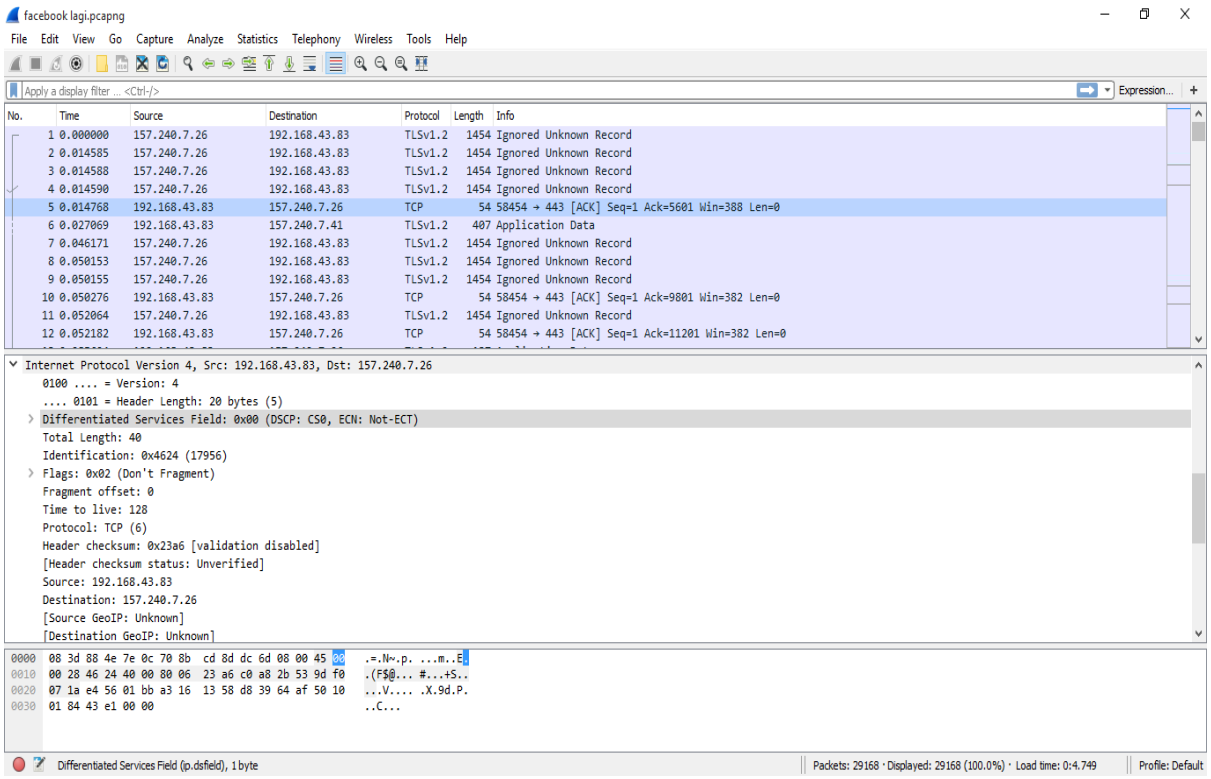
Nama	:	Dini Ayu Lestari
NIM	:	09031181520005
Kelas	:	SI Reguler 4A
Mata Kuliah	:	Komunikasi Data dan Jaringan Komputer
Dosen Pembimbing	:	Deris Stiawan, Ph.D

Analisa Paket Data Menggunakan Wireshark

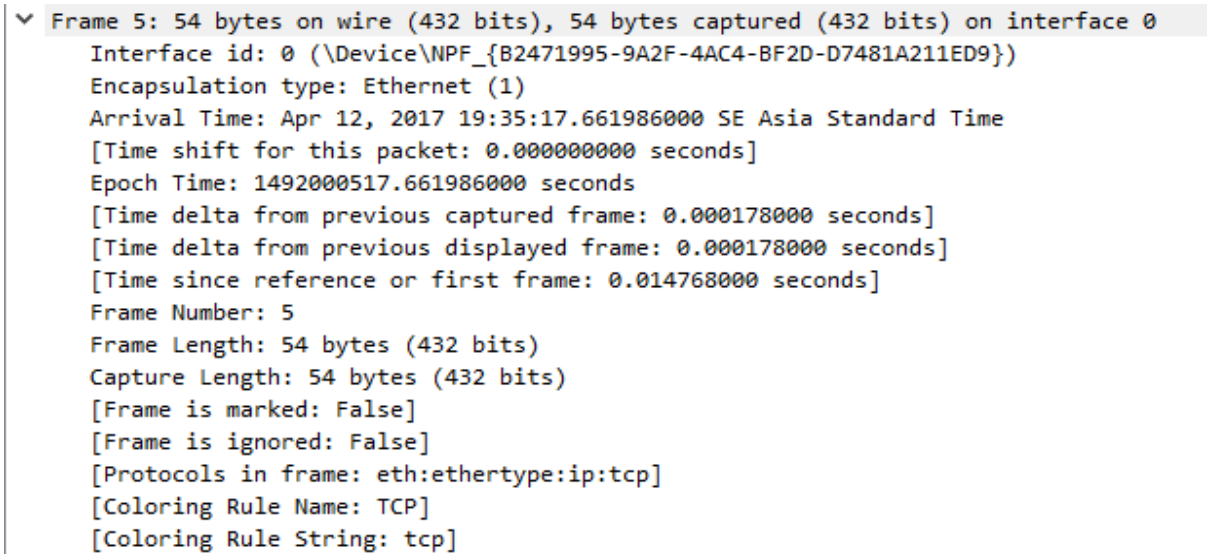
Wireshark merupakan salah satu tools atau aplikasi "Network Analyzer" atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk sniffing (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**

