

# LAB - 2

Ques 1: Display the filter output of the following filters

1. DNS
2. HTTP
3. TCP

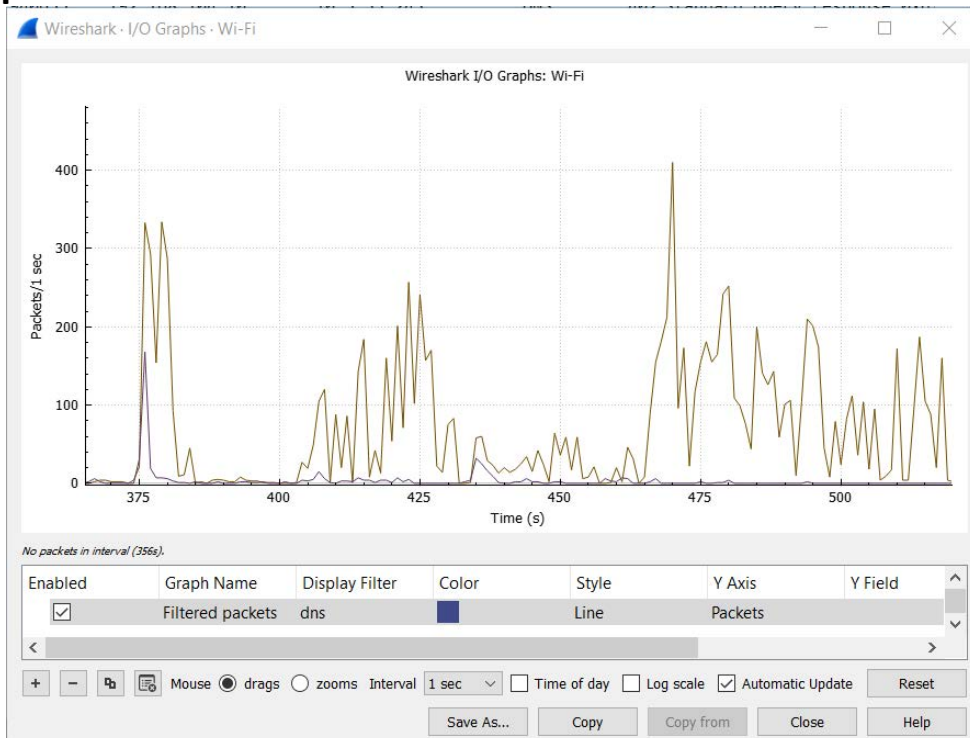
DNS

No.	Time	Source	Destination	Protocol	Length	Info
1571...	758.459214	192.168.104.10	10.5.33.243	DNS	326	Standard query response 0x594b /
1571...	758.452825	10.5.33.243	192.168.104.10	DNS	92	Standard query 0x594b A mobile.e
1491...	743.185885	192.168.104.10	10.5.33.243	DNS	146	Standard query response 0x6c10 h
1491...	743.121757	10.5.33.243	192.168.104.10	DNS	71	Standard query 0x6c10 A wpad.dhc
1460...	737.069796	192.168.104.10	10.5.33.243	DNS	336	Standard query response 0x4f6a /
1460...	737.063441	10.5.33.243	192.168.104.10	DNS	86	Standard query 0x4f6a A checkapp
1444...	734.051329	192.168.104.10	10.5.33.243	DNS	146	Standard query response 0xb739 h
1444...	733.982982	10.5.33.243	192.168.104.10	DNS	71	Standard query 0xb739 A wpad.dhc
1444...	733.980457	192.168.104.10	10.5.33.243	DNS	112	Standard query response 0x10c2 /
1444...	733.978136	10.5.33.243	192.168.104.10	DNS	70	Standard query 0x10c2 A dns.goog
1324...	713.025359	192.168.104.10	10.5.33.243	DNS	332	Standard query response 0x15a3 /
1324...	713.017875	10.5.33.243	192.168.104.10	DNS	92	Standard query 0x15a3 A mobile.e
1218...	692.878361	192.168.104.10	10.5.33.243	DNS	336	Standard query response 0x37f4 /
1218...	692.855946	10.5.33.243	192.168.104.10	DNS	92	Standard query 0x37f4 A mobile.e
1055...	663.099809	192.168.104.10	10.5.33.243	DNS	236	Standard query response 0x018f /
1055...	663.095508	10.5.33.243	192.168.104.10	DNS	103	Standard query 0x018f A img-proc
1050...	662.110099	8.8.8.8	10.5.33.243	DNS	182	Standard query response 0xd6b2 /
1050...	662.080986	192.168.104.10	10.5.33.243	DNS	272	Standard query response 0xd6b2 /
