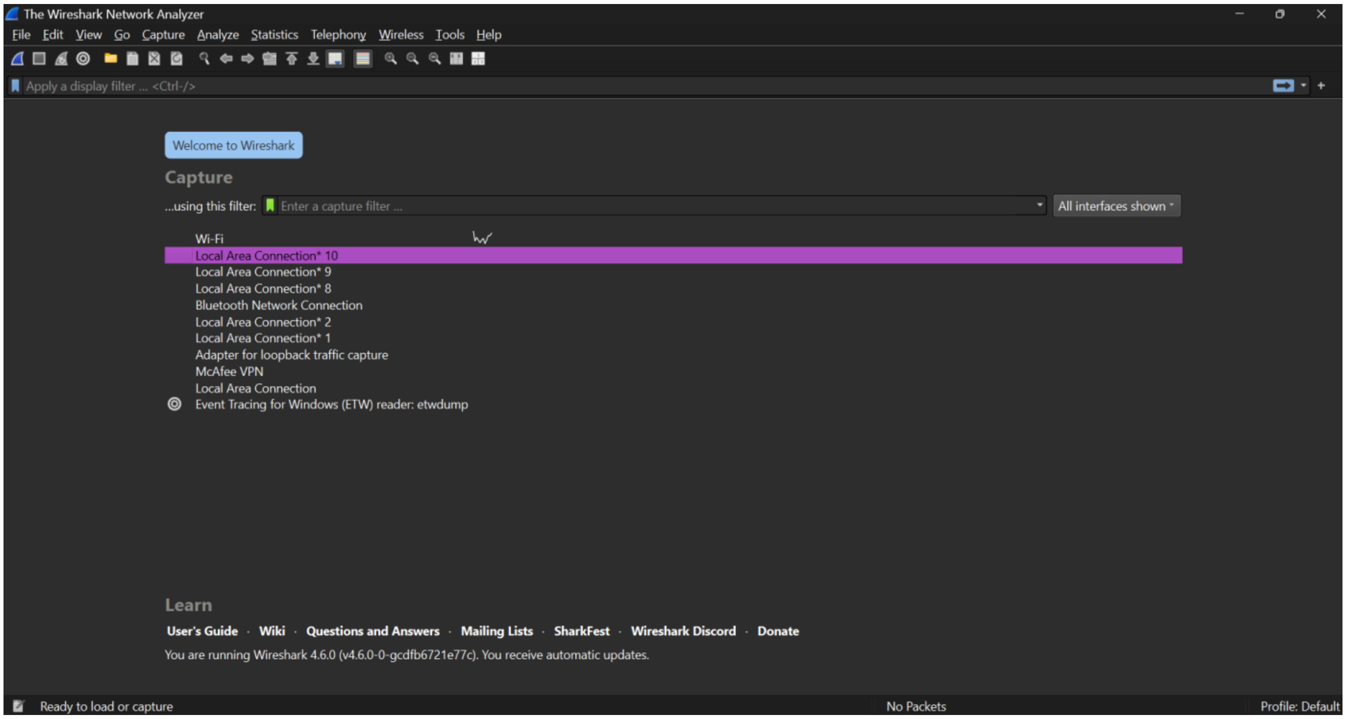
Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.**	
Experiment No: 11	**Date: 24-11-2025**	**Enrolment No:92301733024**

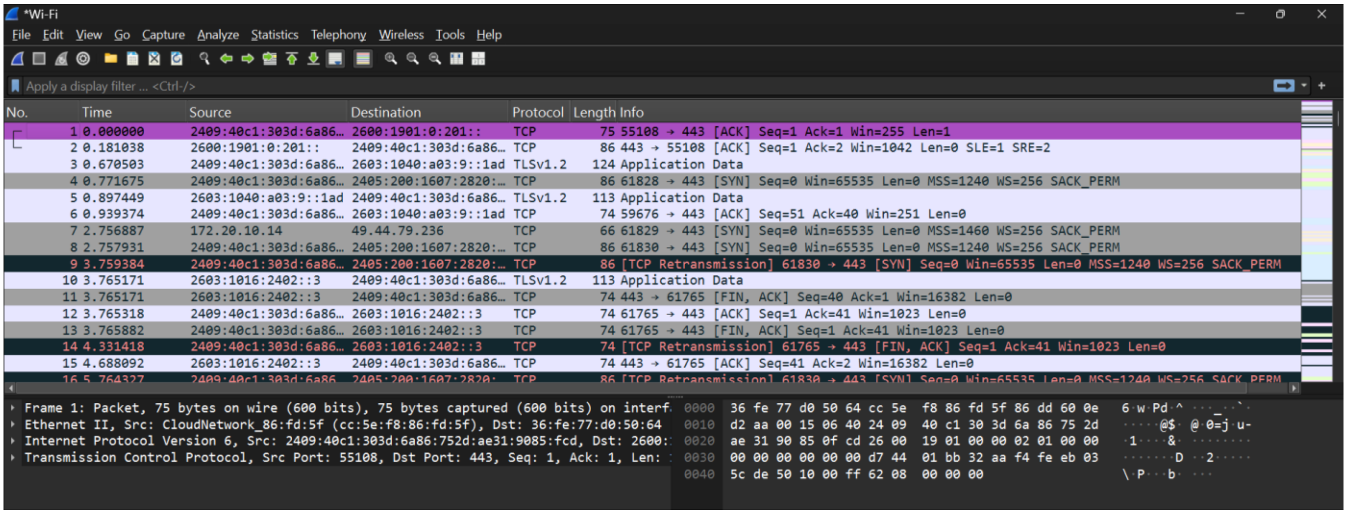
TCP Analysis using Wireshark,

Step – 1:- Open Wireshark



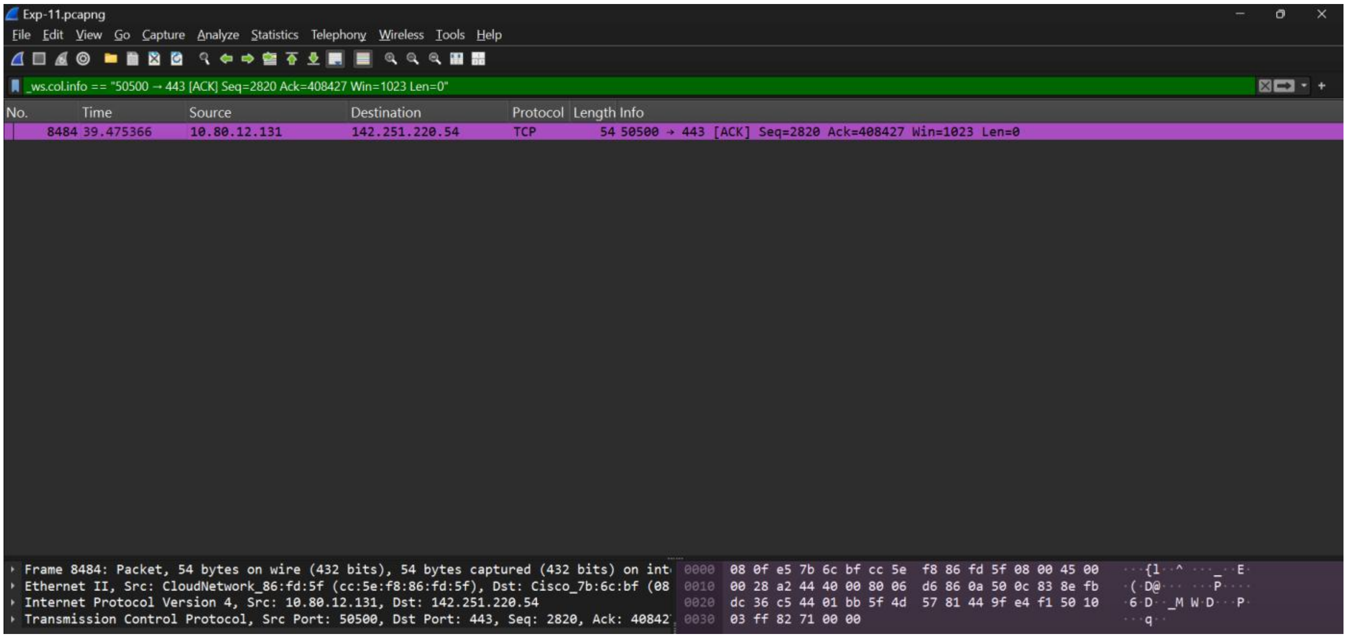
```
The Wireshark Network Analyzer
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture
...using this filter: Enter a capture filter ...                All interfaces shown

   Wi-Fi
   Local Area Connection* 10
   Local Area Connection* 9
   Local Area Connection* 8
   Bluetooth Network Connection
   Local Area Connection* 2
   Local Area Connection* 1
   Adapter for loopback traffic capture
   McAfee VPN
   Local Area Connection
   Event Tracing for Windows (ETW) reader: etwdump

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.6.0 (v4.6.0-0-gcdfb6721e77c). You receive automatic updates.

