Date:

EXPERIMENT NO. 8

AIM: Capturing and analyzing network protocol traffic at different layers of the protocol stack.

Tools required:

- Desktop computer
- Wireshark

Submission: Written file submission is expected with each student ensuring the uniqueness of their submission.

Understanding Require

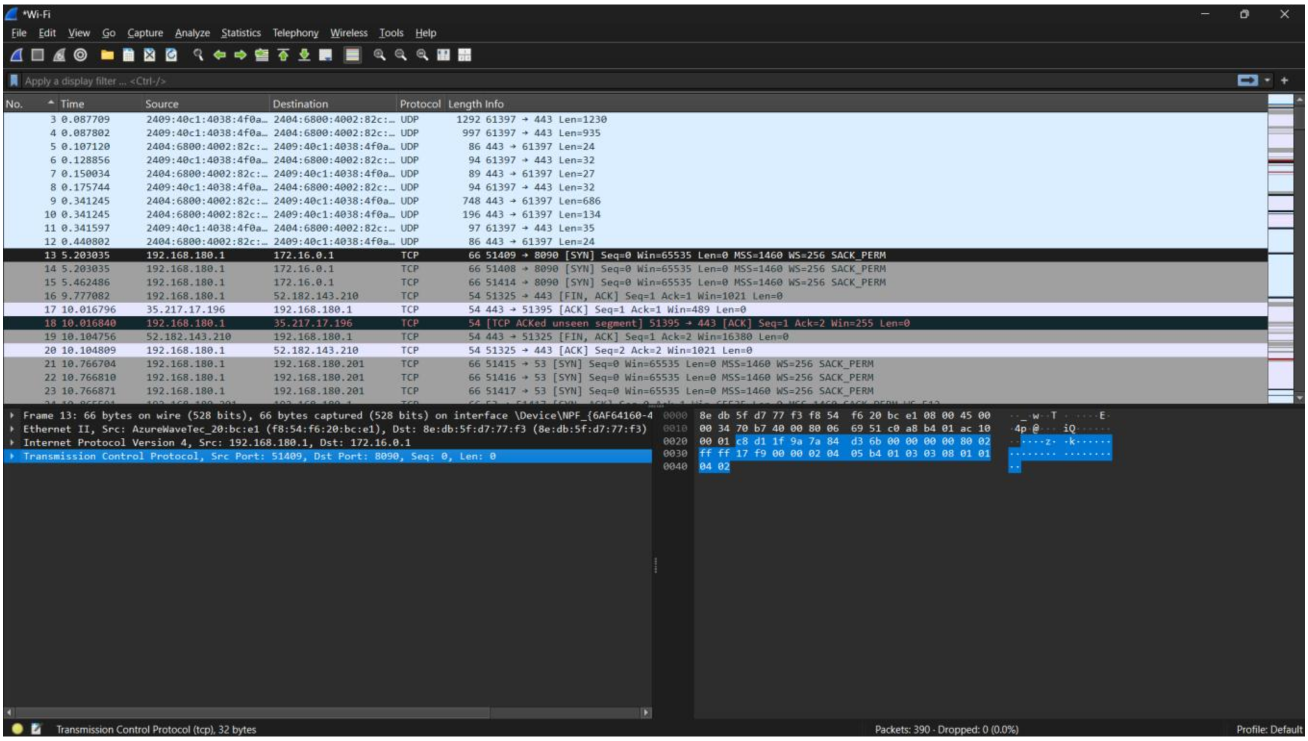
- IP Address
- URL
- Finding IP address from URL
- Finding location from IP Address

Exercise 1: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : TCP Reassembly Setting

Insert screenshots:


*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
   3 0.087709   2409:40c1:4038:4f0a… 2404:6800:4002:82c:… UDP      1292 61397 → 443 Len=1230
   4 0.087802   2409:40c1:4038:4f0a… 2404:6800:4002:82c:… UDP       997 61397 → 443 Len=935
   5 0.107120   2404:6800:4002:82c:… 2409:40c1:4038:4f0a… UDP        86 443 → 61397 Len=24
   6 0.128856   2409:40c1:4038:4f0a… 2404:6800:4002:82c:… UDP        94 61397 → 443 Len=32
   7 0.150034   2404:6800:4002:82c:… 2409:40c1:4038:4f0a… UDP        89 443 → 61397 Len=27
   8 0.175744   2409:40c1:4038:4f0a… 2404:6800:4002:82c:… UDP        94 61397 → 443 Len=32
   9 0.341245   2404:6800:4002:82c:… 2409:40c1:4038:4f0a… UDP       748 443 → 61397 Len=686
  10 0.341245   2404:6800:4002:82c:… 2409:40c1:4038:4f0a… UDP       196 443 → 61397 Len=134
  11 0.341597   2409:40c1:4038:4f0a… 2404:6800:4002:82c:… UDP        97 61397 → 443 Len=35
  12 0.440802   2404:6800:4002:82c:… 2409:40c1:4038:4f0a… UDP        86 443 → 61397 Len=24
  13 5.203035   192.168.180.1         172.16.0.1            TCP        66 51409 → 8090 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  14 5.203035   192.168.180.1         172.16.0.1            TCP        66 51408 → 8090 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  15 5.462486   192.168.180.1         172.16.0.1            TCP        66 51414 → 8090 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  16 9.777082   192.168.180.1         52.182.143.210        TCP        54 51325 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
  17 10.016796  35.217.17.196         192.168.180.1         TCP        54 443 → 51395 [ACK] Seq=1 Ack=1 Win=489 Len=0
  18 10.016840  192.168.180.1         35.217.17.196         TCP        54 [TCP ACKed unseen segment] 51395 → 443 [ACK] Seq=1 Ack=2 Win=255 Len=0
  19 10.104756  52.182.143.210        192.168.180.1         TCP        54 443 → 51325 [FIN, ACK] Seq=1 Ack=2 Win=16380 Len=0
  20 10.104809  192.168.180.1         52.182.143.210        TCP        54 51325 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
  21 10.766704  192.168.180.1         192.168.180.201       TCP        66 51415 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  22 10.766810  192.168.180.1         192.168.180.201       TCP        66 51416 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  23 10.766871  192.168.180.1         192.168.180.201       TCP        66 51417 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
> Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6AF64160-4
> Ethernet II, Src: AzureWaveTec_20:bc:e1 (f8:54:f6:20:bc:e1), Dst: 8e:db:5f:d7:77:f3 (8e:db:5f:d7:77:f3)
> Internet Protocol Version 4, Src: 192.168.180.1, Dst: 172.16.0.1
> Transmission Control Protocol, Src Port: 51409, Dst Port: 8090, Seq: 0, Len: 0
```

```
0000  8e db 5f d7 77 f3 f8 54  f6 20 bc e1 08 00 45 00   ··_·w·T· ·····E·
0010  00 34 70 b7 40 00 80 06  69 51 c0 a8 b4 01 ac 10   ·4p·@··· iQ······
0020  00 01 c8 d1 1f 9a 7a 84  d3 6b 00 00 00 00 80 02   ······z· ·k······
0030  ff ff 17 f9 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Transmission Control Protocol (tcp), 32 bytes

Packets: 390 · Dropped: 0 (0.0%)