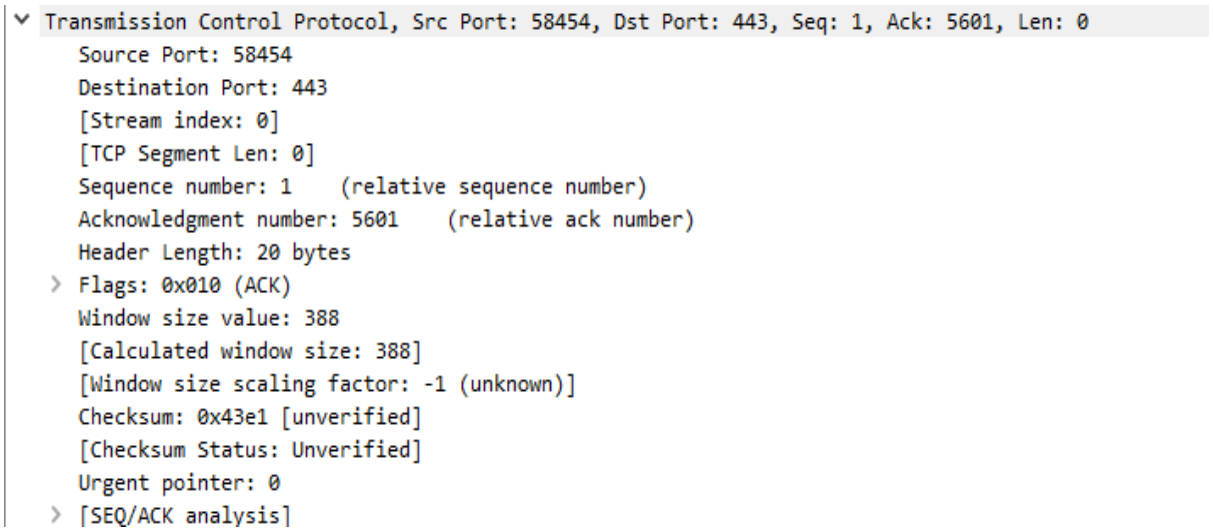


Pada gambar diatas dapat diketahui bahwa **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari website yang dituju** (destination) yaitu Facebook adalah **157.240.7.26** , dikarenakan saya sudah terlebih dahulu membuka facebook dan sedang berinteraksi dihalaman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

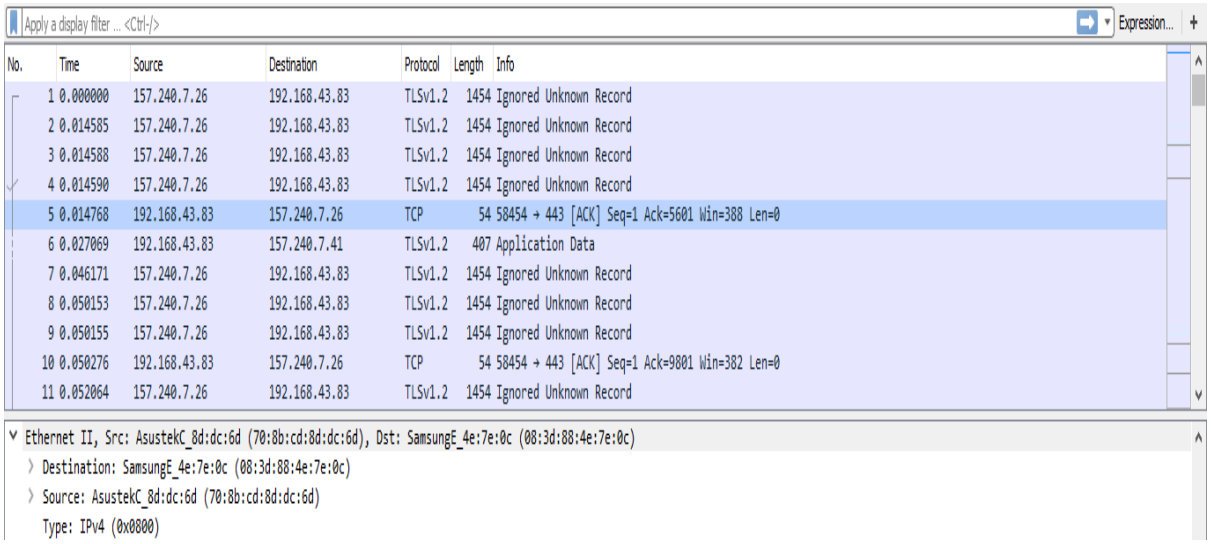
proses ketika paket data dari facebook kembali ke PC saya, dan nomor 5 adalah request dari PC saya ke destination dengan menggunakan protocol TCP. TCP sendiri adalah suatu protokol pengiriman data yang berbasis Internet Protocol (IP) dan bersifat connection oriented.



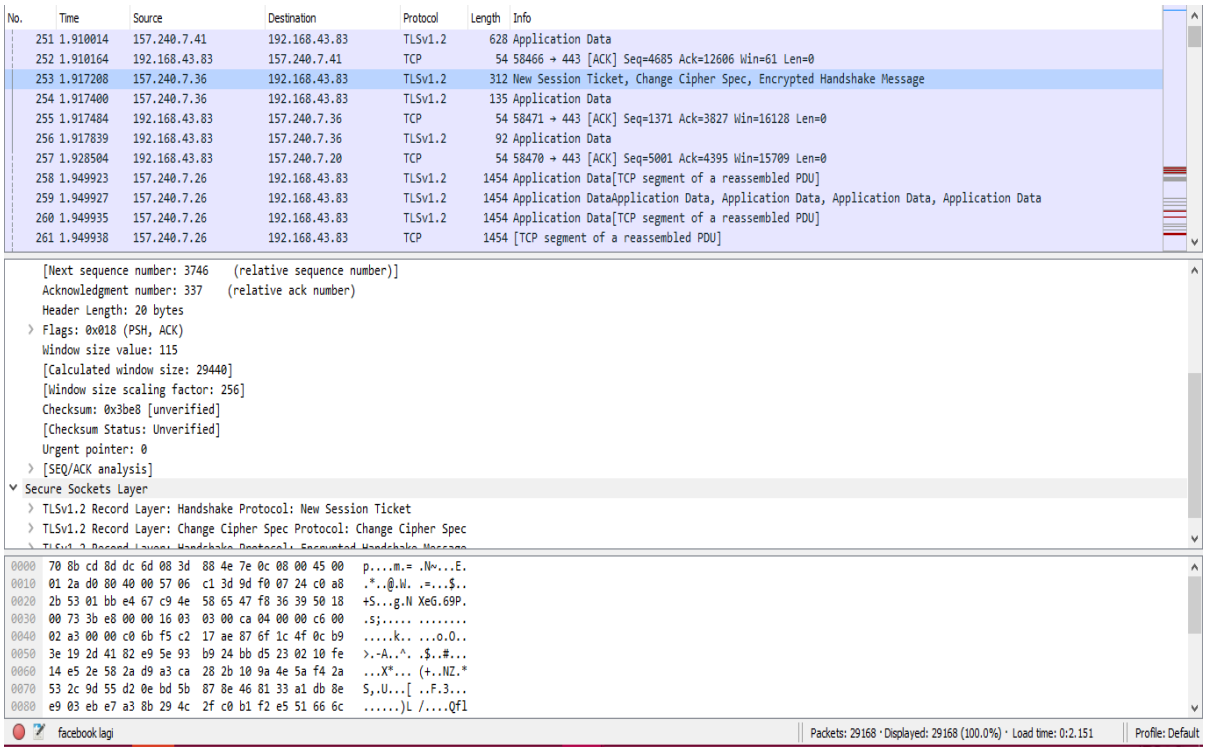
Pada frame diatas dapat dilihat bahwa frame ke 5 ini diakses pada pukul 19:35:17 tanggal 12 April 2017 sesuai dengan standar waktu Asia karena website diakses dari negara yang merupakan bagian dari benua Asia.