Ready to load or capture                    No Packets                    Profile: Default
```

Step – 2 :- Select the Network from which you want to communicate



```
*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
    1 0.000000   2409:40c1:303d:6a86…  2600:1901:0:201::      TCP       75 55108 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
    2 0.181038   2600:1901:0:201::      2409:40c1:303d:6a86…  TCP       86 443 → 55108 [ACK] Seq=1 Ack=2 Win=1042 Len=0 SLE=1 SRE=2
    3 0.670503   2409:40c1:303d:6a86…  2603:1040:a03:9::1ad   TLSv1.2  124 Application Data
    4 0.771675   2409:40c1:303d:6a86…  2405:200:1607:2820:…  TCP       86 61828 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1240 WS=256 SACK_PERM
    5 0.897449   2603:1040:a03:9::1ad   2409:40c1:303d:6a86…  TLSv1.2  113 Application Data
    6 0.939374   2409:40c1:303d:6a86…  2603:1040:a03:9::1ad   TCP       74 59676 → 443 [ACK] Seq=51 Ack=40 Win=251 Len=0
    7 2.756887   172.20.10.14           49.44.79.236           TCP       66 61829 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
    8 2.757931   2409:40c1:303d:6a86…  2405:200:1607:2820:…  TCP       86 61830 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1240 WS=256 SACK_PERM
    9 3.759384   2409:40c1:303d:6a86…  2405:200:1607:2820:…  TCP       86 [TCP Retransmission] 61830 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1240 WS=256 SACK_PERM
   10 3.765171   2603:1016:2402::3      2409:40c1:303d:6a86…  TLSv1.2  113 Application Data
   11 3.765171   2603:1016:2402::3      2409:40c1:303d:6a86…  TCP       74 443 → 61765 [FIN, ACK] Seq=40 Ack=1 Win=16382 Len=0
   12 3.765318   2409:40c1:303d:6a86…  2603:1016:2402::3      TCP       74 61765 → 443 [ACK] Seq=1 Ack=41 Win=1023 Len=0
   13 3.765882   2409:40c1:303d:6a86…  2603:1016:2402::3      TCP       74 61765 → 443 [FIN, ACK] Seq=1 Ack=41 Win=1023 Len=0
   14 4.331418   2409:40c1:303d:6a86…  2603:1016:2402::3      TCP       74 [TCP Retransmission] 61765 → 443 [FIN, ACK] Seq=1 Ack=41 Win=1023 Len=0