1050...	662.042661	10.5.33.243	8.8.8.8	DNS	71	Standard query 0xd6b2 A arc.msn.
1049...	662.016407	10.5.33.243	192.168.104.10	DNS	71	Standard query 0xd6b2 A arc.msn.
1041...	660.382032	192.168.104.10	10.5.33.243	DNS	398	Standard query response 0x8b7d /
1041...	660.375835	10.5.33.243	192.168.104.10	DNS	85	Standard query 0x8b7d A login.mi
8774...	629.015752	192.168.104.10	10.5.33.243	DNS	336	Standard query response 0x2131 /
8774...	629.011200	10.5.33.243	192.168.104.10	DNS	92	Standard query 0x2131 A mobile.e
7936...	613.181491	192.168.104.10	10.5.33.243	DNS	146	Standard query response 0xd710 h
7933...	613.119376	10.5.33.243	192.168.104.10	DNS	71	Standard query 0xd710 A wpad.dhc
7694...	608.413550	192.168.104.10	10.5.33.243	DNS	108	Standard query response 0x9e72 /
7694...	608.408871	10.5.33.243	192.168.104.10	DNS	76	Standard query 0x9e72 A dns.msfl
7522...	605.072368	192.168.104.10	10.5.33.243	DNS	352	Standard query response 0xbd46 /
7521...	605.065003	10.5.33.243	192.168.104.10	DNS	94	Standard query 0xbd46 A umatec

> Frame 316200: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF\_{1DB9E2B8-86E...  
> Ethernet II, Src: Cisco\_b0:95:41 (70:6b:b9:b0:95:41), Dst: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2)  
> Internet Protocol Version 4, Src: 192.168.104.10, Dst: 10.5.33.243  
> User Datagram Protocol, Src Port: 53, Dst Port: 63716  
> Domain Name System (response)

Domain Name System: Protocol | Packets: 1604695 · Displayed: 732 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

DNS I/O Graph



## DNS Encapsulation Details

▼ Frame 316200: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE}

- 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]

< >

Domain Name System: Protocol | Packets: 1604695 · Displayed: 732 (0.0%) · Dropped: 0 (0.0%) | Profile: Default