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 :



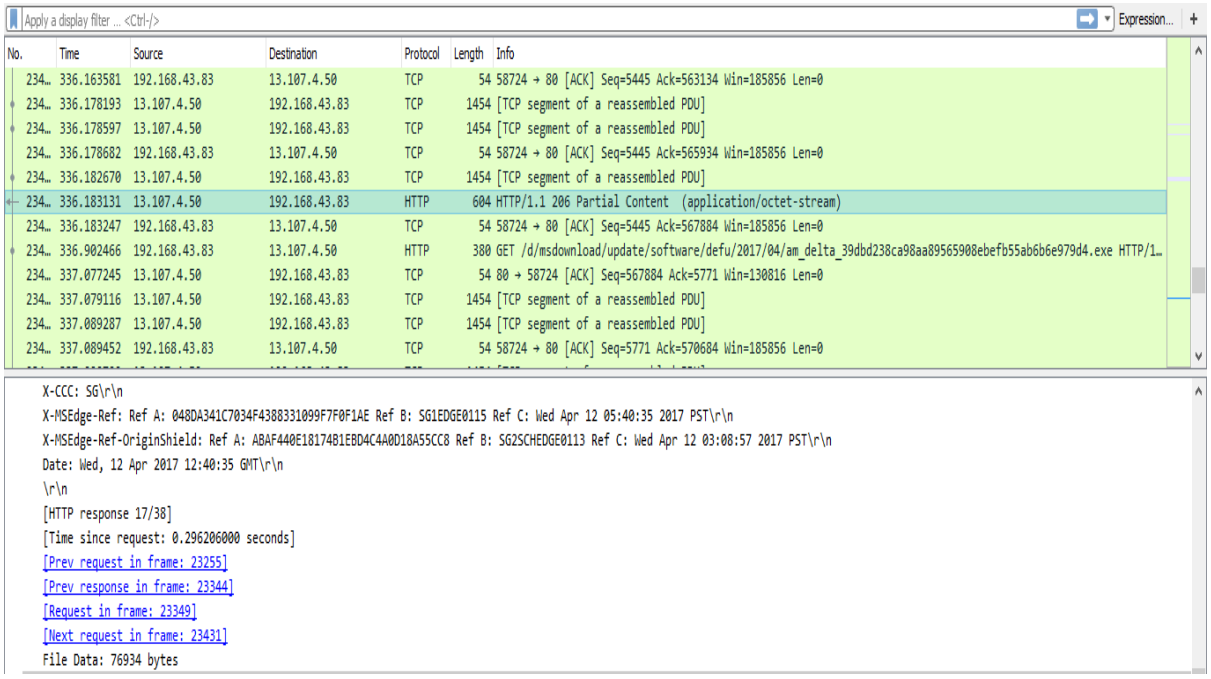
Pada bagian ethernet terlihat bahwa source **(192.168.43.83)** memiliki mac address **70:8b:cd:8d:dc:6d** dan destinationnya **(157.240.7.26)** memiliki mac address **08:3d:88:4e:7e:0c** .



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).

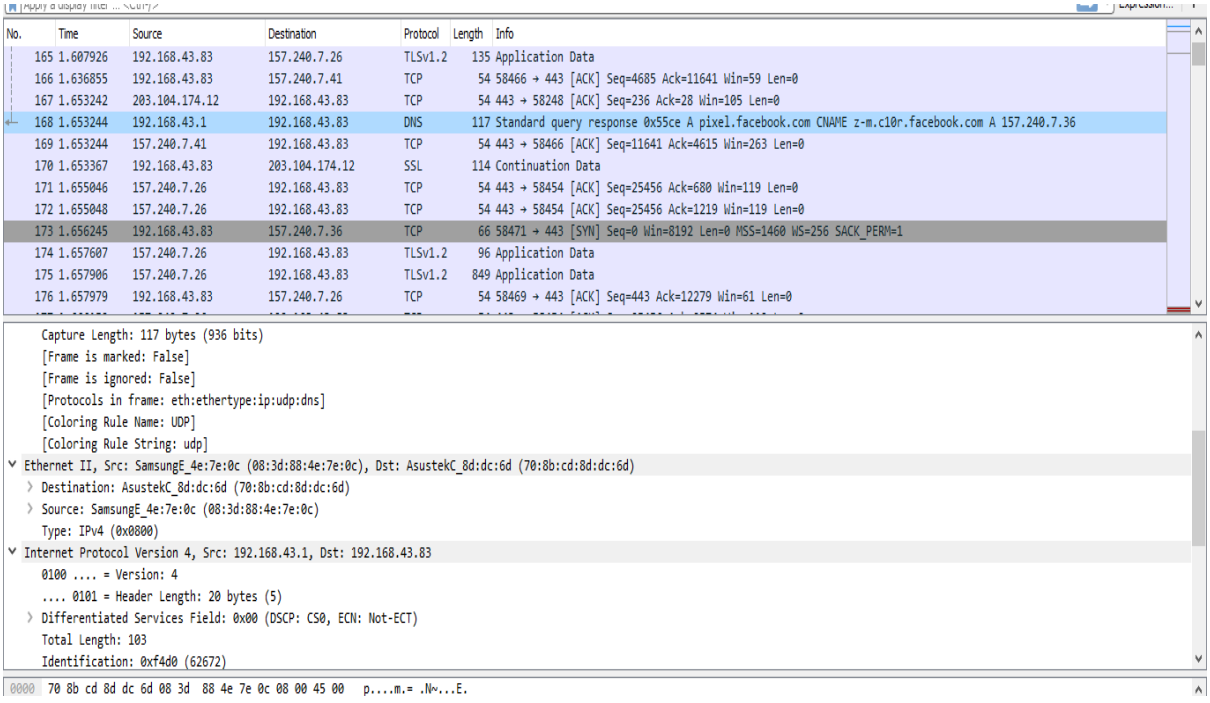
Selain menggunakan protokol TPC, ada juga protokol – protokol lainnya, seperti :

- **HTTP**



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).

