

# 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](http://www.google.com)

The image shows a Wireshark packet capture interface. The top toolbar contains various icons for file operations, editing, and analysis. Below the toolbar is a filter bar with a dropdown menu and buttons for 'Expression...', 'Clear', 'Apply', and 'Save'. The main packet list table has columns for 'No.', 'Time', 'Source', 'Destination', 'Protocol', 'Length', and 'Info'. The packets are listed in a table with alternating light blue and light gray rows. The 'Info' column provides details for each packet, such as '59 [Malformed Packet]', '54 46353 > https [ACK] Seq=6 Ack=6 Win=29312 Len=0', and '59 [Malformed Packet]'. The bottom section of the interface shows the 'Packet 1' details, including 'Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0', 'Ethernet II, Src: 9e:4e:36:f0:dc (9e:4e:36: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)', and 'Transmission Control Protocol, Src Port: http (80), Dst Port: 60012 (60012), Seq: 1, Ack: 1, Len: 0'. At the very bottom, there is a hex dump and ASCII representation of the packet data.

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	7.410760000	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	8.890586000	91.190.218.212	192.168.12.102	TCP	54	https > 46353 [RST] Seq=31 Win=155200 Len=0
40	8.7921712000	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	9.370509000	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:f0:dc (9e:4e:36: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.V0... 0I(.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 >.

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

Transport layer: TCP

## 2) [www.flipkart.com](http://www.flipkart.com)

Filter:  Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
580	8.792219000	163.53.76.21	172.16.3.154	HTTP	1434	Continuation or non-HTTP traffic
581	8.792245000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=9849 Win=1444 Len=0 TSval=232032 TSecr=644098075
582	8.792266000	163.53.76.21	172.16.3.154	HTTP	146	Continuation or non-HTTP traffic
583	8.792272000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=9929 Win=1444 Len=0 TSval=232032 TSecr=644098075
584	8.790130000	163.53.76.21	172.16.3.154	HTTP	1434	Continuation or non-HTTP traffic
585	8.790147000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=11297 Win=1444 Len=0 TSval=232033 TSecr=644098076
586	8.790163000	163.53.76.21	172.16.3.154	TCP	146	[TCP segment of a reassembled PDU]
587	8.790169000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=11377 Win=1444 Len=0 TSval=232033 TSecr=644098076
588	8.790178000	163.53.76.21	172.16.3.154	HTTP	1026	Continuation or non-HTTP traffic
589	8.790185000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=12337 Win=1437 Len=0 TSval=232033 TSecr=644098076
590	8.790192000	163.53.76.21	172.16.3.154	HTTP	146	[TCP Previous segment not captured] Continuation or non-HTTP traffic
591	8.790199000	172.16.3.154	163.53.76.21	TCP	78	[TCP Dup ACK 589#1] 50288 > http [ACK] Seq=1071 Ack=12337 Win=1437 Len=0 TSval=232033 TSecr=644098076 SLE=13705
592	8.790205000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
593	8.790211000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=13785 Win=1434 Len=0 TSval=232033 TSecr=644098076
594	8.790217000	163.53.76.21	172.16.3.154	TCP	146	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
595	8.790222000	172.16.3.154	163.53.76.21	TCP	78	[TCP Window Update] 50288 > http [ACK] Seq=1071 Ack=13785 Win=1444 Len=0 TSval=232033 TSecr=644098076 SLE=15153
596	8.790230000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
597	8.790236000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=15233 Win=1434 Len=0 TSval=232033 TSecr=644098076
598	8.813678000	163.53.76.21	172.16.3.154	HTTP	1274	Continuation or non-HTTP traffic
599	8.813784000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=16441 Win=1444 Len=0 TSval=232037 TSecr=644098081
600	8.815284000	163.53.76.21	172.16.3.154	HTTP	146	[TCP Previous segment not captured] Continuation or non-HTTP traffic
601	8.815304000	172.16.3.154	163.53.76.21	TCP	78	[TCP Dup ACK 599#1] 50288 > http [ACK] Seq=1071 Ack=16441 Win=1444 Len=0 TSval=232037 TSecr=644098081 SLE=17809
602	8.815319000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
603	8.815328000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=17809 Win=1434 Len=0 TSval=232037 TSecr=644098081

► Frame 1: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0  
► Ethernet II, Src: LiteonTe 55:26:ff (20:68:9d:55:26:ff), Dst: IPv6mcast 00:01:00:02 (33:33:00:01:00:02)  
► Internet Protocol Version 6, Src: fe80::80f0:2e6e:16c4:86ed (fe80::80f0:2e6e:16c4:86ed), Dst: ff02::1:2 (ff02::1:2)  
► User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)  
► DHCPv6

0000 33 33 00 01 00 02 20 68 9d 55 26 ff 86 dd 60 00 33... h.U6...  
0010 00 00 00 5f 11 01 fe 80 00 00 00 00 00 00 00 f0 .....  
0020 2e 6e 16 c4 86 ed ff 02 00 00 00 00 00 00 00 00 .....n.....  
0030 00 00 00 01 00 02 02 22 02 23 00 5f 58 e2 01 f1 .....\*.#.X...  
0040 82 51 00 00 00 02 01 2d 00 01 00 0e 00 01 00 01 .Q.....  
0050 17 eb 60 44 20 68 9d 55 26 ff 00 03 00 0c 0f 20 ...D h.U &.....  
0060 68 9d 00 00 00 00 00 00 00 00 27 00 09 00 07 h.....

File: /media/akilesh/E23E13DF3E13AC13/h... Packets: 7157 · Displayed: 7157 (100.0%) · Load time: 0:00.129 Profile: Default

Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

### 3) en.wikipedia.org

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	0.203220000	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=688609 TSecr=1212405609 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	3.832100000	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	7.881909000	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 00 00 45 00 .N6c...g .X....E.						
0010 00 34 ad e4 40 00 00 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](http://www.linkedin.com)

No.	Time	Source	Destination	Protocol	Length	Info
29	3.175585000	192.168.12.102	103.20.92.129	TCP	1434	[TCP segment of a reassembled PDU]
30	3.175596000	192.168.12.102	103.20.92.129	TLV1.2	1217	Application Data
31	3.235269000	103.20.92.129	192.168.12.102	TCP	66	https > 54075 [ACK] Seq=1 Ack=1369 Win=16 Len=0 TSval=3395379392 TSecr=788294
32	3.235312000	103.20.92.129	192.168.12.102	TCP	66	https > 54075 [ACK] Seq=1 Ack=2737 Win=16 Len=0 TSval=3395379392 TSecr=788294
33	3.235320000	103.20.92.129	192.168.12.102	TCP	66	https > 54075 [ACK] Seq=1 Ack=3888 Win=16 Len=0 TSval=3395379392 TSecr=788294
34	3.245931000	192.168.12.102	103.20.92.129	TCP	66	54087 > https [ACK] Seq=1 Ack=1 Win=257 Len=0 TSval=788312 TSecr=3395369378
35	3.301443000	103.20.92.129	192.168.12.102	TCP	66	[TCP ACKed unseen segment] https > 54087 [ACK] Seq=1 Ack=2 Win=16 Len=0 TSval=3395379458 TSecr=773184
36	3.389950000	192.168.12.102	173.223.221.121	TCP	66	36733 > https [ACK] Seq=1 Ack=1 Win=1611 Len=0 TSval=788348 TSecr=2991299783
37	3.525448000	173.223.221.121	192.168.12.102	TCP	66	[TCP ACKed unseen segment] https > 36733 [ACK] Seq=1 Ack=2 Win=620 Len=0 TSval=2991309945 TSecr=785844
38	3.607909000	103.20.92.129	192.168.12.102	TLV1.2	783	Application Data
39	3.608042000	192.168.12.102	103.20.92.129	TCP	66	54075 > https [ACK] Seq=3888 Ack=718 Win=1444 Len=0 TSval=788402 TSecr=3395379725
40	3.665059000	103.20.92.129	192.168.12.102	TLV1.2	339	Application Data
41	3.665106000	192.168.12.102	103.20.92.129	TCP	66	54075 > https [ACK] Seq=3888 Ack=991 Win=1444 Len=0 TSval=788416 TSecr=3395379822
42	4.343910000	23.37.43.27	192.168.12.102	TCP	66	http > 54390 [FIN, ACK] Seq=1 Ack=1 Win=354 Len=0 TSval=1147042282 TSecr=784312
43	4.344122000	192.168.12.102	23.37.43.27	TCP	66	54390 > http [FIN, ACK] Seq=1 Ack=2 Win=260 Len=0 TSval=788586 TSecr=1147042282
44	4.365966000	192.168.12.102	117.18.237.29	TCP	74	46619 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=788592 TSecr=0 WS=128
45	4.395804000	117.18.237.29	192.168.12.102	TCP	74	http > 46619 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=322135263 TSecr=788592 WS=512
46	4.395876000	192.168.12.102	117.18.237.29	TCP	66	46619 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=788599 TSecr=322135263
47	4.744989000	23.37.43.27	192.168.12.102	TCP	66	http > 54390 [ACK] Seq=2 Ack=2 Win=354 Len=0 TSval=1147042685 TSecr=788586
48	4.909956000	192.168.12.102	54.251.241.105	TCP	66	55313 > https [ACK] Seq=1 Ack=1 Win=403 Len=0 TSval=788728 TSecr=3417228148
49	4.967570000	54.251.241.105	192.168.12.102	TCP	66	[TCP ACKed unseen segment] https > 55313 [ACK] Seq=1 Ack=2 Win=136 Len=0 TSval=3417230683 TSecr=783688
50	5.037944000	192.168.12.102	23.223.214.120	TCP	66	44606 > https [ACK] Seq=1 Ack=1 Win=516 Len=0 TSval=788760 TSecr=3699824504
51	5.197964000	192.168.12.102	103.20.92.129	TCP	66	54088 > https [ACK] Seq=1 Ack=1 Win=281 Len=0 TSval=788800 TSecr=3395371298
52	5.235692000	103.20.92.129	192.168.12.102	TCP	66	[TCP ACKed unseen segment] https > 44606 [ACK] Seq=1 Ack=2 Win=583 Len=0 TSval=3500831704 TSecr=783715
▶ 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: 103.20.92.129 (103.20.92.129), Dst: 192.168.12.102 (192.168.12.102)						
▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 54089 (54089), Seq: 1, Ack: 1, Len: 0						
0000 18 67 b0 58 e7 d4 9e 4e 36 63 f0 dc 00 00 45 00 .g.X...N 6c....E.						
0010 00 34 5b 48 40 00 f4 06 9a d7 67 14 5c 81 c0 a8 .4[H]... .g.\...						
0020 0c 66 01 ba d3 49 a5 b5 3c 45 d2 82 07 aa 00 10 .f..I...eI.....						
0030 00 10 6d 88 00 00 01 01 08 0a ca 61 53 e9 00 0b ..m.....a5...						
0040 c8 fe ..						