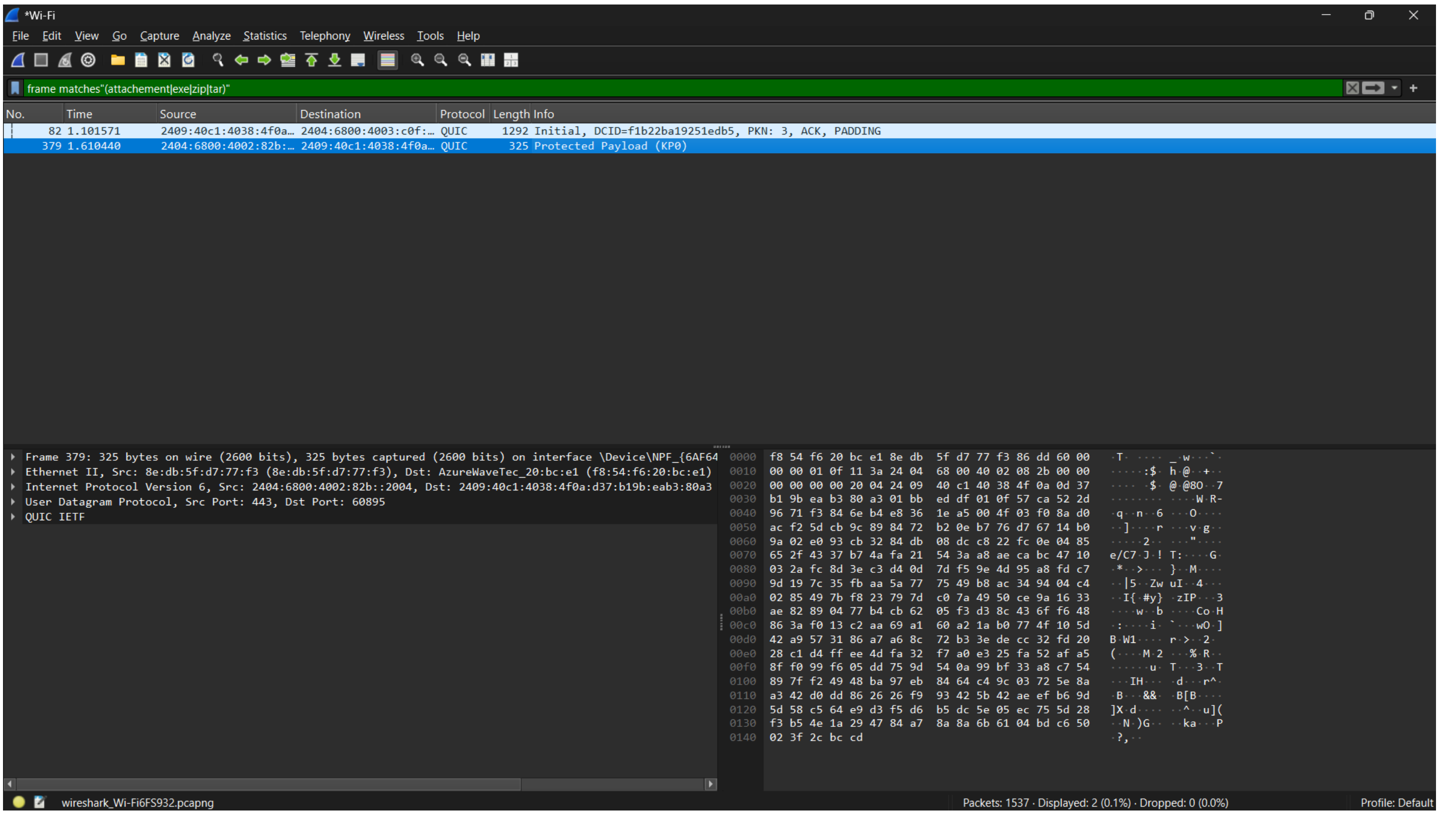
Profile: Default

Exercise 2: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Use Regex to Filter for a Group of Phrases

Insert screenshots:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
frame matches"(attachement|exe|zip|tar)"
```

```
No.   Time      Source                Destination           Protocol Length Info
   82 1.101571  2409:40c1:4038:4f0a…  2404:6800:4003:c0f:…  QUIC     1292 Initial, DCID=f1b22ba19251edb5, PKN: 3, ACK, PADDING
  379 1.610440  2404:6800:4002:82b:…  2409:40c1:4038:4f0a…  QUIC      325 Protected Payload (KP0)
```

```
Frame 379: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface \Device\NPF_{6AF64
Ethernet II, Src: 8e:db:5f:d7:77:f3 (8e:db:5f:d7:77:f3), Dst: AzureWaveTec_20:bc:e1 (f8:54:f6:20:bc:e1)
Internet Protocol Version 6, Src: 2404:6800:4002:82b::2004, Dst: 2409:40c1:4038:4f0a:d37:b19b:eab3:80a3
User Datagram Protocol, Src Port: 443, Dst Port: 60895
QUIC IETF
```

```
0000  f8 54 f6 20 bc e1 8e db  5f d7 77 f3 86 dd 60 00   ·T· ···· _·w···`·
0010  00 00 01 0f 11 3a 24 04  68 00 40 02 08 2b 00 00   ·····:$· h·@··+··
0020  00 00 00 00 20 04 24 09  40 c1 40 38 4f 0a 0d 37   ···· ·$· @·@8O··7
0030  b1 9b ea b3 80 a3 01 bb  ed df 01 0f 57 ca 52 2d   ········ ····W·R-
0040  96 71 f3 84 6e b4 e8 36  1e a5 00 4f 03 f0 8a d0   ·q··n··6 ···O····
0050  ac f2 5d cb 9c 89 84 72  b2 0e b7 76 d7 67 14 b0   ··]····r ···v·g··
0060  9a 02 e0 93 cb 32 84 db  08 dc c8 22 fc 0e 04 85   ·····2·· ···"····
0070  65 2f 43 37 b7 4a fa 21  54 3a a8 ae ca bc 47 10   e/C7·J·! T:····G·
0080  03 2a fc 8d 3e c3 d4 0d  7d f5 9e 4d 95 a8 fd c7   ·*··>··· }··M····
0090  9d 19 7c 35 fb aa 5a 77  75 49 b8 ac 34 94 04 c4   ··|5··Zw uI··4···
00a0  02 85 49 7b f8 23 79 7d  c0 7a 49 50 ce 9a 16 33   ··I{·#y} ·zIP···3
00b0  ae 82 89 04 77 b4 cb 62  05 f3 d3 8c 43 6f f6 48   ····w··b ····Co·H
00c0  86 3a f0 13 c2 aa 69 a1  60 a2 1a b0 77 4f 10 5d   ·:····i· `···wO·]
00d0  42 a9 57 31 86 a7 a6 8c  72 b3 3e de cc 32 fd 20   B·W1···· r·>··2· 
00e0  28 c1 d4 ff ee 4d fa 32  f7 a0 e3 25 fa 52 af a5   (····M·2 ···%·R··
00f0  8f f0 99 f6 05 dd 75 9d  54 0a 99 bf 33 a8 c7 54   ······u· T···3··T
0100  89 7f f2 49 48 ba 97 eb  84 64 c4 9c 03 72 5e 8a   ···IH··· ·d···r^·
0110  a3 42 d0 dd 86 26 26 f9  93 42 5b 42 ae ef b6 9d   ·B···&&· ·B[B····
0120  5d 58 c5 64 e9 d3 f5 d6  b5 dc 5e 05 ec 75 5d 28   ]X·d···· ··^··u](
0130  f3 b5 4e 1a 29 47 84 a7  8a 8a 6b 61 04 bd c6 50   ··N·)G·· ··ka···P
0140  02 3f 2c bc cd                                     ·?,··
```

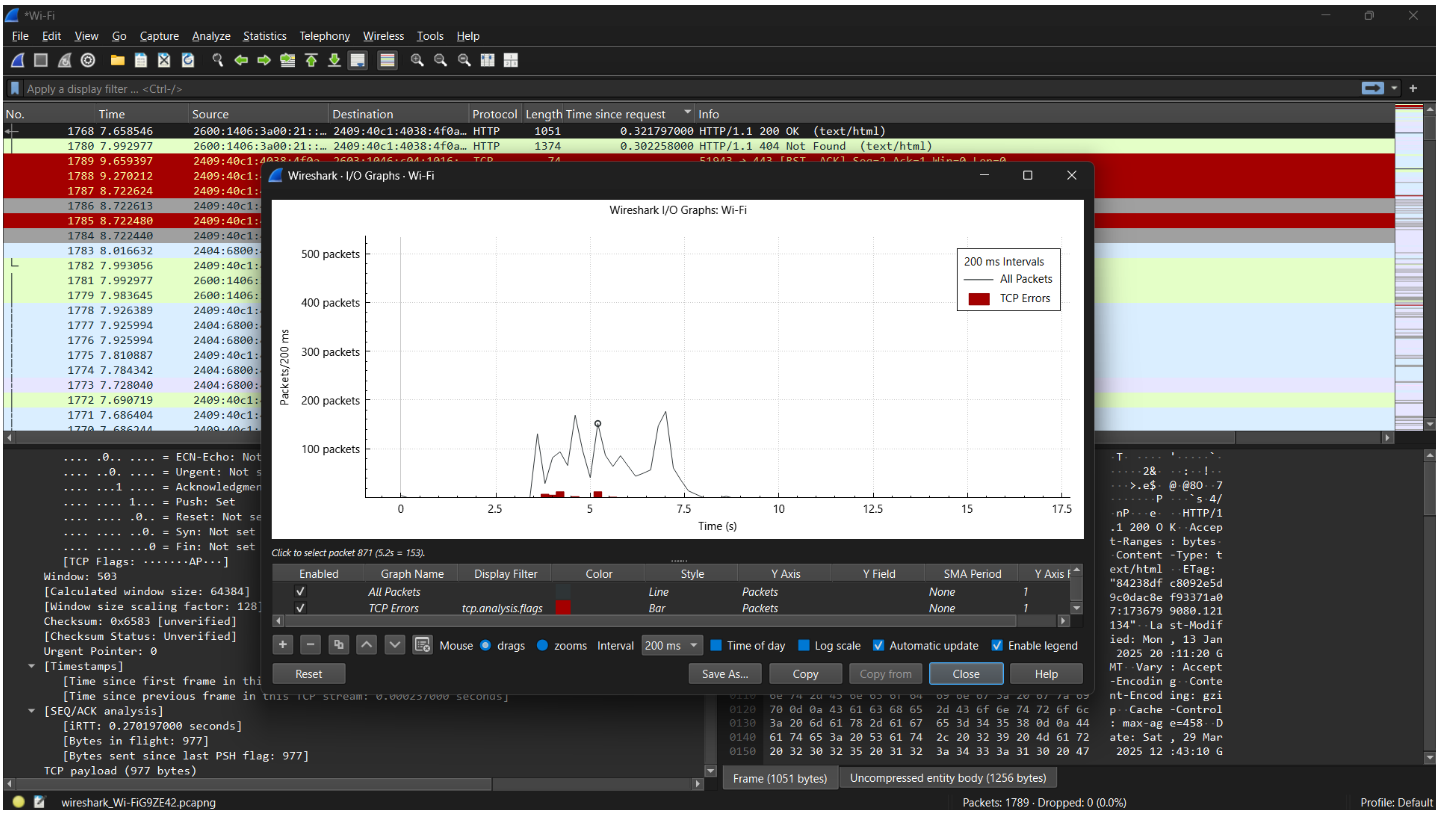
wireshark_Wi-Fi6FS932.pcapng   Packets: 1537 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)   Profile: Default

Exercise 3: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Graph HTTP Response Times

Insert screenshots:



