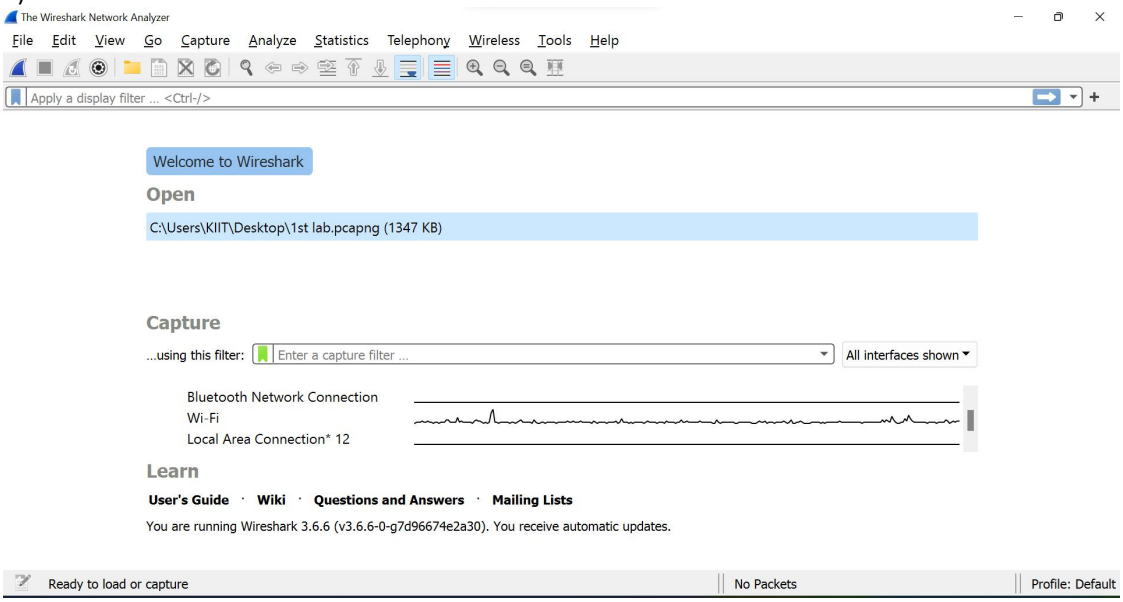
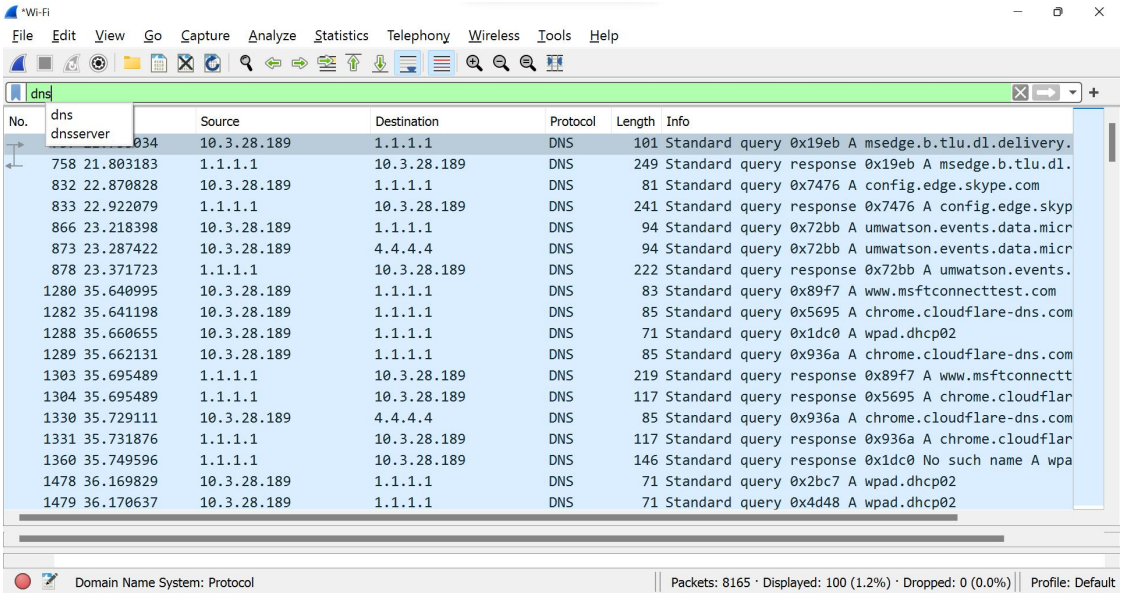
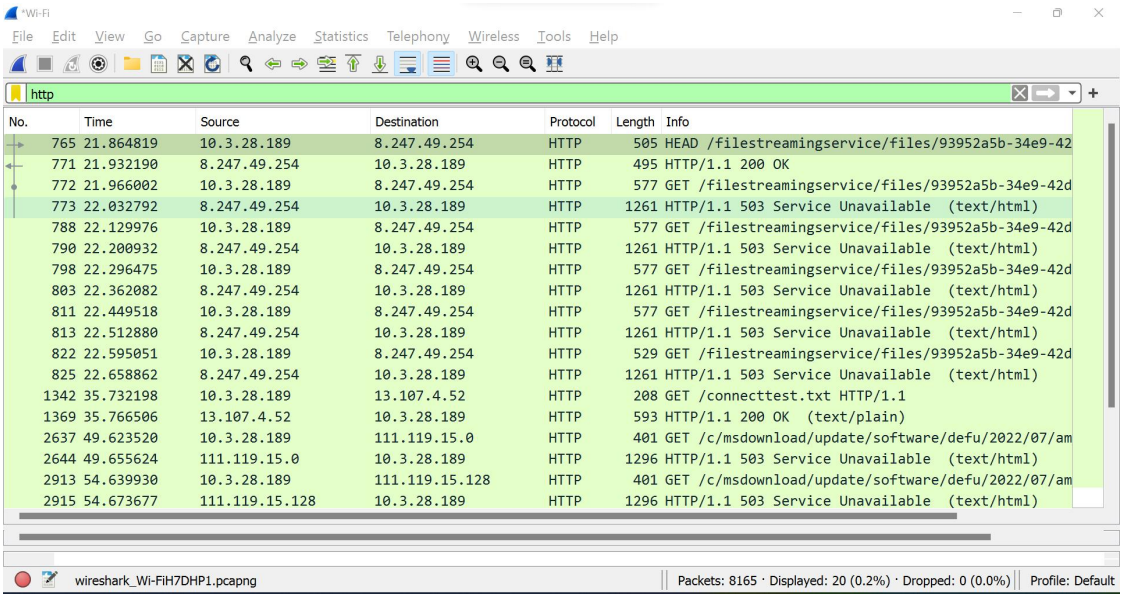
Aditya Nigam 20051634