File: "/media/akilesh/E23E13DF3E13AC13/h... Packets: 282 · Displayed: 282 (100.0%) · Load time: 0:00.043 Profile: Default

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

Transport layer: TCP

5) [www.facebook.com](http://www.facebook.com)

Filter:  Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
18	0.737521000	31.13.79.246	192.168.12.102	TLSv1.2	111	[TCP Retransmission] Application Data
19	0.737570000	192.168.12.102	31.13.79.246	TCP	78	[TCP Dup ACK 15#2] 55596 > https [ACK] Seq=7728 Ack=46 Win=1444 Len=0 TSval=817732 TSecr=1460167553 SLE=1 SRE=46
20	1.414744000	31.13.79.246	192.168.12.102	TLSv1.2	111	[TCP Retransmission] Application Data
21	1.414797000	192.168.12.102	31.13.79.246	TCP	78	[TCP Dup ACK 15#3] 55596 > https [ACK] Seq=7728 Ack=46 Win=1444 Len=0 TSval=817902 TSecr=1460168222 SLE=1 SRE=46
22	2.237611000	117.239.189.56	192.168.12.102	TLSv1.2	111	Application Data
23	2.237668000	117.239.189.48	192.168.12.102	TLSv1.2	111	Application Data
24	2.237699000	192.168.12.102	117.239.189.48	TCP	66	55831 > https [ACK] Seq=1 Ack=46 Win=361 Len=0 TSval=818107 TSecr=1334595403
25	2.237966000	192.168.12.102	117.239.189.48	TLSv1.2	111	Application Data
26	2.238657000	192.168.12.102	117.239.189.56	TLSv1.2	111	Application Data
27	2.239073000	192.168.12.102	117.239.189.56	TLSv1.2	97	Encrypted Alert
28	2.239113000	192.168.12.102	117.239.189.56	TCP	66	45075 > https [FIN, ACK] Seq=77 Ack=46 Win=361 Len=0 TSval=818108 TSecr=1247057299
29	2.239359000	192.168.12.102	117.239.189.48	TLSv1.2	97	Encrypted Alert
30	2.239393000	192.168.12.102	117.239.189.48	TCP	66	55831 > https [FIN, ACK] Seq=77 Ack=46 Win=361 Len=0 TSval=818108 TSecr=1334595403
31	2.310632000	192.168.12.102	117.239.189.56	TCP	66	[TCP Retransmission] 45075 > https [FIN, ACK] Seq=77 Ack=46 Win=361 Len=0 TSval=818126 TSecr=1247057299
32	2.362346000	117.239.189.56	192.168.12.102	TLSv1.2	111	[TCP Retransmission] Application Data
33	2.362350000	192.168.12.102	117.239.189.56	TCP	78	[TCP Dup ACK 31#1] 45075 > https [ACK] Seq=78 Ack=46 Win=361 Len=0 TSval=818130 TSecr=1247057590 SLE=1 SRE=46
34	2.362433000	31.13.79.246	192.168.12.102	TCP	66	https > 55596 [ACK] Seq=46 Ack=3574 Win=877 Len=0 TSval=1460169114 TSecr=817548
35	2.392125000	117.239.189.56	192.168.12.102	TCP	54	https > 45075 [RST] Seq=46 Win=0 Len=0
36	2.395910000	117.239.189.48	192.168.12.102	TCP	54	https > 55831 [RST] Seq=46 Win=0 Len=0
37	2.425502000	31.13.79.246	192.168.12.102	TCP	66	https > 55596 [ACK] Seq=46 Ack=4942 Win=888 Len=0 TSval=1460169240 TSecr=817548
38	2.427944000	31.13.79.246	192.168.12.102	TCP	66	https > 55596 [ACK] Seq=46 Ack=6310 Win=899 Len=0 TSval=1460169241 TSecr=817548
39	2.427999000	31.13.79.246	192.168.12.102	TCP	78	[TCP Dup ACK 38#1] https > 55596 [ACK] Seq=46 Ack=6310 Win=899 Len=0 TSval=1460169241 TSecr=817548 SLE=7678 SRE=46
40	2.428018000	31.13.79.246	192.168.12.102	TLSv1.2	754	Application Data
41	2.428023000	192.168.12.102	31.13.79.246	TCP	66	55596 > https [ACK] Seq=7728 Ack=773 Win=1444 Len=0 TSval=818155 TSecr=1460169241

▶ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 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: 192.168.12.1 (192.168.12.1)  
▶ User Datagram Protocol, Src Port: 53359 (53359), Dst Port: domain (53)  
▶ Domain Name System (query)

0000 9e 4e 36 63 f0 dc 18 67 b0 58 e7 d4 00 00 45 00 .N6c...g .X....E.  
0010 00 3e 9a 05 40 00 40 11 06 72 c0 a0 0c 66 c0 a8 .>..@. .r...f..  
0020 0c 01 00 6f 00 35 00 2a 7c a8 22 95 01 00 00 01 ...0.5.\* |\*.....  
0030 00 00 00 00 00 00 63 77 77 78 08 66 61 63 65 62 .....w ww.faceb  
0040 6f 6f 6b 63 63 6f 64 00 00 01 00 01 00 00 00 00 ok.com. ....

File: /media/akilesh/E23E13DF3E13AC13/h... Packets: 162 - Displayed: 162 (100.0%) - Load time: 0:00.039 Profile: Default