```
No.   Time      Source                 Destination            Protocol Length Time since request Info
1768 7.658546   2600:1406:3a00:21::…   2409:40c1:4038:4f0a…   HTTP     1051   0.321797000 HTTP/1.1 200 OK  (text/html)
1780 7.992977   2600:1406:3a00:21::…   2409:40c1:4038:4f0a…   HTTP     1374   0.302258000 HTTP/1.1 404 Not Found  (text/html)
1789 9.659397   2409:40c1:4038:4f0a…
1788 9.270212   2409:40c1:
1787 8.722624   2409:40c1:
1786 8.722613   2409:40c1:
1785 8.722480   2409:40c1:
1784 8.722440   2409:40c1:
1783 8.016632   2404:6800:
1782 7.993056   2409:40c1:
1781 7.992977   2600:1406:
1779 7.983645   2600:1406:
1778 7.926389   2409:40c1:
1777 7.925994   2404:6800:
1776 7.925994   2404:6800:
1775 7.810887   2409:40c1:
1774 7.784342   2404:6800:
1773 7.728040   2404:6800:
1772 7.690719   2409:40c1:
1771 7.686404   2409:40c1:
```

```
    .... .0.. .... = ECN-Echo: Not
    .... ..0. .... = Urgent: Not s
    .... ...1 .... = Acknowledgmen
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not se
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······AP···]
  Window: 503
  [Calculated window size: 64384]
  [Window size scaling factor: 128]
  Checksum: 0x6583 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
▾ [Timestamps]
    [Time since first frame in thi
    [Time since previous frame in this TCP stream: 0.000237000 seconds]
▾ [SEQ/ACK analysis]
    [iRTT: 0.270197000 seconds]
    [Bytes in flight: 977]
    [Bytes sent since last PSH flag: 977]
  TCP payload (977 bytes)
```

```
                                                   ·T· ···· '·····`·
                                                   ·····2& ··:··!··
                                                   ···>.e$· @·@80··7
                                                   ·······P ···`s·4/
                                                   ·nP···e· ··HTTP/1
                                                   .1 200 O K··Accep
                                                   t-Ranges : bytes·
                                                   ·Content -Type: t
                                                   ext/html ··ETag:
                                                   "84238df c8092e5d
                                                   9c0dac8e f93371a0
                                                   7:173679 9080.121
                                                   134"··La st-Modif
                                                   ied: Mon , 13 Jan
                                                    2025 20 :11:20 G
                                                   MT··Vary : Accept
                                                   -Encodin g··Conte
                                                   nt-Encod ing: gzi
0120  70 0d 0a 43 61 63 68 65  2d 43 6f 6e 74 72 6f 6c   p··Cache -Control
0130  3a 20 6d 61 78 2d 61 67  65 3d 34 35 38 0d 0a 44   : max-ag e=458··D
0140  61 74 65 3a 20 53 61 74  2c 20 32 39 20 4d 61 72   ate: Sat , 29 Mar
0150  20 32 30 32 35 20 31 32  3a 34 33 3a 31 30 20 47    2025 12 :43:10 G
```

Frame (1051 bytes) | Uncompressed entity body (1256 bytes)

Click to select packet 871 (5.2s = 153).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis F
✓	All Packets		■	Line	Packets		None	1
✓	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None	1

Mouse ● drags ● zooms Interval 200 ms ■ Time of day ■ Log scale ☑ Automatic update ☑ Enable legend

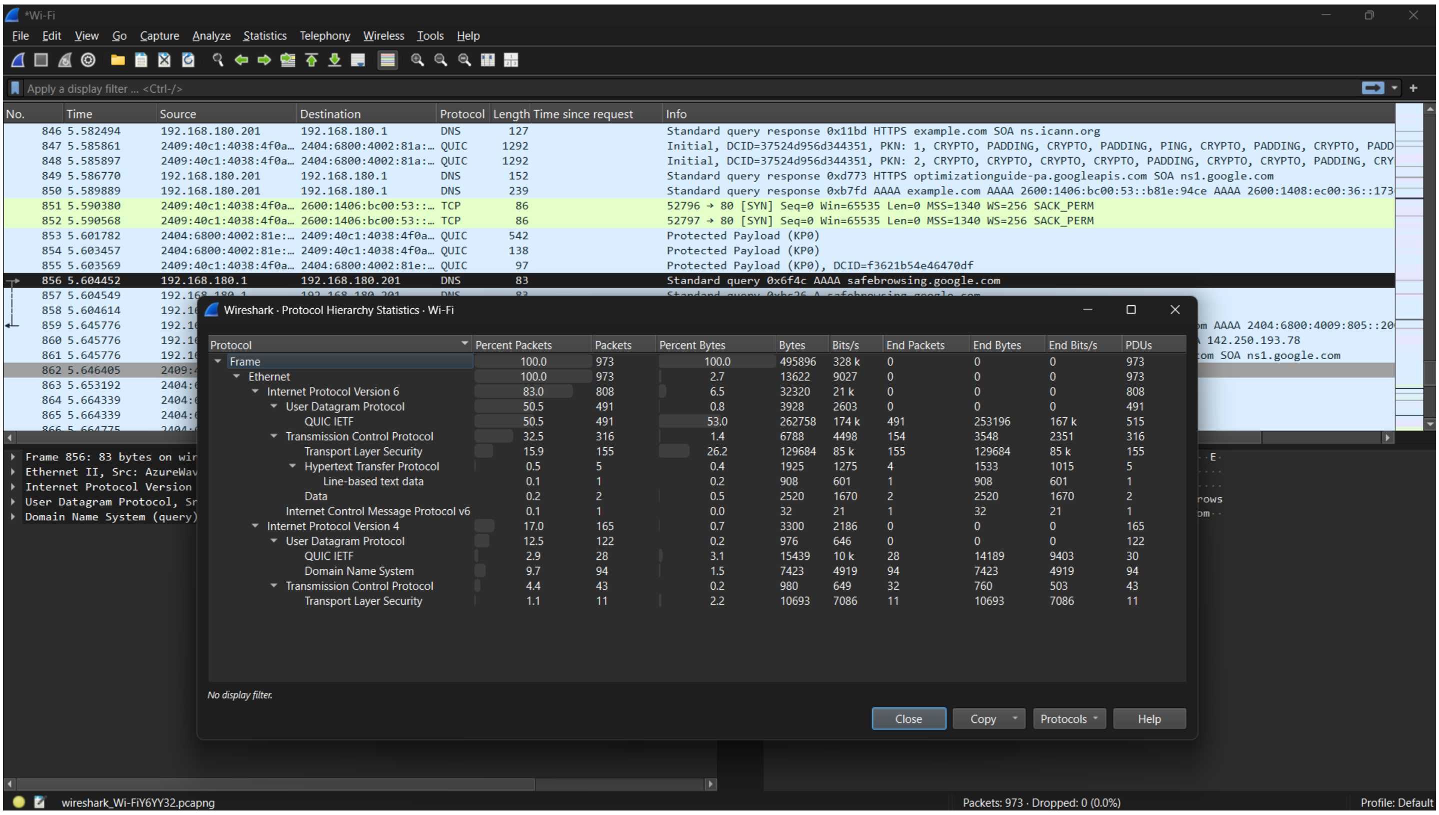
wireshark_Wi-FiG9ZE42.pcapng Packets: 1789 · Dropped: 0 (0.0%) Profile: Default

Exercise 4: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : [Finding Suspicious Traffic in Protocol Hierarchy]()

Insert screenshots:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source                 Destination            Protocol Length Time since request Info
  846 5.582494  192.168.180.201        192.168.180.1          DNS       127   Standard query response 0x11bd HTTPS example.com SOA ns.icann.org
  847 5.585861  2409:40c1:4038:4f0a…   2404:6800:4002:81a:…   QUIC     1292   Initial, DCID=37524d956d344351, PKN: 1, CRYPTO, PADDING, CRYPTO, PADDING, PING, CRYPTO, PADDING, CRYPTO, PADD
  848 5.585897  2409:40c1:4038:4f0a…   2404:6800:4002:81a:…   QUIC     1292   Initial, DCID=37524d956d344351, PKN: 2, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, CRY
  849 5.586770  192.168.180.201        192.168.180.1          DNS       152   Standard query response 0xd773 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
  850 5.589889  192.168.180.201        192.168.180.1          DNS       239   Standard query response 0xb7fd AAAA example.com AAAA 2600:1406:bc00:53::b81e:94ce AAAA 2600:1408:ec00:36::173
  851 5.590380  2409:40c1:4038:4f0a…   2600:1406:bc00:53::…   TCP        86   52796 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
  852 5.590568  2409:40c1:4038:4f0a…   2600:1406:bc00:53::…   TCP        86   52797 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
  853 5.601782  2404:6800:4002:81e:…   2409:40c1:4038:4f0a…   QUIC      542   Protected Payload (KP0)
  854 5.603457  2404:6800:4002:81e:…   2409:40c1:4038:4f0a…   QUIC      138   Protected Payload (KP0)
  855 5.603569  2409:40c1:4038:4f0a…   2404:6800:4002:81e:…   QUIC       97   Protected Payload (KP0), DCID=f3621b54e46470df
  856 5.604452  192.168.180.1          192.168.180.201        DNS        83   Standard query 0x6f4c AAAA safebrowsing.google.com
  857 5.604549  192.168.180.1          192.168.180.201        DNS        83   Standard query 0xbc26 A safebrowsing.google.com
  858 5.604614  192.16
  859 5.645776  192.16                                                       om AAAA 2404:6800:4009:805::20
  860 5.645776  192.16                                                       A 142.250.193.78
  861 5.645776  192.16                                                       om SOA ns1.google.com
  862 5.646405  2409:4
  863 5.653192  2404:6
  864 5.664339  2404:6
  865 5.664339  2404:6
```

```
Frame 856: 83 bytes on wir
Ethernet II, Src: AzureWav
Internet Protocol Version
User Datagram Protocol, Sr
Domain Name System (query)
```