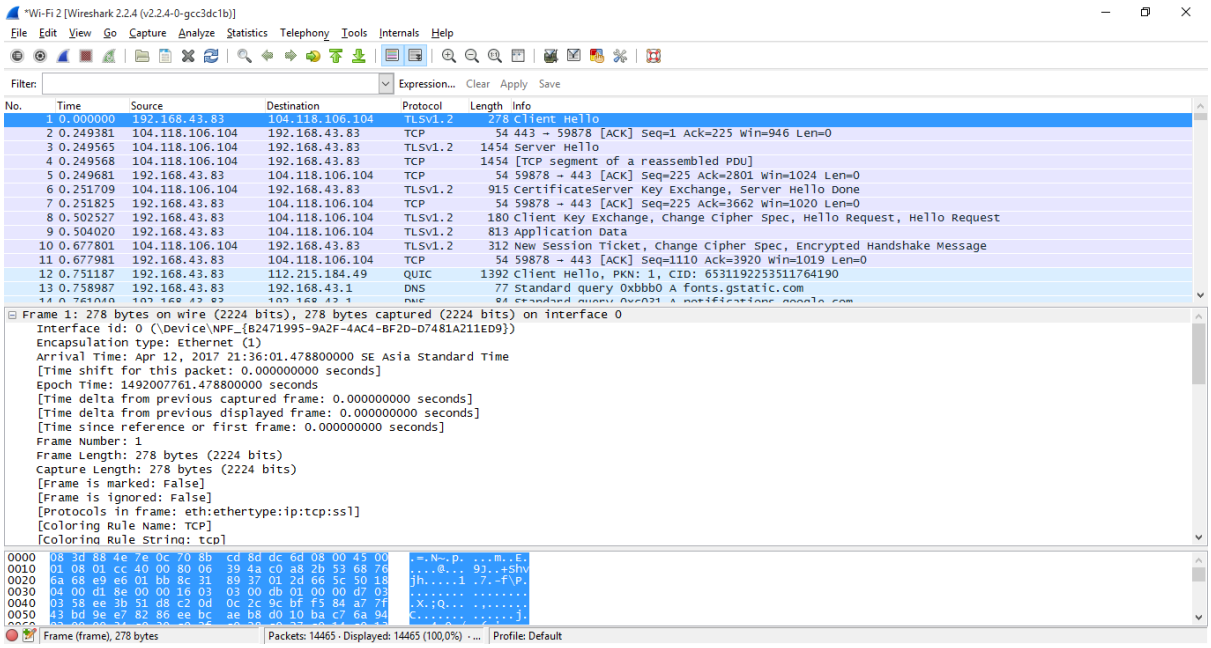
- **DNS**



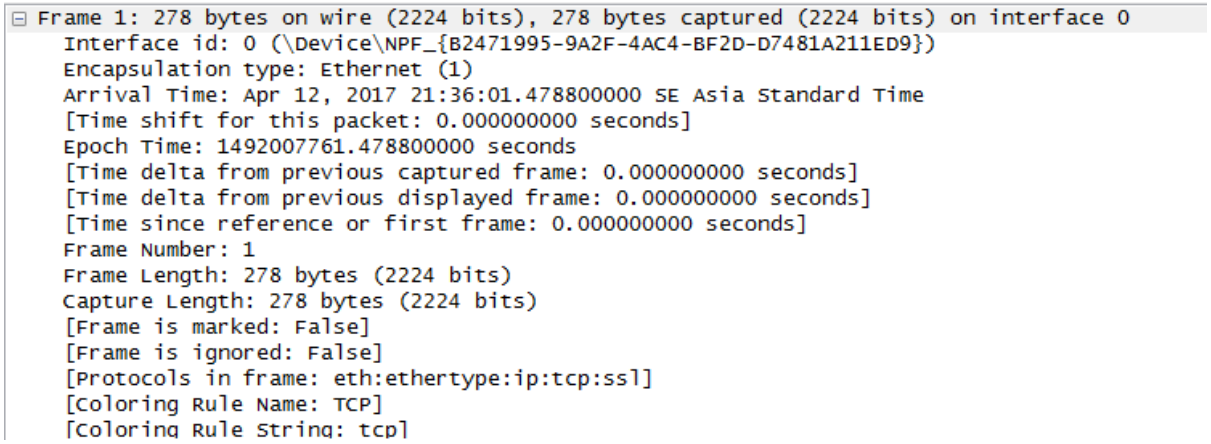
DNS (Domain Name System) adalah protocol yang digunakan untuk mentranslate hostname ke IP address dan sebaliknya. Karena di dunia manusia ini, lebih susah menghafalkan IP dibanding dengan deretan tulisan yang membentuk nama host.

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

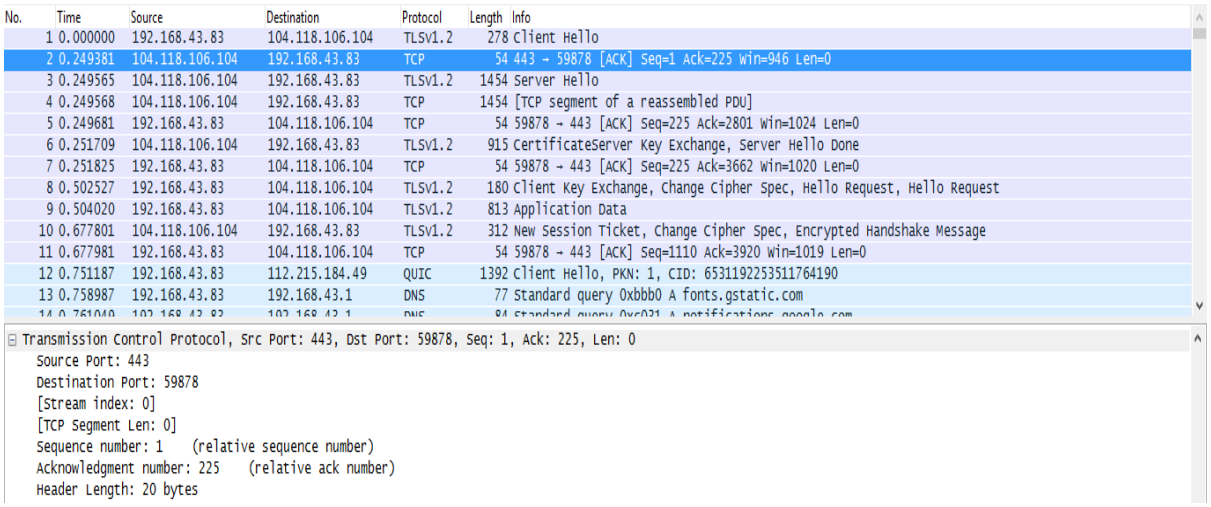
2. **Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website www.twitter.com**



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.