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

Transport layer: TCP

## 6) [www.paypal.com](http://www.paypal.com)

No.	Time	Source	Destination	Protocol	Length	Info
4	0.215599000	216.58.228.35	192.168.12.102	TCP	66	[TCP ACKed unseen segment] http > 47859 [ACK] Seq=1 Ack=2 Win=349 Len=0 TSval=3920836590 TSecr=838566
5	0.239998000	192.168.12.102	63.140.45.104	TCP	66	39847 > https [ACK] Seq=1 Ack=1 Win=45144 Len=0 TSval=843683 TSecr=734284266
6	1.240014000	192.168.12.102	63.140.45.104	TCP	66	[TCP Dup ACK 5#1] 39847 > https [ACK] Seq=1 Ack=1 Win=45144 Len=0 TSval=843853 TSecr=734284266
7	1.521674000	63.140.45.104	192.168.12.102	TCP	66	[TCP ACKed unseen segment] https > 39847 [ACK] Seq=1 Ack=2 Win=8275 Len=0 TSval=734295507 TSecr=841113
8	2.630591000	192.168.12.102	31.13.84.4	TLSv1.2	107	Application Data
9	2.944868000	31.13.84.4	192.168.12.102	TLSv1.2	107	Application Data
10	2.944917000	192.168.12.102	31.13.84.4	TCP	66	37938 > https [ACK] Seq=42 Ack=42 Win=317 Len=0 TSval=844279 TSecr=3846097891
11	3.300013000	192.168.12.102	23.37.43.27	TCP	66	54429 > http [ACK] Seq=1 Ack=1 Win=259 Len=0 TSval=844368 TSecr=1717440993
12	3.631714000	192.168.12.102	31.13.84.4	TLSv1.2	107	Application Data
13	3.763175000	23.37.43.27	192.168.12.102	TCP	66	[TCP ACKed unseen segment] http > 54429 [ACK] Seq=1 Ack=2 Win=354 Len=0 TSval=1717451393 TSecr=836658
14	3.954273000	31.13.84.4	192.168.12.102	TLSv1.2	107	Application Data
15	3.954323000	192.168.12.102	31.13.84.4	TCP	66	37936 > https [ACK] Seq=42 Ack=42 Win=836 Len=0 TSval=844531 TSecr=1006316945
16	4.125177000	117.239.91.9	192.168.12.102	TLSv1.2	111	Application Data
17	4.125230000	192.168.12.102	117.239.91.9	TCP	66	38274 > https [ACK] Seq=1 Ack=46 Win=366 Len=0 TSval=844574 TSecr=1271278610
18	4.125268000	117.239.91.9	192.168.12.102	TLSv1.2	97	Encrypted Alert
19	4.125284000	192.168.12.102	117.239.91.9	TCP	66	38274 > https [ACK] Seq=77 Win=366 Len=0 TSval=844574 TSecr=1271278610
20	4.125302000	117.239.91.9	192.168.12.102	TCP	66	https > 38274 [FIN, ACK] Seq=77 Ack=1 Win=713 Len=0 TSval=1271278610 TSecr=837085
21	4.125508000	192.168.12.102	117.239.91.9	TLSv1.2	111	Application Data
22	4.125960000	192.168.12.102	117.239.91.9	TCP	66	38274 > https [FIN, ACK] Seq=46 Ack=78 Win=366 Len=0 TSval=844574 TSecr=1271278610
23	4.176708000	117.239.91.9	192.168.12.102	TCP	54	https > 38274 [RST] Seq=78 Win=0 Len=0
24	4.455249000	46.137.248.70	192.168.12.102	TLSv1.2	97	Encrypted Alert
25	4.455292000	192.168.12.102	46.137.248.70	TCP	66	49940 > https [ACK] Seq=1 Ack=32 Win=338 Len=0 TSval=844656 TSecr=1154005326
26	4.455324000	46.137.248.70	192.168.12.102	TCP	66	https > 49940 [FIN, ACK] Seq=32 Ack=1 Win=42 Len=0 TSval=1154005326 TSecr=8440905
27	4.455456000	192.168.12.102	46.137.248.70	TCP	66	49940 > https [FIN, ACK] Seq=1 Ack=33 Win=338 Len=0 TSval=844656 TSecr=1154005326
▶ 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: 184.27.142.244 (184.27.142.244)						
▶ Transmission Control Protocol, Src Port: 52428 (52428), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0						
0000 9e 4e 36 63 f0 dc 18 67 b0 58 e7 d4 00 00 45 00 .N6c...g.X....E.						
0010 00 34 66 ed 40 00 40 06 bf b8 c0 a8 0c 66 b8 1b .4f.0.0. ....f..						
0020 0e 14 cc cc 01 bb d9 5f c5 47 0d 4b 48 96 80 10 .....G.KH...						
0030 01 69 11 64 00 00 01 01 08 0a 00 0c df 17 b2 4e .i.d....N						
0040 fb 4e .N						

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

Transport layer: TCP

7) `filestream.me`

Filter:

Expression...

Clear

Apply

Save

No.	Time	Source	Destination	Protocol	Length	Info
158	1.476796000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=129961 Win=2030 Len=0 TSval=937769 TSecr=2342676738
159	1.477411000	82.198.29.149	192.168.12.102	TLV1.2	1434	Application Data
160	1.477438000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=131329 Win=2030 Len=0 TSval=937769 TSecr=2342676738
161	1.478156000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
162	1.478179000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=132697 Win=2030 Len=0 TSval=937769 TSecr=2342676738
163	1.480692000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
164	1.480720000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=134065 Win=2030 Len=0 TSval=937770 TSecr=2342676738
165	1.480747000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
166	1.480756000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=135433 Win=2030 Len=0 TSval=937770 TSecr=2342676738
167	1.480767000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
168	1.480774000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=136801 Win=2030 Len=0 TSval=937770 TSecr=2342676738
169	1.480782000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
170	1.480803000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=138169 Win=2030 Len=0 TSval=937770 TSecr=2342676738
171	1.480813000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
172	1.480819000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=139537 Win=2027 Len=0 TSval=937770 TSecr=2342676738
173	1.806327000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
174	1.806363000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=140905 Win=2030 Len=0 TSval=937851 TSecr=2342676820
175	1.806393000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
176	1.806405000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
177	1.806411000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=143641 Win=2030 Len=0 TSval=937851 TSecr=2342676820
178	1.806423000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
179	1.806431000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
180	1.806440000	82.198.29.149	192.168.12.102	TLV1.2	1434	Application Data
181	1.806465000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=147745 Win=2018 Len=0 TSval=937851 TSecr=2342676820

▶ Frame 1: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0

▶ Ethernet II, Src: 9e:4e:36:63:f0:d0 (9e:4e:36:63:f0:d0), Dst: SamsungE 58:e7:d4 (18:67:b0:58:e7:d4)

▶ Internet Protocol Version 4, Src: 82.198.29.149 (82.198.29.149), Dst: 192.168.12.102 (192.168.12.102)

▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 50005 (50005), Seq: 1, Ack: 1, Len: 1368

0000

18 67 b0 58 e7 d4 9e 4e 36 63 f0 dc 08 00 45 00

.g.X...N 6c....E.

0010

05 8c c8 ad 40 00 f4 06 7b 54 52 c6 1d 95 c0 a8

...0...[TR....

0020

0c 66 01 bb c3 55 7f fd 4b 31 bb aa f9 e4 80 10

.f...U. K1.....

0030

00 24 29 b2 00 00 01 01 08 0a 8b a2 67 b1 00 0e

.\$).....g....

0040

4d 87 17 03 03 40 18 ab 1b 51 f8 a0 fa 04 01 ea

M.....0...Q.....

0050

ad 37 6c e4 15 e9 67 4f 86 59 15 13 0c 6e 6f fa

..71...g0 Y.....0.

0060

60 26 66 b8 b8 24 13 68 83 26 a7 8d ad 87 64 0d

h6f...\$..h...6...1..

File: /media/akilshy/E23E13DF3E13AC13/h...

Packets: 13016 - Displayed: 13016 (100.0%) - Load time: 0:00.190

Profile: Default

Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

## 8) github.com

The image shows a Wireshark packet capture interface. The top toolbar contains various icons for file operations, editing, and analysis. Below the toolbar is a filter bar with a dropdown menu and buttons for 'Expression...', 'Clear', 'Apply', and 'Save'.

No.	Time	Source	Destination	Protocol	Length	Info
158	1.476796000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=129961 Win=2030 Len=0 TSval=937769 TSecr=2342676738
159	1.477411000	82.198.29.149	192.168.12.102	TLSv1.2	1434	Application Data
160	1.477438000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=131329 Win=2030 Len=0 TSval=937769 TSecr=2342676738
161	1.478156000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
162	1.478179000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=132697 Win=2030 Len=0 TSval=937769 TSecr=2342676738
163	1.480692000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
164	1.480720000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=134065 Win=2030 Len=0 TSval=937770 TSecr=2342676738
165	1.480747000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
166	1.480756000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=135433 Win=2030 Len=0 TSval=937770 TSecr=2342676738
167	1.480767000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
168	1.480774000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=136801 Win=2030 Len=0 TSval=937770 TSecr=2342676738
169	1.480782000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
170	1.480803000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=138169 Win=2030 Len=0 TSval=937770 TSecr=2342676738
171	1.480813000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
172	1.480819000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=139537 Win=2027 Len=0 TSval=937770 TSecr=2342676738
173	1.806327000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
174	1.806363000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=140905 Win=2030 Len=0 TSval=937851 TSecr=2342676820
175	1.806393000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
176	1.806405000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
177	1.806411000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=143641 Win=2030 Len=0 TSval=937851 TSecr=2342676820
178	1.806423000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
179	1.806431000	82.198.29.149	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
180	1.806440000	82.198.29.149	192.168.12.102	TLSv1.2	1434	Application Data
181	1.806450000	192.168.12.102	82.198.29.149	TCP	66	50005 > https [ACK] Seq=1 Ack=147745 Win=2010 Len=0 TSval=937851 TSecr=2342676820

Frame 1: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0  
Ethernet II, Src: 9e:4e:36:63:f8:dc (9e:4e:36:63:f8:dc), Dst: SamsungE\_58:e7:d4 (18:67:b8:58:e7:d4)  
Internet Protocol Version 4, Src: 82.198.29.149 (82.198.29.149), Dst: 192.168.12.102 (192.168.12.102)  
Transmission Control Protocol, Src Port: https (443), Dst Port: 50005 (50005), Seq: 1, Ack: 1, Len: 1368

0000 18 67 b0 58 e7 d4 9e 4e 36 63 f0 dc 08 00 45 00 .g.X...N 6c....E.  
0010 05 0c c8 ad 40 00 14 06 7b 54 52 c8 1d 95 c0 a8 ...@... {TR....  
0020 0c 66 01 b0 c3 55 7f fd 4b 31 bb aa f9 e4 80 10 .f...U.. KI.....  
0030 00 24 29 b2 00 00 01 01 08 0a 8b a2 67 b1 00 0e .\$.)..... .g....  
0040 4d 87 17 03 03 40 18 ab 1b 51 f8 a0 fa d4 01 ea M....@.. .0.....  
0050 ad 37 6c e4 15 e0 67 4f 86 59 15 13 0c dc 6f fa .7L...g0 .Y.....0.  
0060 68 26 66 b8 0c 24 13 68 83 26 a7 8d ad 87 6a 0d h&f..\$.h .&....j.