   15 4.688092   2603:1016:2402::3      2409:40c1:303d:6a86…  TCP       74 443 → 61765 [ACK] Seq=41 Ack=2 Win=16382 Len=0
   16 5.764327   2409:40c1:303d:6a86   2405:200:1607:2820:    TCP       86 [TCP Retransmission] 61830 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1240 WS=256 SACK_PERM

› Frame 1: Packet, 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interf
› Ethernet II, Src: CloudNetwork_86:fd:5f (cc:5e:f8:86:fd:5f), Dst: 36:fe:77:d0:50:64
› Internet Protocol Version 6, Src: 2409:40c1:303d:6a86:752d:ae31:9085:fcd, Dst: 2600::
› Transmission Control Protocol, Src Port: 55108, Dst Port: 443, Seq: 1, Ack: 1, Len:

0000  36 fe 77 d0 50 64 cc 5e  f8 86 fd 5f 86 dd 60 0e   6·w·Pd·^ ···_··`·
0010  d2 aa 00 15 06 40 24 09  40 c1 30 3d 6a 86 75 2d   ·····@$· @·0=j·u-
0020  ae 31 90 85 0f cd 26 00  19 01 00 00 02 01 00 00   ·1····&· ········
0030  00 00 00 00 00 00 d7 44  01 bb 32 aa f4 fe eb 03   ·······D ··2·····
0040  5c de 50 10 00 ff 62 08  00 00 00                  \·P···b· ···
```

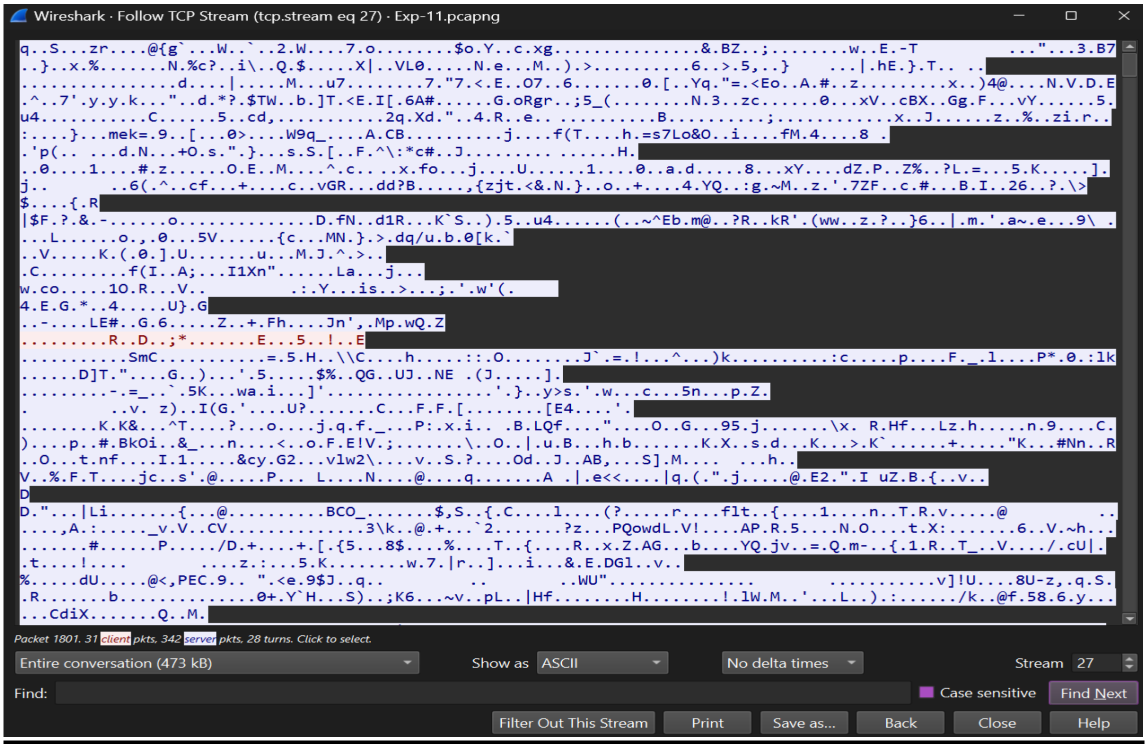
Step – 3 :- Apply Display Filters for TCP Traffic(tcp.port == 80 or tcp.port == 443)



Exp-11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
_ws.col.info == "50500 → 443 [ACK] Seq=2820 Ack=408427 Win=1023 Len=0"

No.   Time       Source         Destination      Protocol Length Info
 8484 39.475366  10.80.12.131   142.251.220.54   TCP          54 50500 → 443 [ACK] Seq=2820 Ack=408427 Win=1023 Len=0

› Frame 8484: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on int
› Ethernet II, Src: CloudNetwork_86:fd:5f (cc:5e:f8:86:fd:5f), Dst: Cisco_7b:6c:bf (08
› Internet Protocol Version 4, Src: 10.80.12.131, Dst: 142.251.220.54
› Transmission Control Protocol, Src Port: 50500, Dst Port: 443, Seq: 2820, Ack: 40842

0000  08 0f e5 7b 6c bf cc 5e  f8 86 fd 5f 08 00 45 00   ···{l··^ ···_··E·
0010  00 28 a2 44 40 00 80 06  d6 86 0a 50 0c 83 8e fb   ·(·D@··· ···P····
0020  dc 36 c5 44 01 bb 5f 4d  57 81 44 9f e4 f1 50 10   ·6·D··_M W·D···P·
0030  03 ff 82 71 00 00                                  ···q··
```

Step – 4 :- Follow a TCP Stream.