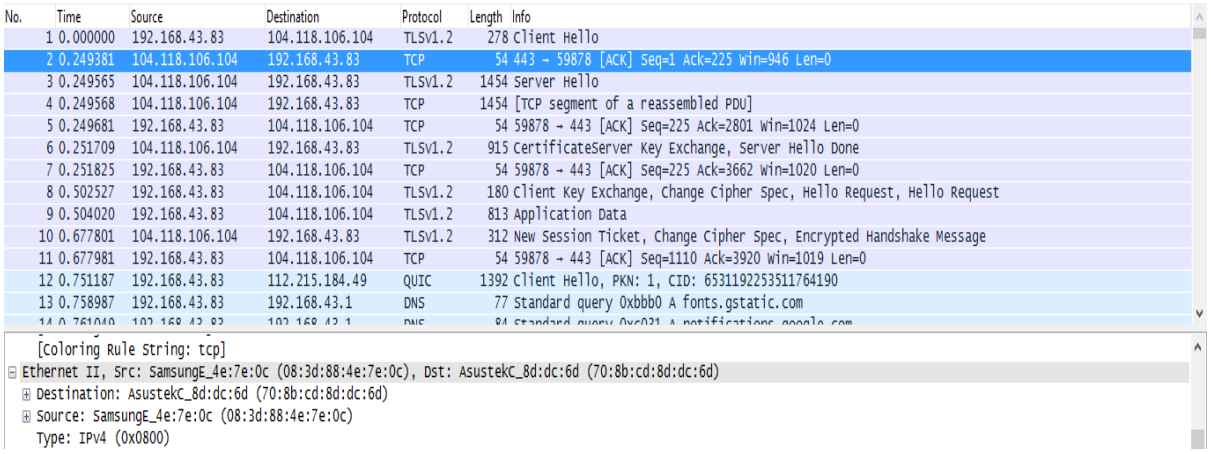
Pada frame diatas dapat dilihat bahwa frame ke 1 ini diakses pada pukul 21:36:01 tanggal 12 April 2017 sesuai dengan standar waktu Asia karena website diakses dari negara yang merupakan bagian dari benua Asia.



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

```
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
```

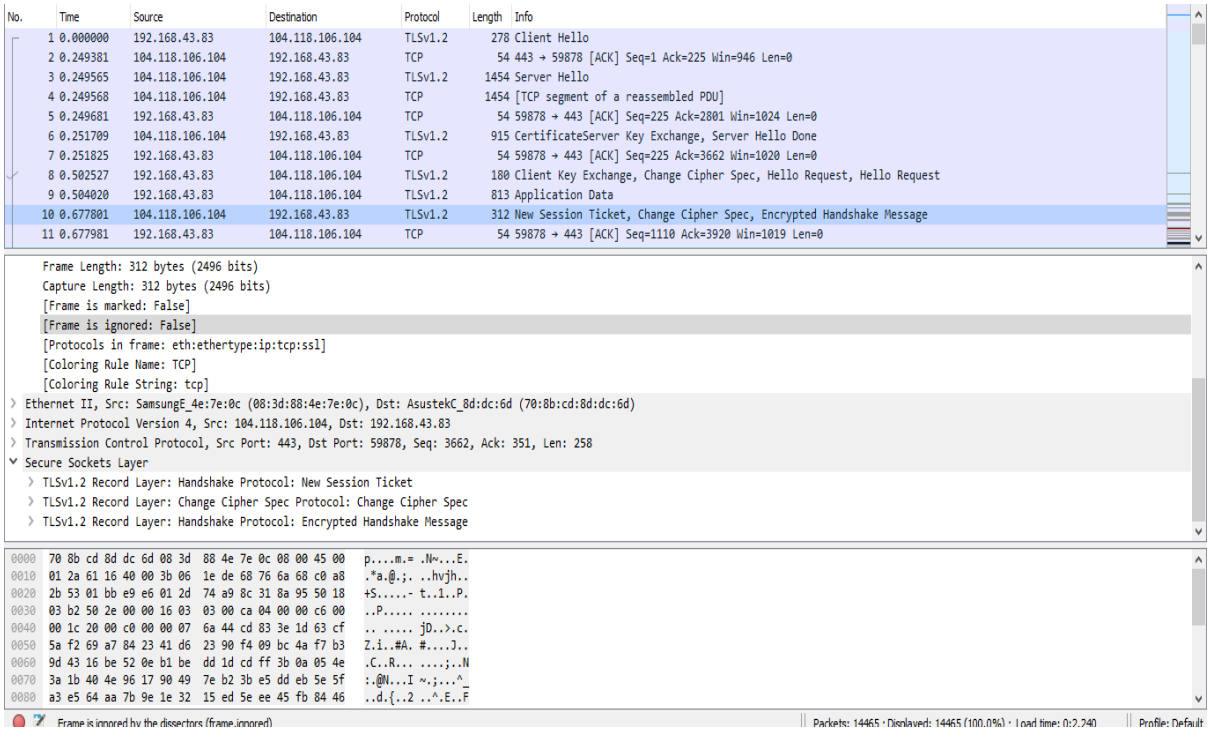
Untuk frame kedua ini, **IP address dari source nya adalah 104.118.106.104** (twitter) dan **IP address destination nya adalah 192.168.43.83** (PC) , frame kedua ini merupakan respon dari frame 1 yang mana frame 1 adalah request ketika PC mengirimkan paket ke destination. Frame kedua ini menggunakan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

