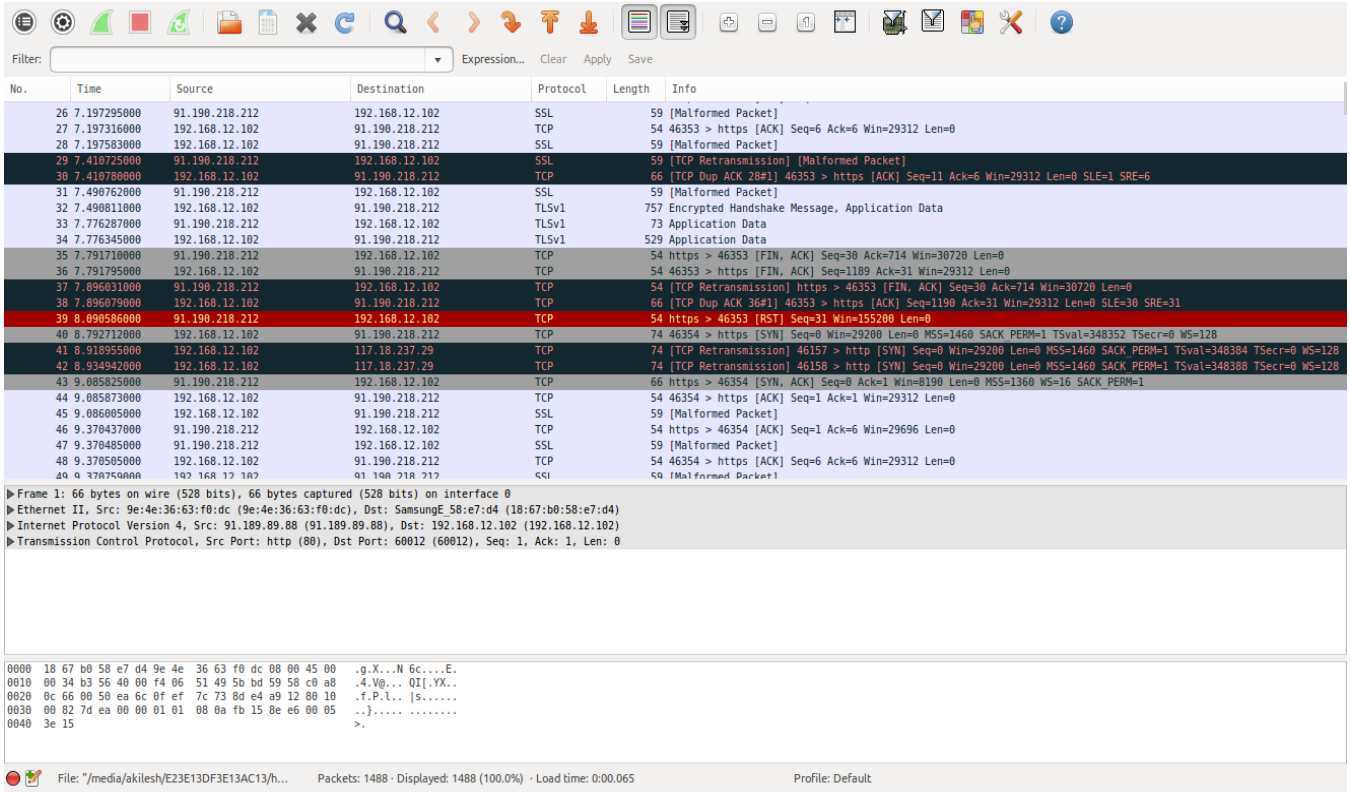
Networks assignment 1

Aim: To find application and network layer protocols for various internet services.

Part 1: For atleast 10 popular websites

1) **www.google.com**



No.	Time	Source	Destination	Protocol	Length	Info
26	7.197295000	91.190.218.212	192.168.12.102	SSL	59	[Malformed Packet]
27	7.197316000	192.168.12.102	91.190.218.212	TCP	54	46353 > https [ACK] Seq=6 Ack=6 Win=29312 Len=0
28	7.197583000	192.168.12.102	91.190.218.212	SSL	59	[Malformed Packet]
29	7.410725000	91.190.218.212	192.168.12.102	SSL	59	[TCP Retransmission] [Malformed Packet]
30	7.410780000	192.168.12.102	91.190.218.212	TCP	66	[TCP Dup ACK 28#1] 46353 > https [ACK] Seq=11 Ack=6 Win=29312 Len=0 SLE=1 SRE=6
31	7.490762000	91.190.218.212	192.168.12.102	SSL	59	[Malformed Packet]
32	7.490811000	192.168.12.102	91.190.218.212	TLSv1	757	Encrypted Handshake Message, Application Data
33	7.776287000	91.190.218.212	192.168.12.102	TLSv1	73	Application Data
34	7.776345000	192.168.12.102	91.190.218.212	TLSv1	529	Application Data
35	7.791710000	91.190.218.212	192.168.12.102	TCP	54	https > 46353 [FIN, ACK] Seq=30 Ack=714 Win=30720 Len=0
36	7.791795000	192.168.12.102	91.190.218.212	TCP	54	46353 > https [FIN, ACK] Seq=1189 Ack=31 Win=29312 Len=0
37	7.896031000	91.190.218.212	192.168.12.102	TCP	54	[TCP Retransmission] https > 46353 [FIN, ACK] Seq=30 Ack=714 Win=30720 Len=0
38	7.896079000	192.168.12.102	91.190.218.212	TCP	66	[TCP Dup ACK 36#1] 46353 > https [ACK] Seq=1190 Ack=31 Win=29312 Len=0 SLE=30 SRE=31
39	8.090586000	91.190.218.212	192.168.12.102	TCP	54	https > 46353 [RST] Seq=31 Win=155200 Len=0
40	8.792712000	192.168.12.102	91.190.218.212	TCP	74	46354 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=348352 TSecr=0 WS=128
41	8.918955000	192.168.12.102	117.18.237.29	TCP	74	[TCP Retransmission] 46157 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=348384 TSecr=0 WS=128
42	8.934942000	192.168.12.102	117.18.237.29	TCP	74	[TCP Retransmission] 46158 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=348388 TSecr=0 WS=128
43	9.085825000	91.190.218.212	192.168.12.102	TCP	66	https > 46354 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360 WS=16 SACK_PERM=1
44	9.085873000	192.168.12.102	91.190.218.212	TCP	54	46354 > https [ACK] Seq=1 Ack=1 Win=29312 Len=0
45	9.086005000	192.168.12.102	91.190.218.212	SSL	59	[Malformed Packet]
46	9.370437000	91.190.218.212	192.168.12.102	TCP	54	https > 46354 [ACK] Seq=1 Ack=6 Win=29696 Len=0
47	9.370485000	91.190.218.212	192.168.12.102	SSL	59	[Malformed Packet]
48	9.370505000	192.168.12.102	91.190.218.212	TCP	54	46354 > https [ACK] Seq=6 Ack=6 Win=29312 Len=0
49	9.370759000	192.168.12.102	91.190.218.212	SSL	59	[Malformed Packet]

```
▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: 9e:4e:36:63:f0:dc (9e:4e:36:63:f0:dc), Dst: SamsungE_58:e7:d4 (18:67:b0:58:e7:d4)
▶ Internet Protocol Version 4, Src: 91.189.89.88 (91.189.89.88), Dst: 192.168.12.102 (192.168.12.102)
▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 60012 (60012), Seq: 1, Ack: 1, Len: 0
```