Wireshark · Protocol Hierarchy Statistics · Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	973	100.0	495896	328 k	0	0	0	973
Ethernet	100.0	973	2.7	13622	9027	0	0	0	973
Internet Protocol Version 6	83.0	808	6.5	32320	21 k	0	0	0	808
User Datagram Protocol	50.5	491	0.8	3928	2603	0	0	0	491
QUIC IETF	50.5	491	53.0	262758	174 k	491	253196	167 k	515
Transmission Control Protocol	32.5	316	1.4	6788	4498	154	3548	2351	316
Transport Layer Security	15.9	155	26.2	129684	85 k	155	129684	85 k	155
Hypertext Transfer Protocol	0.5	5	0.4	1925	1275	4	1533	1015	5
Line-based text data	0.1	1	0.2	908	601	1	908	601	1
Data	0.2	2	0.5	2520	1670	2	2520	1670	2
Internet Control Message Protocol v6	0.1	1	0.0	32	21	1	32	21	1
Internet Protocol Version 4	17.0	165	0.7	3300	2186	0	0	0	165
User Datagram Protocol	12.5	122	0.2	976	646	0	0	0	122
QUIC IETF	2.9	28	3.1	15439	10 k	28	14189	9403	30
Domain Name System	9.7	94	1.5	7423	4919	94	7423	4919	94
Transmission Control Protocol	4.4	43	0.2	980	649	32	760	503	43
Transport Layer Security	1.1	11	2.2	10693	7086	11	10693	7086	11

No display filter.

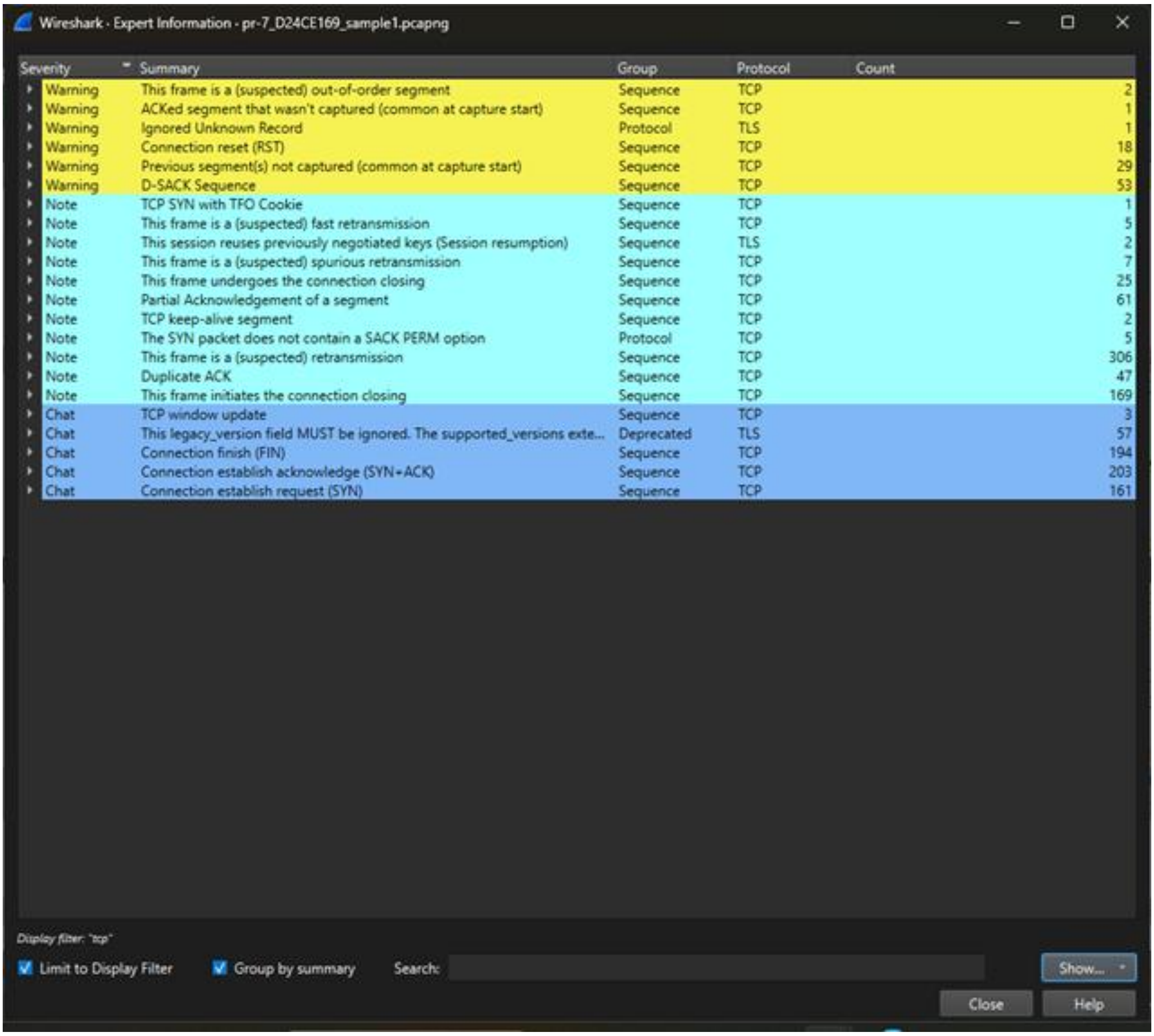
Close
Copy
Protocols
Help
wireshark_Wi-FiY6YY32.pcapng
Packets: 973 · Dropped: 0 (0.0%)
Profile: Default

Exercise 5: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Find TCP Problems Fast with a BadTCP Button

Insert screenshots:



Wireshark · Expert Information · pr-7_D24CE169_sample1.pcapng

Severity	Summary	Group	Protocol	Count
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	2
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	1
Warning	Ignored Unknown Record	Protocol	TLS	1
Warning	Connection reset (RST)	Sequence	TCP	18
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	29
Warning	D-SACK Sequence	Sequence	TCP	53
Note	TCP SYN with TFO Cookie	Sequence	TCP	1
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	5
Note	This session reuses previously negotiated keys (Session resumption)	Sequence	TLS	2
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	7
Note	This frame undergoes the connection closing	Sequence	TCP	25
Note	Partial Acknowledgement of a segment	Sequence	TCP	61
Note	TCP keep-alive segment	Sequence	TCP	2
Note	The SYN packet does not contain a SACK PERM option	Protocol	TCP	5
Note	This frame is a (suspected) retransmission	Sequence	TCP	306
Note	Duplicate ACK	Sequence	TCP	47
Note	This frame initiates the connection closing	Sequence	TCP	169
Chat	TCP window update	Sequence	TCP	3
Chat	This legacy_version field MUST be ignored. The supported_versions exte...	Deprecated	TLS	57
Chat	Connection finish (FIN)	Sequence	TCP	194
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	203
Chat	Connection establish request (SYN)	Sequence	TCP	161

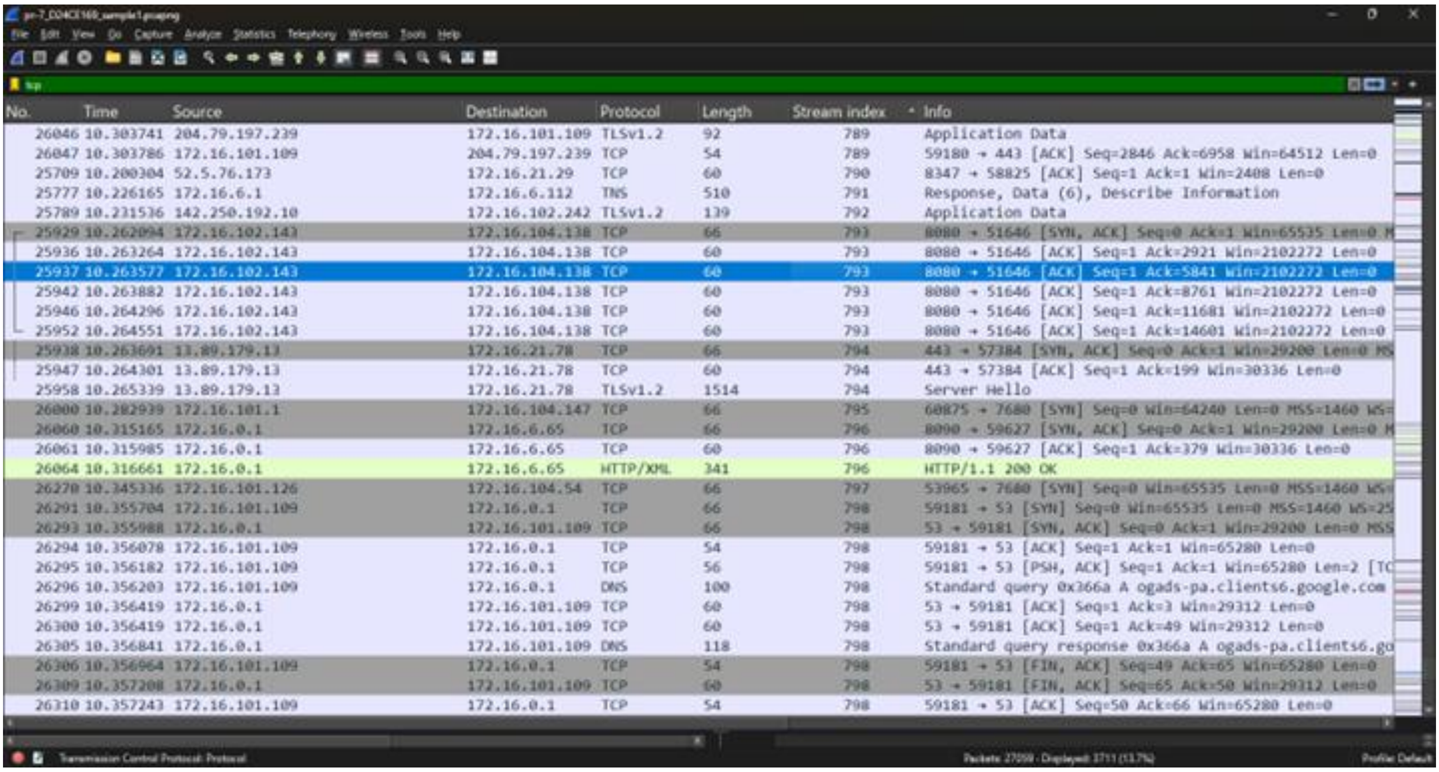
Display filter: "tcp"

☑ Limit to Display Filter ☑ Group by summary Search:

Exercise 6: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

Video : Identify Separate TCP Conversations with TCP Stream Index

Insert screenshots:


pr-7_D24CE168_sample1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

No.	Time	Source	Destination	Protocol	Length	Stream index	Info
26046	10.303741	204.79.197.239	172.16.101.109	TLSv1.2	92	789	Application Data
26047	10.303786	172.16.101.109	204.79.197.239	TCP	54	789	59180 → 443 [ACK] Seq=2846 Ack=6958 Win=64512 Len=0
25709	10.200304	52.5.76.173	172.16.21.29	TCP	60	790	8347 → 58825 [ACK] Seq=1 Ack=1 Win=2408 Len=0
25777	10.226165	172.16.6.1	172.16.6.112	TNS	510	791	Response, Data (6), Describe Information
25789	10.231536	142.250.192.10	172.16.102.242	TLSv1.2	139	792	Application Data
25929	10.262094	172.16.102.143	172.16.104.138	TCP	66	793	8080 → 51646 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
25936	10.263264	172.16.102.143	172.16.104.138	TCP	60	793	8080 → 51646 [ACK] Seq=1 Ack=2921 Win=2102272 Len=0
25937	10.263577	172.16.102.143	172.16.104.138	TCP	60	793	8080 → 51646 [ACK] Seq=1 Ack=5841 Win=2102272 Len=0
25942	10.263882	172.16.102.143	172.16.104.138	TCP	60	793	8080 → 51646 [ACK] Seq=1 Ack=8761 Win=2102272 Len=0
25946	10.264296	172.16.102.143	172.16.104.138	TCP	60	793	8080 → 51646 [ACK] Seq=1 Ack=11681 Win=2102272 Len=0
25952	10.264551	172.16.102.143	172.16.104.138	TCP	60	793	8080 → 51646 [ACK] Seq=1 Ack=14601 Win=2102272 Len=0
25938	10.263691	13.89.179.13	172.16.21.78	TCP	66	794	443 → 57384 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MS
25947	10.264301	13.89.179.13	172.16.21.78	TCP	60	794	443 → 57384 [ACK] Seq=1 Ack=199 Win=30336 Len=0
25958	10.265339	13.89.179.13	172.16.21.78	TLSv1.2	1514	794	Server Hello
26000	10.282939	172.16.101.1	172.16.104.147	TCP	66	795	60875 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
26060	10.315165	172.16.0.1	172.16.6.65	TCP	66	796	8090 → 59627 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M
26061	10.315985	172.16.0.1	172.16.6.65	TCP	60	796	8090 → 59627 [ACK] Seq=1 Ack=379 Win=30336 Len=0
26064	10.316661	172.16.0.1	172.16.6.65	HTTP/XML	341	796	HTTP/1.1 200 OK
26270	10.345336	172.16.101.126	172.16.104.54	TCP	66	797	53965 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
26291	10.355704	172.16.101.109	172.16.0.1	TCP	66	798	59181 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=25
26293	10.355988	172.16.0.1	172.16.101.109	TCP	66	798	53 → 59181 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS
26294	10.356078	172.16.101.109	172.16.0.1	TCP	54	798	59181 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
26295	10.356182	172.16.101.109	172.16.0.1	TCP	56	798	59181 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TC
26296	10.356203	172.16.101.109	172.16.0.1	DNS	100	798	Standard query 0x366a A ogads-pa.clients6.google.com
26299	10.356419	172.16.0.1	172.16.101.109	TCP	60	798	53 → 59181 [ACK] Seq=1 Ack=3 Win=29312 Len=0
26300	10.356419	172.16.0.1	172.16.101.109	TCP	60	798	53 → 59181 [ACK] Seq=1 Ack=49 Win=29312 Len=0
26305	10.356841	172.16.0.1	172.16.101.109	DNS	118	798	Standard query response 0x366a A ogads-pa.clients6.go
26306	10.356964	172.16.101.109	172.16.0.1	TCP	54	798	59181 → 53 [FIN, ACK] Seq=49 Ack=65 Win=65280 Len=0
26309	10.357208	172.16.0.1	172.16.101.109	TCP	60	798	53 → 59181 [FIN, ACK] Seq=65 Ack=50 Win=29312 Len=0
26310	10.357243	172.16.101.109	172.16.0.1	TCP	54	798	59181 → 53 [ACK] Seq=50 Ack=66 Win=65280 Len=0