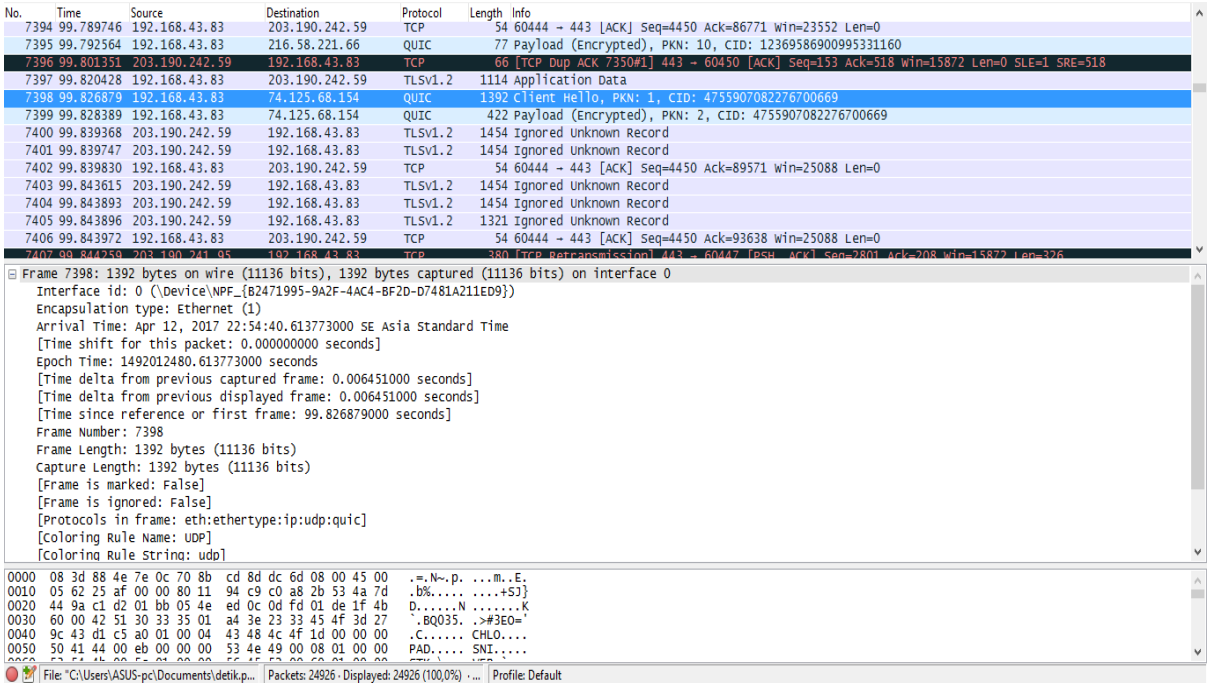
```
    [Coloring Rule String: tcp]
Ethernet II, Src: SamsungE_4e:7e:0c (08:3d:88:4e:7e:0c), Dst: AsustekC_8d:dc:6d (70:8b:cd:8d:dc:6d)
  Destination: AsustekC_8d:dc:6d (70:8b:cd:8d:dc:6d)
  Source: SamsungE_4e:7e:0c (08:3d:88:4e:7e:0c)
    Type: IPv4 (0x0800)
```

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** .

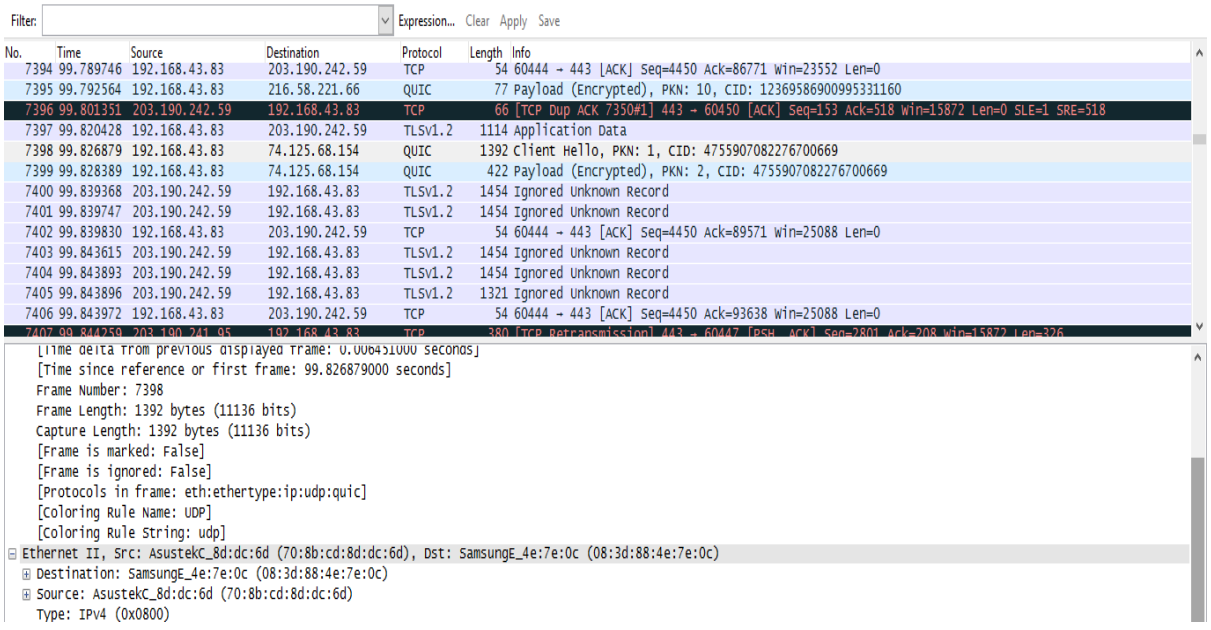


Pada gambar diatas, yaitu pada **frame 10** terdapat **handshake** dari source 104.118.106.104 (IP address dari twitter) ke destination dengan IP address 192.168.43.83 (PC). Pada frame ke 9, 192.168.43.83 melakukan request kedestinationnya yaitu 104.118.106.104 kemudian ada respon dari 104.118.106.104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

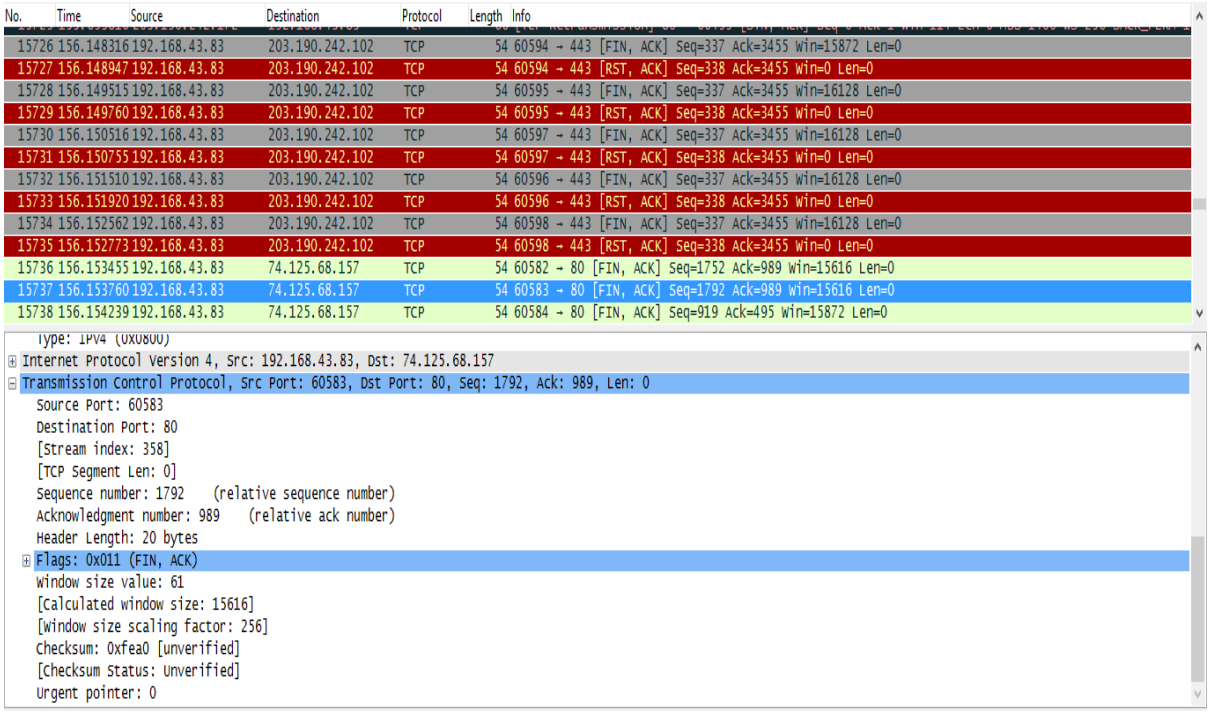
3. **Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website www.detik.com**