# HTTP

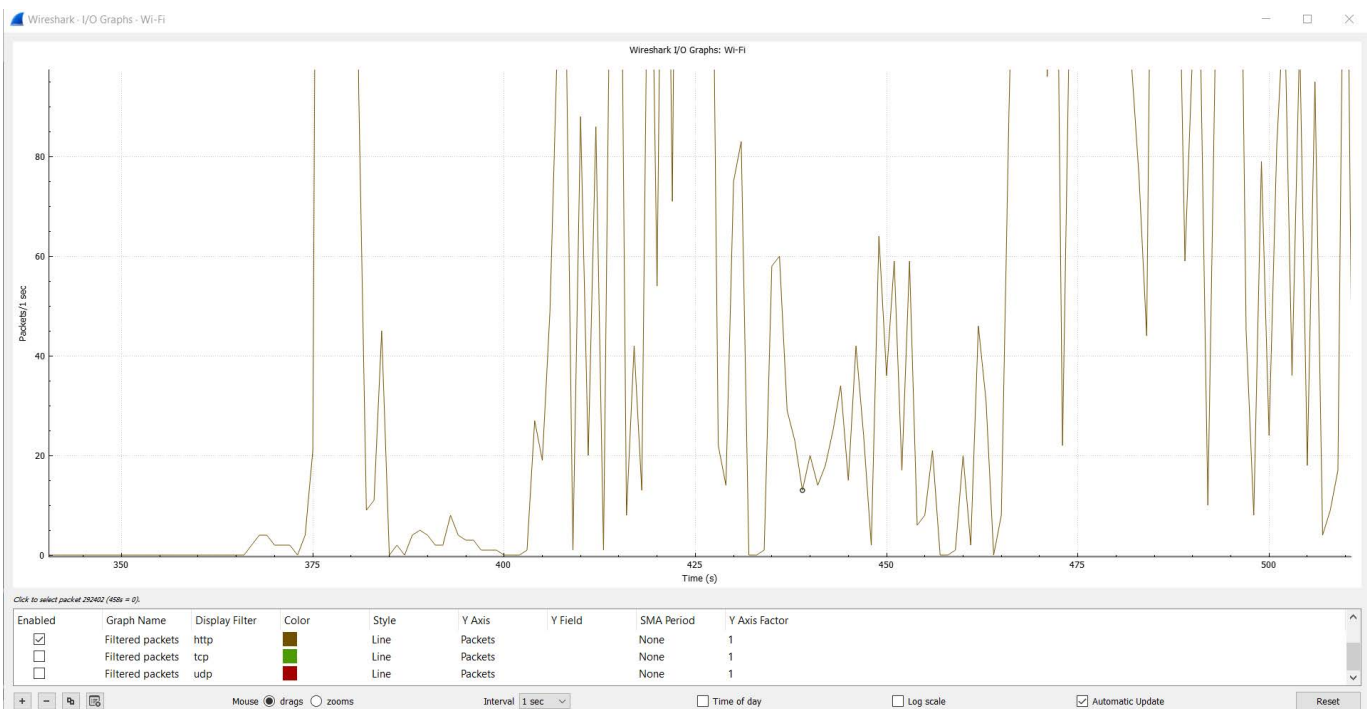
The screenshot shows the Wireshark network protocol analyzer interface. The title bar reads '\*Wi-Fi'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions like opening files, saving, zooming, and capturing. The main display area has a green filter bar set to 'http'.

No.	Time	Source	Destination	Protocol	Length	Info
30	0.249753	10.5.33.243	13.107.4.52	HTTP	208	GET /connecttest.txt
36	0.285066	13.107.4.52	10.5.33.243	HTTP	593	HTTP/1.1 200 OK (tex
49	0.684242	10.5.33.243	8.255.130.254	HTTP	471	GET /filestreamingser
50	0.761821	8.255.130.254	10.5.33.243	HTTP	971	HTTP/1.1 206 Partial
51	0.762598	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
807	1.188306	8.255.130.254	10.5.33.243	HTTP	174	HTTP/1.1 206 Partial
809	1.190791	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
1266	1.381784	8.255.130.254	10.5.33.243	HTTP	1370	HTTP/1.1 206 Partial
1272	1.505126	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
1275	1.538875	10.5.33.243	8.255.130.254	HTTP	471	GET /filestreamingser
1604	1.608358	8.255.130.254	10.5.33.243	HTTP	972	HTTP/1.1 206 Partial
1615	1.608930	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
1765	1.690384	8.255.130.254	10.5.33.243	HTTP	1370	HTTP/1.1 206 Partial
1769	1.690879	10.5.33.243	8.255.130.254	HTTP	485	GET /filestreamingser
1971	1.735617	8.255.130.254	10.5.33.243	HTTP	1199	HTTP/1.1 206 Partial
1972	1.737415	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
1975	1.755460	10.5.33.243	8.255.130.254	HTTP	471	GET /filestreamingser
1978	1.758536	10.5.33.243	8.255.130.254	HTTP	471	GET /filestreamingser
2188	1.812166	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
2213	1.817245	8.255.130.254	10.5.33.243	HTTP	972	HTTP/1.1 206 Partial
2214	1.817861	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
2243	1.823269	8.255.130.254	10.5.33.243	HTTP	971	HTTP/1.1 206 Partial
2245	1.824113	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
2699	1.887665	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser

Below the packet list, the details pane shows information for the selected frame (Frame 2214):

- > Frame 2214: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF{...}
- > Ethernet II, Src: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-MSRP-routers\_31 (00:00:0c:07:ac:1f)
- > Internet Protocol Version 4, Src: 10.5.33.243, Dst: 8.255.130.254
- > Transmission Control Protocol, Src Port: 51017, Dst Port: 80, Seq: 418, Ack: 919, Len: 433
- > Hypertext Transfer Protocol