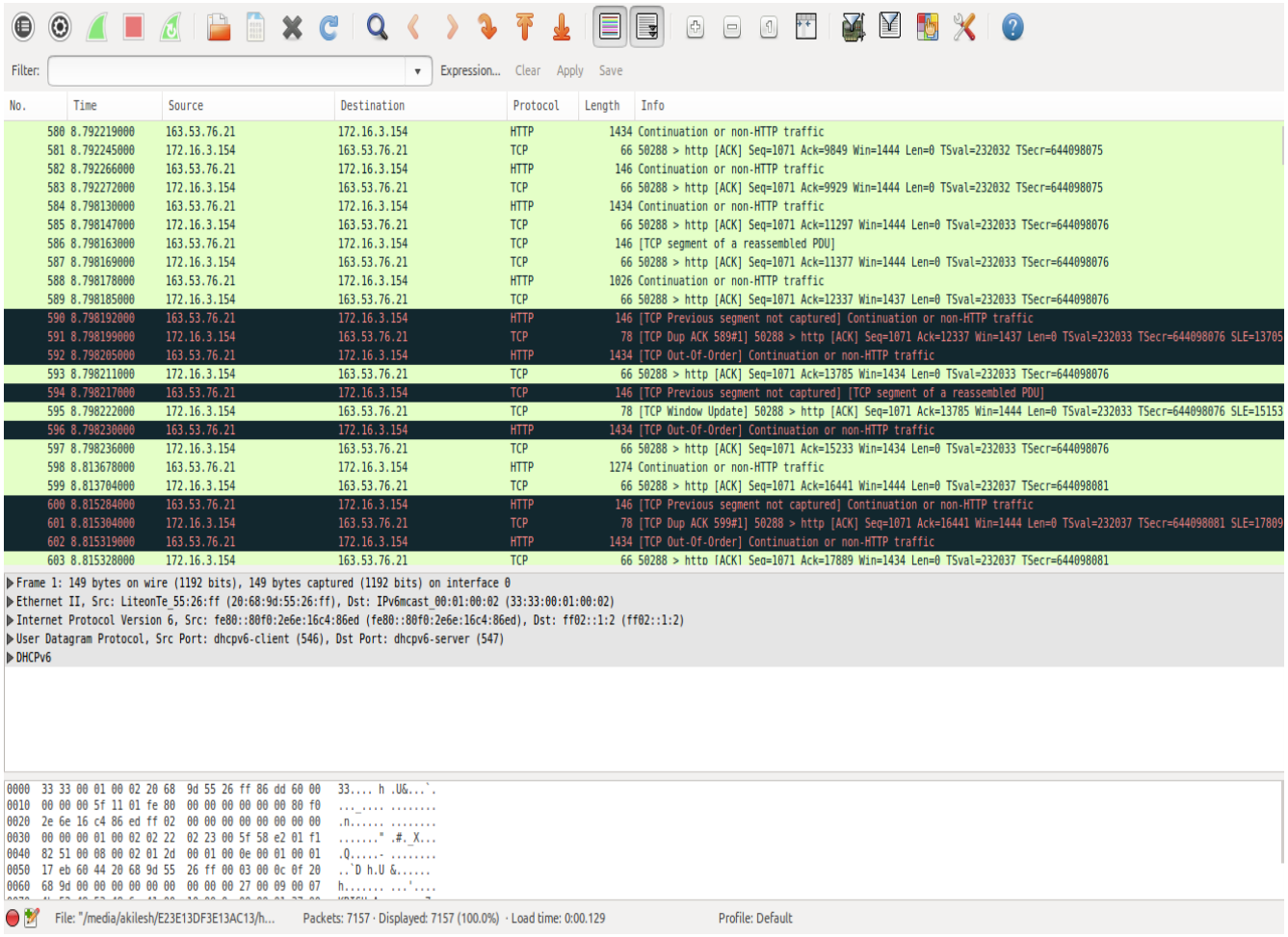
```
0000  18 67 b0 58 e7 d4 9e 4e  36 63 f0 dc 08 00 45 00   .g.X...N 6c....E.
0010  00 34 b3 56 40 00 f4 06  51 49 5b bd 59 58 c0 a8   .4.V@... QI[.YX..
0020  0c 66 00 50 ea 6c 0f ef  7c 73 8d e4 a9 12 80 10   .f.P.l.. |s......
0030  00 82 7d ea 00 00 01 01  08 0a fb 15 8e e6 00 05   ..}..... ........
0040  3e 15                                              >.
```

File: "/media/akilesh/E23E13DF3E13AC13/h... Packets: 1488 · Displayed: 1488 (100.0%) · Load time: 0:00.065 Profile: Default

