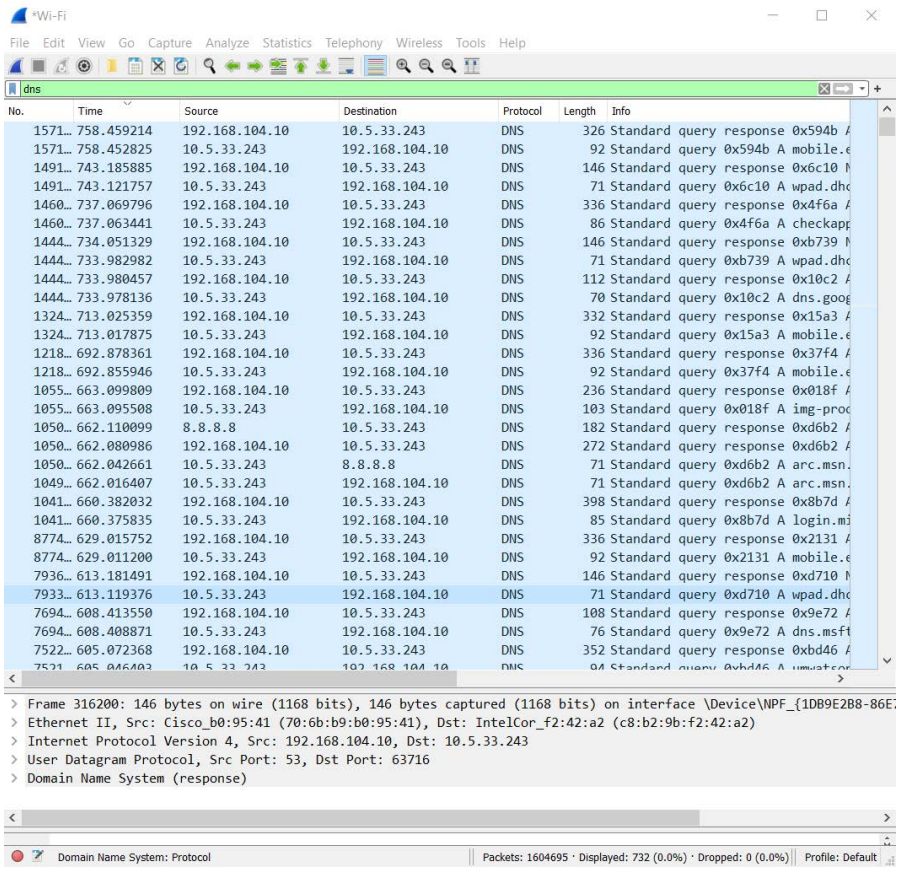
LAB - 2

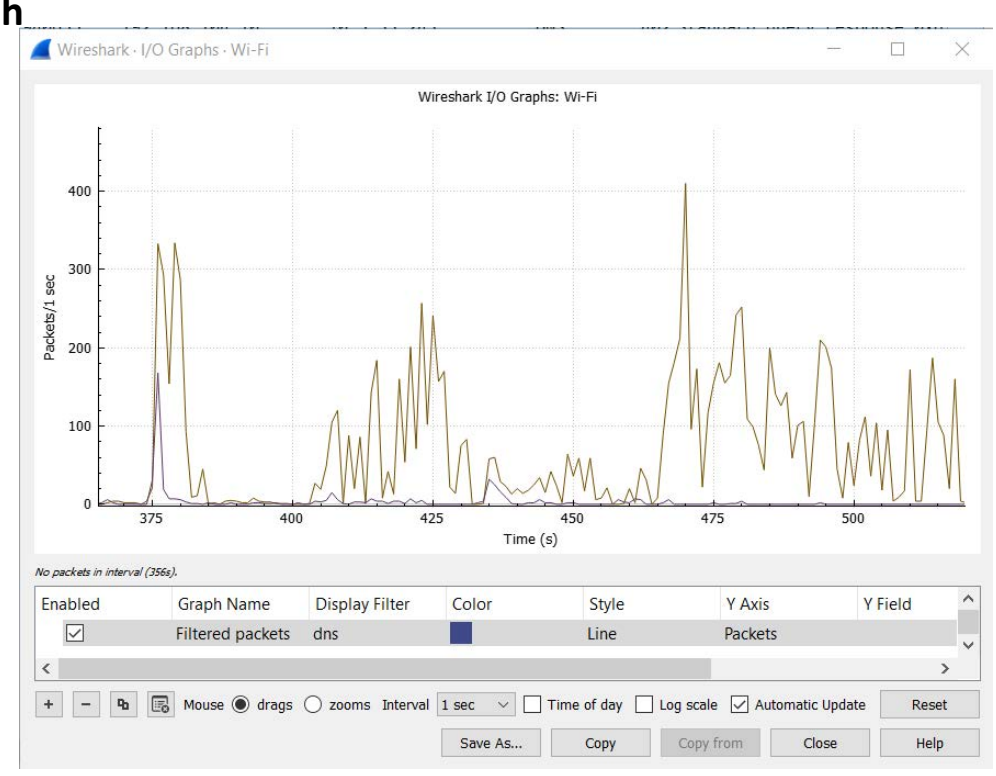
Ques 1: Display the filter output of the following filters