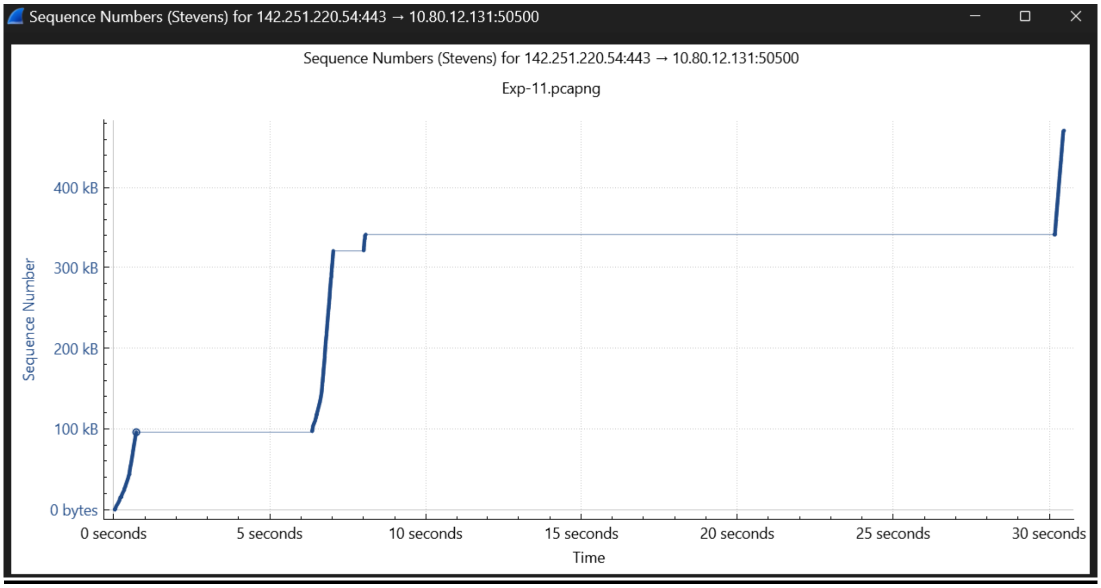
Wireshark · Follow TCP Stream (tcp.stream eq 27) · Exp-11.pcapng

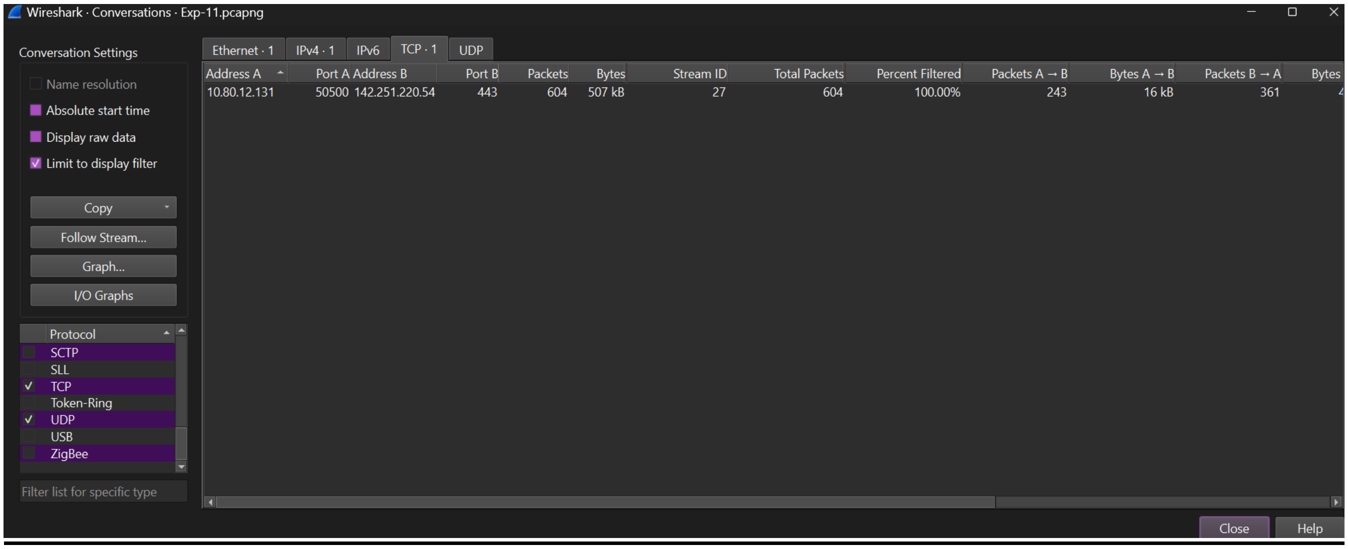
```
q..S...zr....@{g`...W..`..2.W....7.o........$o.Y..c.xg...............&.BZ..;........w..E.-T          ...."...3.B7
..}..x.%.......N.%c?..i\..Q.$.....X|..VL0.....N.e...M..).>..........6..>.5,..}     ...|.hE.}.T..  ..