Application layer: HTTPS (Secure), TLSv1.2, TLSv1, SSL

Transport layer: TCP

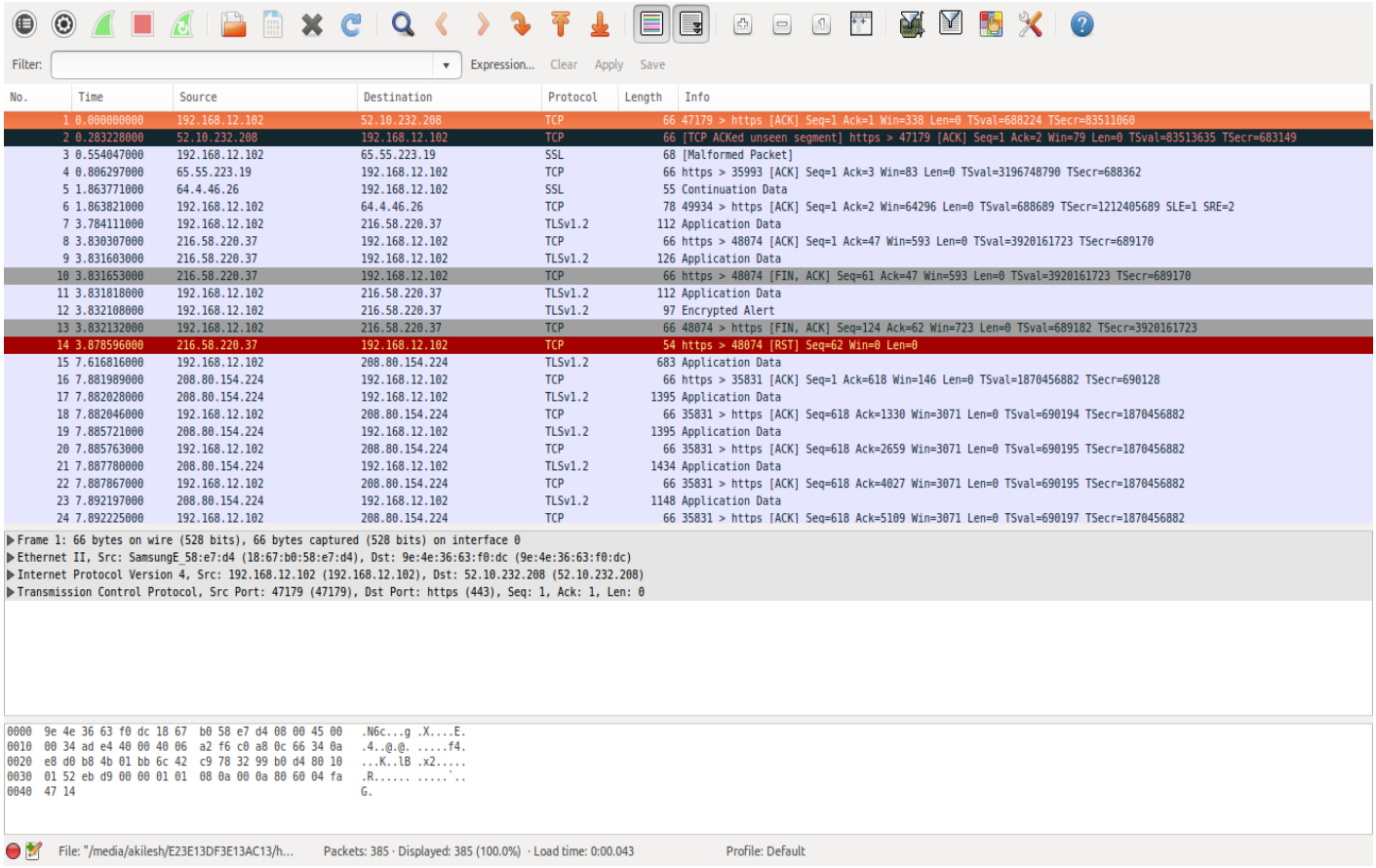
2) www.flipkart.com



Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

3) en.wikipedia.org



Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.12.102	52.10.232.208	TCP	66	47179 > https [ACK] Seq=1 Ack=1 Win=338 Len=0 TSval=688224 TSecr=83511060
2	0.283228000	52.10.232.208	192.168.12.102	TCP	66	[TCP ACKed unseen segment] https > 47179 [ACK] Seq=1 Ack=2 Win=79 Len=0 TSval=83513635 TSecr=683149
3	0.554047000	192.168.12.102	65.55.223.19	SSL	68	[Malformed Packet]
4	0.806297000	65.55.223.19	192.168.12.102	TCP	66	https > 35993 [ACK] Seq=1 Ack=3 Win=83 Len=0 TSval=3196748790 TSecr=688362
5	1.863771000	64.4.46.26	192.168.12.102	SSL	55	Continuation Data
6	1.863821000	192.168.12.102	64.4.46.26	TCP	78	49934 > https [ACK] Seq=1 Ack=2 Win=64296 Len=0 TSval=688689 TSecr=1212405689 SLE=1 SRE=2
7	3.784111000	192.168.12.102	216.58.220.37	TLSv1.2	112	Application Data
8	3.830307000	216.58.220.37	192.168.12.102	TCP	66	https > 48074 [ACK] Seq=1 Ack=47 Win=593 Len=0 TSval=3920161723 TSecr=689170
9	3.831603000	216.58.220.37	192.168.12.102	TLSv1.2	126	Application Data
10	3.831653000	216.58.220.37	192.168.12.102	TCP	66	https > 48074 [FIN, ACK] Seq=61 Ack=47 Win=593 Len=0 TSval=3920161723 TSecr=689170
11	3.831818000	192.168.12.102	216.58.220.37	TLSv1.2	112	Application Data
12	3.832108000	192.168.12.102	216.58.220.37	TLSv1.2	97	Encrypted Alert
13	3.832132000	192.168.12.102	216.58.220.37	TCP	66	48074 > https [FIN, ACK] Seq=124 Ack=62 Win=723 Len=0 TSval=689182 TSecr=3920161723
14	3.878596000	216.58.220.37	192.168.12.102	TCP	54	https > 48074 [RST] Seq=62 Win=0 Len=0
15	7.616816000	192.168.12.102	208.80.154.224	TLSv1.2	683	Application Data
16	7.881989000	208.80.154.224	192.168.12.102	TCP	66	https > 35831 [ACK] Seq=1 Ack=618 Win=146 Len=0 TSval=1870456882 TSecr=690128
17	7.882028000	208.80.154.224	192.168.12.102	TLSv1.2	1395	Application Data
18	7.882046000	192.168.12.102	208.80.154.224	TCP	66	35831 > https [ACK] Seq=618 Ack=1330 Win=3071 Len=0 TSval=690194 TSecr=1870456882
19	7.885721000	208.80.154.224	192.168.12.102	TLSv1.2	1395	Application Data
20	7.885763000	192.168.12.102	208.80.154.224	TCP	66	35831 > https [ACK] Seq=618 Ack=2659 Win=3071 Len=0 TSval=690195 TSecr=1870456882
21	7.887780000	208.80.154.224	192.168.12.102	TLSv1.2	1434	Application Data
22	7.887867000	192.168.12.102	208.80.154.224	TCP	66	35831 > https [ACK] Seq=618 Ack=4027 Win=3071 Len=0 TSval=690195 TSecr=1870456882
23	7.892197000	208.80.154.224	192.168.12.102	TLSv1.2	1148	Application Data
24	7.892225000	192.168.12.102	208.80.154.224	TCP	66	35831 > https [ACK] Seq=618 Ack=5109 Win=3071 Len=0 TSval=690197 TSecr=1870456882

```
▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: SamsungE_58:e7:d4 (18:67:b0:58:e7:d4), Dst: 9e:4e:36:63:f0:dc (9e:4e:36:63:f0:dc)
▶ Internet Protocol Version 4, Src: 192.168.12.102 (192.168.12.102), Dst: 52.10.232.208 (52.10.232.208)
▶ Transmission Control Protocol, Src Port: 47179 (47179), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0
```

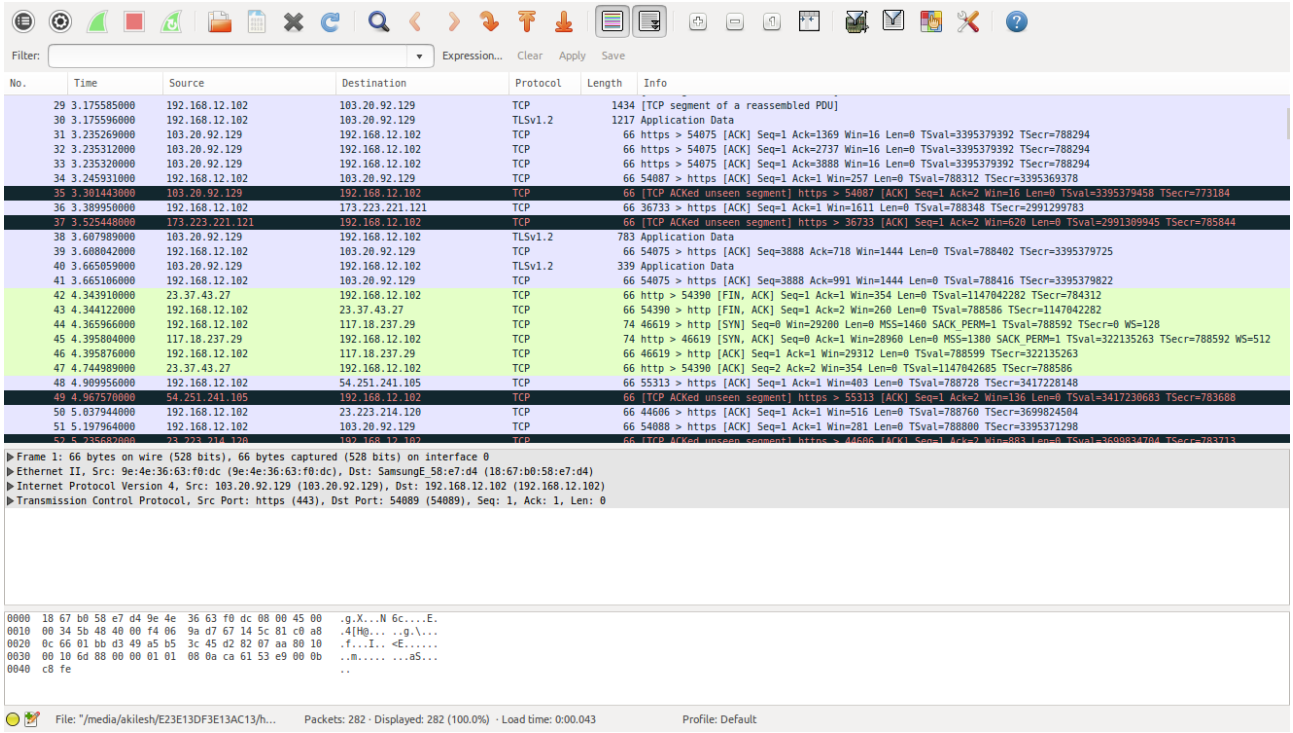
```
0000  9e 4e 36 63 f0 dc 18 67  b0 58 e7 d4 08 00 45 00   .N6c...g .X....E.
0010  00 34 ad e4 40 00 40 06  a2 f6 c0 a8 0c 66 34 0a   .4..@.@. .....f4.
0020  e8 d0 b8 4b 01 bb 6c 42  c9 78 32 99 b0 d4 80 10   ...K..lB .x2.....
0030  01 52 eb d9 00 00 01 01  08 0a 00 0a 80 60 04 fa   .R...... .....`..
0040  47 14                                              G.
```

File: "/media/akilesh/E23E13DF3E13AC13/h... Packets: 385 · Displayed: 385 (100.0%) · Load time: 0:00.043 Profile: Default