## HTTP I/O Graph



# HTTP Encapsulation Details

- ▼ Frame 2214: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE}
  - > Interface id: 0 (\Device\NPF\_{1DB9E2B8-86E7-46E8-A0A9-C62914CE7CBE})
  - Encapsulation type: Ethernet (1)
  - Arrival Time: Jul 30, 2022 14:23:14.190069000 India Standard Time
  - [Time shift for this packet: 0.000000000 seconds]
  - Epoch Time: 1659171194.190069000 seconds
  - [Time delta from previous captured frame: 0.000616000 seconds]
  - [Time delta from previous displayed frame: 0.000616000 seconds]
  - [Time since reference or first frame: 1.817861000 seconds]
  - Frame Number: 2214
  - Frame Length: 487 bytes (3896 bits)
  - Capture Length: 487 bytes (3896 bits)
  - [Frame is marked: False]
  - [Frame is ignored: False]
  - [Protocols in frame: eth:ethertype:ip:tcp:http]
  - [Coloring Rule Name: HTTP]
  - [Coloring Rule String: http || tcp.port == 80 || http2]
- ▼ Ethernet II, Src: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-HSRP-routers\_31 (00:00:0c:07:ac: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: 8.255.130.254
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 473
  - Identification: 0x4348 (17224)
  - > 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: 8.255.130.254
- ▼ Transmission Control Protocol, Src Port: 51017, Dst Port: 80, Seq: 418, Ack: 919, Len: 433
  - Source Port: 51017
  - Destination Port: 80
  - Sequence Number: 418
  - Acknowledgment Number: 919
  - Window Size: 65535
  - Length: 433
  - Flags: 0x00000000, Reset, Urgent
  - Urgent Pointer: 0
  - Reset Sequence: 418
  - Reset Offset: 0
  - Urgent Pointer: 0
- ▼ Hypertext Transfer Protocol
  - > GET /filestreamingservice/files/c3352b3e-ddb3-450c-a243-795700e29fdb?P1=1659179985&P2=404&P3=404 HTTP/1.1
  - Connection: Keep-Alive\r\n
  - Accept: \*/\*\r\n
  - Range: bytes=292814848-293076991\r\n
  - User-Agent: Microsoft-Delivery-Optimization/10.0\r\n
  - MS-CV: 6a8/bKlrPkaSJCVE.1.1.33.90.7.10.1.2\r\n
  - > Content-Length: 0\r\n
  - Host: tlu.dl.delivery.mp.microsoft.com\r\n
  - \r\n
  - [Full request URI [truncated]: http://tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/c3352b3e-ddb3-450c-a243-795700e29fdb?P1=1659179985&P2=404&P3=404]
  - [HTTP request 2/13]
  - [Prev request in frame: 1975]
  - [Response in frame: 3695]
  - [Next request in frame: 3713]