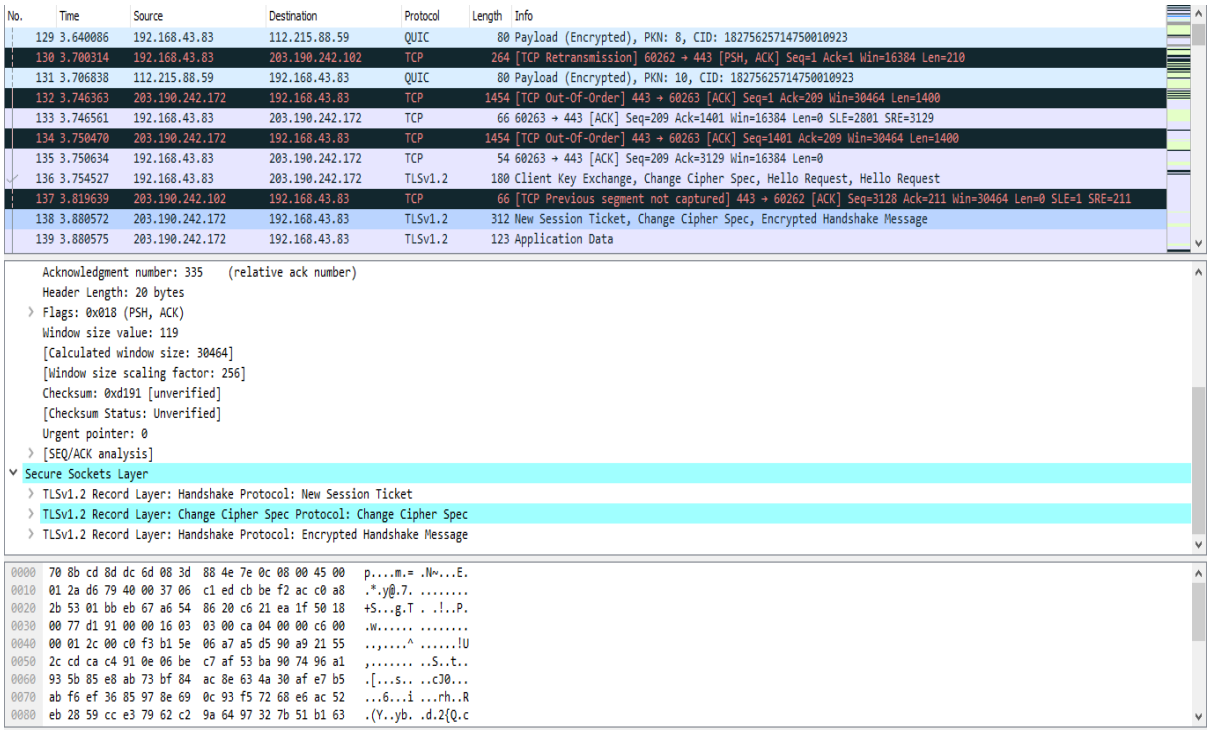
Pada gambar diatas dapat diketahui bahwa pada frame 7398 **IP address dari komputer (source)** yang digunakan adalah **192.168.43.83** dan **IP address dari halaman yang dituju (destination)** yaitu detik.com adalah **74.125.68.154** . Selain itu dapat kita ketahui pada bagian frame bahwa frame 7398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



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** .

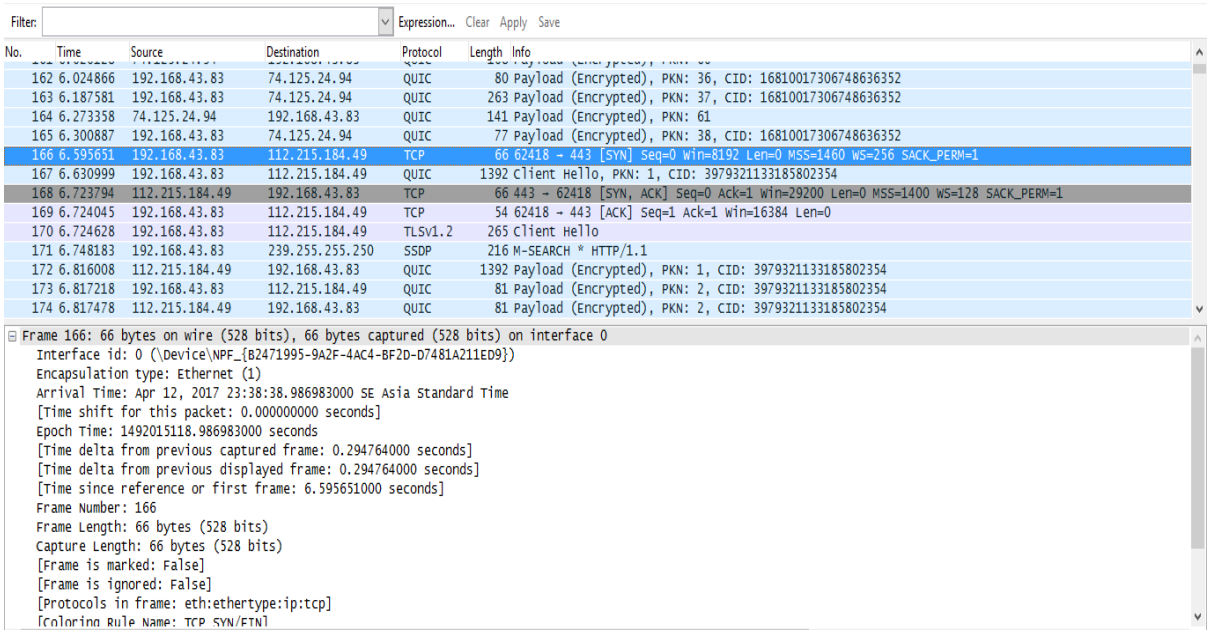


Untuk frame ke 15736 request dari source ke destination (detik.com) menggunakan protokol TPC dengan **Source Port nya 192** dan **Destination Port nya 80.**