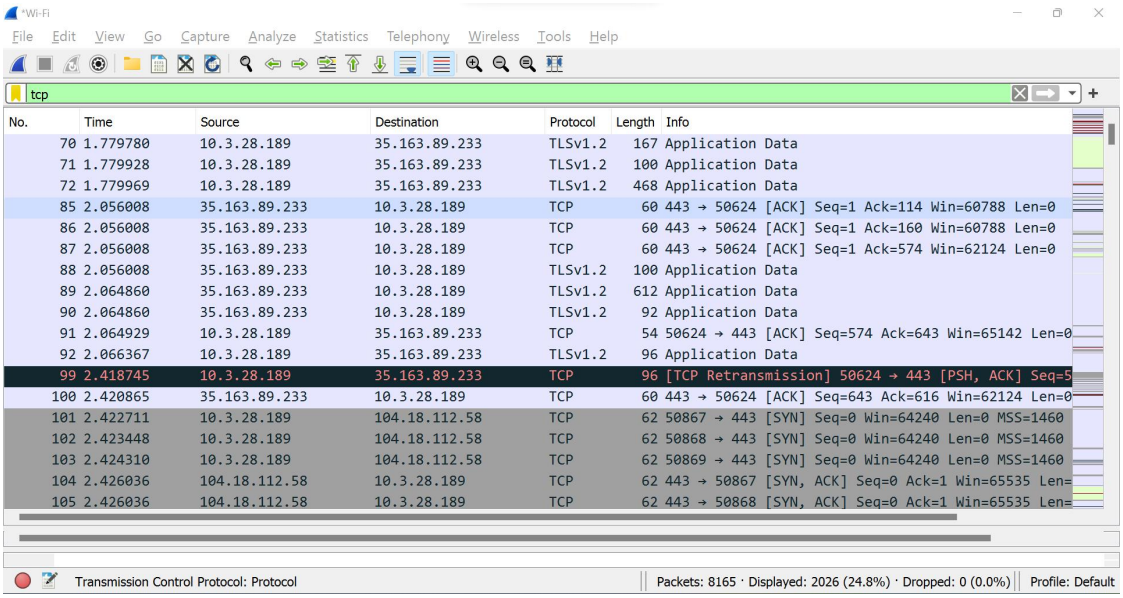
1)