1. DNS
2. HTTP
3. TCP

DNS



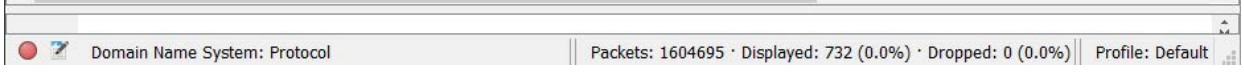
DNS I/O Graph



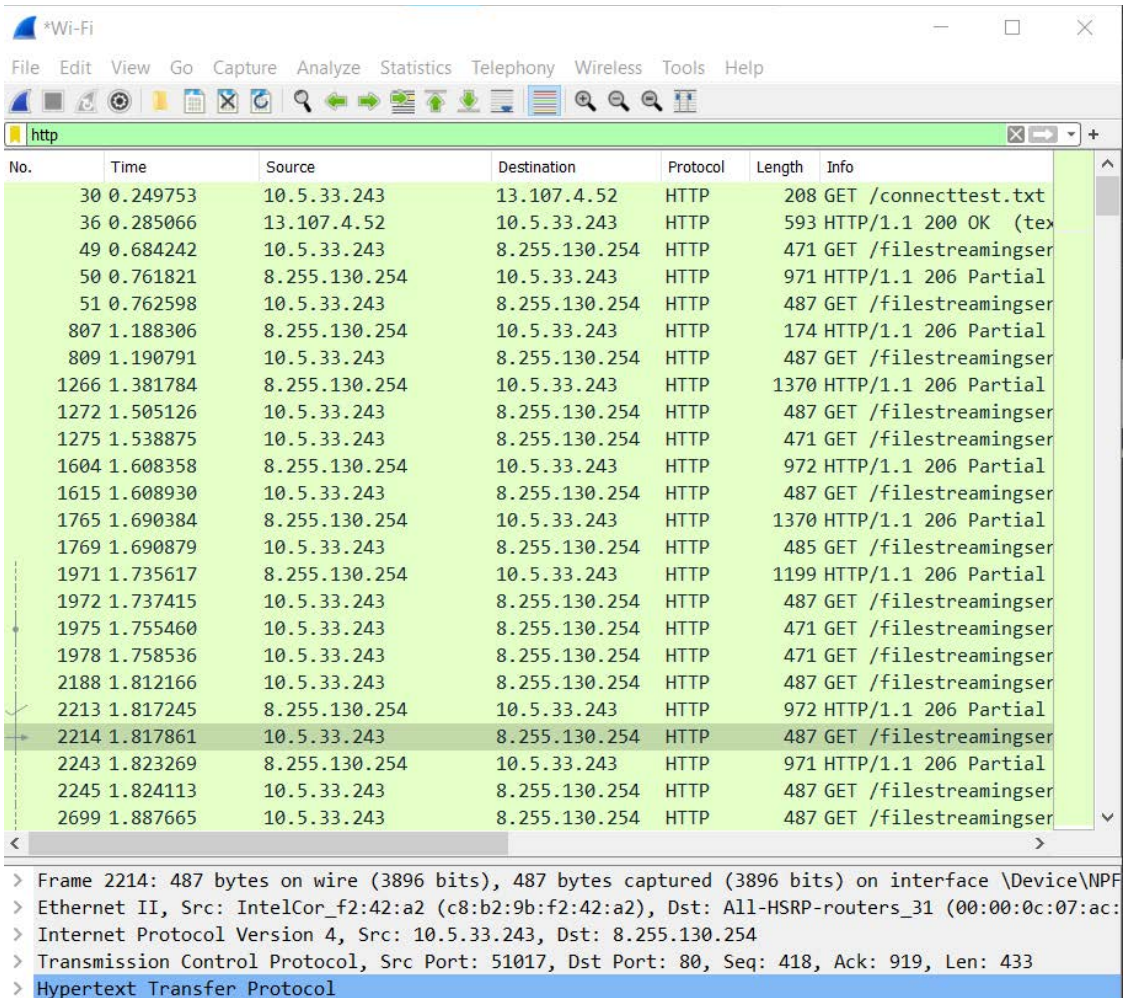
DNS Encapsulation Details

```
Frame 316200: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\N
  Interface id: 0 (\Device\NPF_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE})
  Encapsulation type: Ethernet (1)
  Arrival Time: Jul 30, 2022 14:11:55.156914000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1659170515.156914000 seconds
  [Time delta from previous captured frame: 0.002043000 seconds]
  [Time delta from previous displayed frame: 0.087761000 seconds]
  [Time since reference or first frame: 475.424452000 seconds]
  Frame Number: 316200
  Frame Length: 146 bytes (1168 bits)
  Capture Length: 146 bytes (1168 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: Cisco_b0:95:41 (70:6b:b9:b0:95:41), Dst: IntelCor_f2:42:a2 (c8:b2:9b:f2:42:a2)
  Destination: IntelCor_f2:42:a2 (c8:b2:9b:f2:42:a2)
  Source: Cisco_b0:95:41 (70:6b:b9:b0:95:41)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.104.10, Dst: 10.5.33.243
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 132
  Identification: 0x3e0b (15883)
  Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 63
  Protocol: UDP (17)
  Header Checksum: 0xa8b3 [validation disabled]
  [Header checksum status: Unverified]
```

