 c6 00  ..P.....
0040  00 1c 20 00 c0 00 00 07 6a 44 cd 83 3e 1d 63 cf  .. .... jD...c.
0050  5a f2 69 a7 84 23 41 d6 23 90 f4 09 bc 4a f7 b3  Z.i..#A.#....J..
0060  9d 43 16 be 52 0e b1 be dd 1d cd ff 3b 0a 05 4e  .C..R... ..N
0070  3a 1b 40 4e 96 17 90 49 7e b2 3b e5 dd eb 5e 5f  :@N...I ~;...^
0080  a3 e5 64 aa 7b 9e 1e 32 15 ed 5e ee 45 fb 84 46  ..d.{...^..E..F
  
```

Frame is ignored by the dissectors (frame.ignored) | Packets: 14465 · Dissected: 14465 (100.0%) · Load time: 0:2.740 | Profile: Default

Pada gambar diatas, yaitu pada **frame 10** terdapat **handshake** dari source 104.118.106.104 (IP address dari twitter) ke destination dengan IP address 192.168.43.83 (PC). Pada frame ke 9, 192.168.43.83 melakukan request kedestinationnya yaitu 104.118.106.104 kemudian ada respon dari 104.118.106.104 kembali ke IP address dari PC yang digunakan.



### 3. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website [www.detik.com](http://www.detik.com)

The screenshot shows a Wireshark capture of network traffic. The packet list pane at the top shows several packets, with packet 7398 highlighted in red. The packet details pane below shows the structure of frame 7398, which is a QUIC Client Hello. The packet bytes pane at the bottom shows the raw hex and ASCII data of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
7394	99.789746	192.168.43.83	203.190.242.59	TCP	54	60444 - 443 [ACK] Seq=4450 Ack=86771 Win=23552 Len=0
7395	99.792564	192.168.43.83	216.58.221.66	QUIC	77	Payload (Encrypted), PKN: 10, CID: 12369586900995331160
7396	99.801351	203.190.242.59	192.168.43.83	TCP	66	[TCP Dup ACK 7350#1] 443 - 60450 [ACK] Seq=153 Ack=518 win=15872 Len=0 SLE=1 SRE=518
7397	99.820428	192.168.43.83	203.190.242.59	TLSv1.2	1114	Application Data
7398	99.826879	192.168.43.83	74.125.68.154	QUIC	1392	Client Hello, PKN: 1, CID: 4755907082276700669
7399	99.828389	192.168.43.83	74.125.68.154	QUIC	422	Payload (Encrypted), PKN: 2, CID: 4755907082276700669

**Frame 7398: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface 0**  
 Interface id: 0 (\Device\NPF\_{B2471995-9A2F-4AC4-BF2D-D7481A211ED9})  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Apr 12, 2017 22:54:40.613773000 SE Asia Standard Time  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1492012480.613773000 seconds  
 [Time delta from previous captured frame: 0.006451000 seconds]  
 [Time delta from previous displayed frame: 0.006451000 seconds]  
 [Time since reference or first frame: 99.826879000 seconds]  
 Frame Number: 7398  
 Frame Length: 1392 bytes (11136 bits)  
 Capture Length: 1392 bytes (11136 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:udp:quic]  
 [Coloring Rule Name: UDP]  
 [Coloring Rule String: udp]

0000 08 3d 88 4e 7e 0c 70 8b cd 8d dc 6d 08 00 45 00 ..=N~.p. ...m..E.  
 0010 05 62 25 af 00 00 80 11 94 c9 c0 a8 2b 53 4a 7d .b%..... ....+S}  
 0020 44 9a c1 d2 01 bb 05 4e ed 0c 0d fd 01 de 1f 4b D.....N .....K  
 0030 60 00 42 51 30 33 35 01 a4 3e 23 33 45 4f 3d 27 .BQ035. .>#3EO"  
 0040 9c 43 d1 c5 a0 01 00 04 43 48 4c 4f 1d 00 00 00 .C..... CHLO....  
 0050 50 41 44 00 eb 00 00 00 53 4e 49 00 08 01 00 00 PAD..... SNI.....

Pada gambar diatas dapat diketahui bahwa pada frame 7398 IP address dari komputer (source) yang digunakan adalah 192.168.43.83 dan IP address dari halaman yang dituju (destination) yaitu detik.com adalah 74.125.68.154 . Selain itu dapat kita ketahui pada bagian frame bahwa frame 7398 ini diakses pada pukul 22:54:40 tanggal 12 april 2017.