TCP

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
5	0.150297	10.5.33.243	20.198.118.190	TLSv1.2	153	Application Data
21	0.213415	20.198.118.190	10.5.33.243	TLSv1.2	223	Application Data
23	0.215150	10.5.33.243	13.107.4.52	TCP	66	51014 → 80 [SYN] Seq=
24	0.220144	10.5.33.243	8.8.8.8	TCP	66	51013 → 53 [SYN] Seq=
25	0.249284	8.8.8.8	10.5.33.243	TCP	66	53 → 51013 [SYN, ACK]
26	0.249284	13.107.4.52	10.5.33.243	TCP	66	80 → 51014 [SYN, ACK]
27	0.249360	10.5.33.243	8.8.8.8	TCP	54	51013 → 53 [ACK] Seq=
28	0.249465	10.5.33.243	13.107.4.52	TCP	54	51014 → 80 [ACK] Seq=
29	0.249467	10.5.33.243	8.8.8.8	DNS	90	Standard query 0x0000
30	0.249753	10.5.33.243	13.107.4.52	HTTP	208	GET /connecttest.txt
31	0.267241	10.5.33.243	20.198.118.190	TCP	54	53253 → 443 [ACK] Seq=
32	0.278086	8.8.8.8	10.5.33.243	TCP	60	53 → 51013 [ACK] Seq=
33	0.282498	8.8.8.8	10.5.33.243	DNS	106	Standard query respon
34	0.282498	13.107.4.52	10.5.33.243	TCP	60	80 → 51014 [ACK] Seq=
35	0.283096	10.5.33.243	8.8.8.8	TCP	54	51013 → 53 [FIN, ACK]
36	0.285066	13.107.4.52	10.5.33.243	HTTP	593	HTTP/1.1 200 OK (tex
37	0.285066	13.107.4.52	10.5.33.243	TCP	60	80 → 51014 [FIN, ACK]
38	0.285233	10.5.33.243	13.107.4.52	TCP	54	51014 → 80 [ACK] Seq=
39	0.285277	10.5.33.243	13.107.4.52	TCP	54	51014 → 80 [FIN, ACK]
40	0.311593	8.8.8.8	10.5.33.243	TCP	60	53 → 51013 [FIN, ACK]
41	0.311635	10.5.33.243	8.8.8.8	TCP	54	51013 → 53 [ACK] Seq=
42	0.317767	13.107.4.52	10.5.33.243	TCP	60	80 → 51014 [ACK] Seq=
46	0.621051	10.5.33.243	8.255.130.254	TCP	66	59574 → 80 [SYN] Seq=
47	0.684008	8.255.130.254	10.5.33.243	TCP	66	80 → 59574 [SYN, ACK]
48	0.684079	10.5.33.243	8.255.130.254	TCP	54	59574 → 80 [ACK] Seq=
49	0.684242	10.5.33.243	8.255.130.254	HTTP	471	GET /filestreamingser
50	0.761821	8.255.130.254	10.5.33.243	HTTP	971	HTTP/1.1 206 Partial
51	0.762598	10.5.33.243	8.255.130.254	HTTP	487	GET /filestreamingser
52	0.835361	8.255.130.254	10.5.33.243	TCP	1440	80 → 59574 [PSH, ACK]
53	0.835361	8.255.130.254	10.5.33.243	TCP	1440	80 → 59574 [PSH, ACK]
54	0.925400	10.5.33.243	8.255.130.254	TCP	54	59574 → 80 [ACK] Seq=

> Frame 5: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface \Device\NPF\_{1DB9E21}

> Ethernet II, Src: IntelCor\_f2:42:a2 (c8:b2:9b:f2:42:a2), Dst: All-HSRP-routers\_31 (00:00:0c:07:ac:31)

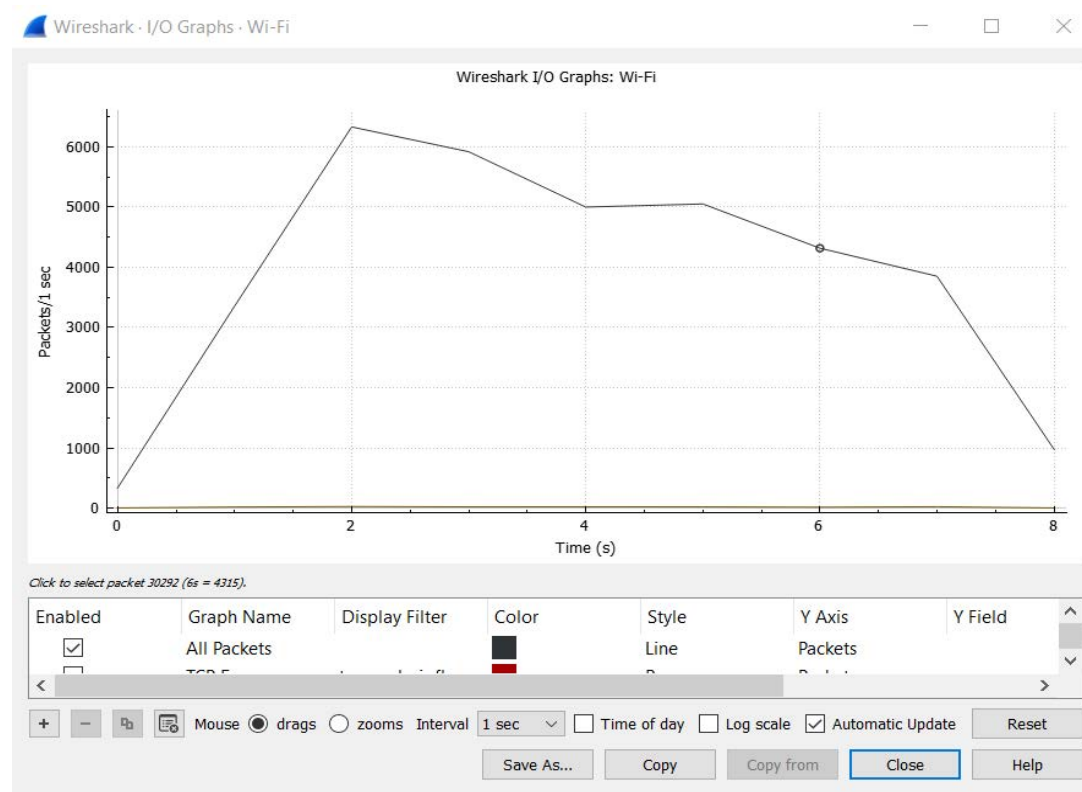
> Internet Protocol Version 4, Src: 10.5.33.243, Dst: 20.198.118.190