2)Filter Output
DNS HTTP TCP

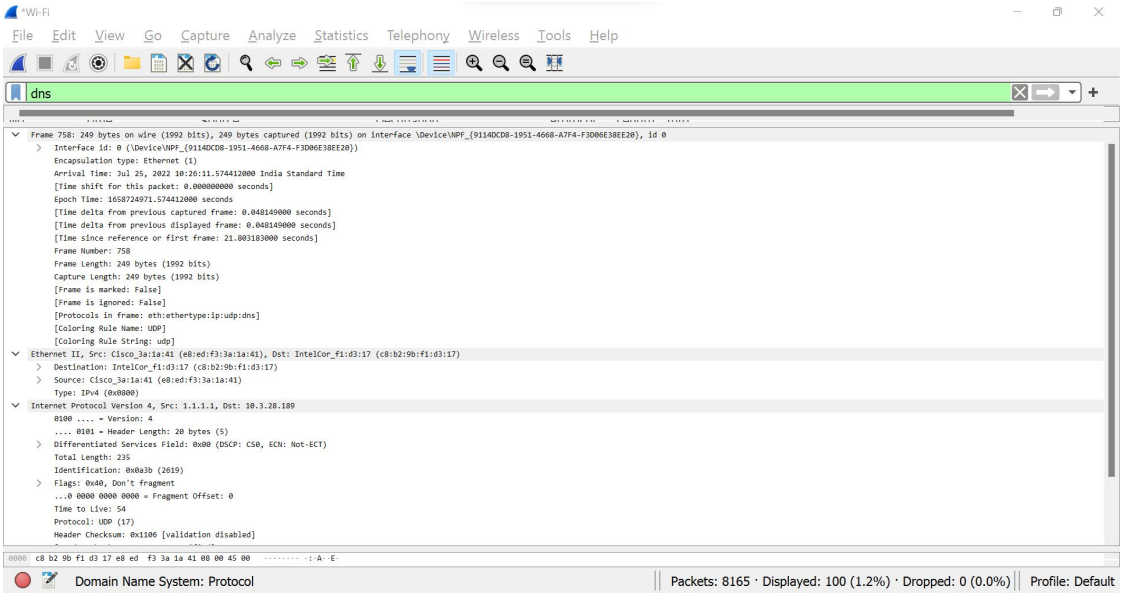


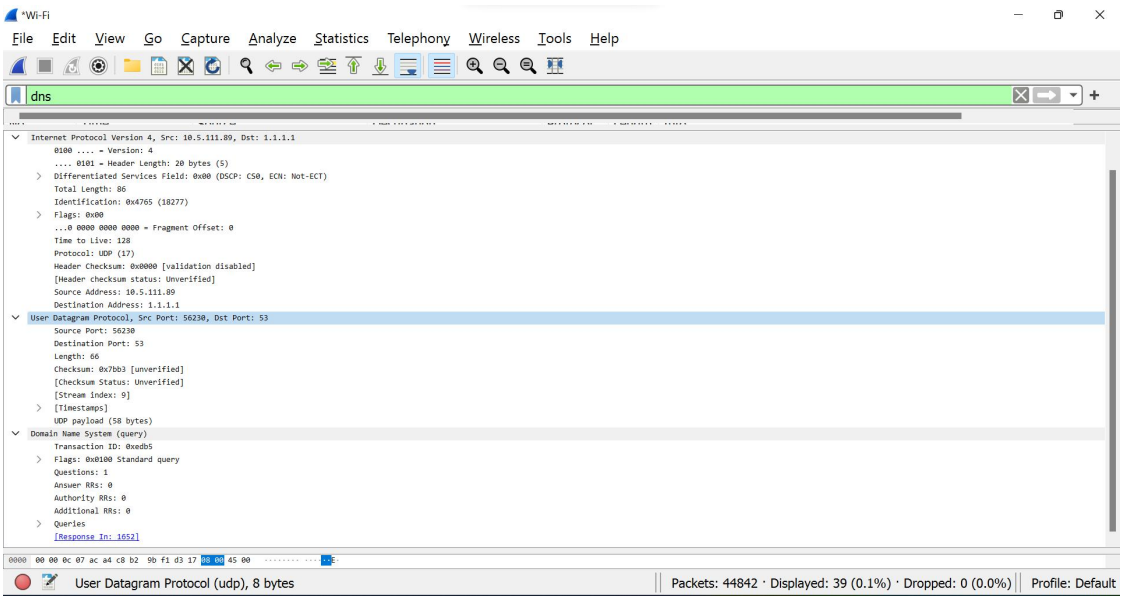


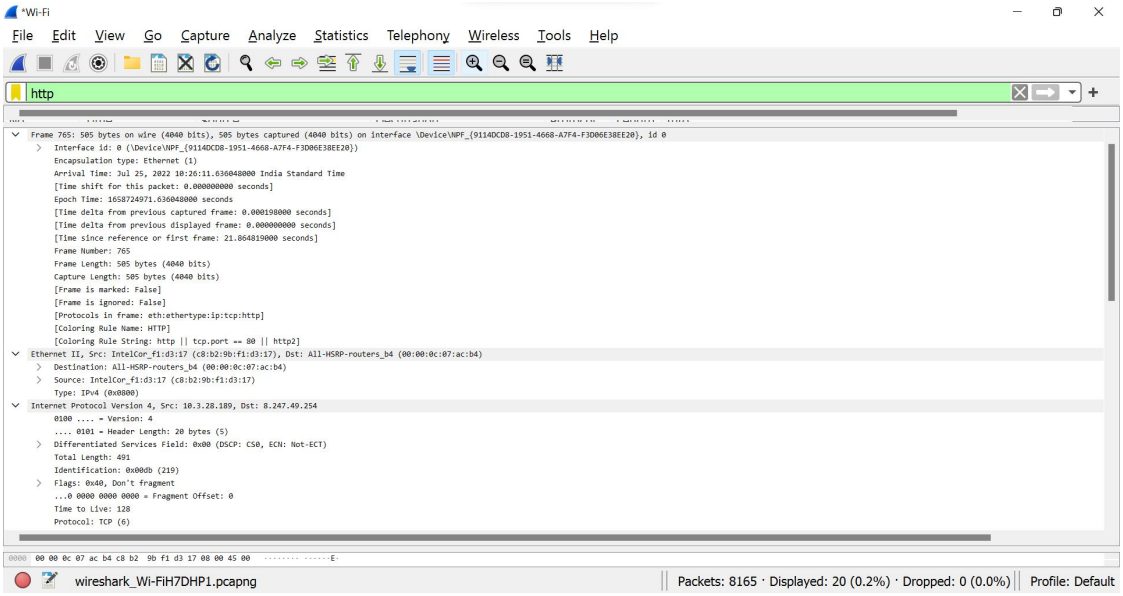


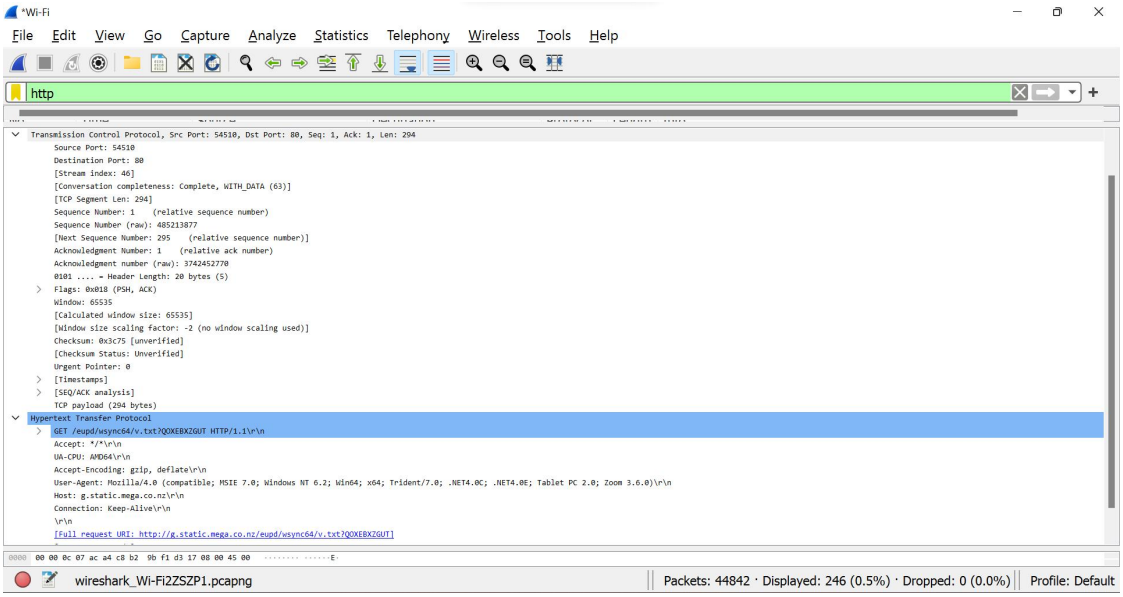
3) Encapsulation

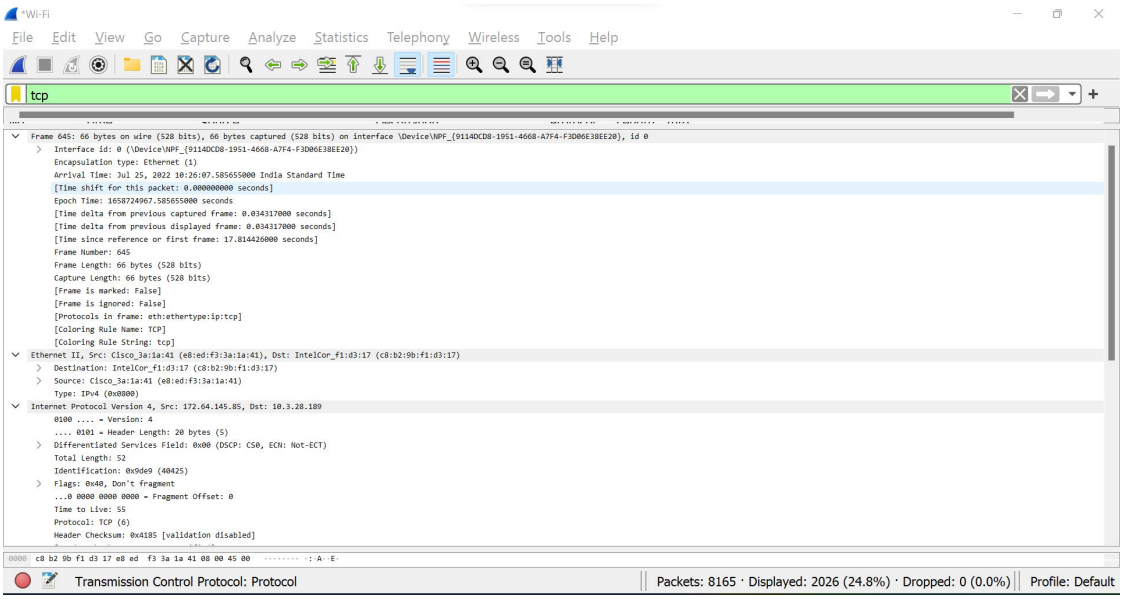
DNS FRAMES AND ETHERNET

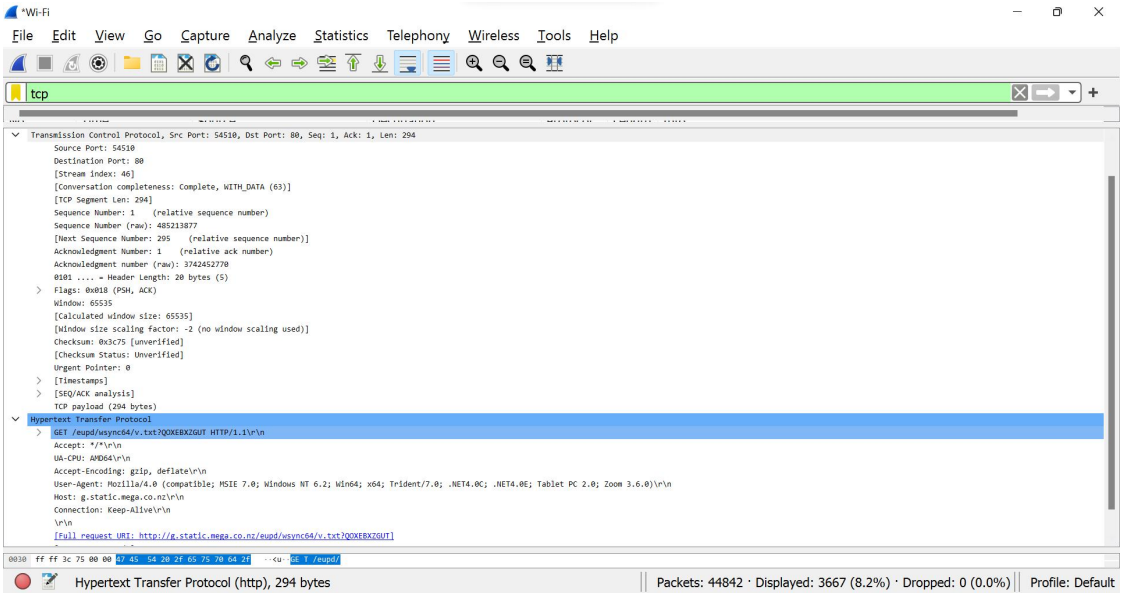




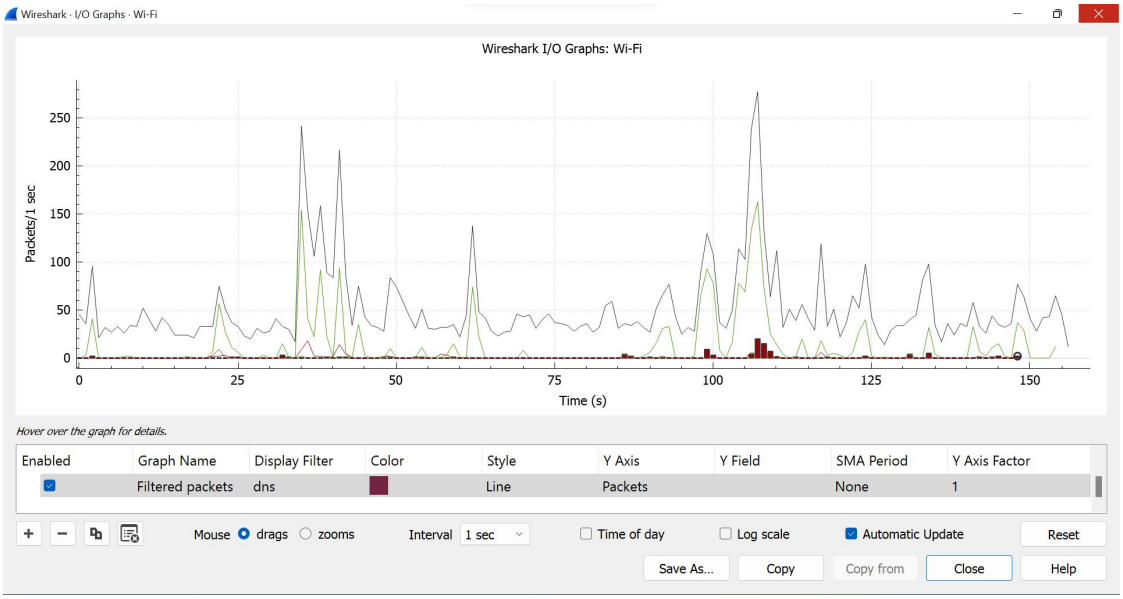

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Frame 765: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface \Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20}, id 0
Interface id: 0 (\Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20})
Encapsulation type: Ethernet (1)
Arrival Time: Jul 25, 2022 10:26:11.636048000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1658724971.636048000 seconds
[Time delta from previous captured frame: 0.000198000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 21.864819000 seconds]
Frame Number: 765
Frame Length: 505 bytes (4040 bits)
Capture Length: 505 bytes (4040 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_f1:d3:17 (c8:b2:9b:f1:d3:17), Dst: All-HSRP-routers_b4 (00:00:0c:07:ac:b4)
Destination: All-HSRP-routers_b4 (00:00:0c:07:ac:b4)
Source: IntelCor_f1:d3:17 (c8:b2:9b:f1:d3:17)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.3.28.189, Dst: 8.247.49.254
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 491
Identification: 0x00db (219)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
0000 00 00 0c 07 ac b4 c8 b2 9b f1 d3 17 08 00 45 00
wireshark_Wi-FiH7DHP1.pcapng
Packets: 8165 · Displayed: 20 (0.2%) · Dropped: 0 (0.0%)
Profile: Default