This screenshot is similar to the one above but shows a different detail pane for frame 7398, focusing on the Ethernet II layer. The packet list pane is the same, with frame 7398 highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
7394	99.789746	192.168.43.83	203.190.242.59	TCP	54	60444 - 443 [ACK] Seq=4450 Ack=86771 Win=23552 Len=0
7395	99.792564	192.168.43.83	216.58.221.66	QUIC	77	Payload (Encrypted), PKN: 10, CID: 12369586900995331160
7396	99.801351	203.190.242.59	192.168.43.83	TCP	66	[TCP Dup ACK 7350#1] 443 - 60450 [ACK] Seq=153 Ack=518 win=15872 Len=0 SLE=1 SRE=518
7397	99.820428	192.168.43.83	203.190.242.59	TLSv1.2	1114	Application Data
7398	99.826879	192.168.43.83	74.125.68.154	QUIC	1392	Client Hello, PKN: 1, CID: 4755907082276700669

**Frame 7398: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface 0**  
 Interface id: 0 (\Device\NPF\_{B2471995-9A2F-4AC4-BF2D-D7481A211ED9})  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Apr 12, 2017 22:54:40.613773000 SE Asia Standard Time  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1492012480.613773000 seconds  
 [Time delta from previous captured frame: 0.006451000 seconds]  
 [Time delta from previous displayed frame: 0.006451000 seconds]  
 [Time since reference or first frame: 99.826879000 seconds]  
 Frame Number: 7398  
 Frame Length: 1392 bytes (11136 bits)  
 Capture Length: 1392 bytes (11136 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:udp:quic]  
 [Coloring Rule Name: UDP]  
 [Coloring Rule String: udp]

**Ethernet II, Src: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d), Dst: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c)**  
 Destination: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c)  
 Source: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d)  
 Type: IPv4 (0x0800)

Pada bagian ethernet terlihat bahwa source (**192.168.43.83**) memiliki mac address **70:8b:cd:8d:dc:6d** dan destinationnya (**74.125.68.154**) memiliki mac address **08:3d:88:4e:7e:0c**.

No.	Time	Source	Destination	Protocol	Length	Info
15726	156.148316	192.168.43.83	203.190.242.102	TCP	54	60594 → 443 [FIN, ACK] Seq=337 Ack=3455 win=15872 Len=0
15727	156.148947	192.168.43.83	203.190.242.102	TCP	54	60594 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0
15728	156.149515	192.168.43.83	203.190.242.102	TCP	54	60595 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0
15729	156.149760	192.168.43.83	203.190.242.102	TCP	54	60595 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0
15730	156.150516	192.168.43.83	203.190.242.102	TCP	54	60597 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0
15731	156.150755	192.168.43.83	203.190.242.102	TCP	54	60597 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0
15732	156.151510	192.168.43.83	203.190.242.102	TCP	54	60596 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0
15733	156.151920	192.168.43.83	203.190.242.102	TCP	54	60596 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0
15734	156.152562	192.168.43.83	203.190.242.102	TCP	54	60598 → 443 [FIN, ACK] Seq=337 Ack=3455 win=16128 Len=0
15735	156.152773	192.168.43.83	203.190.242.102	TCP	54	60598 → 443 [RST, ACK] Seq=338 Ack=3455 win=0 Len=0
15736	156.153455	192.168.43.83	74.125.68.157	TCP	54	60582 → 80 [FIN, ACK] Seq=1752 Ack=989 win=15616 Len=0
15737	156.153760	192.168.43.83	74.125.68.157	TCP	54	60583 → 80 [FIN, ACK] Seq=1792 Ack=989 win=15616 Len=0
15738	156.154239	192.168.43.83	74.125.68.157	TCP	54	60584 → 80 [FIN, ACK] Seq=919 Ack=495 win=15872 Len=0

type: IPV4 (0x0800)

Internet Protocol Version 4, Src: 192.168.43.83, Dst: 74.125.68.157

Transmission Control Protocol, Src Port: 60583, Dst Port: 80, Seq: 1792, Ack: 989, Len: 0

Source Port: 60583  
 Destination Port: 80  
 [Stream index: 358]  
 [TCP Segment Len: 0]  
 Sequence number: 1792 (relative sequence number)  
 Acknowledgment number: 989 (relative ack number)  
 Header Length: 20 bytes

Flags: 0x011 (FIN, ACK)  
 Window size value: 61  
 [Calculated window size: 15616]  
 [Window size scaling factor: 256]  
 Checksum: 0xfea0 [unverified]  
 [Checksum status: Unverified]  
 Urgent pointer: 0

Untuk frame ke 15736 request dari source ke destination (detik.com) menggunakan protokol TPC dengan **Source Port nya 192** dan **Destination Port nya 80**.