File: /media/akilesh/E23E13DF3E13AC13/h... Packets: 13016 · Displayed: 13016 (100.0%) · Load time: 0:00.190 Profile: Default

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

Transport layer: TCP



## 9) dropbox.com

No.	Time	Source	Destination	Protocol	Length	Info
251	51.379688000	216.58.220.46	192.168.12.102	TCP	66	[TCP Dup ACK 745] [TCP ACKed unseen segment] http > 58039 [ACK] Seq=1 Ack=2 Win=341 Len=0 TSval=3920611597 TSecr=3920631211
252	51.406971000	216.58.220.38	192.168.12.102	TCP	54	https > 55820 [RST] Seq=62 Win=0 Len=0
253	51.419289000	115.112.4.5	192.168.12.102	TCP	66	[TCP Dup ACK 10#5] [TCP ACKed unseen segment] http > 53567 [ACK] Seq=1 Ack=2 Win=486 Len=0 TSval=1275059516 TSecr=3920631211
254	52.077963000	192.168.12.102	173.223.214.134	TCP	66	[TCP Dup ACK 12#5] 50638 > https [ACK] Seq=1 Ack=1 Win=489 Len=0 TSval=800520 TSecr=2991348470
255	52.138931000	173.223.214.134	192.168.12.102	TCP	66	[TCP Dup ACK 14#5] [TCP ACKed unseen segment] https > 50638 [ACK] Seq=1 Ack=2 Win=1227 Len=0 TSval=2991358550 TSecr=3920631211
256	52.205942000	192.168.12.102	103.20.92.129	TCP	66	[TCP Dup ACK 13#5] 54078 > https [ACK] Seq=1 Ack=1 Win=1289 Len=0 TSval=800552 TSecr=3395418273
257	52.265536000	103.20.92.129	192.168.12.102	TCP	66	[TCP Dup ACK 15#5] [TCP ACKed unseen segment] https > 54078 [ACK] Seq=1 Ack=2 Win=16 Len=0 TSval=3395428419 TSecr=3920631211
258	52.781956000	192.168.12.102	103.20.92.129	TCP	66	[TCP Dup ACK 16#5] 54086 > https [ACK] Seq=1 Ack=1 Win=436 Len=0 TSval=800696 TSecr=3395418915
259	52.835805000	103.20.92.129	192.168.12.102	TCP	66	[TCP Dup ACK 17#5] [TCP ACKed unseen segment] https > 54086 [ACK] Seq=1 Ack=2 Win=16 Len=0 TSval=3395428993 TSecr=3920631211
260	53.005938000	192.168.12.102	103.20.92.129	TCP	66	[TCP Dup ACK 34#5] 54087 > https [ACK] Seq=1 Ack=1 Win=257 Len=0 TSval=800952 TSecr=3395419930
261	53.060406000	103.20.92.129	192.168.12.102	TCP	66	[TCP Dup ACK 35#5] [TCP ACKed unseen segment] https > 54087 [ACK] Seq=1 Ack=2 Win=16 Len=0 TSval=3395430018 TSecr=3920631211
262	53.069055000	192.168.12.102	173.223.221.121	TCP	66	[TCP Dup ACK 36#5] 36733 > https [ACK] Seq=1 Ack=1 Win=1611 Len=0 TSval=800960 TSecr=2991350261
263	53.017271000	173.223.221.121	192.168.12.102	TCP	66	[TCP Dup ACK 37#5] [TCP ACKed unseen segment] https > 36733 [ACK] Seq=1 Ack=2 Win=620 Len=0 TSval=2991360330 TSecr=3920631211
264	53.997957000	192.168.12.102	103.20.92.129	TCP	66	[TCP Keep-Alive] 54075 > https [ACK] Seq=3887 Ack=991 Win=1444 Len=0 TSval=801000 TSecr=3395420129
265	54.052051000	103.20.92.129	192.168.12.102	TCP	66	[TCP Keep-Alive ACK] https > 54075 [ACK] Seq=991 Ack=3888 Win=16 Len=0 TSval=3395430209 TSecr=788416
266	55.218027000	103.20.92.129	192.168.12.102	TCP	66	[TCP ACKed unseen segment] https > 54089 [FIN, ACK] Seq=1 Ack=1 Win=16 Len=0 TSval=3395431378 TSecr=772350
267	55.218285000	192.168.12.102	103.20.92.129	TLSv1.2	97	[TCP Previous segment not captured] Encrypted Alert
268	55.218351000	192.168.12.102	103.20.92.129	TCP	66	54089 > https [FIN, ACK] Seq=32 Ack=2 Win=247 Len=0 TSval=801305 TSecr=3395431378
269	55.311225000	103.20.92.129	192.168.12.102	TCP	54	https > 54089 [RST] Seq=2 Win=0 Len=0
270	55.397998000	192.168.12.102	216.58.220.46	TCP	66	[TCP Previous segment not captured] 58028 > http [FIN, ACK] Seq=2 Ack=1 Win=252 Len=0 TSval=801350 TSecr=3920631211
271	55.398108000	192.168.12.102	216.58.220.46	TCP	66	[TCP Previous segment not captured] 58039 > http [FIN, ACK] Seq=2 Ack=1 Win=240 Len=0 TSval=801350 TSecr=3920631211
272	55.530937000	216.58.220.46	192.168.12.102	TCP	66	[TCP ACKed unseen segment] http > 58028 [FIN, ACK] Seq=1 Ack=3 Win=350 Len=0 TSval=3920631211 TSecr=801350
273	55.539933000	192.168.12.102	216.58.220.46	TCP	66	58028 > http [ACK] Seq=3 Ack=2 Win=252 Len=0 TSval=801385 TSecr=3920631211
▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0						
▶ Ethernet II, Src: 9e:4e:36:f0:dc (9e:4e:36:f0:dc), Dst: SamsungE_58:e7:d4 (18:67:b0:58:e7:d4)						
▶ Internet Protocol Version 4, Src: 103.20.92.129 (103.20.92.129), Dst: 192.168.12.102 (192.168.12.102)						
▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 54089 (54089), 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 5b 48 40 00 f4 06 9a d7 67 14 5c 01 c0 a8 .4[H0... .g.\...						
0020 0c 66 01 bb d3 49 a5 b5 3c 45 d2 82 07 aa 00 10 .f...I...<E.....						
0030 00 10 6d 88 00 00 01 01 08 0a ca 61 53 e9 00 0b ..m.....<a5....						
0040 c8 fe ..						
File: "/media/akilesh/E23E13DF3E13AC13/h... Packets: 282 - Displayed: 282 (100.0%) - Load time: 0:00.063 Profile: Default						

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

Transport layer: TCP

10) [www.quora.com](http://www.quora.com)