> Transmission Control Protocol, Src Port: 53253, Dst Port: 443, Seq: 1, Ack: 1, Len: 99

> Transport Layer Security

Transmission Control Protocol: Protocol | Packets: 35120 · Displayed: 35036 (99.8%) · Dropped: 0 (0.0%) | Profile: Default

TCP I/O Graph



## TCP Encapsulation Details

- ▼ Frame 5: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface
  - > 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

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains kiit

No.	Time	Source	Destination	Protocol	Length	Info
85	5.012856	10.5.33.243	34.93.223.163	TLSv1.2	571	Client Hello
86	5.013112	10.5.33.243	34.93.223.163	TLSv1.2	571	Client Hello
99	5.439186	10.5.33.243	34.93.223.163	TLSv1.2	571	Client Hello
120	5.734030	34.93.223.163	10.5.33.243	TLSv1.2	1440	Server Hello
125	5.747685	34.93.223.163	10.5.33.243	TLSv1.2	1440	Server Hello
135	5.954061	34.93.223.163	10.5.33.243	TLSv1.2	1440	Server Hello
152	6.218623	10.5.33.243	34.93.223.163	TLSv1.2	571	Client Hello
160	6.226094	10.5.33.243	34.93.223.163	TLSv1.2	571	Client Hello
166	6.420485	34.93.223.163	10.5.33.243	TLSv1.2	1440	Server Hello

Server Name list length: 32  
Server Name Type: host\_name (0)  
Server Name length: 29  
Server Name: kiitportal.kiituniversity.net  
Extension: extended\_master\_secret (len=0)

00b0 00 20 00 00 1d 6b 69 69 74 70 6f 72 74 61 6c 2e . . . . .kiit portal.  
00c0 6b 69 69 74 75 6e 69 76 65 72 73 69 74 79 2e 6e kiituniv ersity.n  
00d0 65 74 00 17 00 00 ff 01 00 01 00 00 0a 00 0a 00 et . . . . .  
00e0 08 ea ea 00 1d 00 17 00 18 00 0b 00 02 01 00 00 . . . . .  
00f0 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 74 74 # . . . . .h2.htt  
0100 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 0d p/1.1 . . . . .  
0110 00 12 00 10 04 03 08 04 04 01 05 03 08 05 05 01 . . . . .  
0120 08 06 06 01 00 12 00 00 00 33 00 2b 00 29 ea ea . . . . .3+. )..  
0130 00 01 00 00 1d 00 20 ee 61 72 b8 b2 60 7b c7 87 . . . . .ar. {..  
0140 75 6a c0 14 a1 90 8a 6d df a1 5d 0d fa 25 6d 03 uj . . . . .m .]. %m  
0150 0f b6 54 3d 0d a3 21 00 2d 00 02 01 01 00 2b 00 .T= . . . . .+  
0160 07 06 5a 5a 03 04 03 03 00 1b 00 03 02 00 02 44 .ZZ . . . . .D  
0170 69 00 05 00 03 02 68 32 da da 00 01 00 00 15 00 i . . . . .h2 . . . . .  
0180 ba 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 . . . . .