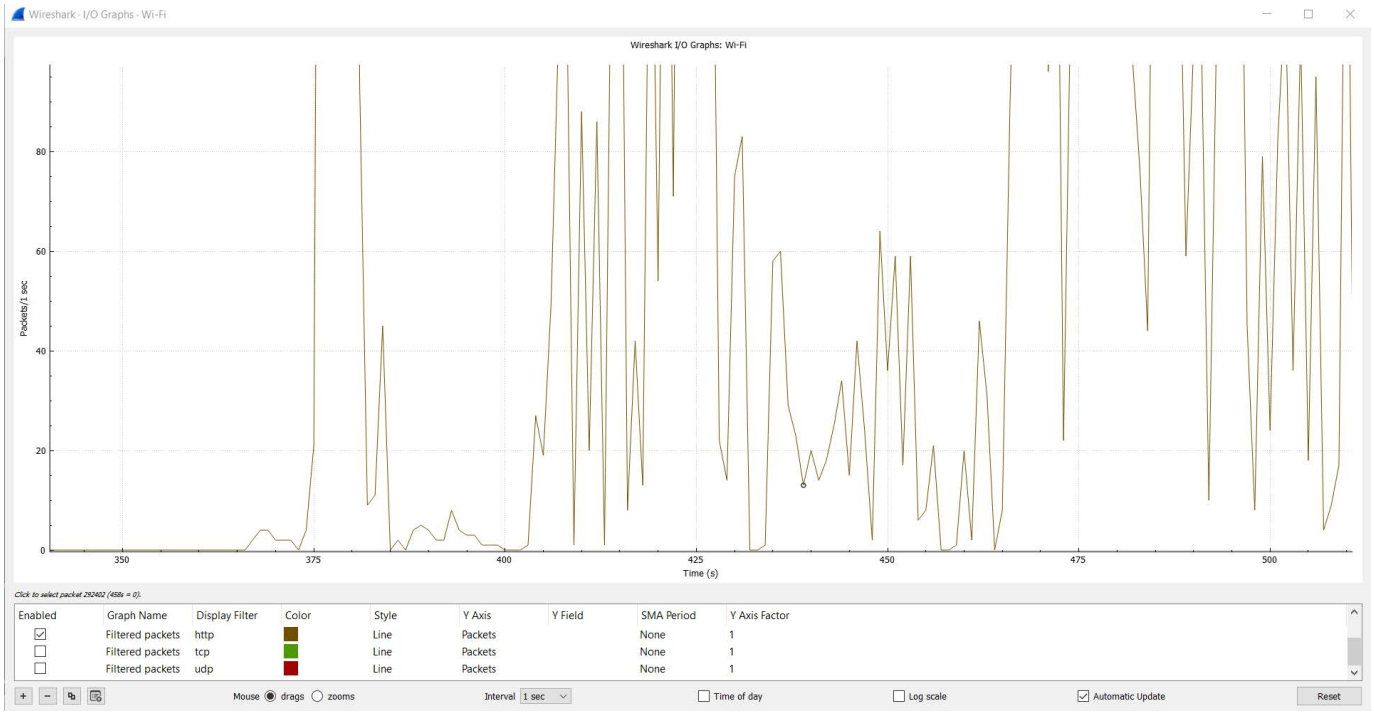
```
User Datagram Protocol, Src Port: 53, Dst Port: 63716
  Source Port: 53
  Destination Port: 63716
  Length: 112
  Checksum: 0x55b4 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 273]
  [Timestamps]
  UDP payload (104 bytes)
Domain Name System (response)
  Transaction ID: 0x6e5d
  Flags: 0x8183 Standard query response, No such name
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  Queries
  Authoritative nameservers
  [Request In: 315882]
  [Time: 0.087761000 seconds]
```