No.	Time	Source	Destination	Protocol	Length	Info
580	8.792219000	163.53.76.21	172.16.3.154	HTTP	1434	Continuation or non-HTTP traffic
581	8.792245000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=9849 Win=1444 Len=0 TSval=232032 TSecr=644098075
582	8.792256000	163.53.76.21	172.16.3.154	HTTP	146	Continuation or non-HTTP traffic
583	8.792272000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=9929 Win=1444 Len=0 TSval=232032 TSecr=644098075
584	8.798130000	163.53.76.21	172.16.3.154	HTTP	1434	Continuation or non-HTTP traffic
585	8.798147000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=11297 Win=1444 Len=0 TSval=232033 TSecr=644098076
586	8.798163000	163.53.76.21	172.16.3.154	TCP	146	[TCP segment of a reassembled PDU]
587	8.798169000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=11377 Win=1444 Len=0 TSval=232033 TSecr=644098076
588	8.798178000	163.53.76.21	172.16.3.154	HTTP	1026	Continuation or non-HTTP traffic
589	8.798185000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=12337 Win=1437 Len=0 TSval=232033 TSecr=644098076
590	8.798192000	163.53.76.21	172.16.3.154	HTTP	146	[TCP Previous segment not captured] Continuation or non-HTTP traffic
591	8.798199000	172.16.3.154	163.53.76.21	TCP	78	[TCP Dup ACK 589#1] 50288 > http [ACK] Seq=1071 Ack=12337 Win=1437 Len=0 TSval=232033 TSecr=644098076 SLE=13785
592	8.798205000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
593	8.798211000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=13785 Win=1434 Len=0 TSval=232033 TSecr=644098076
594	8.798217000	163.53.76.21	172.16.3.154	TCP	146	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
595	8.798222000	172.16.3.154	163.53.76.21	TCP	78	[TCP Window Update] 50288 > http [ACK] Seq=1071 Ack=13785 Win=1444 Len=0 TSval=232033 TSecr=644098076 SLE=15153
596	8.798230000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
597	8.798236000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=15233 Win=1434 Len=0 TSval=232033 TSecr=644098076
598	8.813678000	163.53.76.21	172.16.3.154	HTTP	1274	Continuation or non-HTTP traffic
599	8.813704000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=16441 Win=1444 Len=0 TSval=232037 TSecr=644098081
600	8.815284000	163.53.76.21	172.16.3.154	HTTP	146	[TCP Previous segment not captured] Continuation or non-HTTP traffic
601	8.815304000	172.16.3.154	163.53.76.21	TCP	78	[TCP Dup ACK 599#1] 50288 > http [ACK] Seq=1071 Ack=16441 Win=1444 Len=0 TSval=232037 TSecr=644098081 SLE=17809
602	8.815319000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
603	8.815328000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=17809 Win=1434 Len=0 TSval=232037 TSecr=644098081
▶ Frame 1: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0						
▶ Ethernet II, Src: LiteonTe 55:26:ff (20:68:9d:55:26:ff), Dst: IPv6mcast 00:01:00:02 (33:33:00:01:00:02)						
▶ Internet Protocol Version 6, Src: fe80::80f0:2e6e:16c4:86ed (fe80::80f0:2e6e:16c4:86ed), Dst: ff02::1:2 (ff02::1:2)						
▶ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)						
▶ DHCPv6						
0000 33 33 00 01 00 02 20 68 9d 55 26 ff 86 dd 60 00 33....h.U6....						
0010 00 00 00 5f 11 01 fe 80 00 00 00 00 00 00 00 .....						
0020 2e 6e 16 c4 86 ed ff 02 00 00 00 00 00 00 00 .h.....						
0030 00 00 01 00 02 02 22 02 23 00 5f 58 e2 01 f1 .....#.X...						
0040 82 51 00 00 02 01 2d 00 01 00 0e 00 01 00 01 .0.....						
0050 17 eb 60 44 20 68 9d 55 26 ff 00 03 00 0c 0f 20 ...D h.U &....						
0060 68 9d 00 00 00 00 00 00 00 00 27 00 09 00 07 h.....						
File: ~/media/akilesh/E23E13DF3E13AC13/h... Packets: 7157 · Displayed: 7157 (100.0%) · Load time: 0:00.129 Profile: Default						

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](http://www.youtube.com)

No.	Time	Source	Destination	Protocol	Length	Info
580	8.792219000	163.53.76.21	172.16.3.154	HTTP	1434	Continuation or non-HTTP traffic
581	8.792245000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=9849 Win=1444 Len=0 TSval=232032 TSecr=644098075
582	8.792266000	163.53.76.21	172.16.3.154	HTTP	146	Continuation or non-HTTP traffic
583	8.792272000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=9929 Win=1444 Len=0 TSval=232032 TSecr=644098075
584	8.798130000	163.53.76.21	172.16.3.154	HTTP	1434	Continuation or non-HTTP traffic
585	8.798147000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=11297 Win=1444 Len=0 TSval=232033 TSecr=644098076
586	8.798163000	163.53.76.21	172.16.3.154	TCP	146	[TCP segment of a reassembled PDU]
587	8.798169000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=11377 Win=1444 Len=0 TSval=232033 TSecr=644098076
588	8.798178000	163.53.76.21	172.16.3.154	HTTP	1026	Continuation or non-HTTP traffic
589	8.798185000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=12337 Win=1437 Len=0 TSval=232033 TSecr=644098076
590	8.798192000	163.53.76.21	172.16.3.154	HTTP	146	[TCP Previous segment not captured] Continuation or non-HTTP traffic
591	8.798199000	172.16.3.154	163.53.76.21	TCP	78	[TCP Dup ACK 589#1] 50288 > http [ACK] Seq=1071 Ack=12337 Win=1437 Len=0 TSval=232033 TSecr=644098076 SLE=13705
592	8.798205000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
593	8.798211000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=13785 Win=1434 Len=0 TSval=232033 TSecr=644098076
594	8.798217000	163.53.76.21	172.16.3.154	TCP	146	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
595	8.798222000	172.16.3.154	163.53.76.21	TCP	78	[TCP Window Update] 50288 > http [ACK] Seq=1071 Ack=13785 Win=1444 Len=0 TSval=232033 TSecr=644098076 SLE=15153
596	8.798228000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
597	8.798236000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=15233 Win=1434 Len=0 TSval=232033 TSecr=644098076
598	8.813678000	163.53.76.21	172.16.3.154	HTTP	1274	Continuation or non-HTTP traffic
599	8.813784000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=16441 Win=1444 Len=0 TSval=232037 TSecr=644098081
600	8.815284000	163.53.76.21	172.16.3.154	HTTP	146	[TCP Previous segment not captured] Continuation or non-HTTP traffic
601	8.815304000	172.16.3.154	163.53.76.21	TCP	78	[TCP Dup ACK 599#1] 50288 > http [ACK] Seq=1071 Ack=16441 Win=1444 Len=0 TSval=232037 TSecr=644098081 SLE=17809
602	8.815319000	163.53.76.21	172.16.3.154	HTTP	1434	[TCP Out-Of-Order] Continuation or non-HTTP traffic
603	8.815328000	172.16.3.154	163.53.76.21	TCP	66	50288 > http [ACK] Seq=1071 Ack=17889 Win=1434 Len=0 TSval=232037 TSecr=644098081

► Frame 1: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0  
► Ethernet II, Src: LiteonTe 55:26:ff (20:68:9d:55:26:ff), Dst: IPv6mcast 00:01:00:02 (33:33:00:01:00:02)  
► Internet Protocol Version 6, Src: fe80::80f0:2e6e:16c4:86ed (fe80::80f0:2e6e:16c4:86ed), Dst: ff02::1:2 (ff02::1:2)  
► User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)  
► DHCPv6

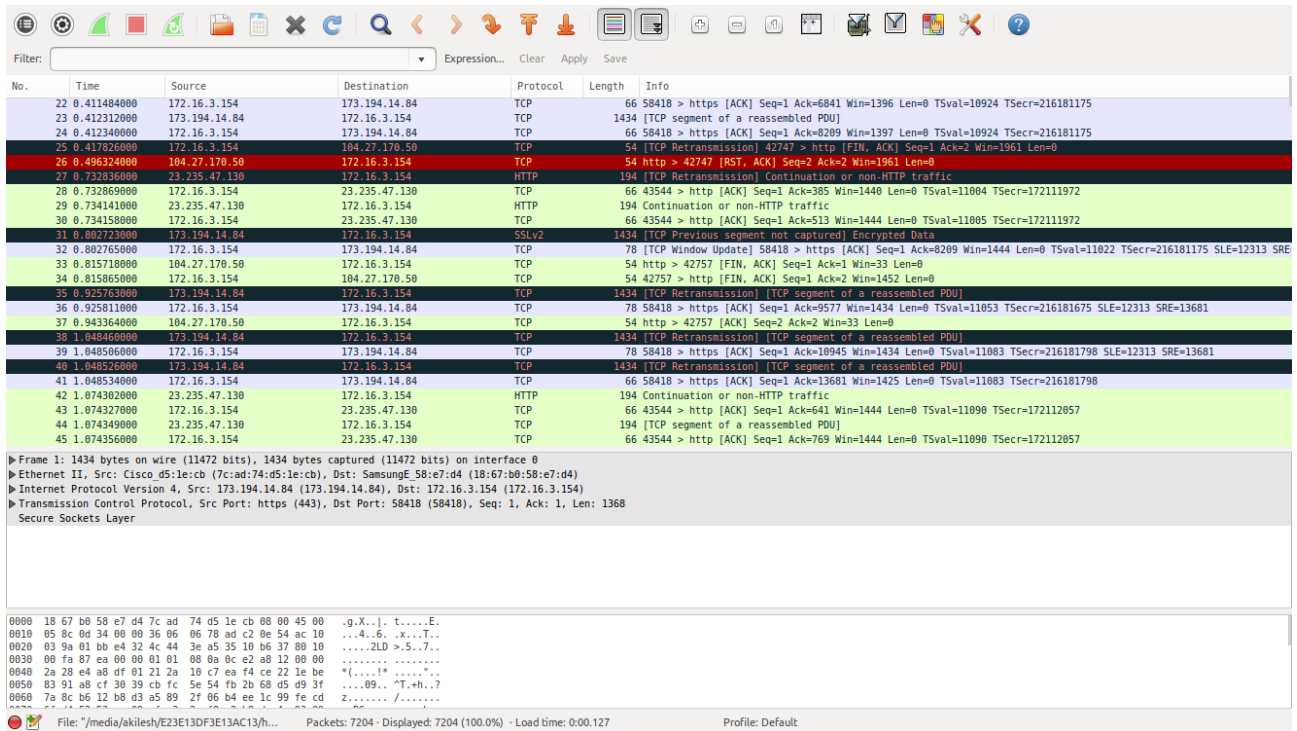
0000 33 33 00 01 00 02 20 68 9d 55 26 ff 86 dd 60 00 33....h.U6...  
0010 00 00 00 5f 11 01 fe 80 00 00 00 00 00 00 00 ....  
0020 2e 6e 16 c4 86 ed ff 02 00 00 00 00 00 00 00 .n.....  
0030 00 00 00 01 00 02 22 02 23 00 5f 58 e2 01 f1 .....#.X...  
0040 82 51 00 00 00 02 01 20 00 01 00 0e 00 01 00 .Q.....  
0050 17 eb 60 44 20 68 9d 55 26 ff 00 03 00 0c 0f 20 ..D.h.U 6.....  
0060 68 9d 00 00 00 00 00 00 00 00 27 00 09 00 07 h.....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