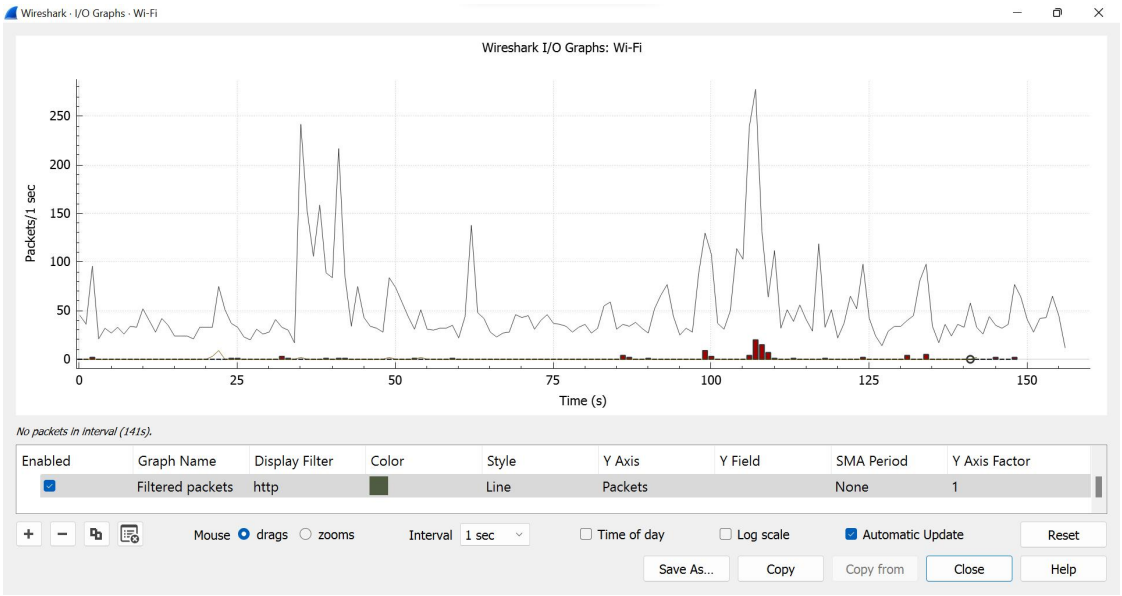

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Transmission Control Protocol, Src Port: 54510, Dst Port: 80, Seq: 1, Ack: 1, Len: 294
Source Port: 54510
Destination Port: 80
[Stream index: 46]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 294]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 485213877
[Next Sequence Number: 295 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3742452770
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x3c75 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (294 bytes)
Hypertext Transfer Protocol
GET /eupd/wsync64/v.txt?QOXEBXZGUT HTTP/1.1\r\n
Accept: */*\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; Tablet PC 2.0; Zoom 3.6.0)\r\n
Host: g.static.mega.co.nz\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://g.static.mega.co.nz/eupd/wsync64/v.txt?QOXEBXZGUT]
0000 00 00 0c 07 ac a4 c8 b2 9b f1 d3 17 08 00 45 00
wireshark_Wi-Fi2ZSZP1.pcapng
Packets: 44842 · Displayed: 246 (0.5%) · Dropped: 0 (0.0%)
Profile: Default