Application layer: HTTPS (Secure), TLSv1.2, SSL

Transport layer: TCP

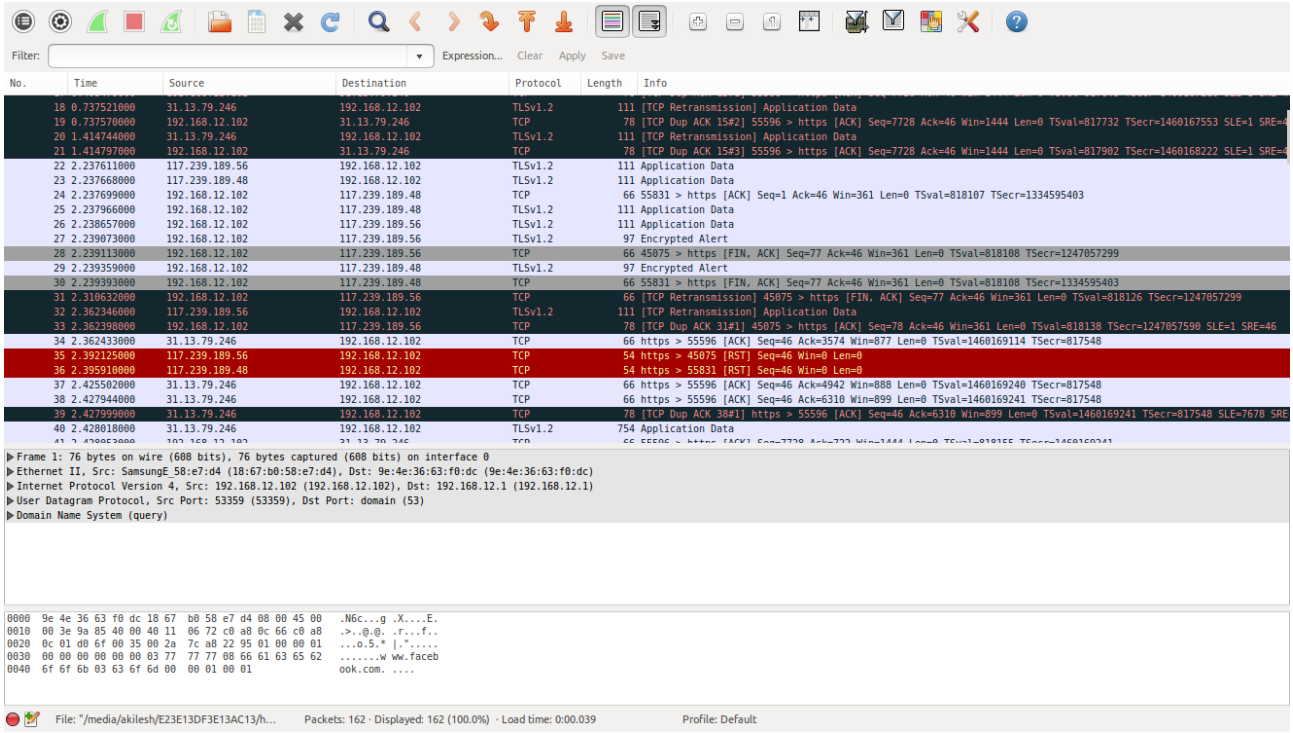
4) www.linkedin.com



Application layer: HTTPS(Secure), TLSv1.2, SSL

Transport layer: TCP

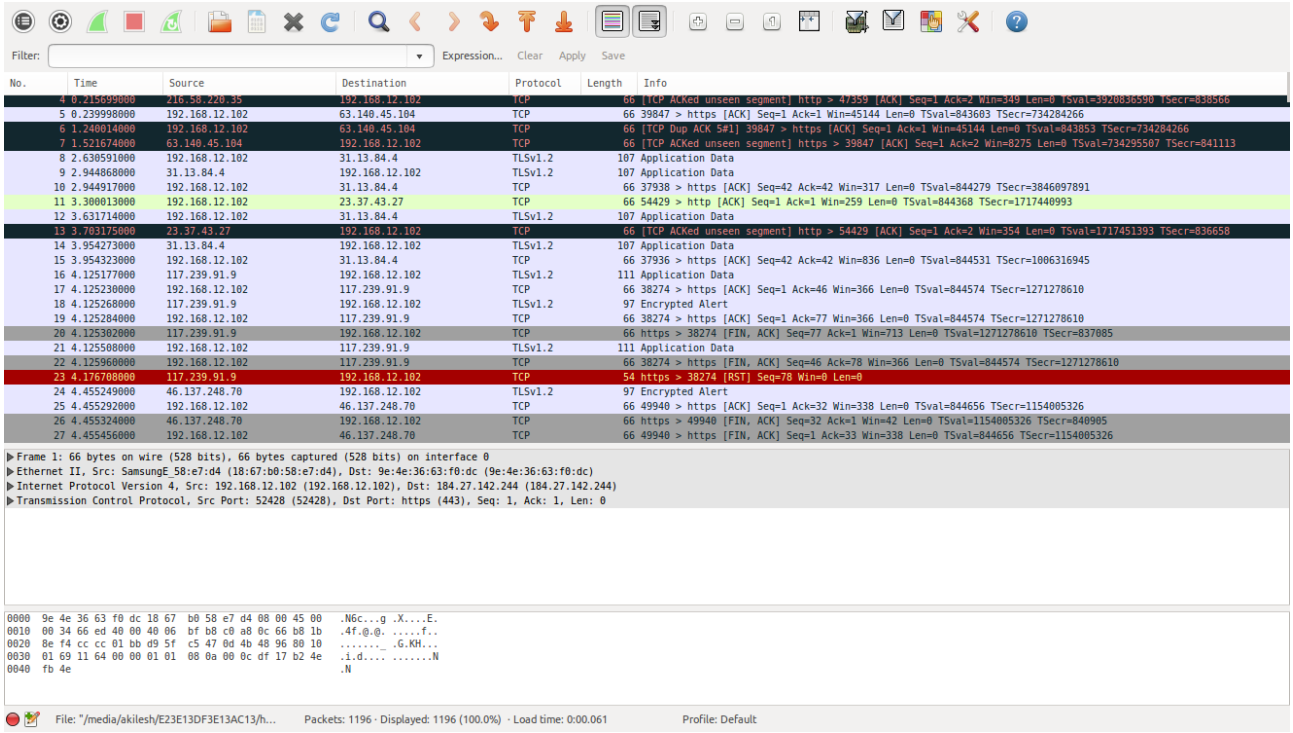
5) www.facebook.com



Application layer: HTTPS(Secure), TLSv1.2, SSL

Transport layer: TCP

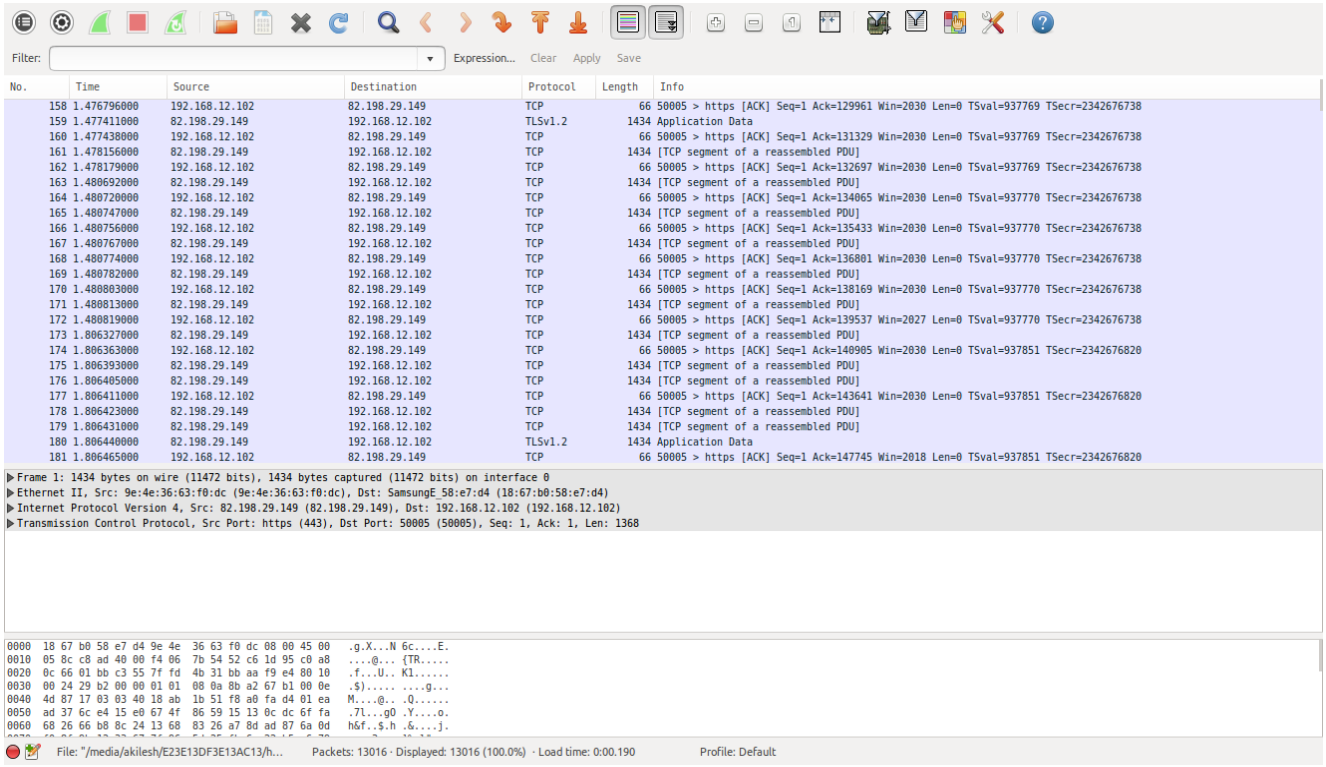
6) www.paypal.com



Application layer: HTTPS (Secure), TLSv1.2, SSL

Transport layer: TCP

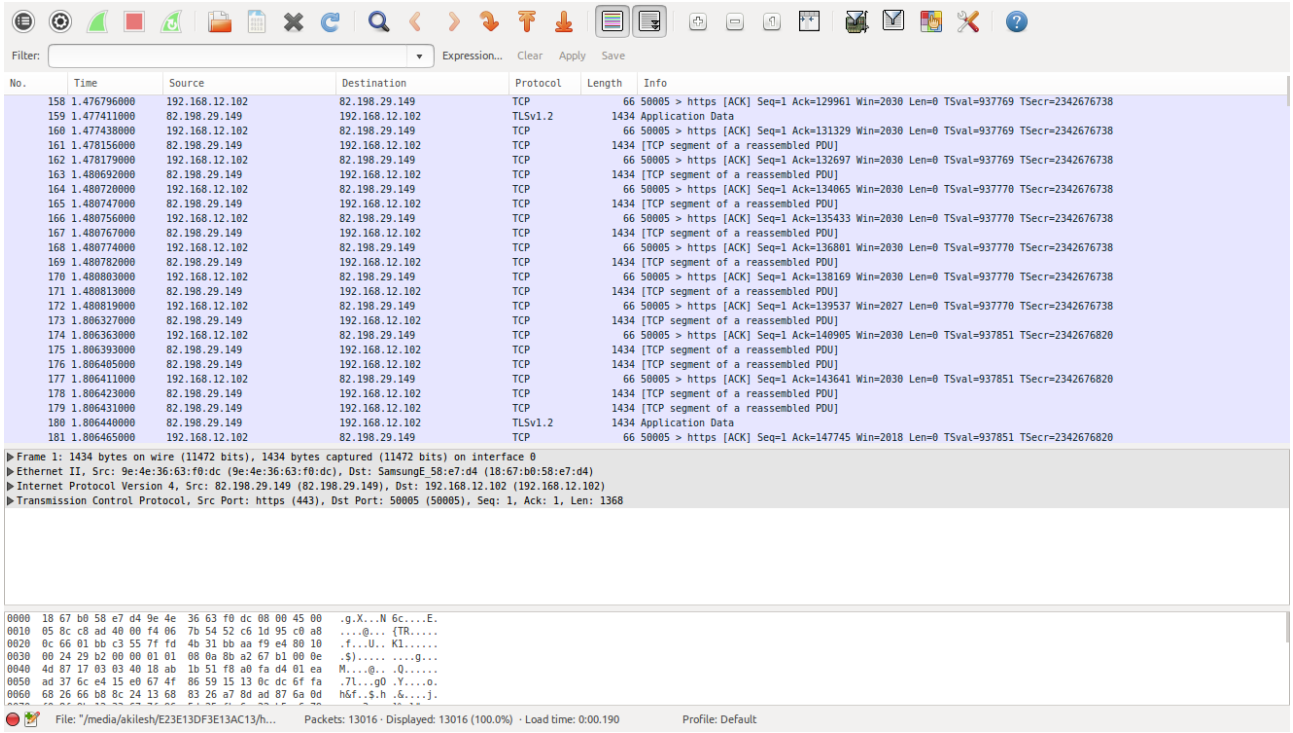
7) filestream.me



Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

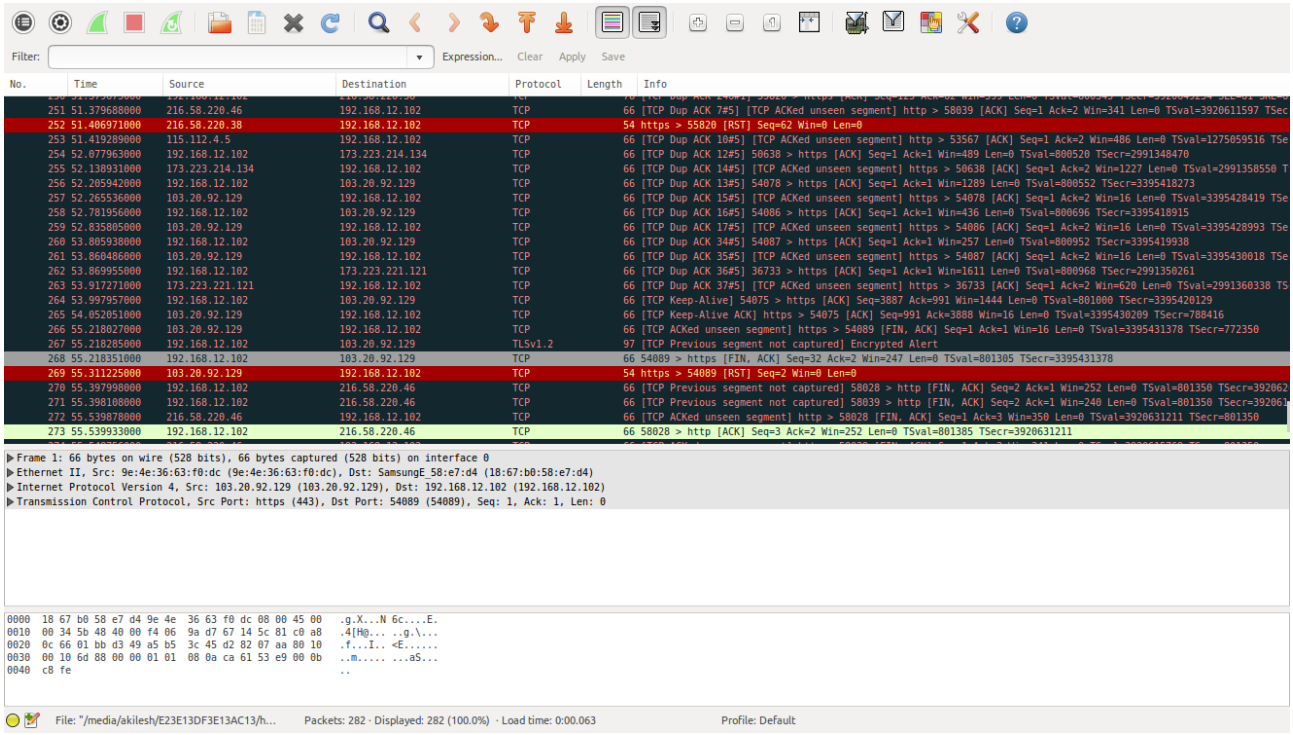
8) github.com