File: "/media/akilesh/E23E13DF3E13AC13/h... Packets: 7157 - Displayed: 7157 (100.0%) - Load time: 0:00.129 Profile: Default

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

Transport layer: TCP

## 2) shush.se



The image shows a Wireshark packet capture analysis of traffic to shush.se. The main display area shows a list of 45 packets. The first 14 packets are related to a retransmission of a TCP segment (Seq=1, Ack=6841, Win=1396, Len=0). The 15th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 16th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 17th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 18th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 19th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 20th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 21st packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 22nd packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 23rd packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 24th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 25th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 26th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 27th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 28th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 29th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 30th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 31st packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 32nd packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 33rd packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 34th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 35th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 36th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 37th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 38th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 39th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 40th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 41st packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 42nd packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 43rd packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 44th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0). The 45th packet is a TCP segment (Seq=1, Ack=8209, Win=1397, Len=0).

Frame 1: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0  
Ethernet II, Src: Cisco\_d5:1e:cb (7c:ad:74:d5:1e:cb), Dst: SamsungE\_58:e7:d4 (18:67:b0:58:e7:d4)  
Internet Protocol Version 4, Src: 173.194.14.84 (173.194.14.84), Dst: 172.16.3.154 (172.16.3.154)  
Transmission Control Protocol, Src Port: https (443), Dst Port: 58418 (58418), Seq: 1, Ack: 1, Len: 1368  
Secure Sockets Layer

0000 18 67 b0 58 e7 d4 7c ad 74 d5 1e cb 00 00 45 00 .g.X..]. t.....E.  
0010 05 0c 0d 34 00 00 36 06 06 78 ad c2 0e 54 ac 10 ...4..6. .x...I..  
0020 03 9a 01 b0 e4 32 4c 44 3e a5 35 10 b6 37 00 10 .....2L0>.5..7..  
0030 00 fa 87 ea 00 00 01 01 08 0a 0c e2 a8 12 00 00 .....  
0040 2a 28 e4 a8 df 01 21 2a 10 c7 ea f4 ce 22 1e be \*(!!!!) .....  
0050 83 91 a8 cf 30 39 cb fc 5e 54 fb 2b 68 d5 d9 3f ...09.. "T.+h...?  
0060 7a 8c b6 12 b8 d3 a5 89 2f 06 b4 ee 1c 99 fe cd z...../.....

File: ~/media/akilesh/E23E13DF3E13AC13/h... Packets: 7204 - Displayed: 7204 (100.0%) - Load time: 0:00.127 Profile: Default

Application layer: HTTP, TLSv1.2, SSL

Transport layer: TCP

### 3) dailymotion.com

No.	Time	Source	Destination	Protocol	Length	Info
72	1.673829000	172.16.3.154	104.27.170.50	TCP	54	42756 > http [ACK] Seq=1 Ack=1 Win=2177 Len=0
73	1.800657000	23.235.47.130	172.16.3.154	HTTP	194	Continuation or non-HTTP traffic
74	1.800685000	172.16.3.154	23.235.47.130	TCP	66	43544 > http [ACK] Seq=1 Ack=1537 Win=1444 Len=0 TSval=11271 TSecr=172112232
75	1.802323000	23.235.47.130	172.16.3.154	TCP	194	[TCP segment of a reassembled PDU]
76	1.802341000	172.16.3.154	23.235.47.130	TCP	66	43544 > http [ACK] Seq=1 Ack=1665 Win=1444 Len=0 TSval=11272 TSecr=172112232
77	1.822514000	23.235.47.130	172.16.3.154	TCP	194	[TCP segment of a reassembled PDU]
78	1.822545000	172.16.3.154	23.235.47.130	TCP	66	43544 > http [ACK] Seq=1 Ack=1793 Win=1444 Len=0 TSval=11277 TSecr=172112234
79	1.822952000	23.235.47.130	172.16.3.154	HTTP	194	Continuation or non-HTTP traffic
80	1.822965000	172.16.3.154	23.235.47.130	TCP	66	43544 > http [ACK] Seq=1 Ack=1921 Win=1444 Len=0 TSval=11277 TSecr=172112235
81	1.859357000	173.194.14.84	172.16.3.154	TCP	1434	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
82	1.859404000	172.16.3.154	173.194.14.84	TCP	78	[TCP Dup ACK 63#1] 58418 > https [ACK] Seq=1 Ack=24625 Win=1444 Len=0 TSval=11286 TSecr=216182160 SLE=28729 SRE
83	1.868105000	104.27.170.50	172.16.3.154	TCP	54	[TCP ACKed unseen segment] http > 42756 [ACK] Seq=1 Ack=2 Win=37 Len=0
84	1.993964000	173.194.14.84	172.16.3.154	TCP	1434	[TCP Retransmission] [TCP segment of a reassembled PDU]
85	1.994012000	172.16.3.154	173.194.14.84	TCP	78	58418 > https [ACK] Seq=1 Ack=25993 Win=1434 Len=0 TSval=11320 TSecr=216182729 SLE=28729 SRE=30097
86	2.138359000	173.194.14.84	172.16.3.154	TCP	1434	[TCP Retransmission] [TCP segment of a reassembled PDU]
87	2.138418000	172.16.3.154	173.194.14.84	TCP	78	58418 > https [ACK] Seq=1 Ack=27361 Win=1434 Len=0 TSval=11356 TSecr=216182864 SLE=28729 SRE=30097
88	2.157134000	23.235.47.130	172.16.3.154	HTTP	194	Continuation or non-HTTP traffic
89	2.157165000	172.16.3.154	23.235.47.130	TCP	66	43544 > http [ACK] Seq=1 Ack=2049 Win=1444 Len=0 TSval=11360 TSecr=172112324
90	2.157190000	23.235.47.130	172.16.3.154	TCP	194	[TCP segment of a reassembled PDU]
91	2.157196000	172.16.3.154	23.235.47.130	TCP	66	43544 > http [ACK] Seq=1 Ack=2177 Win=1444 Len=0 TSval=11360 TSecr=172112324
92	2.176111000	23.235.47.130	172.16.3.154	TCP	194	[TCP segment of a reassembled PDU]
93	2.176143000	23.235.47.130	172.16.3.154	TCP	122	[TCP segment of a reassembled PDU]
94	2.176160000	172.16.3.154	23.235.47.130	TCP	66	43544 > http [ACK] Seq=1 Ack=2361 Win=1444 Len=0 TSval=11365 TSecr=172112329
95	2.255714000	173.194.14.84	172.16.3.154	TCP	1434	[TCP segment of a reassembled PDU]
▶ Frame 1: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0						
▶ Ethernet II, Src: Cisco:d5:1e:cb (7:cad:74:d5:1e:cb), Dst: SamsungE_58:e7:d4 (18:67:b0:58:e7:d4)						
▶ Internet Protocol Version 4, Src: 173.194.14.84 (173.194.14.84), Dst: 172.16.3.154 (172.16.3.154)						
▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 58418 (58418), Seq: 1, Ack: 1, Len: 1368						
Secure Sockets Layer						
0000 18 67 b0 58 e7 d4 7c ad 74 d5 1e cb 08 00 45 00 .g.X..].t....E.						
0010 05 8c 0d 34 00 00 36 06 06 78 ad c2 0e 54 ac 10 ...4..6..x..I..						
0020 03 9a 01 bb e4 32 4c 44 3e a5 35 10 b6 37 80 10 ....2LD >.5..7..						
0030 00 fa 87 ea 00 00 01 01 08 0a 0c e2 a8 12 00 00 ..... .....						
0040 2a 28 e4 a8 df 01 21 2a 10 c7 ea f4 ce 22 1e be *((...)* ..... .....						
0050 83 91 a8 cf 30 39 cb 1c 5e 54 fb 2b 68 d5 09 3f ...09...T...h...?						
0060 7a 8c b6 12 b8 d3 a5 89 2f 06 b4 ee 1c 99 fe cd z...../.....						
File: /media/akilesh/E23E13DF3E13AC13/h... Packets: 7204 - Displayed: 7204 (100.0%) - Load time: 0:00.127 Profile: Default						