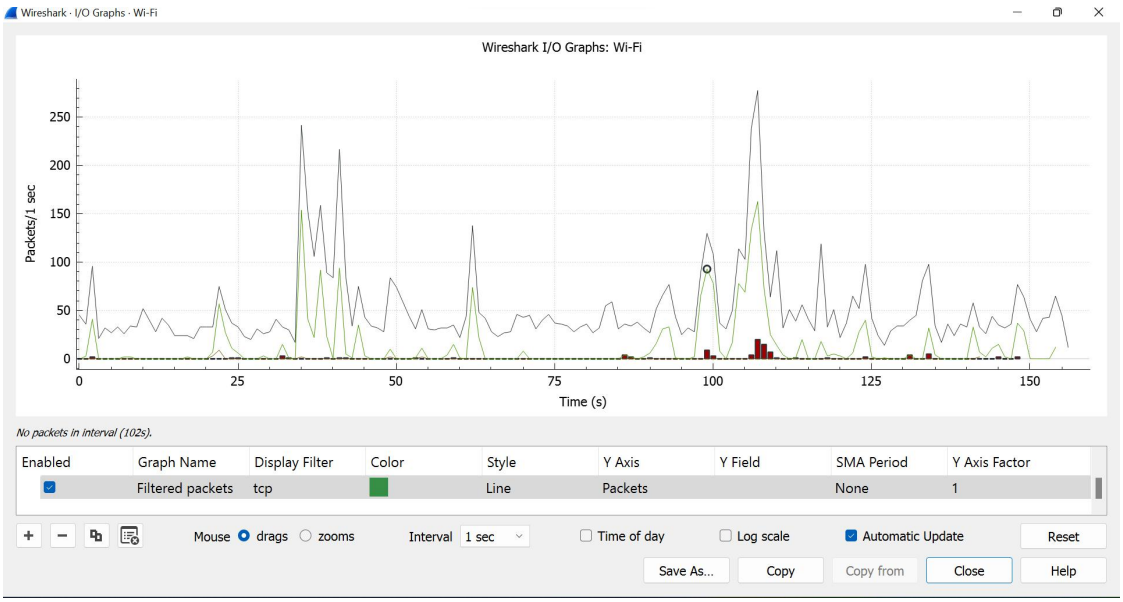

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Frame 645: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20}, id 0
Interface id: 0 (\Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20})
Encapsulation type: Ethernet (1)
Arrival Time: Jul 25, 2022 10:26:07.585655000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1658724967.585655000 seconds
[Time delta from previous captured frame: 0.034317000 seconds]
[Time delta from previous displayed frame: 0.034317000 seconds]
[Time since reference or first frame: 17.814426000 seconds]
Frame Number: 645
Frame Length: 66 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Cisco_3a:1a:41 (e8:ed:f3:3a:1a:41), Dst: IntelCor_f1:d3:17 (c8:b2:9b:f1:d3:17)
Destination: IntelCor_f1:d3:17 (c8:b2:9b:f1:d3:17)
Source: Cisco_3a:1a:41 (e8:ed:f3:3a:1a:41)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.64.145.85, Dst: 10.3.28.189
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x9de9 (40425)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 55
Protocol: TCP (6)
Header Checksum: 0x4185 [validation disabled]
0000 c8 b2 9b f1 d3 17 e8 ed f3 3a 1a 41 08 00 45 00
Transmission Control Protocol: Protocol
Packets: 8165 · Displayed: 2026 (24.8%) · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Transmission Control Protocol, Src Port: 54510, Dst Port: 80, Seq: 1, Ack: 1, Len: 294
Source Port: 54510
Destination Port: 80
[Stream index: 46]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 294]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 485213877
[Next Sequence Number: 295 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3742452770
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x3c75 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (294 bytes)
Hypertext Transfer Protocol
GET /eupd/wsync64/v.txt?QOXEBXZGUT HTTP/1.1\r\n
Accept: */*\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; Tablet PC 2.0; Zoom 3.6.0)\r\n
Host: g.static.mega.co.nz\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://g.static.mega.co.nz/eupd/wsync64/v.txt?QOXEBXZGUT]
Hypertext Transfer Protocol (http), 294 bytes
Packets: 44842 · Displayed: 3667 (8.2%) · Dropped: 0 (0.0%)
Profile: Default

IO GRAPH

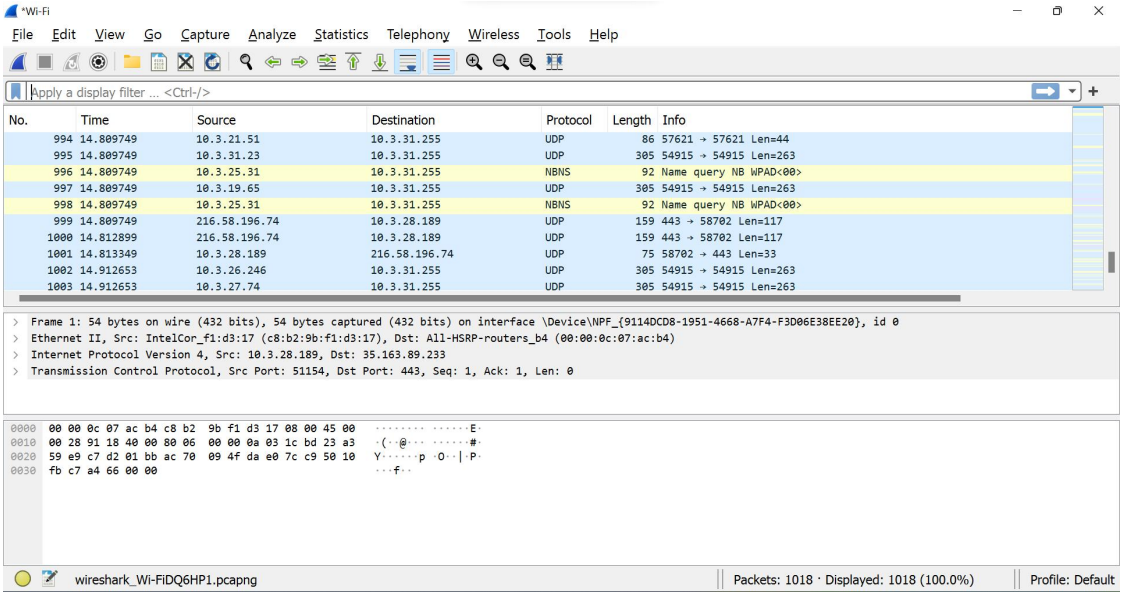

Wireshark · I/O Graphs · Wi-Fi
Wireshark I/O Graphs: Wi-Fi
Packets/1 sec
Time (s)
Hover over the graph for details.
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period Y Axis Factor
Filtered packets dns Line Packets None 1
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Automatic Update
Reset
Save As...
Copy
Copy from
Close
Help


Wireshark · I/O Graphs · Wi-Fi
Wireshark I/O Graphs: Wi-Fi
Packets/1 sec
Time (s)
No packets in interval (141s).
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period Y Axis Factor
Filtered packets http Line Packets None 1
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Automatic Update
Reset
Save As...
Copy
Copy from
Close
Help