Transmission Control Protocol: Protocol

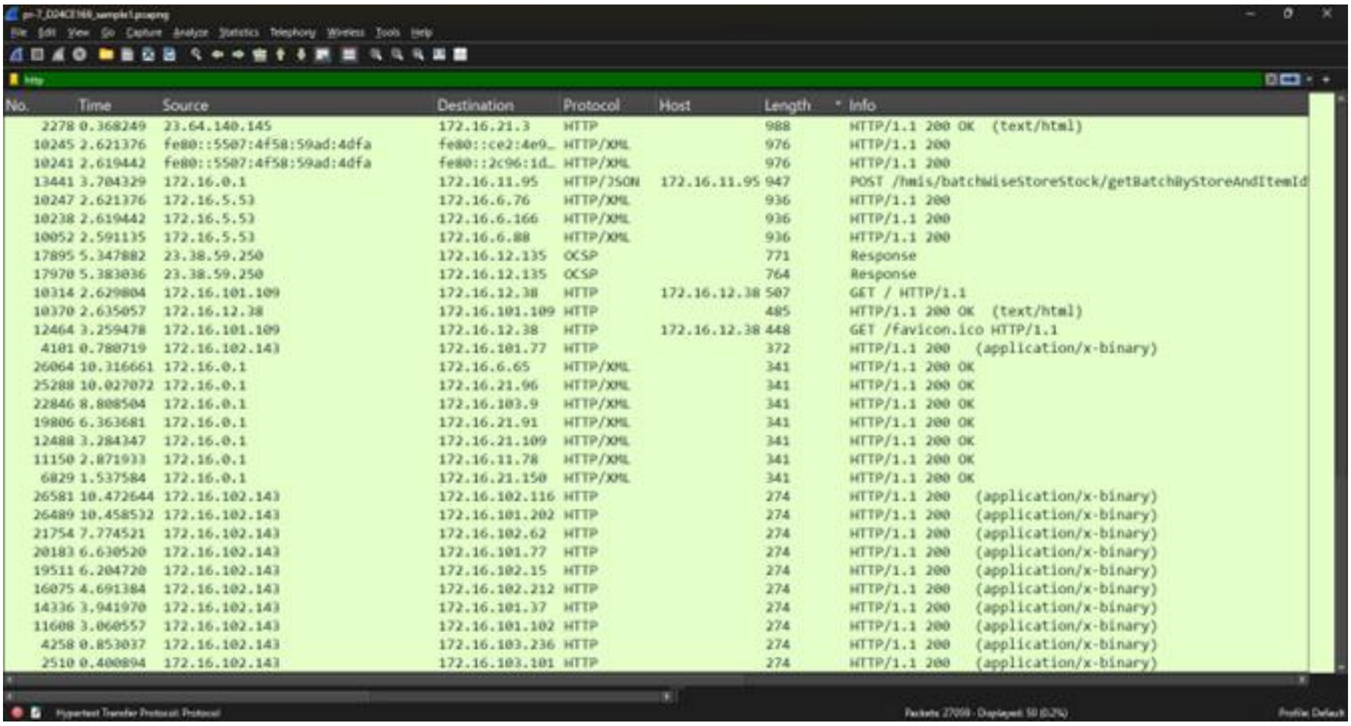
Packets: 27059 · Displayed: 3711 (13.7%)

Profile: Default

Exercise 7: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

Video : Add an httphost Column

Insert screenshots:

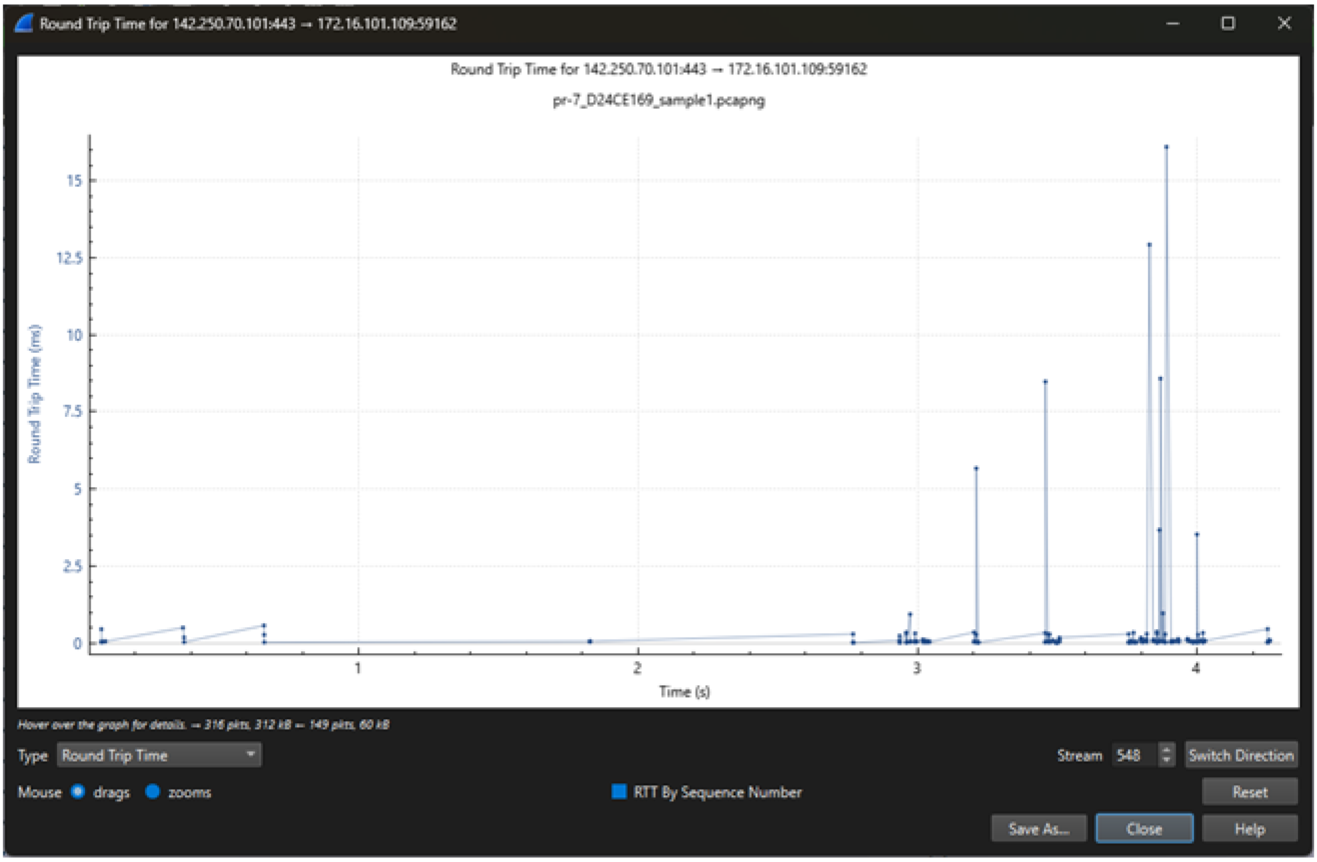

pr-7_D24CE166_sample1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol: Protocol
Packets: 27099 · Displayed: 50 (0.2%)
Profile: Default