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

No.	Time	Source	Destination	Protocol	Length	Info
6105	90.105567000	31.13.79.193	192.168.12.102	TCP	66	https > 59810 [ACK] Seq=269 Ack=1233 Win=19968 Len=0 TSval=1278357353 TSecr=179349
6106	90.105600000	192.168.12.102	31.13.79.193	SSL	214	Continuation Data
6107	90.119619000	192.168.12.102	172.16.8.146	UDP	103	Source port: 56973 Destination port: 50667
6108	90.127117000	172.16.8.146	192.168.12.102	UDP	182	Source port: 50667 Destination port: 56973
6109	90.134624000	172.16.133.1	31.13.79.193	SSL	214	Continuation Data
6110	90.141350000	192.168.12.102	172.16.8.146	UDP	102	Source port: 56973 Destination port: 50667
6111	90.142580000	172.16.8.146	192.168.12.102	UDP	147	Source port: 50667 Destination port: 56973
6112	90.153850000	31.13.79.193	192.168.36.1	TCP	66	https > 54193 [ACK] Seq=269 Ack=1233 Win=19968 Len=0 TSval=1278357398 TSecr=179359
6113	90.153899000	192.168.36.1	31.13.79.193	SSL	214	Continuation Data
6114	90.159186000	192.168.12.102	172.16.8.146	UDP	96	Source port: 56973 Destination port: 50667
6115	90.164572000	192.168.12.102	172.16.8.146	UDP	482	Source port: 56973 Destination port: 50667
6116	90.169374000	31.13.79.193	192.168.12.102	TCP	66	https > 59810 [ACK] Seq=269 Ack=1381 Win=20992 Len=0 TSval=1278357409 TSecr=179362
6117	90.169980000	172.16.8.146	192.168.12.102	UDP	151	Source port: 50667 Destination port: 56973
6118	90.173310000	31.13.79.246	192.168.12.102	TLSv1.2	789	Application Data
6119	90.173407000	192.168.12.102	31.13.79.246	TCP	66	54913 > https [ACK] Seq=188140 Ack=328306 Win=1623 Len=0 TSval=179379 TSecr=1207239427
6120	90.174984000	192.168.12.102	172.16.8.146	UDP	482	Source port: 56973 Destination port: 50667
6121	90.180060000	192.168.12.102	172.16.8.146	UDP	102	Source port: 56973 Destination port: 50667
6122	90.185064000	172.16.8.146	192.168.12.102	UDP	146	Source port: 50667 Destination port: 56973
6123	90.185395000	192.168.12.102	31.13.79.246	TLSv1.2	1286	Application Data
6124	90.190497000	31.13.79.193	172.16.133.1	TCP	66	https > 60219 [ACK] Seq=269 Ack=1233 Win=20992 Len=0 TSval=1278357436 TSecr=179370
6125	90.190522000	172.16.133.1	31.13.79.193	SSL	214	Continuation Data
6126	90.194633000	172.16.8.146	192.168.12.102	UDP	475	Source port: 50667 Destination port: 56973
6127	90.199448000	192.168.12.102	172.16.8.146	UDP	99	Source port: 56973 Destination port: 50667

▶ Frame 6121: 102 bytes on wire (816 bits), 102 bytes captured (816 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: 172.16.8.146 (172.16.8.146)  
▶ User Datagram Protocol, Src Port: 56973 (56973), Dst Port: 50667 (50667)  
▶ Data (60 bytes)

```
0000  9e 4e 36 63 f0 dc 18 67 b0 58 e7 d4 00 00 45 00  .N6c...g .X....E.
0010  00 58 00 46 40 00 40 11 b8 9e c0 a0 0c 66 ac 10  .X.F@.@. ....f..
0020  00 92 de 0d c5 eb 00 44 3c 35 90 6f 4a d2 ec d0  .....D <S.oj...
0030  70 41 6d 88 cc 3f be de 00 01 10 a2 00 00 12 4e  pA...?.. ....N
0040  00 cf d9 dc ba b0 62 a9 3e 73 b5 d5 bf c0 39 40  .....b. >S....9@
0050  40 f3 b7 50 46 6c 4a 9b 14 9d 78 65 d0 56 c2 5b  @..PFLJ. ..xe.V.[
0060  df ef cb f5 de e3  ....
```

File: /media/akilesh/E23E13DF3E13AC13/h... Packets: 16665 · Displayed: 16665 (100.0%) · Load time: 0:00.... Profile: Default

Application layer: TLSv1.2, SSL, STUN

Transport layer: TCP, UDP



## 2) Google hangouts

No.	Time	Source	Destination	Protocol	Length	Info
677	2.453996000	192.168.12.102	74.125.200.127	TCP	192	[TCP segment of a reassembled PDU]
678	2.454242000	192.168.12.102	74.125.200.127	TCP	166	[TCP segment of a reassembled PDU]
679	2.455393000	192.168.12.102	74.125.200.127	TCP	991	[TCP segment of a reassembled PDU]
680	2.460801000	192.168.12.102	74.125.200.127	TCP	839	[TCP segment of a reassembled PDU]
681	2.462335000	74.125.200.127	192.168.12.102	TCP	66	https > 33696 [ACK] Seq=121871 Ack=223322 Win=469 Len=0 TSval=312715223 TSecr=550796
682	2.473907000	192.168.12.102	74.125.200.127	TCP	183	[TCP segment of a reassembled PDU]
683	2.474523000	216.58.220.46	192.168.12.102	TLSv1.2	194	Application Data
684	2.474553000	216.58.220.46	192.168.12.102	TLSv1.2	242	Application Data
685	2.474563000	216.58.220.46	192.168.12.102	TLSv1.2	112	Application Data
686	2.474570000	74.125.200.127	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
687	2.475005000	192.168.12.102	216.58.220.46	TCP	66	34169 > https [ACK] Seq=4944 Ack=351 Win=2992 Len=0 TSval=550836 TSecr=3916094425
688	2.475114000	192.168.12.102	216.58.220.46	TLSv1.2	112	Application Data
689	2.482958000	74.125.200.127	192.168.12.102	TCP	66	https > 33696 [ACK] Seq=123239 Ack=226416 Win=446 Len=0 TSval=312715273 TSecr=550811
690	2.489159000	74.125.200.127	192.168.12.102	TCP	468	[TCP segment of a reassembled PDU]
691	2.489204000	192.168.12.102	74.125.200.127	TCP	66	33696 > https [ACK] Seq=233359 Ack=123641 Win=1444 Len=0 TSval=550840 TSecr=312715264
692	2.489249000	74.125.200.127	192.168.12.102	TCP	66	https > 33696 [ACK] Seq=123641 Ack=228145 Win=469 Len=0 TSval=312715282 TSecr=550816
693	2.491884000	192.168.12.102	74.125.200.127	TCP	178	[TCP segment of a reassembled PDU]
694	2.503427000	192.168.12.102	74.125.200.127	TCP	322	[TCP segment of a reassembled PDU]
695	2.505556000	216.58.220.46	192.168.12.102	TCP	66	https > 34169 [ACK] Seq=351 Ack=4709 Win=1652 Len=0 TSval=3916094461 TSecr=550825
696	2.505576000	216.58.220.46	192.168.12.102	TCP	66	https > 34169 [ACK] Seq=351 Ack=4788 Win=1653 Len=0 TSval=3916094462 TSecr=550825
697	2.508849000	192.168.12.102	74.125.200.127	TCP	1235	[TCP segment of a reassembled PDU]
698	2.511609000	192.168.12.102	74.125.200.127	TCP	188	[TCP segment of a reassembled PDU]
699	2.513895000	216.58.220.46	192.168.12.102	TCP	66	https > 34169 [ACK] Seq=351 Ack=4944 Win=1653 Len=0 TSval=3916094464 TSecr=550825
700	2.513923000	74.125.200.127	192.168.12.102	TCP	66	https > 33696 [ACK] Seq=123641 Ack=228145 Win=469 Len=0 TSval=312715300 TSecr=550817
▶ 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: 74.125.200.127 (74.125.200.127), Dst: 192.168.12.102 (192.168.12.102)						
▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 33696 (33696), Seq: 1, Ack: 1, Len: 0						
0000 18 67 b0 58 e7 d4 9e 4e 36 63 f0 dc 00 00 45 00 .g.X...N6c...E.						
0010 00 34 51 24 00 00 2b 06 5e 95 4a 7d c8 7f c0 a8 .405.p.^.]...						
0020 0c 66 01 bb 83 a0 0e b7 a9 03 23 7c 70 37 80 10 .f.....[p7..						
0030 01 d5 ad fc 00 00 01 01 00 0a 12 a3 9e 50 00 08 .....P..						
0040 65 1b e.						