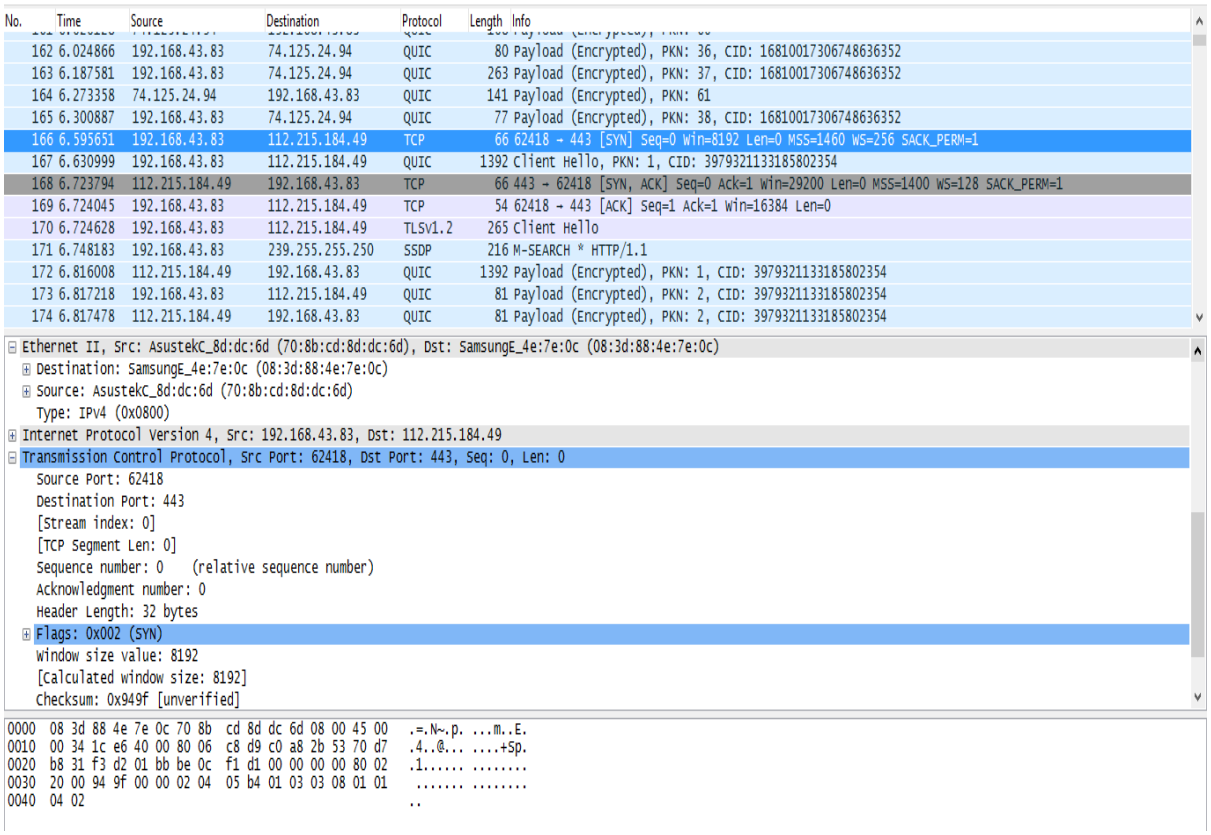


Pada gambar diatas, yaitu pada **frame 138** terdapat **handshake** dari source 203.190.242.172 ke destination dengan IP address 192.168.43.83 (PC).

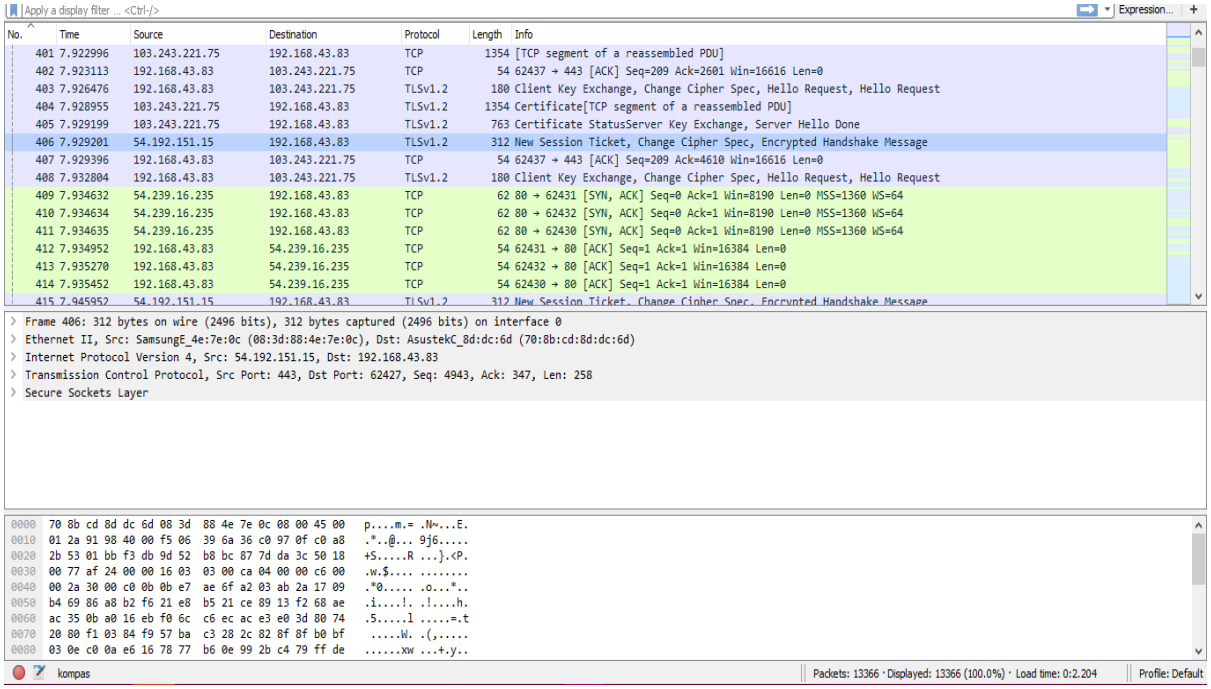
4. **Menggunakan Wireshark untuk mengcapture packet protocol saat membuka website www.kompas.com**



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 .



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.**



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).