Application layer: HTTPS (secure). TLSv1.2, SSL

Transport layer: TCP

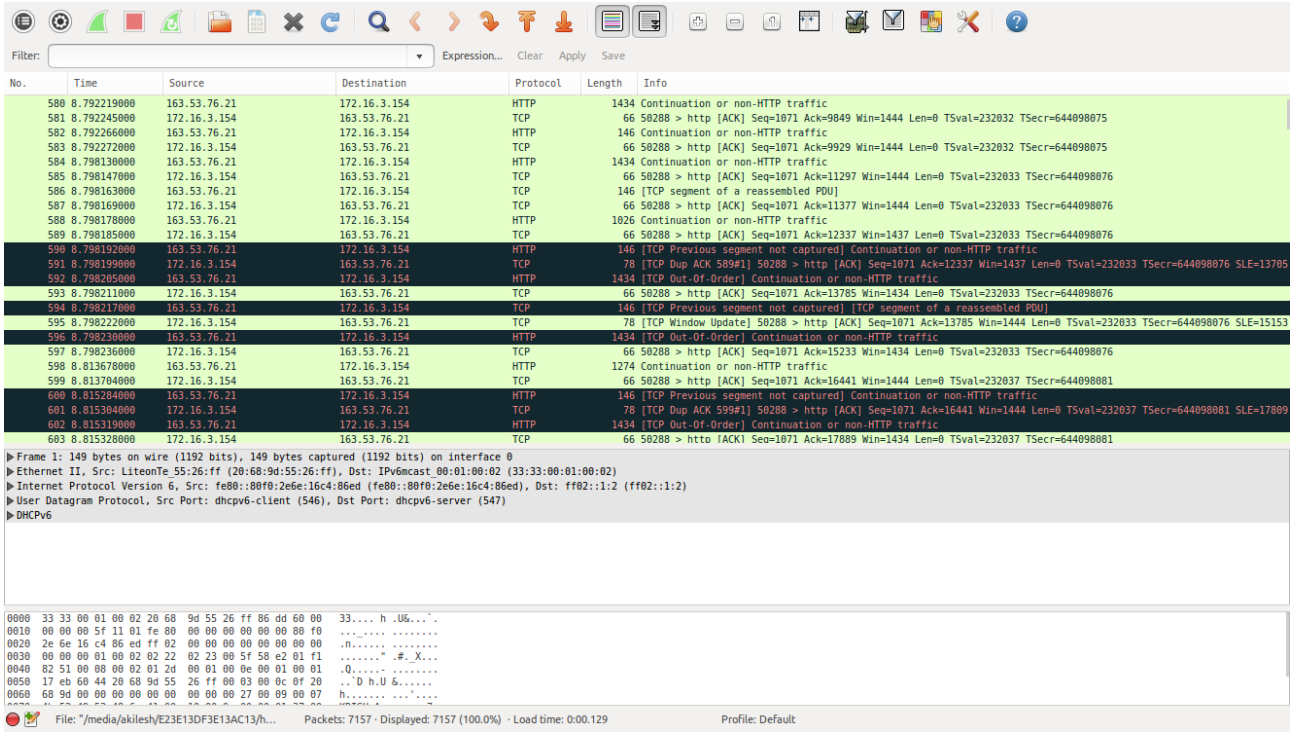
9) dropbox.com



Application layer: TLSv1.2, HTTPS (Secure), SSL

Transport layer: TCP

10) www.quora.com



Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

Explanation:

Every site is using TCP as their transport layer because TCP is the common transport layer protocol used by all these services. It enables two hosts to establish a connection and exchange some streams of data. Delivery of data is guaranteed by TCP and it also ensures that the order in which they are delivered is the same as that in which they are sent.