HTTP

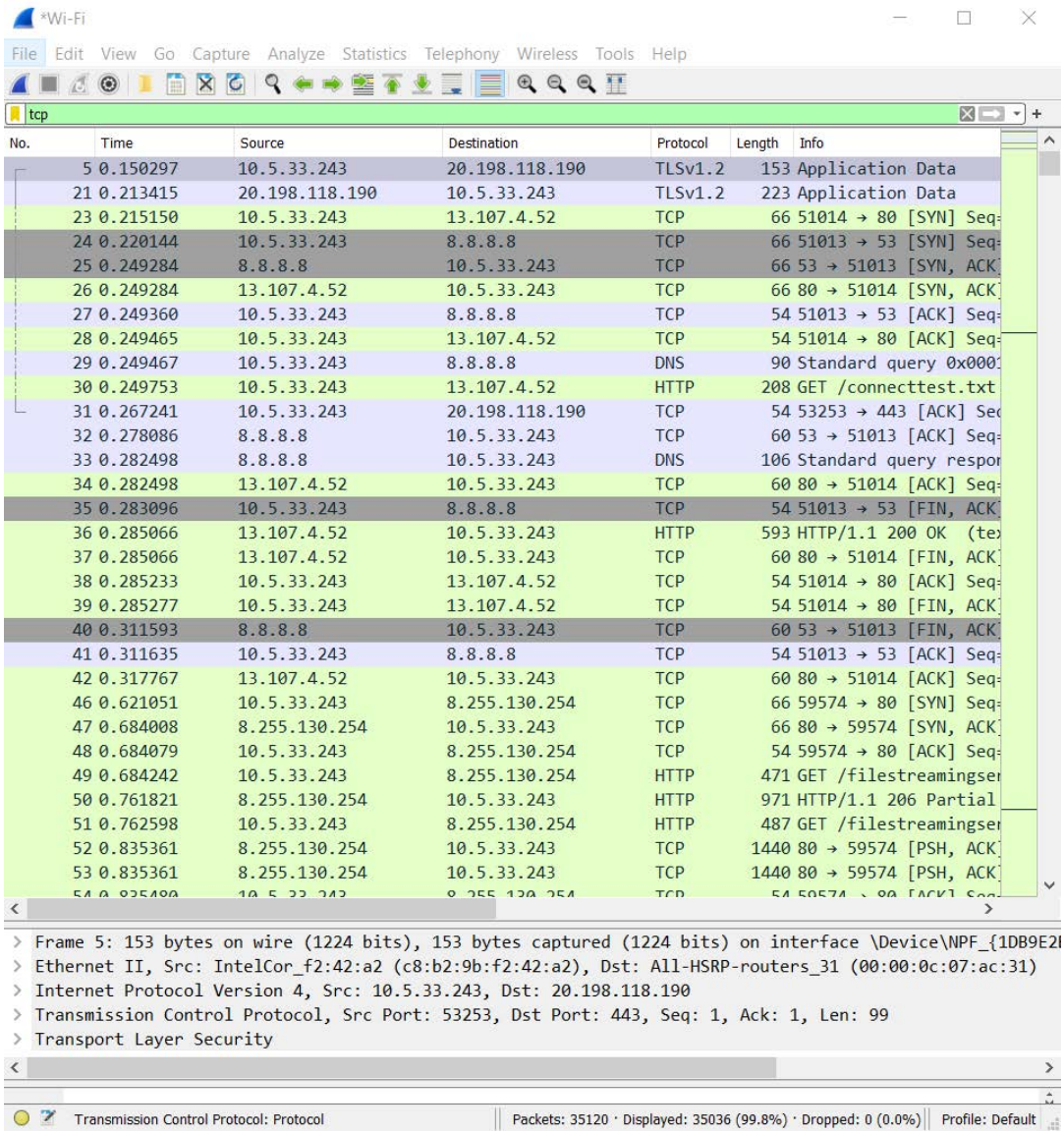


HTTP I/O Graph

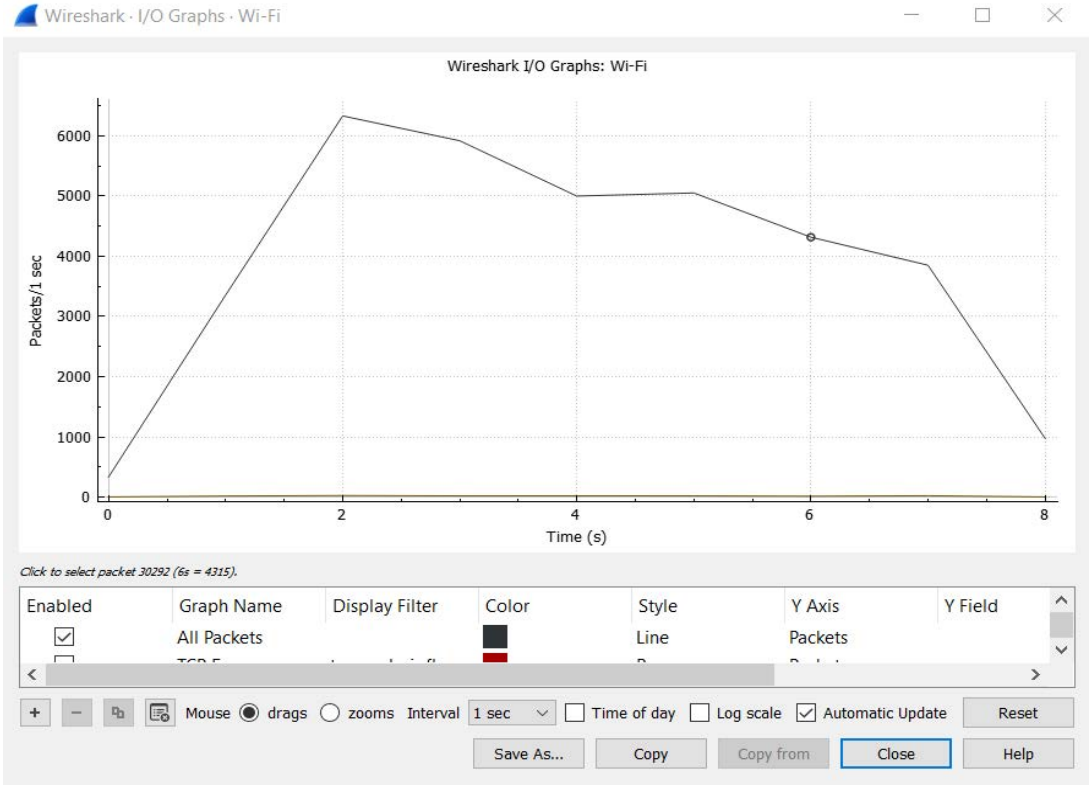


HTTP Encapsulation Details

TCP



TCP I/O Graph



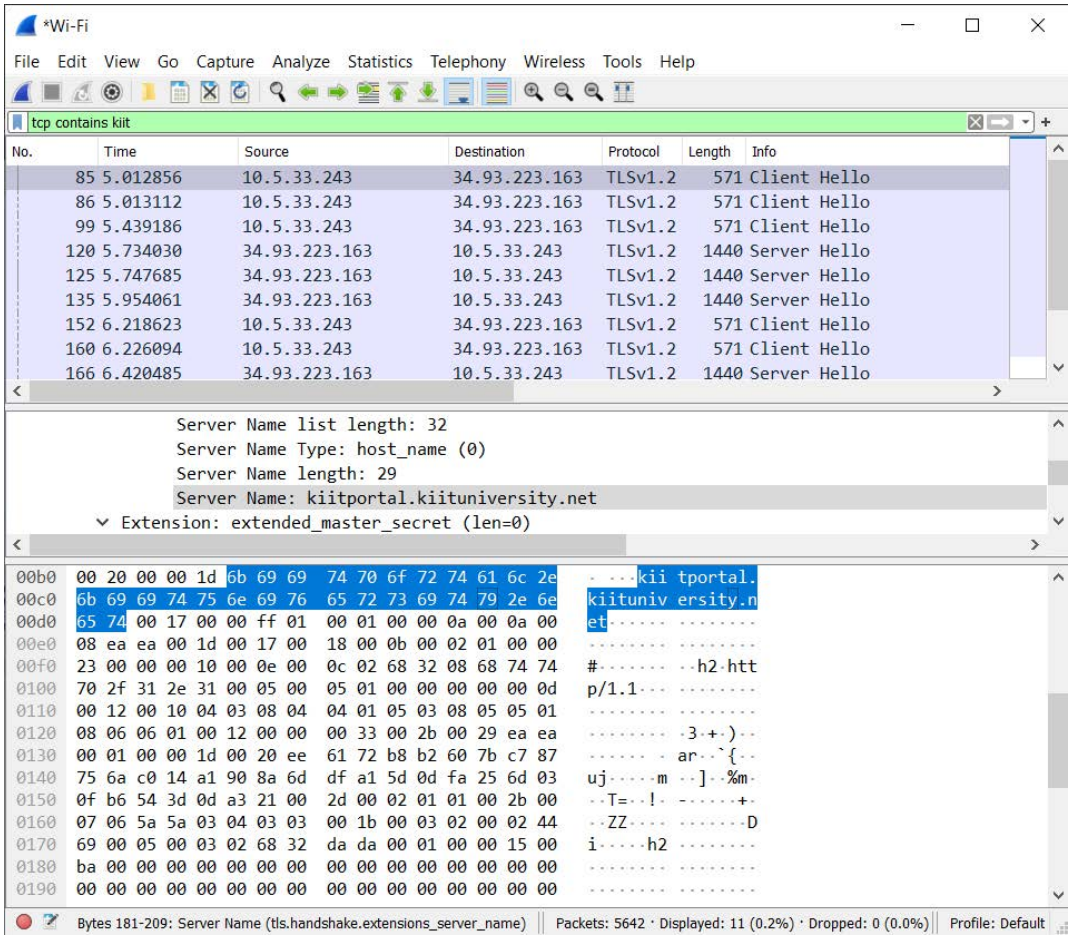
TCP Encapsulation Details

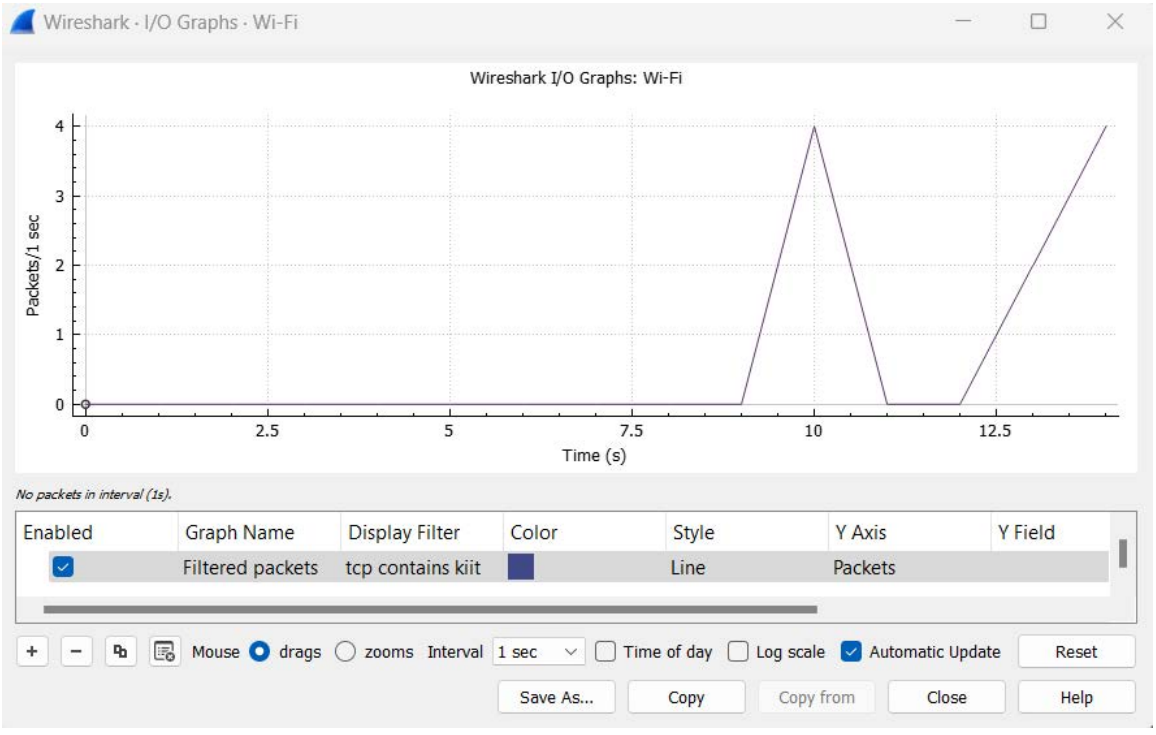
```
Frame 5: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interfac
  Interface id: 0 (\Device\NPF_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE})
  Encapsulation type: Ethernet (1)
  Arrival Time: Jul 30, 2022 14:23:12.522505000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1659171192.522505000 seconds
  [Time delta from previous captured frame: 0.000066000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.150297000 seconds]
  Frame Number: 5
  Frame Length: 153 bytes (1224 bits)
  Capture Length: 153 bytes (1224 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:tls]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
Ethernet II, Src: IntelCor_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-HSRP-routers_31
  Destination: All-HSRP-routers_31 (00:00:0c:07:ac:31)
  Source: IntelCor_f2:42:a2 (c8:b2:9b:f2:42:a2)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.5.33.243, Dst: 20.198.118.190
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 139
  Identification: 0x68ab (26795)
  Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.5.33.243
  Destination Address: 20.198.118.190
```

```
Transmission Control Protocol, Src Port: 53253, Dst Port: 443, Seq: 1,
  Source Port: 53253
  Destination Port: 443
  [Stream index: 0]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 99]
  Sequence Number: 1    (relative sequence number)
  Sequence Number (raw): 2427264007
  [Next Sequence Number: 100    (relative sequence number)]
  Acknowledgment Number: 1    (relative ack number)
  Acknowledgment number (raw): 2435123058
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 513
  [Calculated window size: 513]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xb7f9 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (99 bytes)
Transport Layer Security
  TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
```