No.	Time	Source	Destination	Protocol	Host	Length	Info
2278	0.368249	23.64.140.145	172.16.21.3	HTTP		988	HTTP/1.1 200 OK (text/html)
10245	2.621376	fe80::5507:4f58:59ad:4dfa	fe80::ce2:4e9…	HTTP/XML		976	HTTP/1.1 200
10241	2.619442	fe80::5507:4f58:59ad:4dfa	fe80::2c96:1d…	HTTP/XML		976	HTTP/1.1 200
13441	3.704329	172.16.0.1	172.16.11.95	HTTP/JSON	172.16.11.95	947	POST /hmis/batchWiseStoreStock/getBatchByStoreAndItemId
10247	2.621376	172.16.5.53	172.16.6.76	HTTP/XML		936	HTTP/1.1 200
10238	2.619442	172.16.5.53	172.16.6.166	HTTP/XML		936	HTTP/1.1 200
10052	2.591135	172.16.5.53	172.16.6.88	HTTP/XML		936	HTTP/1.1 200
17895	5.347882	23.38.59.250	172.16.12.135	OCSP		771	Response
17970	5.383036	23.38.59.250	172.16.12.135	OCSP		764	Response
10314	2.629804	172.16.101.109	172.16.12.38	HTTP	172.16.12.38	507	GET / HTTP/1.1
10370	2.635057	172.16.12.38	172.16.101.109	HTTP		485	HTTP/1.1 200 OK (text/html)
12464	3.259478	172.16.101.109	172.16.12.38	HTTP	172.16.12.38	448	GET /favicon.ico HTTP/1.1
4101	0.780719	172.16.102.143	172.16.101.77	HTTP		372	HTTP/1.1 200 (application/x-binary)
26064	10.316661	172.16.0.1	172.16.6.65	HTTP/XML		341	HTTP/1.1 200 OK
25288	10.027072	172.16.0.1	172.16.21.96	HTTP/XML		341	HTTP/1.1 200 OK
22846	8.808504	172.16.0.1	172.16.103.9	HTTP/XML		341	HTTP/1.1 200 OK
19806	6.363681	172.16.0.1	172.16.21.91	HTTP/XML		341	HTTP/1.1 200 OK
12488	3.284347	172.16.0.1	172.16.21.109	HTTP/XML		341	HTTP/1.1 200 OK
11150	2.871933	172.16.0.1	172.16.11.78	HTTP/XML		341	HTTP/1.1 200 OK
6829	1.537584	172.16.0.1	172.16.21.150	HTTP/XML		341	HTTP/1.1 200 OK
26581	10.472644	172.16.102.143	172.16.102.116	HTTP		274	HTTP/1.1 200 (application/x-binary)
26489	10.458532	172.16.102.143	172.16.101.202	HTTP		274	HTTP/1.1 200 (application/x-binary)
21754	7.774521	172.16.102.143	172.16.102.62	HTTP		274	HTTP/1.1 200 (application/x-binary)
20183	6.630520	172.16.102.143	172.16.101.77	HTTP		274	HTTP/1.1 200 (application/x-binary)
19511	6.204720	172.16.102.143	172.16.102.15	HTTP		274	HTTP/1.1 200 (application/x-binary)
16075	4.691384	172.16.102.143	172.16.102.212	HTTP		274	HTTP/1.1 200 (application/x-binary)
14336	3.941970	172.16.102.143	172.16.101.37	HTTP		274	HTTP/1.1 200 (application/x-binary)
11608	3.060557	172.16.102.143	172.16.101.102	HTTP		274	HTTP/1.1 200 (application/x-binary)
4258	0.853037	172.16.102.143	172.16.103.236	HTTP		274	HTTP/1.1 200 (application/x-binary)
2510	0.400894	172.16.102.143	172.16.103.101	HTTP		274	HTTP/1.1 200 (application/x-binary)

Exercise 8: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

Video : Filter to Determine TCP Round Trip Times and Capabilities

Insert screenshots:


Round Trip Time for 142.250.70.101:443 → 172.16.101.109:59162

Round Trip Time for 142.250.70.101:443 → 172.16.101.109:59162

pr-7_D24CE169_sample1.pcapng

Hover over the graph for details. → 316 pkts, 312 kB ← 149 pkts, 60 kB

Type Round Trip Time

Stream 548

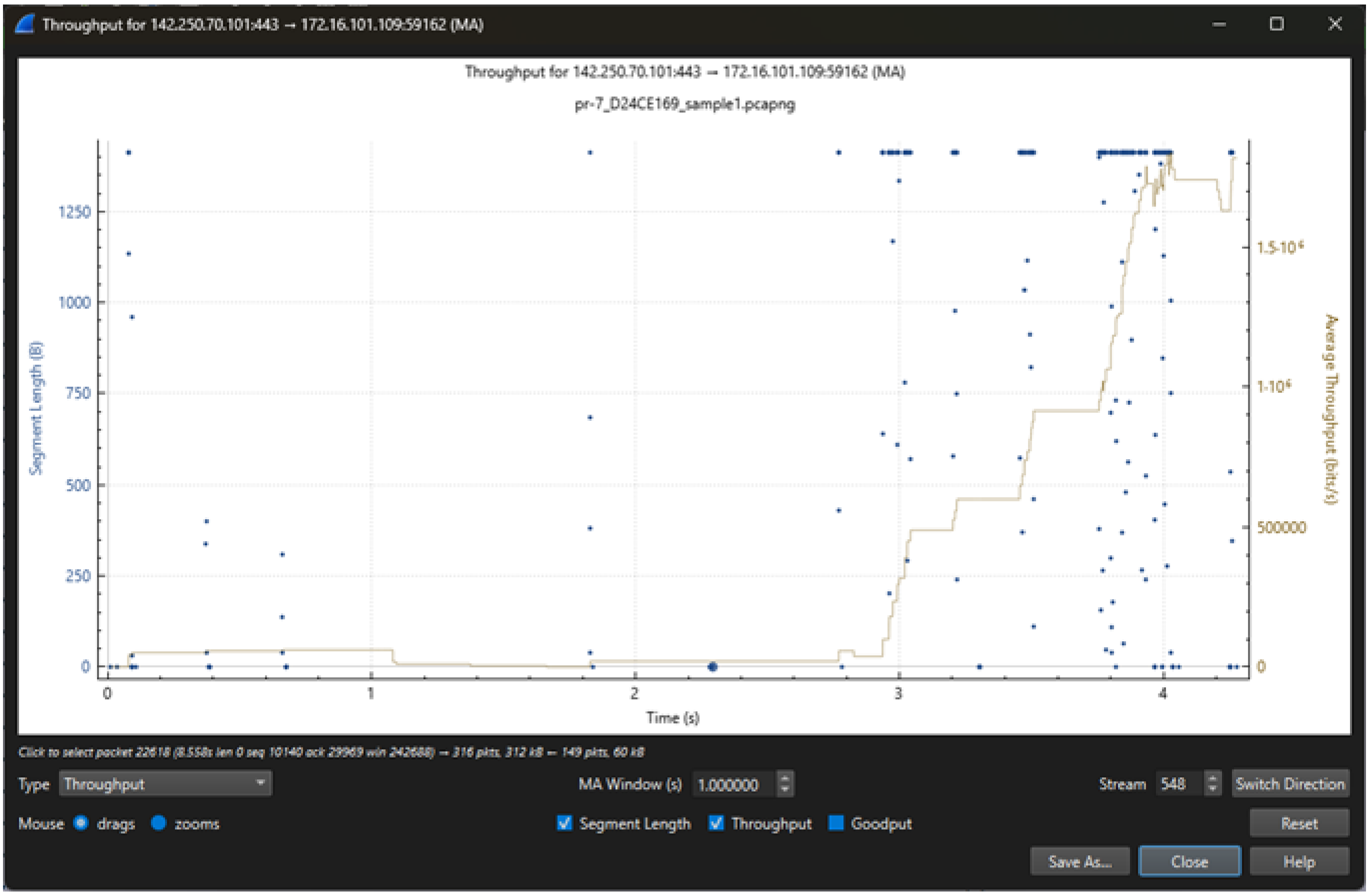
Mouse ● drags ● zooms

🟦 RTT By Sequence Number

Exercise 9: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

Video : Correlate TCP Problems to IO Drops

Insert screenshots:


Throughput for 142.250.70.101:443 → 172.16.101.109:59162 (MA)
Throughput for 142.250.70.101:443 → 172.16.101.109:59162 (MA)
pr-7_D24CE169_sample1.pcapng
Segment Length (B)
1250
1000
750
500
250
0
0
1
2
3
4
Time (s)
Average Throughput (bits/s)
1.5·10⁶
1·10⁶
500000
0
Save As...
Close
Help
Reset
Switch Direction

Click to select packet 22618 (8.558s len 0 seq 10140 ack 29969 win 242688) → 316 pkts, 312 kB ← 149 pkts, 60 kB