No.	Time	Source	Destination	Protocol	Length	Info
129	3.640086	192.168.43.83	112.215.88.59	QUIC	80	Payload (Encrypted), PKN: 8, CID: 18275625714750018923
130	3.700314	192.168.43.83	203.190.242.102	TCP	264	[TCP Retransmission] 60262 → 443 [PSH, ACK] Seq=1 Ack=1 Win=16384 Len=210
131	3.706838	112.215.88.59	192.168.43.83	QUIC	80	Payload (Encrypted), PKN: 18, CID: 18275625714750018923
132	3.746363	203.190.242.172	192.168.43.83	TCP	1454	[TCP Out-Of-Order] 443 → 60263 [ACK] Seq=1 Ack=209 Win=30464 Len=1400
133	3.746561	192.168.43.83	203.190.242.172	TCP	66	60263 → 443 [ACK] Seq=209 Ack=1401 Win=16384 Len=0 SLE=2801 SRE=3129
134	3.750470	203.190.242.172	192.168.43.83	TCP	1454	[TCP Out-Of-Order] 443 → 60263 [ACK] Seq=1401 Ack=209 Win=30464 Len=1400
135	3.750634	192.168.43.83	203.190.242.172	TCP	54	60263 → 443 [ACK] Seq=209 Ack=3129 Win=16384 Len=0
136	3.754527	192.168.43.83	203.190.242.172	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
137	3.819639	203.190.242.102	192.168.43.83	TCP	66	[TCP Previous segment not captured] 443 → 60262 [ACK] Seq=3128 Ack=211 Win=30464 Len=0 SLE=1 SRE=211
138	3.880572	203.190.242.172	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
139	3.880575	203.190.242.172	192.168.43.83	TLSv1.2	123	Application Data

Acknowledgment number: 335 (relative ack number)  
 Header Length: 20 bytes  
 Flags: 0x018 (PSH, ACK)  
 Window size value: 119  
 [Calculated window size: 30464]  
 [Window size scaling factor: 256]  
 Checksum: 0xd191 [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 [SEQ/ACK analysis]

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
- TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

```

0000 70 8b cd 8d dc 6d 08 3d 88 4e 7e 0c 08 00 45 00  p...m.=.N...E.
0010 01 2a d6 79 40 00 37 06 c1 ed cb be f2 ac c0 a8  .*.y@.7. ....
0020 2b 53 01 bb eb 67 ae 54 86 20 c6 21 ea 1f 50 18  +S...g.T. .!..P.
0030 00 77 d1 91 00 00 16 03 03 00 ca 04 00 00 c6 00  .w.....
0040 00 01 2c 00 c0 f3 b1 5e 06 a7 a5 d5 90 a9 21 55  .,.....^.....!U
0050 2c cd ca c4 91 0e 06 be c7 af 53 ba 90 74 96 a1  ,.....S..t...
0060 93 5b 85 e8 ab 73 bf 84 ac 0e 63 4a 30 af e7 b5  .[...s...c]0...
0070 ab f6 ef 36 85 97 8e 69 0c 93 f5 72 68 e6 ac 52  ...6...i...rh..R
0080 eb 28 59 cc e3 79 6d c2 9a 64 97 32 7b 51 b1 63  .(Y..yb. .d.2[0.c
  
```

Pada gambar diatas, yaitu pada **frame 138** terdapat **handshake** dari source 203.190.242.172 ke destination dengan IP address 192.168.43.83 (PC).