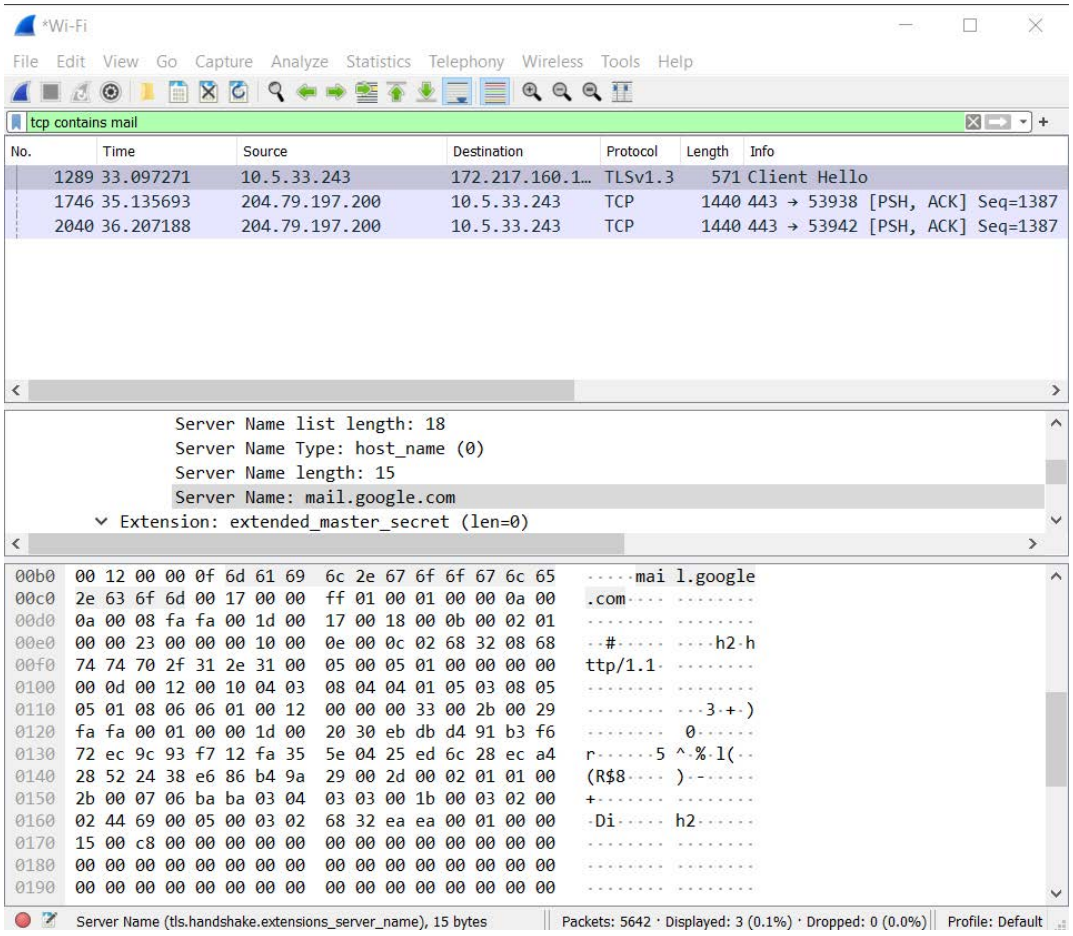
Ques 2. Capture packets for SAP Portal, Gmail, facebook seperately