Type Throughput

MA Window (s) 1.000000

Stream 548

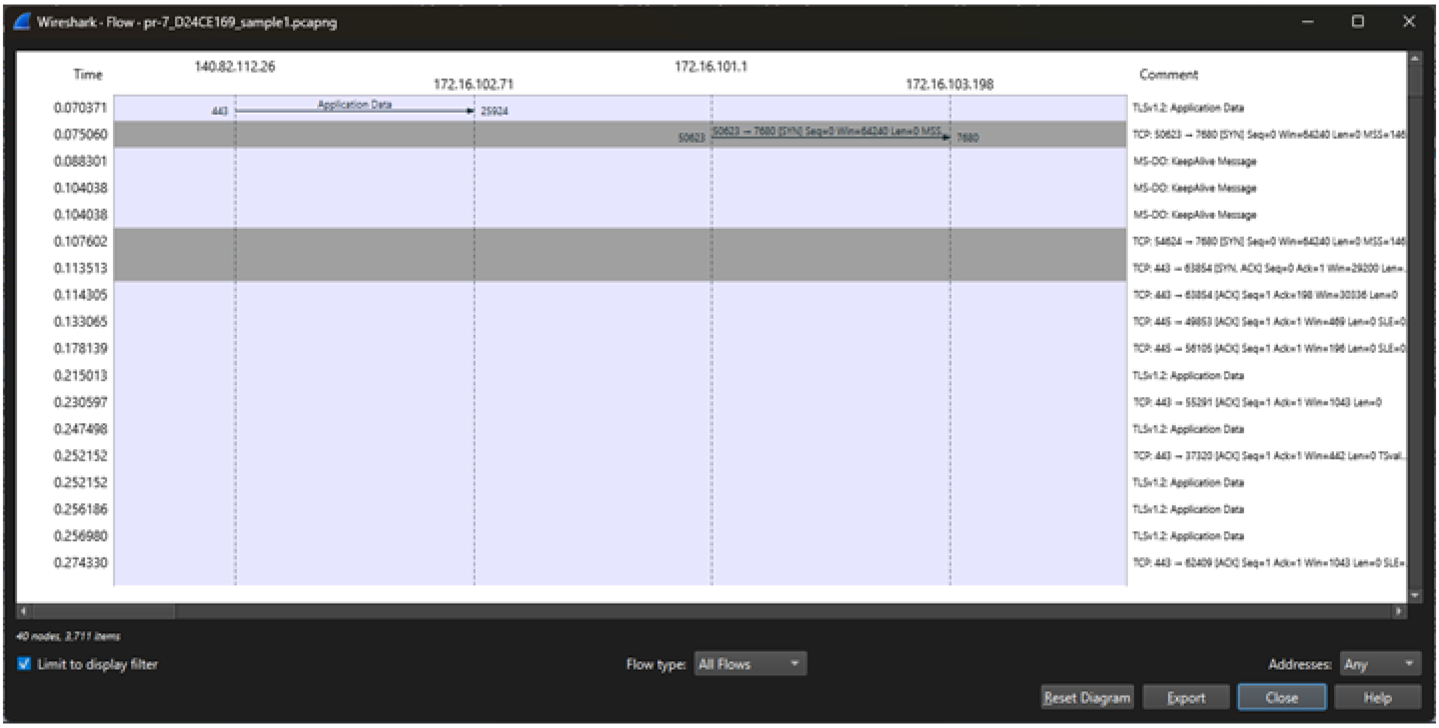
Mouse ● drags ● zooms

☑ Segment Length ☑ Throughput □ Goodput

Exercise 10: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

Video : Find Delays with TCP Calculate Conversation Timestamps

Insert screenshots:



Time	Comment
0.070371	TLSv1.2: Application Data
0.075060	TCP: 50623 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=146
0.088301	MS-DO: KeepAlive Message
0.104038	MS-DO: KeepAlive Message
0.104038	MS-DO: KeepAlive Message
0.107602	TCP: 54624 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=146
0.113513	TCP: 443 → 63854 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=...
0.114305	TCP: 443 → 63854 [ACK] Seq=1 Ack=198 Win=30336 Len=0
0.133065	TCP: 445 → 49853 [ACK] Seq=1 Ack=1 Win=469 Len=0 SLE=0
0.178139	TCP: 445 → 58105 [ACK] Seq=1 Ack=1 Win=196 Len=0 SLE=0
0.215013	TLSv1.2: Application Data
0.230597	TCP: 443 → 55291 [ACK] Seq=1 Ack=1 Win=1043 Len=0
0.247498	TLSv1.2: Application Data
0.252152	TCP: 443 → 37320 [ACK] Seq=1 Ack=1 Win=442 Len=0 TSval...
0.252152	TLSv1.2: Application Data
0.256186	TLSv1.2: Application Data
0.256980	TLSv1.2: Application Data
0.274330	TCP: 443 → 62409 [ACK] Seq=1 Ack=1 Win=1043 Len=0 SLE=...

☑ Limit to display filter

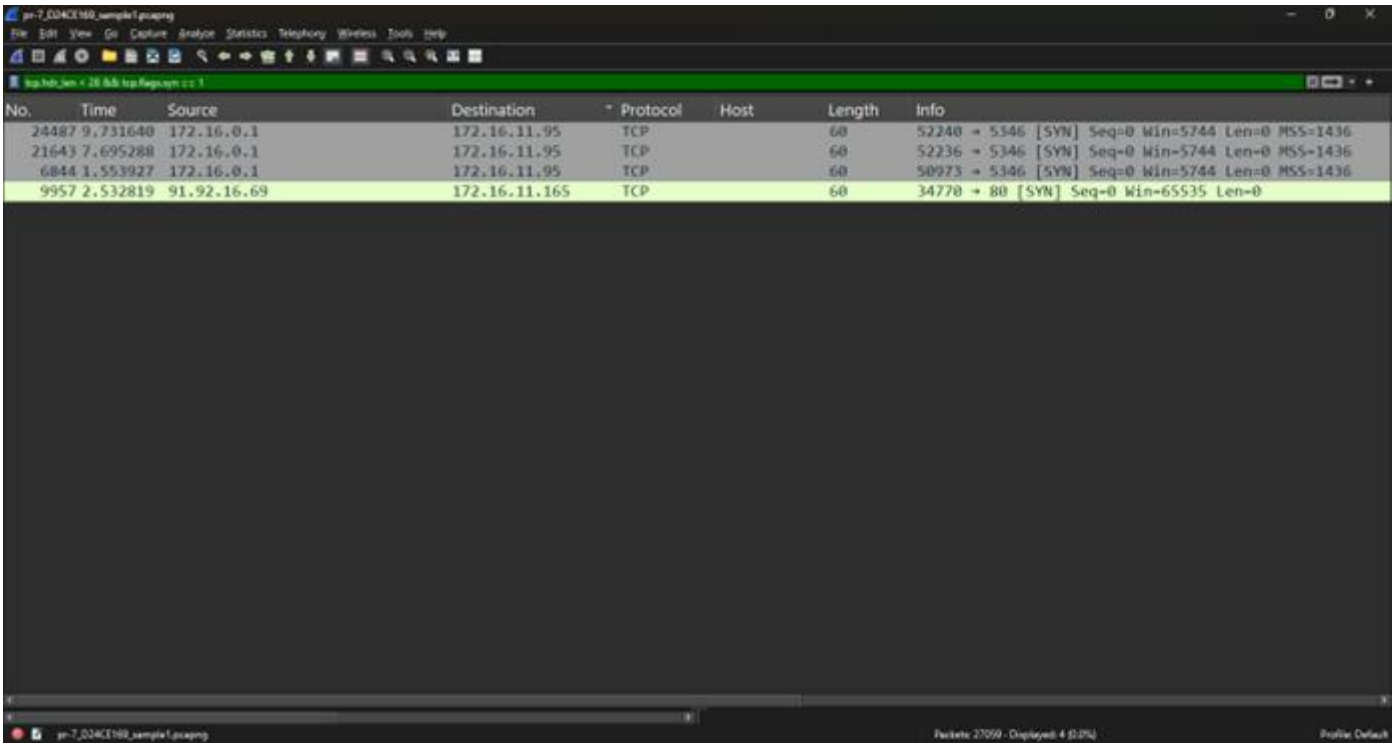
Flow type: All Flows

Addresses: Any

Exercise 11: Refer to the given Wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

Video : Find TCP Connections with Limited Options

Insert screenshots:


pr-7_D24CE169_sample1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.hdr_len < 28 && tcp.flags.syn == 1

No.	Time	Source	Destination	Protocol	Host	Length	Info
24487	9.731640	172.16.0.1	172.16.11.95	TCP		60	52240 → 5346 [SYN] Seq=0 Win=5744 Len=0 MSS=1436
21643	7.695288	172.16.0.1	172.16.11.95	TCP		60	52236 → 5346 [SYN] Seq=0 Win=5744 Len=0 MSS=1436
6844	1.553927	172.16.0.1	172.16.11.95	TCP		60	50973 → 5346 [SYN] Seq=0 Win=5744 Len=0 MSS=1436
9957	2.532819	91.92.16.69	172.16.11.165	TCP		60	34770 → 80 [SYN] Seq=0 Win=65535 Len=0

pr-7_D24CE169_sample1.pcapng Packets: 27059 · Displayed: 4 (0.0%) Profile: Default