#### 4. Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website [www.kompas.com](http://www.kompas.com)

No.	Time	Source	Destination	Protocol	Length	Info
162	6.024866	192.168.43.83	74.125.24.94	QUIC	80	Payload (Encrypted), PKN: 36, CID: 16810017306748636352
163	6.187581	192.168.43.83	74.125.24.94	QUIC	263	Payload (Encrypted), PKN: 37, CID: 16810017306748636352
164	6.273358	74.125.24.94	192.168.43.83	QUIC	141	Payload (Encrypted), PKN: 61
165	6.300887	192.168.43.83	74.125.24.94	QUIC	77	Payload (Encrypted), PKN: 38, CID: 16810017306748636352
166	6.595651	192.168.43.83	112.215.184.49	TCP	66	62418 → 443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
167	6.630999	192.168.43.83	112.215.184.49	QUIC	1392	Client Hello, PKN: 1, CID: 3979321133185802354
168	6.723794	112.215.184.49	192.168.43.83	TCP	66	443 → 62418 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 WS=128 SACK_PERM=1
169	6.724045	192.168.43.83	112.215.184.49	TCP	54	62418 → 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0
170	6.724628	192.168.43.83	112.215.184.49	TLSv1.2	265	Client Hello
171	6.748183	192.168.43.83	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
172	6.816008	112.215.184.49	192.168.43.83	QUIC	1392	Payload (Encrypted), PKN: 1, CID: 3979321133185802354
173	6.817218	192.168.43.83	112.215.184.49	QUIC	81	Payload (Encrypted), PKN: 2, CID: 3979321133185802354
174	6.817478	112.215.184.49	192.168.43.83	QUIC	81	Payload (Encrypted), PKN: 2, CID: 3979321133185802354

Frame 166: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
 Interface id: 0 (\Device\NPF\_{82471995-9A2F-4AC4-BF2D-D7481A211ED9})  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Apr 12, 2017 23:38:38.986983000 SE Asia Standard Time  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1492015118.986983000 seconds  
 [Time delta from previous captured frame: 0.294764000 seconds]  
 [Time delta from previous displayed frame: 0.294764000 seconds]  
 [Time since reference or first frame: 6.595651000 seconds]  
 Frame Number: 166  
 Frame Length: 66 bytes (528 bits)  
 Capture Length: 66 bytes (528 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:tcp]  
 [Coloring Rule Name: TCP SYN/ETN]

Pada gambar diatas dapat diketahui bahwa pada frame 166, **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari halaman yang dituju (destination)** yaitu kompas adalah **112.215.184.49** . Frame 166 terakses pada pukul 23:38:38 .

No.	Time	Source	Destination	Protocol	Length	Info
162	6.024866	192.168.43.83	74.125.24.94	QUIC	80	Payload (Encrypted), PKN: 36, CID: 16810017306748636352
163	6.187581	192.168.43.83	74.125.24.94	QUIC	263	Payload (Encrypted), PKN: 37, CID: 16810017306748636352
164	6.273358	74.125.24.94	192.168.43.83	QUIC	141	Payload (Encrypted), PKN: 61
165	6.300887	192.168.43.83	74.125.24.94	QUIC	77	Payload (Encrypted), PKN: 38, CID: 16810017306748636352
166	6.595651	192.168.43.83	112.215.184.49	TCP	66	62418 → 443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
167	6.630999	192.168.43.83	112.215.184.49	QUIC	1392	Client Hello, PKN: 1, CID: 3979321133185802354
168	6.723794	112.215.184.49	192.168.43.83	TCP	66	443 → 62418 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 WS=128 SACK_PERM=1
169	6.724045	192.168.43.83	112.215.184.49	TCP	54	62418 → 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0
170	6.724628	192.168.43.83	112.215.184.49	TLSv1.2	265	Client Hello
171	6.748183	192.168.43.83	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
172	6.816008	112.215.184.49	192.168.43.83	QUIC	1392	Payload (Encrypted), PKN: 1, CID: 3979321133185802354
173	6.817218	192.168.43.83	112.215.184.49	QUIC	81	Payload (Encrypted), PKN: 2, CID: 3979321133185802354
174	6.817478	112.215.184.49	192.168.43.83	QUIC	81	Payload (Encrypted), PKN: 2, CID: 3979321133185802354

Ethernet II, Src: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d), Dst: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c)  
 Destination: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c)  
 Source: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d)  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 192.168.43.83, Dst: 112.215.184.49  
 Transmission Control Protocol, Src Port: 62418, Dst Port: 443, Seq: 0, Len: 0  
 Source Port: 62418  
 Destination Port: 443  
 [Stream index: 0]  
 [TCP Segment Len: 0]  
 Sequence number: 0 (relative sequence number)  
 Acknowledgment number: 0  
 Header Length: 32 bytes  
 Flags: 0x002 (SYN)  
 Window size value: 8192  
 [Calculated window size: 8192]  
 Checksum: 0x949f [unverified]

```

0000 08 3d 88 4e 7e 0c 70 8b cd 8d dc 6d 08 00 45 00  .=.N~.p. ...m..E.
0010 00 34 1c e6 40 00 80 06 c8 d9 c0 a8 2b 53 70 d7  .4..@... ..+Sp.