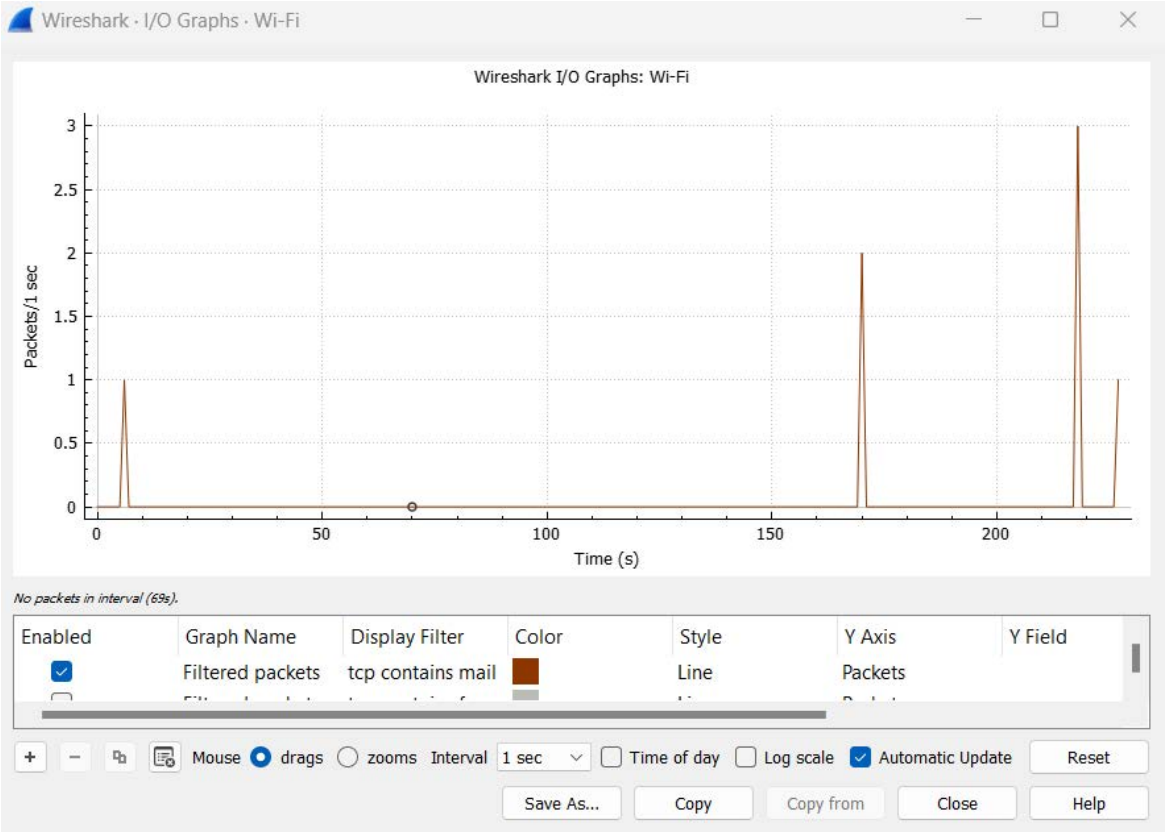
SAP



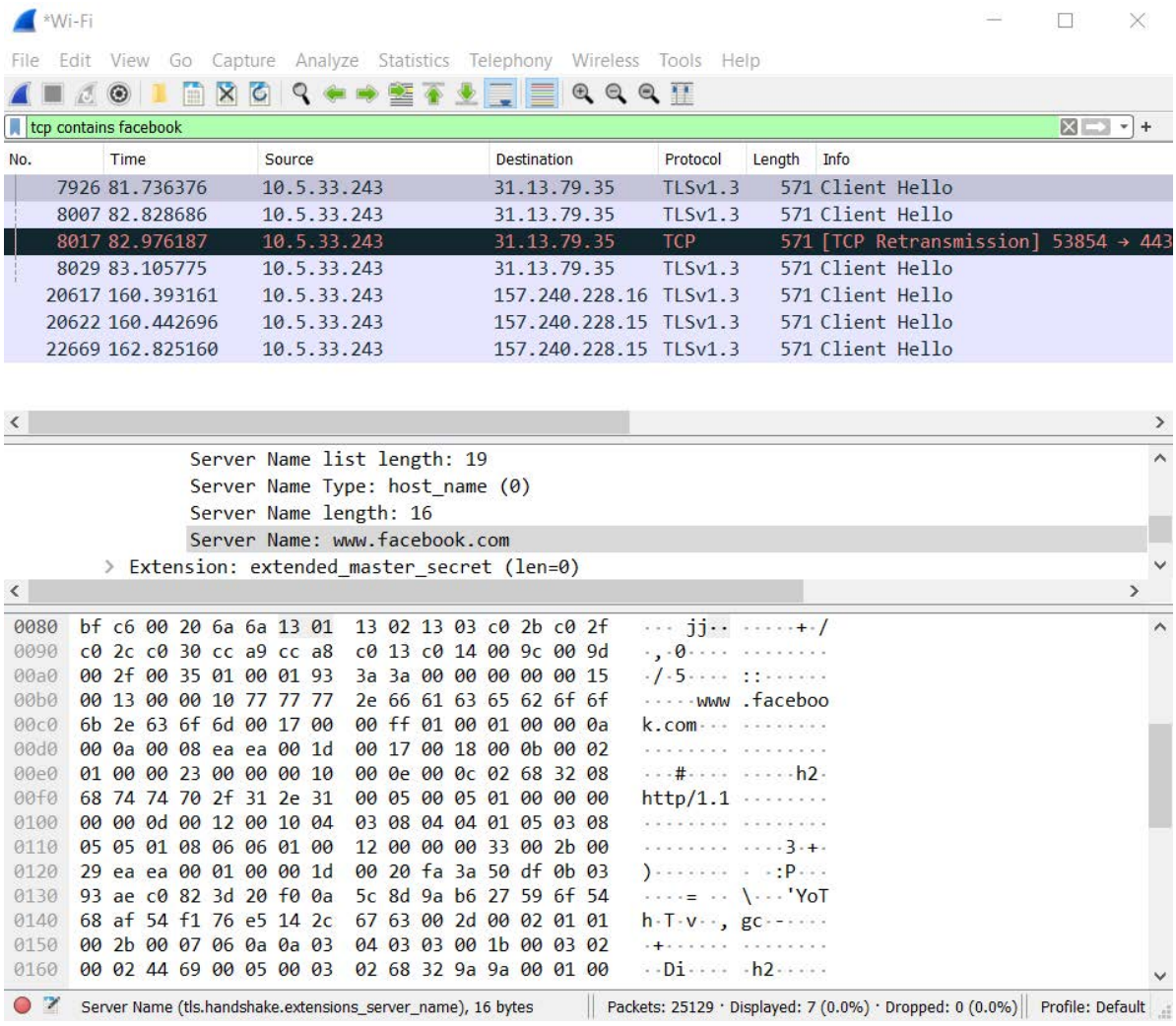


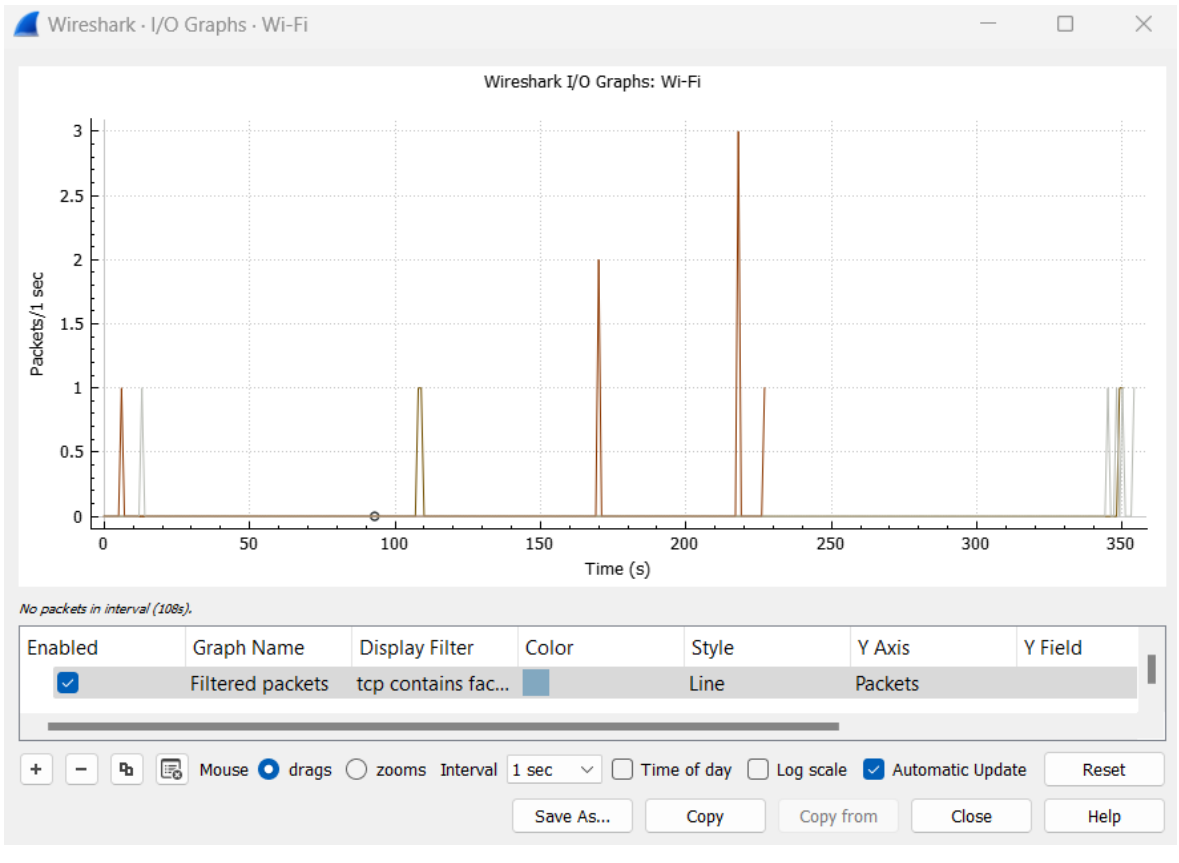
GMAIL


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp contains mail
No. Time Source Destination Protocol Length Info
1289 33.097271 10.5.33.243 172.217.160.1… TLSv1.3 571 Client Hello
1746 35.135693 204.79.197.200 10.5.33.243 TCP 1440 443 → 53938 [PSH, ACK] Seq=1387
2040 36.207188 204.79.197.200 10.5.33.243 TCP 1440 443 → 53942 [PSH, ACK] Seq=1387
Server Name list length: 18
Server Name Type: host_name (0)
Server Name length: 15
Server Name: mail.google.com
Extension: extended_master_secret (len=0)
00b0 00 12 00 00 0f 6d 61 69 6c 2e 67 6f 6f 67 6c 65 ·····mai l.google
00c0 2e 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 .com····
00d0 0a 00 08 fa fa 00 1d 00 17 00 18 00 0b 00 02 01
00e0 00 00 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 ··#····· ····h2·h
00f0 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 ttp/1.1·
0100 00 0d 00 12 00 10 04 03 08 04 04 01 05 03 08 05
0110 05 01 08 06 06 01 00 12 00 00 00 33 00 2b 00 29 ···3·+·)
0120 fa fa 00 01 00 00 1d 00 20 30 eb db d4 91 b3 f6 0·····
0130 72 ec 9c 93 f7 12 fa 35 5e 04 25 ed 6c 28 ec a4 r·····5 ^·%·l(··
0140 28 52 24 38 e6 86 b4 9a 29 00 2d 00 02 01 01 00 (R$8····)·-·····
0150 2b 00 07 06 ba ba 03 04 03 03 00 1b 00 03 02 00 +·····
0160 02 44 69 00 05 00 03 02 68 32 ea ea 00 01 00 00 ·Di····· h2·····
0170 15 00 c8 00 00 00 00 00 00 00 00 00 00 00 00 00
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Server Name (tls.handshake.extensions_server_name), 15 bytes
Packets: 5642 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%)
Profile: Default


Wireshark · I/O Graphs · Wi-Fi
Wireshark I/O Graphs: Wi-Fi
Packets/1 sec
Time (s)
No packets in interval (69s).
Enabled Graph Name Display Filter Color Style Y Axis Y Field
Filtered packets tcp contains mail Line Packets
Mouse drags zooms Interval 1 sec Time of day Log scale Automatic Update Reset
Save As... Copy Copy from Close Help

Facebook