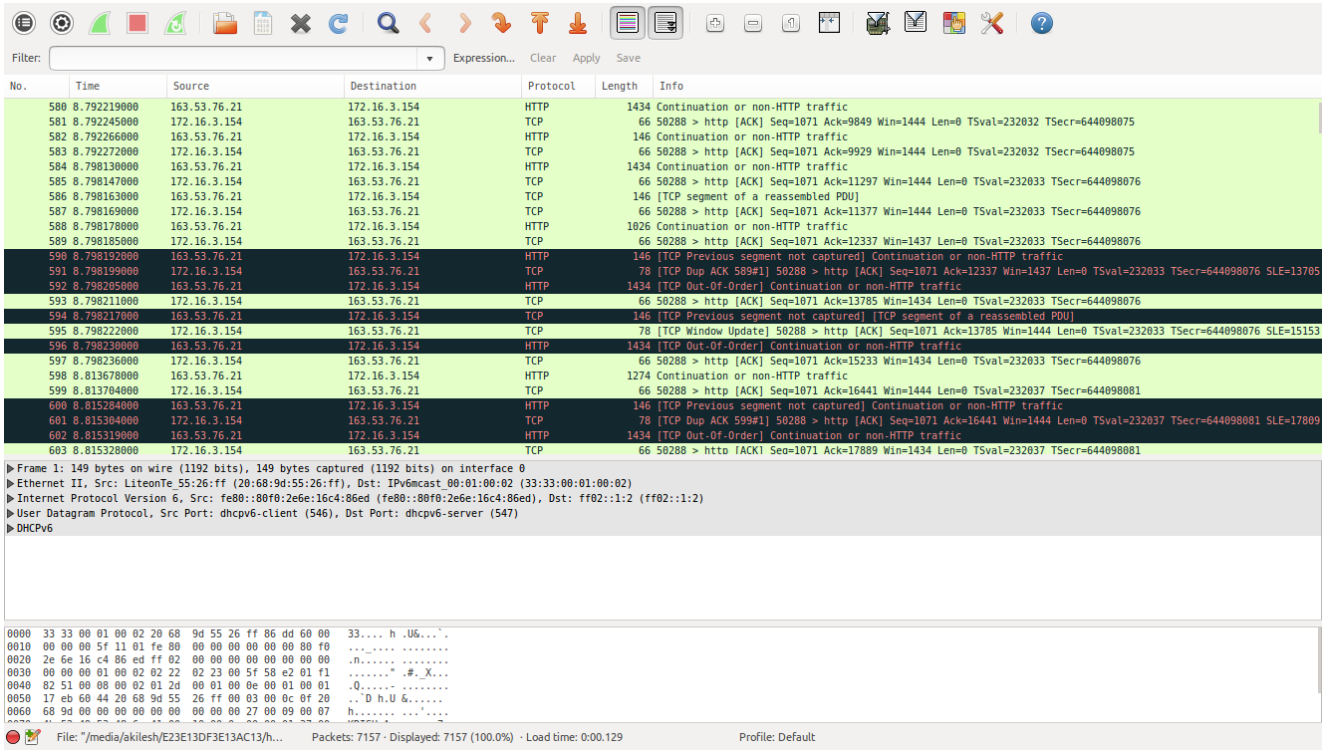
Whenever there is a secure connection HTTPS is in the application layer, HTTP otherwise.

TCP utilizes different flags, or 1-bit boolean fields, in its header to control the state of a connection. The three most important are: SYN - (Synchronize) Initiates a connection FIN - (Final) Cleanly terminates a connection ACK - Acknowledges received data. This is called three way handshaking.