0020 b8 31 f3 d2 01 bb be 0c f1 d1 00 00 00 80 02  .1..... ..
0030 20 00 94 9f 00 00 02 04 05 b4 01 03 03 08 01 01  .....
0040 04 02  ..
  
```

Pada bagian ethernet terlihat bahwa source (**192.168.43.83**) memiliki mac address **70:8b:cd:8d:dc:6d** dan destinationnya (**112.215.184.49**) memiliki mac address **08:3d:88:4e:7e:0c** . Sedangkan untuk Frame 166a ini menggunakan protokol TCP yang mana **Source Portnya** dalah **62418** dan **Destination Port nya** **433**.

The image shows a Wireshark network traffic capture. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 406 is highlighted in blue, showing a 'New Session Ticket, Change Cipher Spec, Encrypted Handshake Message' from source 54.192.151.15 to destination 192.168.43.83 over TLSv1.2.

The middle pane shows the packet details for frame 406, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Secure Sockets Layer.

The bottom pane shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
401	7.922996	103.243.221.75	192.168.43.83	TCP	1354	[TCP segment of a reassembled PDU]
402	7.923113	192.168.43.83	103.243.221.75	TCP	54	62437 → 443 [ACK] Seq=209 Ack=2601 Win=16616 Len=0
403	7.926476	192.168.43.83	103.243.221.75	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
404	7.928955	103.243.221.75	192.168.43.83	TLSv1.2	1354	Certificate [TCP segment of a reassembled PDU]
405	7.929199	103.243.221.75	192.168.43.83	TLSv1.2	763	Certificate StatusServer Key Exchange, Server Hello Done
406	7.929201	54.192.151.15	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
407	7.929396	192.168.43.83	103.243.221.75	TCP	54	62437 → 443 [ACK] Seq=209 Ack=4610 Win=16616 Len=0
408	7.932804	192.168.43.83	103.243.221.75	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
409	7.934632	54.239.16.235	192.168.43.83	TCP	62	80 → 62431 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=64
410	7.934634	54.239.16.235	192.168.43.83	TCP	62	80 → 62432 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=64
411	7.934635	54.239.16.235	192.168.43.83	TCP	62	80 → 62430 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=64
412	7.934952	192.168.43.83	54.239.16.235	TCP	54	62431 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0
413	7.935270	192.168.43.83	54.239.16.235	TCP	54	62432 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0
414	7.935452	192.168.43.83	54.239.16.235	TCP	54	62430 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0
415	7.945952	54.192.151.15	192.168.43.83	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

Frame 406: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface 0  
 Ethernet II, Src: SamsungE\_4e:7e:0c (08:3d:88:4e:7e:0c), Dst: AsustekC\_8d:dc:6d (70:8b:cd:8d:dc:6d)  
 Internet Protocol Version 4, Src: 54.192.151.15, Dst: 192.168.43.83  
 Transmission Control Protocol, Src Port: 443, Dst Port: 62427, Seq: 4943, Ack: 347, Len: 258  
 Secure Sockets Layer

```

0000  70 8b cd 8d dc 6d 08 3d 88 4e 7e 0c 08 00 45 00  p...m.=.N*...E.
0010  01 2a 91 98 40 00 f5 06 39 6a 36 c0 97 0f c0 a8  .*... 9j6....
0020  2b 53 01 bb f3 db 9d 52 b8 bc 87 7d da 3c 50 18  +$...R ...}<P.
0030  00 77 af 24 00 00 16 03 03 00 ca 04 00 00 c6 00  .w$.... ..
0040  00 2a 30 00 c0 0b 0e e7 ae 6f a2 03 ab 2a 17 09  .*0.... .o...*.
0050  b4 69 86 a8 b2 f6 21 e8 b5 21 ce 89 13 f2 68 ae  .i.....!.....h.
0060  ac 35 0b a0 16 eb f0 6c c6 ec ac e3 0d 3d 80 74  .5.....l.....t
0070  20 80 f1 03 84 f9 57 ba c3 28 2c 82 8f 8f b0 bf  .....W. (.....
0080  03 0e c0 0a e6 16 78 77 b6 0e 99 2b c4 79 ff de  ....XW ...+y..
  
```

kompas | Packets: 13366 · Displayed: 13366 (100.0%) · Load time: 0:2.204 | Profile: Default

Pada gambar diatas, yaitu pada **frame 1406** terdapat **handshake** dari source **54.192.151.15** ke destination dengan IP address **192.168.43.83** (PC).