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp contains facebook
No. Time Source Destination Protocol Length Info
7926 81.736376 10.5.33.243 31.13.79.35 TLSv1.3 571 Client Hello
8007 82.828686 10.5.33.243 31.13.79.35 TLSv1.3 571 Client Hello
8017 82.976187 10.5.33.243 31.13.79.35 TCP 571 [TCP Retransmission] 53854 → 443
8029 83.105775 10.5.33.243 31.13.79.35 TLSv1.3 571 Client Hello
20617 160.393161 10.5.33.243 157.240.228.16 TLSv1.3 571 Client Hello
20622 160.442696 10.5.33.243 157.240.228.15 TLSv1.3 571 Client Hello
22669 162.825160 10.5.33.243 157.240.228.15 TLSv1.3 571 Client Hello
Server Name list length: 19
Server Name Type: host_name (0)
Server Name length: 16
Server Name: www.facebook.com
Extension: extended_master_secret (len=0)
0080 bf c6 00 20 6a 6a 13 01 13 02 13 03 c0 2b c0 2f
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d
00a0 00 2f 00 35 01 00 01 93 3a 3a 00 00 00 00 00 15
00b0 00 13 00 00 10 77 77 77 2e 66 61 63 65 62 6f 6f
00c0 6b 2e 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a
00d0 00 0a 00 08 ea ea 00 1d 00 17 00 18 00 0b 00 02
00e0 01 00 00 23 00 00 00 10 00 0e 00 0c 02 68 32 08
00f0 68 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00
0100 00 00 0d 00 12 00 10 04 03 08 04 04 01 05 03 08
0110 05 05 01 08 06 06 01 00 12 00 00 00 33 00 2b 00
0120 29 ea ea 00 01 00 00 1d 00 20 fa 3a 50 df 0b 03
0130 93 ae c0 82 3d 20 f0 0a 5c 8d 9a b6 27 59 6f 54
0140 68 af 54 f1 76 e5 14 2c 67 63 00 2d 00 02 01 01
0150 00 2b 00 07 06 0a 0a 03 04 03 03 00 1b 00 03 02
0160 00 02 44 69 00 05 00 03 02 68 32 9a 9a 00 01 00
Server Name (tls.handshake.extensions_server_name), 16 bytes
Packets: 25129 · Displayed: 7 (0.0%) · Dropped: 0 (0.0%)
Profile: Default


Wireshark · I/O Graphs · Wi-Fi
Wireshark I/O Graphs: Wi-Fi
Packets/1 sec
Time (s)
No packets in interval (108s).
Enabled Graph Name Display Filter Color Style Y Axis Y Field
Filtered packets tcp contains fac... Line Packets
Mouse drags zooms Interval 1 sec Time of day Log scale Automatic Update Reset
Save As... Copy Copy from Close Help