Part 2

Video streaming

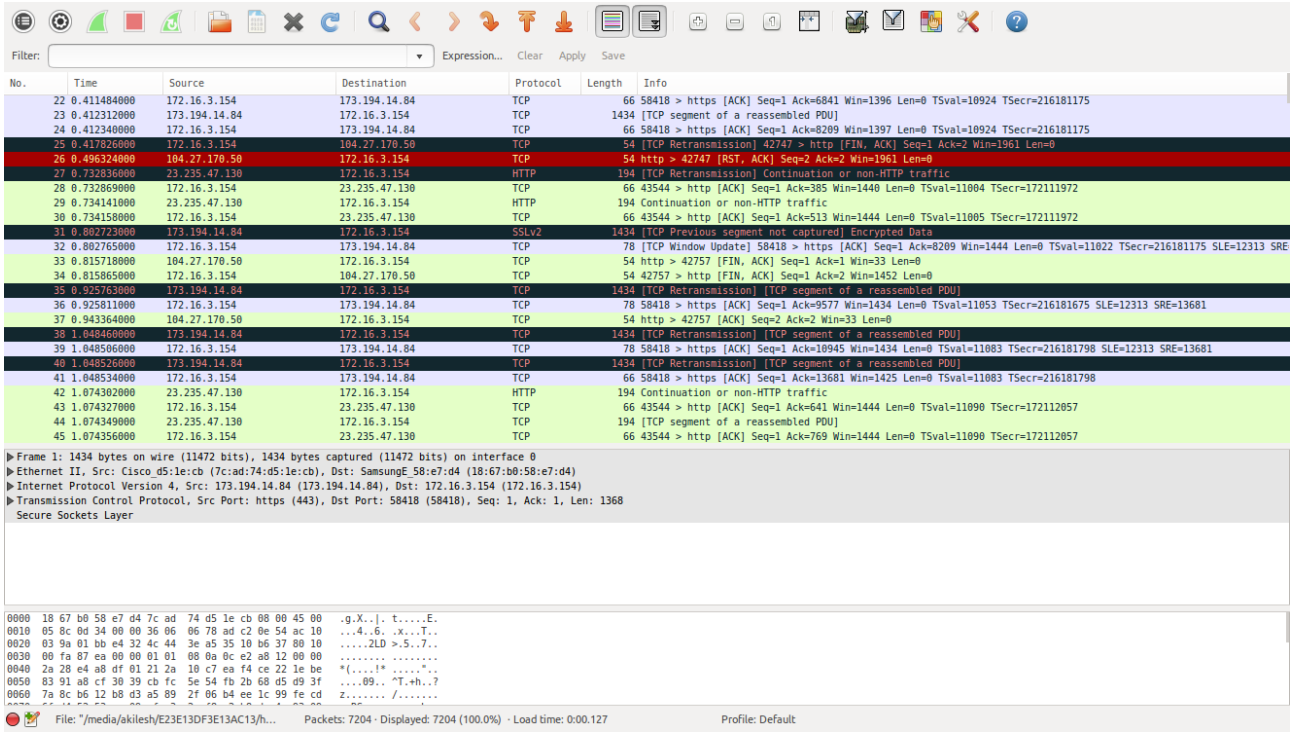
1) www.youtube.com



Application layer: HTTPS (Secure), TLSv1.2, SSL

Transport layer: TCP

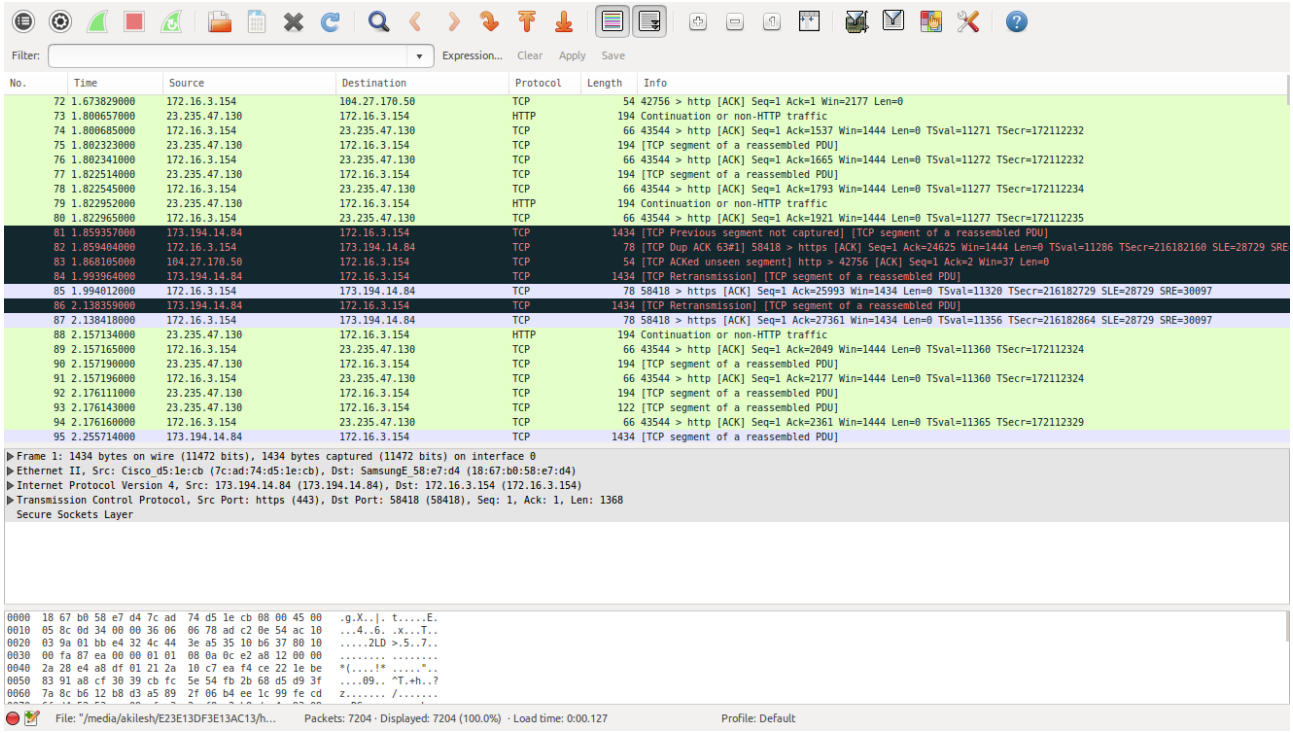
2) shush.se



Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

3) dailymotion.com



Application layer: HTTP, TLSv1.2, SSL

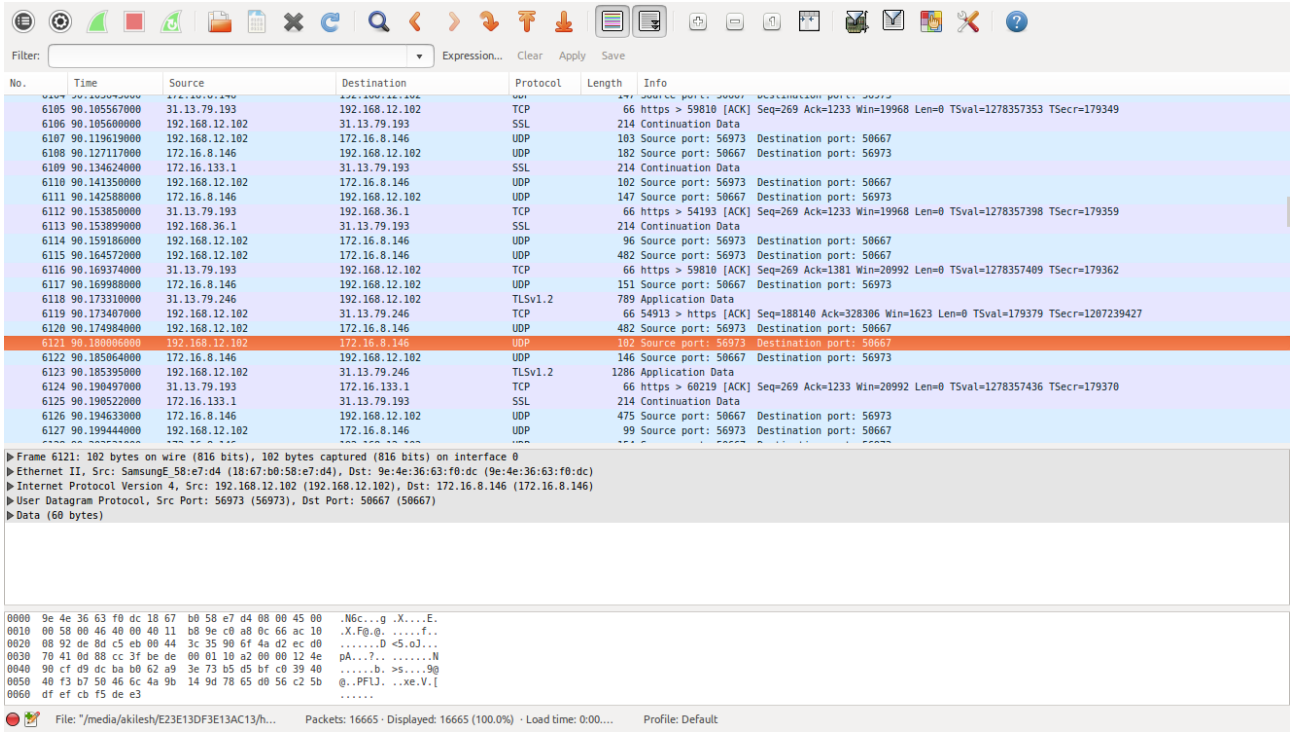
Transport layer: TCP

Explanation: I captured the packets for three video streaming sites as shown above. Youtube uses a secure link (HTTPS) where as the other two shush.se and dailymotion use HTTP.
When the video starts playing a huge increase in number of packets captured was observed. When the video is paused or is buffering then relatively less packets were captured.