Bytes 181-209: Server Name (tls.handshake.extensions\_server\_name) | Packets: 5642 · Displayed: 11 (0.2%) · Dropped: 0 (0.0%) | Profile: Default



# GMAIL

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

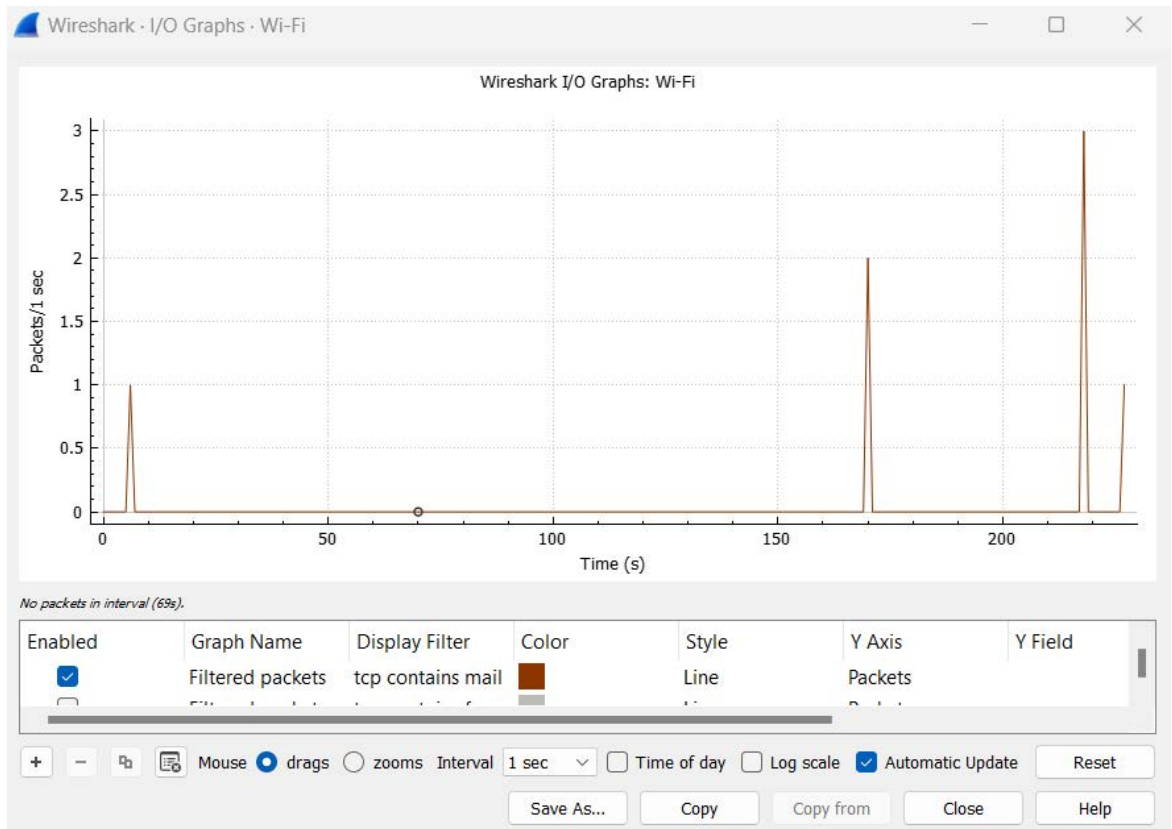
tcp contains mail

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 ^%.1(..  
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 .....  
0180 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 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





# 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 ... jj... ..+./  
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d ... 0... ..  
00a0 00 2f 00 35 01 00 01 93 3a 3a 00 00 00 00 15 ... /-5... ::...  
00b0 00 13 00 00 10 77 77 77 2e 66 61 63 65 62 6f 6f ... www .faceboo  
00c0 6b 2e 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a k.com... ..  
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 ... #... ..h2.  
00f0 68 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 http/1.1 ... ..  
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 ... ..3+..  
0120 29 ea ea 00 01 00 00 1d 00 20 fa 3a 50 df 0b 03 )... ..:P..  
0130 93 ae c0 82 3d 20 f0 0a 5c 8d 9a b6 27 59 6f 54 ... = .. \...'YoT  
0140 68 af 54 f1 76 e5 14 2c 67 63 00 2d 00 02 01 01 h-T-v... , gc...  
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 ...Di... ..h2...

Server Name (tls.handshake.extensions\_server\_name), 16 bytes | Packets: 25129 · Displayed: 7 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