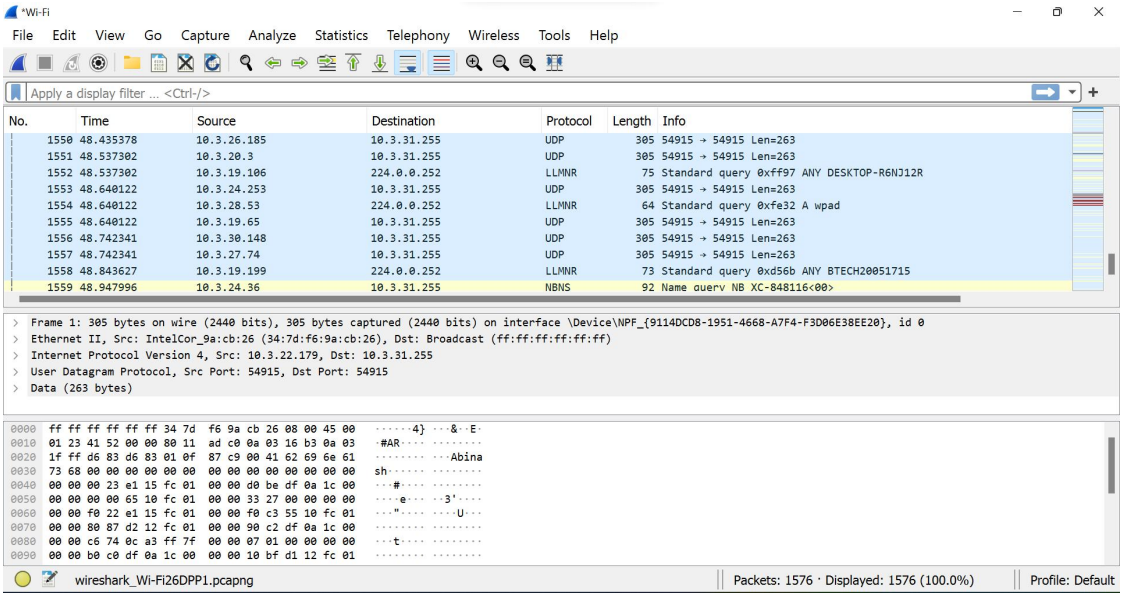


2)

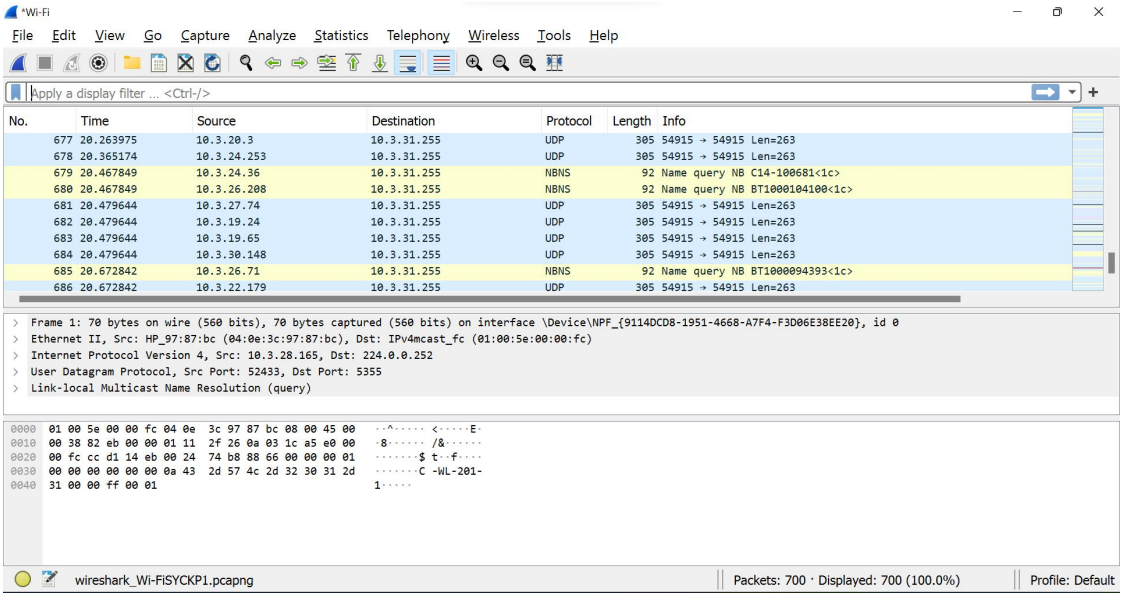
Gmail



SAP



FB


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
677 20.263975 10.3.20.3 10.3.31.255 UDP 305 54915 → 54915 Len=263
678 20.365174 10.3.24.253 10.3.31.255 UDP 305 54915 → 54915 Len=263
679 20.467849 10.3.24.36 10.3.31.255 NBNS 92 Name query NB C14-100681<1c>
680 20.467849 10.3.26.208 10.3.31.255 NBNS 92 Name query NB BT1000104100<1c>
681 20.479644 10.3.27.74 10.3.31.255 UDP 305 54915 → 54915 Len=263
682 20.479644 10.3.19.24 10.3.31.255 UDP 305 54915 → 54915 Len=263
683 20.479644 10.3.19.65 10.3.31.255 UDP 305 54915 → 54915 Len=263
684 20.479644 10.3.30.148 10.3.31.255 UDP 305 54915 → 54915 Len=263
685 20.672842 10.3.26.71 10.3.31.255 NBNS 92 Name query NB BT1000094393<1c>
686 20.672842 10.3.22.179 10.3.31.255 UDP 305 54915 → 54915 Len=263
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E3BEE20}, id 0
Ethernet II, Src: HP_97:87:bc (04:0e:3c:97:87:bc), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
Internet Protocol Version 4, Src: 10.3.28.165, Dst: 224.0.0.252
User Datagram Protocol, Src Port: 52433, Dst Port: 5355
Link-local Multicast Name Resolution (query)
0000 01 00 5e 00 00 fc 04 0e 3c 97 87 bc 08 00 45 00
0010 00 38 82 eb 00 00 01 11 2f 26 0a 03 1c a5 e0 00
0020 00 fc cc d1 14 eb 00 24 74 b8 88 66 00 00 00 01
0030 00 00 00 00 00 00 0a 43 2d 57 4c 2d 32 30 31 2d
0040 31 00 00 ff 00 01
wireshark_Wi-FiSYCKP1.pcapng
Packets: 700 · Displayed: 700 (100.0%)
Profile: Default