Part 3

Voice calling

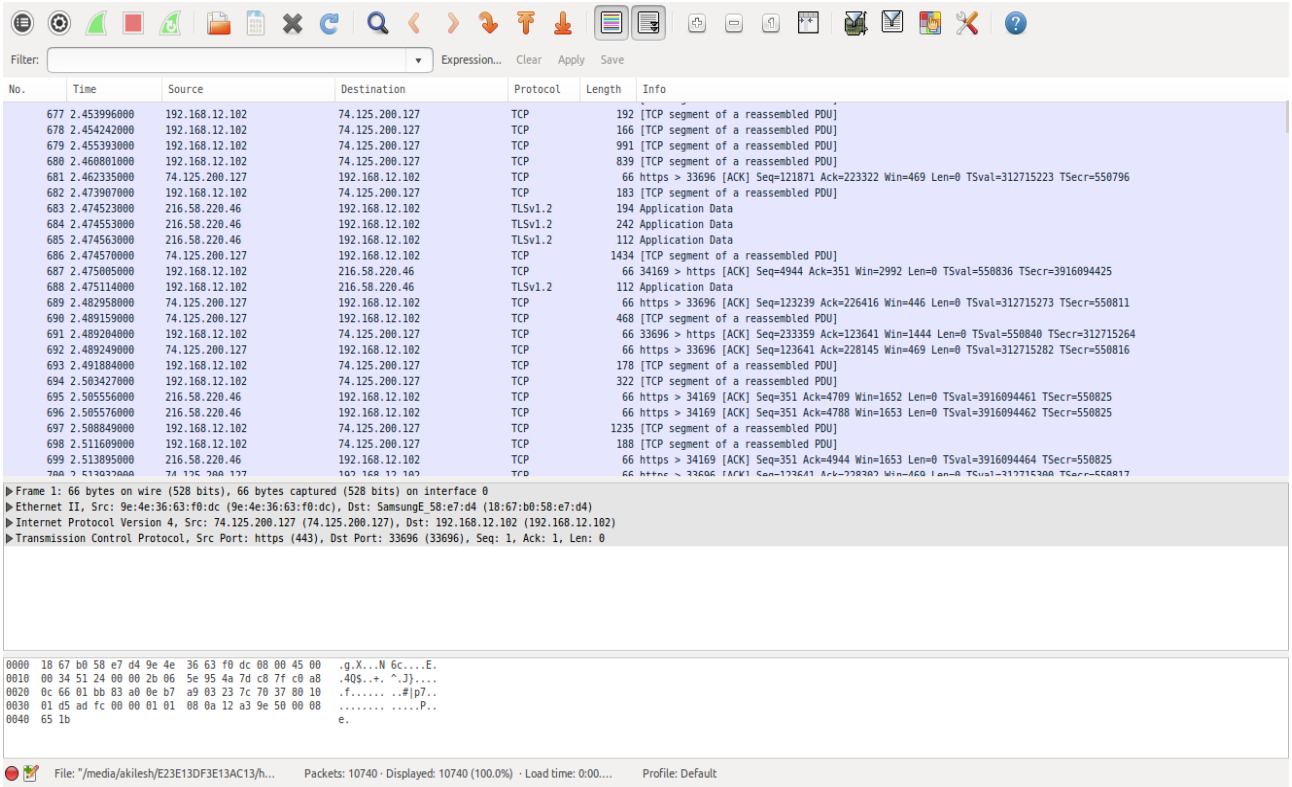
1) Facebook video call



Application layer: TLSv1.2, SSL, STUN

Transport layer: TCP, UDP

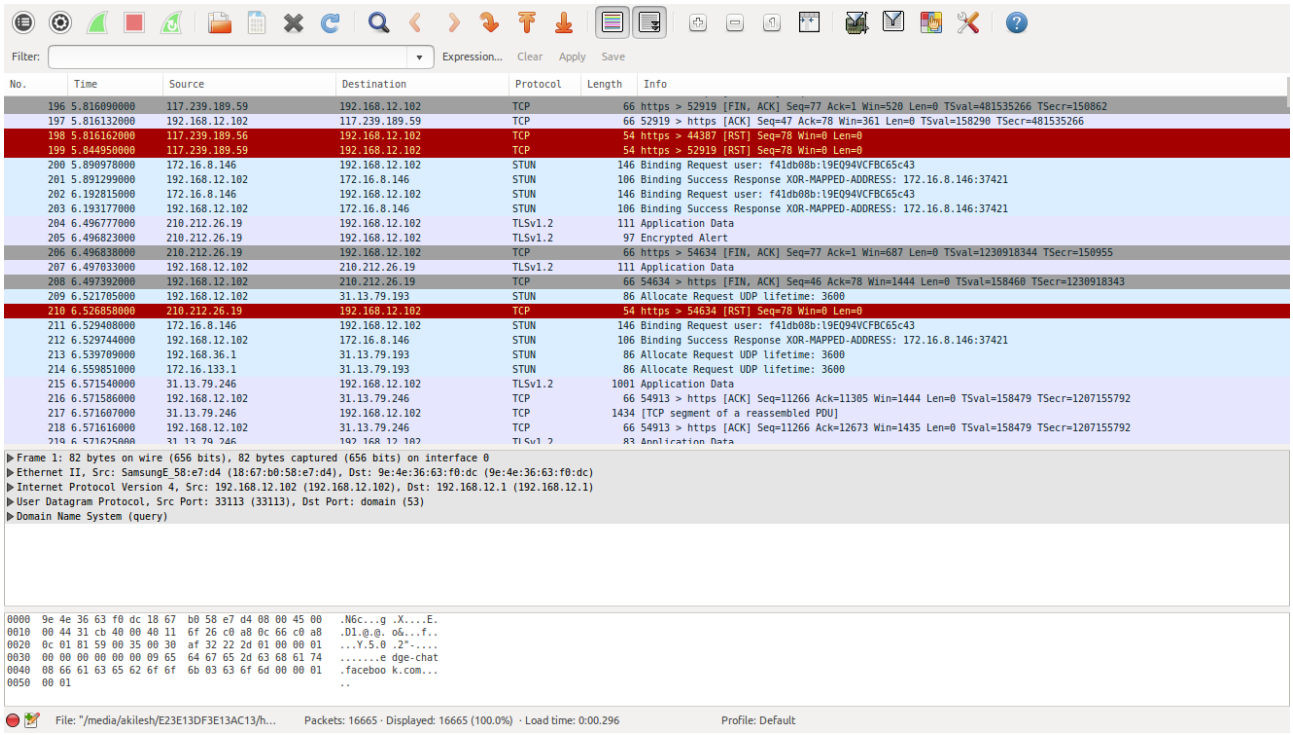
2) Google hangouts



Application layer: TLSv1.2, SSL

Transport : TCP

3) Skype



Application layer: TLSv1.2, SSL, STUN

Transport: TCP, UDP

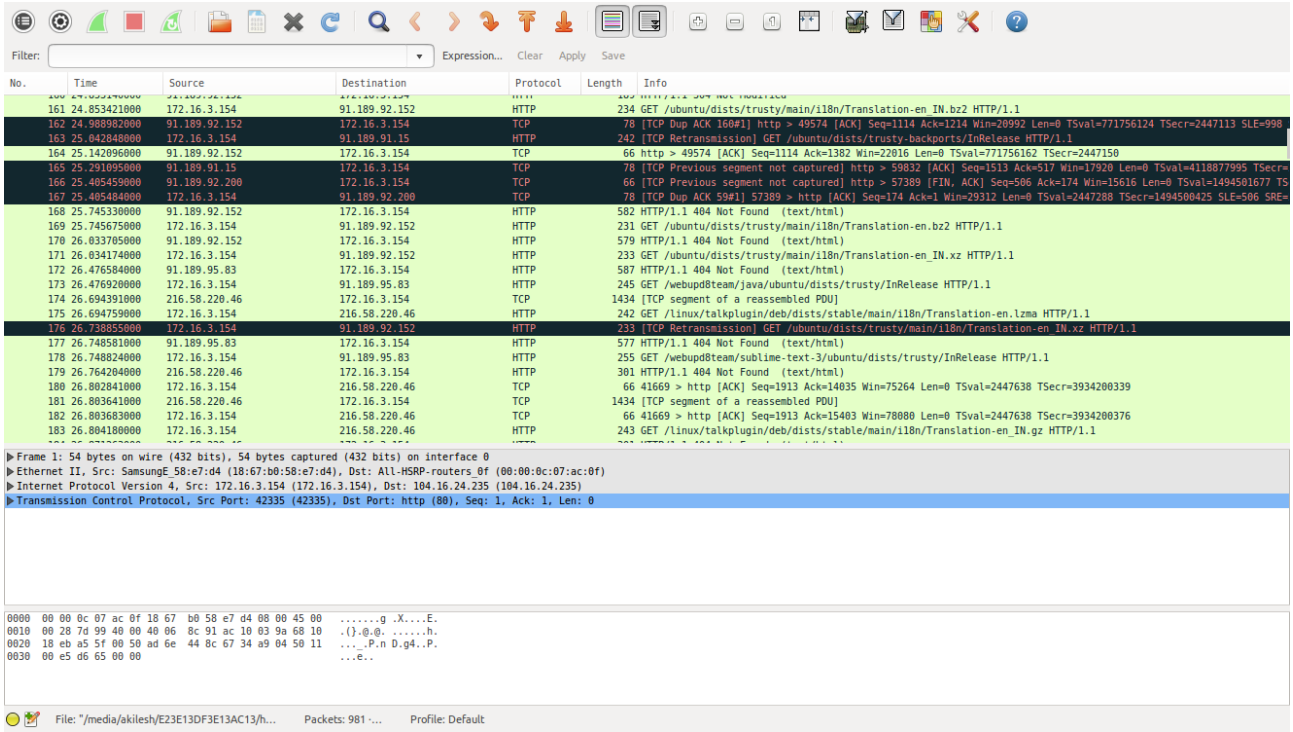
Explanation:

For three VoIP services as above packets were captured.
Facebook video call and Skype use both TCP and UDP as transport layer protocol.
UDP is relatively faster than TCP but it is unreliable (as packets may be lost).
Google hangouts on the other hand uses only TCP so it is relatively slower but reliable.
All three uses STUN which tries to establish peer to peer link.
The main purpose of the STUN protocol is to enable a device running behind a NAT device to discover its public IP and what type of NAT is running on the gateway it is connected to.

Part 4

System updates

1) Linux update



Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

2) Windows update

No.	Time	Source	Destination	Protocol	Length	Info
673	50.3477580	192.168.35.52	172.16.6.111	DNS	412	Standard query response 0x0d07 CNAME bg.v4.dl.windowsupdate.com.nsatc.net CNAME w8v4.audownload.wi
674	50.3481740	192.168.35.52	172.16.6.111	DNS	317	Standard query response 0x5682 CNAME bg.v4.dl.windowsupdate.com.nsatc.net CNAME w8v4.audownload.wi
675	50.3486400	172.16.6.111	191.234.4.50	TCP	66	54368→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
676	50.3688380	191.234.4.50	172.16.6.111	TCP	66	80→54368 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
677	50.3689400	172.16.6.111	191.234.4.50	TCP	54	54368→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
678	50.3690460	172.16.6.111	191.234.4.50	HTTP	323	HEAD /d/msdownload/update/software/defu/2015/08/am_delta_patch_1.203.2087.0_ff2a97a7b124a88e06a803c
679	50.3890030	191.234.4.50	172.16.6.111	TCP	54	80→54368 [ACK] Seq=1 Ack=270 Win=131072 Len=0
680	50.3935200	191.234.4.50	172.16.6.111	TCP	472	[TCP segment of a reassembled PDU]
681	50.4439160	172.16.6.111	191.234.4.50	TCP	54	54368→80 [ACK] Seq=270 Ack=419 Win=65792 Len=0
682	50.5022680	23.103.189.157	172.16.6.111	TCP	54	443→54367 [FIN, ACK] Seq=4263 Ack=1839 Win=66048 Len=0
683	50.5023420	172.16.6.111	23.103.189.157	TCP	54	54367→443 [ACK] Seq=1839 Ack=4264 Win=66048 Len=0
684	51.5269570	204.79.197.200	172.16.6.111	TCP	54	443→54354 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
685	53.6861980	fe80::501e:5661:c96	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::501e:5661:c963:9e4b (ovr) is at a4:db:30:2c:39:e5
686	53.6864260	2405:8a00:4001:228:	ff02::1	ICMPv6	86	Neighbor Advertisement 2405:8a00:4001:228:501e:5661:c963:9e4b (ovr) is at a4:db:30:2c:39:e5
687	53.6866820	2405:8a00:4001:228:	ff02::1	ICMPv6	86	Neighbor Advertisement 2405:8a00:4001:228:a9a9:ccc3:1e1d:4f96 (ovr) is at a4:db:30:2c:39:e5
688	54.4133370	172.16.6.111	191.234.4.50	HTTP	395	GET /d/msdownload/update/software/defu/2015/08/am_delta_patch_1.203.2087.0_ff2a97a7b124a88e06a803d4
689	54.4345710	191.234.4.50	172.16.6.111	TCP	54	80→54368 [ACK] Seq=419 Ack=611 Win=130560 Len=0
690	54.4380250	191.234.4.50	172.16.6.111	TCP	1434	[TCP segment of a reassembled PDU]
691	54.4381800	191.234.4.50	172.16.6.111	TCP	1434	[TCP segment of a reassembled PDU]
692	54.4382240	172.16.6.111	191.234.4.50	TCP	54	54368→80 [ACK] Seq=611 Ack=3179 Win=66048 Len=0
693	54.4383380	191.234.4.50	172.16.6.111	TCP	1434	[TCP segment of a reassembled PDU]
694	54.4400220	191.234.4.50	172.16.6.111	TCP	1434	[TCP segment of a reassembled PDU]
695	54.4400620	172.16.6.111	191.234.4.50	TCP	54	54368→80 [ACK] Seq=611 Ack=5939 Win=66048 Len=0
696	54.4400940	191.234.4.50	172.16.6.111	TCP	346	[TCP segment of a reassembled PDU]
697	54.4909350	172.16.6.111	191.234.4.50	TCP	54	54368→80 [ACK] Seq=611 Ack=6231 Win=65792 Len=0

Application layer: HTTP, TLSv1.2

Transport layer: TCP