Application layer: TLSv1.2, SSL

Transport : TCP

### 3) Skype

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
196	5.816990000	117.239.189.59	192.168.12.102	TCP	66	https > 52919 [FIN, ACK] Seq=77 Ack=1 Win=520 Len=0 TSval=481535266 TSecr=150862
197	5.816132000	192.168.12.102	117.239.189.59	TCP	66	52919 > https [ACK] Seq=47 Ack=78 Win=361 Len=0 TSval=158290 TSecr=481535266
198	5.816162000	117.239.189.59	192.168.12.102	TCP	54	https > 44387 [RST] Seq=78 Win=0 Len=0
199	5.844950000	117.239.189.59	192.168.12.102	TCP	54	https > 52919 [RST] Seq=78 Win=0 Len=0
200	5.890978000	172.16.8.146	192.168.12.102	STUN	146	Binding Request user: f41db08b:19E094VCFBC65c43
201	5.891299000	192.168.12.102	172.16.8.146	STUN	106	Binding Success Response XOR-MAPPED-ADDRESS: 172.16.8.146:37421
202	6.192815000	172.16.8.146	192.168.12.102	STUN	146	Binding Request user: f41db08b:19E094VCFBC65c43
203	6.193177000	192.168.12.102	172.16.8.146	STUN	106	Binding Success Response XOR-MAPPED-ADDRESS: 172.16.8.146:37421
204	6.496777000	210.212.26.19	192.168.12.102	TLSv1.2	111	Application Data
205	6.496823000	210.212.26.19	192.168.12.102	TLSv1.2	97	Encrypted Alert
206	6.496838000	210.212.26.19	192.168.12.102	TCP	66	https > 54634 [FIN, ACK] Seq=77 Ack=1 Win=687 Len=0 TSval=1230918344 TSecr=150855
207	6.497033000	192.168.12.102	210.212.26.19	TLSv1.2	111	Application Data
208	6.497392000	192.168.12.102	210.212.26.19	TCP	66	54634 > https [FIN, ACK] Seq=46 Ack=78 Win=1444 Len=0 TSval=158460 TSecr=1230918343
209	6.521076500	192.168.12.102	31.13.79.193	STUN	86	Allocate Request UDP lifetime: 3600
210	6.526858000	210.212.26.19	192.168.12.102	TCP	54	https > 54634 [RST] Seq=78 Win=0 Len=0
211	6.529408000	172.16.8.146	192.168.12.102	STUN	146	Binding Request user: f41db08b:19E094VCFBC65c43
212	6.529744000	192.168.12.102	172.16.8.146	STUN	106	Binding Success Response XOR-MAPPED-ADDRESS: 172.16.8.146:37421
213	6.539709000	192.168.36.1	31.13.79.193	STUN	86	Allocate Request UDP lifetime: 3600
214	6.559851000	172.16.133.1	31.13.79.193	STUN	86	Allocate Request UDP lifetime: 3600
215	6.571540000	31.13.79.246	192.168.12.102	TLSv1.2	1001	Application Data
216	6.571566000	192.168.12.102	31.13.79.246	TCP	66	54913 > https [ACK] Seq=11266 Ack=11305 Win=1444 Len=0 TSval=158479 TSecr=1207155792
217	6.571607000	31.13.79.246	192.168.12.102	TCP	1434	[TCP segment of a reassembled PDU]
218	6.571616000	192.168.12.102	31.13.79.246	TCP	66	54913 > https [ACK] Seq=11266 Ack=12673 Win=1435 Len=0 TSval=158479 TSecr=1207155792
219	6.571635000	210.212.26.19	192.168.12.102	TLSv1.2	82	Application Data

▶ Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 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: 192.168.12.1 (192.168.12.1)

▶ User Datagram Protocol, Src Port: 33113 (33113), Dst Port: domain (53)

▶ Domain Name System (query)

<pre> 0000  9e 4e 36 63 f0 dc 18 67 b0 58 e7 d4 08 00 45 00    .N6c...g.X...E. 0010  00 00 21 28 00 00 40 11 6f 26 c0 08 66 c0 a0     .01.0.0.06...f. 0020  0c 01 81 59 00 35 00 30 af 32 22 2d 01 00 00 01    ...Y.5.0.2*.... 0030  00 00 00 00 00 00 09 65 64 67 65 2d 63 68 61 74    .....0.dge.chat 0040  08 66 61 63 65 62 6f 6f 6b 03 63 6f 6d 00 00 01    .facebook.k.com... 0050  00 01   ..           </pre>	<pre> .N6c...g.X...E. .01.0.0.06...f. ...Y.5.0.2*.... .....0.dge.chat .facebook.k.com... ..           </pre>
---	--

File: "/media/akilesh/E23E13DF3E13AC13/h...

Packets: 16665 · Displayed: 16665 (100.0%) · Load time: 0:00.296

Profile: Default

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

No.	Time	Source	Destination	Protocol	Length	Info
161	24.853421800	172.16.3.154	91.189.92.152	HTTP	234	GET /ubuntu/dists/trusty/main/118n/Translation-en_IN.bz2 HTTP/1.1
162	24.988982900	91.189.92.152	172.16.3.154	TCP	78	[TCP Dup ACK 160#1] http > 49574 [ACK] Seq=1114 Ack=1214 Win=20992 Len=0 TSval=771756124 TSecr=24471113 SLE=998
163	25.042848000	172.16.3.154	91.189.91.15	HTTP	242	[TCP Retransmission] GET /ubuntu/dists/trusty-backports/InRelease HTTP/1.1
164	25.142096000	91.189.92.152	172.16.3.154	TCP	66	http > 49574 [ACK] Seq=1114 Ack=1382 Win=22016 Len=0 TSval=771756162 TSecr=2447150
165	25.291095000	91.189.91.15	172.16.3.154	TCP	78	[TCP Previous segment not captured] http > 59832 [ACK] Seq=1513 Ack=517 Win=17920 Len=0 TSval=4118877995 TSecr=
166	25.405459000	91.189.92.200	172.16.3.154	TCP	66	[TCP Previous segment not captured] http > 57389 [FIN, ACK] Seq=506 Ack=174 Win=15616 Len=0 TSval=1494501677 TS
167	25.405484000	172.16.3.154	91.189.92.200	TCP	78	[TCP Dup ACK 59#1] 57389 > http [ACK] Seq=174 Ack=1 Win=29312 Len=0 TSval=2447288 TSecr=1494500425 SLE=506 SRE=
168	25.745330000	91.189.92.152	172.16.3.154	HTTP	582	HTTP/1.1 404 Not Found (text/html)
169	25.745675000	172.16.3.154	91.189.92.152	HTTP	231	GET /ubuntu/dists/trusty/main/118n/Translation-en.bz2 HTTP/1.1
170	26.033705000	91.189.92.152	172.16.3.154	HTTP	579	HTTP/1.1 404 Not Found (text/html)
171	26.034174000	172.16.3.154	91.189.92.152	HTTP	233	GET /ubuntu/dists/trusty/main/118n/Translation-en_IN.xz HTTP/1.1
172	26.476584000	91.189.95.83	172.16.3.154	HTTP	587	HTTP/1.1 404 Not Found (text/html)
173	26.476920000	172.16.3.154	91.189.95.83	HTTP	245	GET /webupd8team/java/ubuntu/dists/trusty/InRelease HTTP/1.1
174	26.694391000	216.58.220.46	172.16.3.154	TCP	1434	[TCP segment of a reassembled PDU]
175	26.694759000	172.16.3.154	216.58.220.46	HTTP	242	GET /linux/talkplugin/deb/dists/stable/main/118n/Translation-en.lzma HTTP/1.1
176	26.738855000	172.16.3.154	91.189.92.152	HTTP	233	[TCP Retransmission] GET /ubuntu/dists/trusty/main/118n/Translation-en_IN.xz HTTP/1.1
177	26.748581000	91.189.95.83	172.16.3.154	HTTP	577	HTTP/1.1 404 Not Found (text/html)
178	26.748824000	172.16.3.154	91.189.95.83	HTTP	255	GET /webupd8team/subline-text-3/ubuntu/dists/trusty/InRelease HTTP/1.1
179	26.764204000	216.58.220.46	172.16.3.154	HTTP	301	HTTP/1.1 404 Not Found (text/html)
180	26.802841000	172.16.3.154	216.58.220.46	TCP	66	41669 > http [ACK] Seq=1913 Ack=14035 Win=75264 Len=0 TSval=2447638 TSecr=3934200339
181	26.803641000	216.58.220.46	172.16.3.154	TCP	1434	[TCP segment of a reassembled PDU]
182	26.803683000	172.16.3.154	216.58.220.46	TCP	66	41669 > http [ACK] Seq=1913 Ack=15403 Win=78080 Len=0 TSval=2447638 TSecr=3934200376
183	26.804180000	172.16.3.154	216.58.220.46	HTTP	243	GET /linux/talkplugin/deb/dists/stable/main/118n/Translation-en_IN.gz HTTP/1.1

▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
▶ Ethernet II, Src: SamsungE:58:e7:d4 (18:67:b0:58:e7:d4), Dst: All-HSRP-routers\_0f (00:00:0c:07:ac:0f)  
▶ Internet Protocol Version 4, Src: 172.16.3.154 (172.16.3.154), Dst: 104.16.24.235 (104.16.24.235)  
▶ Transmission Control Protocol, Src Port: 42335 (42335), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

0000 00 00 0c 07 ac 0f 18 67 b0 58 e7 d4 00 00 45 00 .....g.X....E.  
0010 00 28 7d 99 40 00 40 06 8c 91 ac 10 03 9a 68 10 .().@.@. ....h.  
0020 18 eb a5 5f 00 50 ad 6e 44 8c 67 34 a9 04 50 11 ....P.n D.g4..P.  
0030 00 e5 06 65 00 00 .....E..

File: /media/akilesh/E23E13DF3E13AC13/h... Packets: 981 ... Profile: Default

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