................d....|.....M...u7........7."7.<.E..O7..6.......0.[..Yq."=.<Eo..A.#..z.........x..)4@....N.V.D.E
.^..7'.y.y.k..."..d.*?.$TW..b.]T.<E.I[.6A#......G.oRgr..;5_(........N.3..zc......0...xV..cBX..Gg.F...vY......5.
u4..........C......5..cd,...........2q.Xd."..4.R..e.. ..........B..........;............x..J......z..%..zi.r..
:....}...mek=.9..[...0>....W9q_....A.CB..........j....f(T....h.=s7Lo&O..i....fM.4....8 .
.'p(.. ...d.N...+O.s.".}...s.S.[..F.^\:*c#..J......... ......H.
..0....1....#.z......O.E..M....^.c.. ..x.fo...j....U......1....0..a.d.....8...xY....dZ.P..Z%..?L.=...5.K.....].
j..        ..6(.^..cf...+....c..vGR...dd?B.....,{zjt.<&.N.}..o..+....4.YQ..:g.~M..z.'.7ZF..c.#...B.I..26..?.\>
$....{.R
|$F.?.&.-......o.............D.fN..d1R...K`S..).5..u4......(..~^Eb.m@..?R..kR'.(ww..z.?..}6..|.m.'.a~.e...9\ .
...L......o.,.0...5V......{c...MN.}.>.dq/u.b.0[k.`
..V.....K.(.0.].U.......u...M.J.^.>..
.C.........f(I..A;...I1Xn"......La...j...
w.co.....1O.R...V..          .:.Y...is..>...;.'.w'(.
4.E.G.*..4.....U}.G
..-....LE#..G.6.....Z..+.Fh....Jn',.Mp.wQ.Z
.........R..D..;*.......E...5..!..E
..........SmC...........=.5.H..\\C....h.....::.O........J`.=.!...^...)k..........:c.....p....F._.1....P*.0.:1k
......D]T."....G..)...'.5.....$%..QG..UJ..NE .(J.....].
.........-.=_..`.5K...wa.i...]'.................'.}..y>s.'.w...c...5n...p.Z.
.        ..v. z)..I(G.'....U?.......C...F.F.[........[E4....'.
........K.K&...^T....?...o....j.q.f._...P:.x.i.. .B.LQf...."....O..G...95.j.......\x. R.Hf...Lz.h.....n.9....C.
)....p..#.BkOi..&_...n....<..o.F.E!V.;.......\..O..|.u.B...h.b.......K.X..s.d...K...>.K`......+....."K...#Nn..R
..O...t.nf....I.1.....&cy.G2...vlw2\....v..S.?....Od..J..AB,...S].M....   ...h..
V..%.F.T....jc..s'.@.....P...  L....N....@....q.......A .|.e<<....|q.(.".j.....@.E2.".I uZ.B.{..v..
D
D."...|Li.......{...@..........BCO_.......$,S..{.C....l....(?.....r....flt..{....1....n..T.R.v.....@         ..
....,A.:....._v.V..CV..............3\k..@.+...`2.......?z...PQowdL.V!....AP.R.5....N.O....t.X:.......6..V.~h...
.......#......P...../D.+....+.[.{5...8$....%....T..{....R..x.Z.AG...b....YQ.jv..=.Q.m-..{.1.R..T_..V..../.cU|.
.t....!....        ....z.:...5.K........w.7.|r..]...i...&.E.DGl..v..
%.....dU.....@<,PEC.9..  ".<e.9$J..q..          ..        ..WU"...............        ...........v]!U....8U-z,.q.S.
.R.......b...............0+.Y`H...S)..;K6...~v..pL..|Hf........H.........!.1W.M..'...L..).:....../k..@f.58.6.y...
...CdiX.......Q..M.
```

Packet 1801. 31 client pkts, 342 server pkts, 28 turns. Click to select.

Entire conversation (473 kB) | Show as: ASCII | No delta times | Stream: 27

Step – 5 :- View TCP Statistics and Graphs.

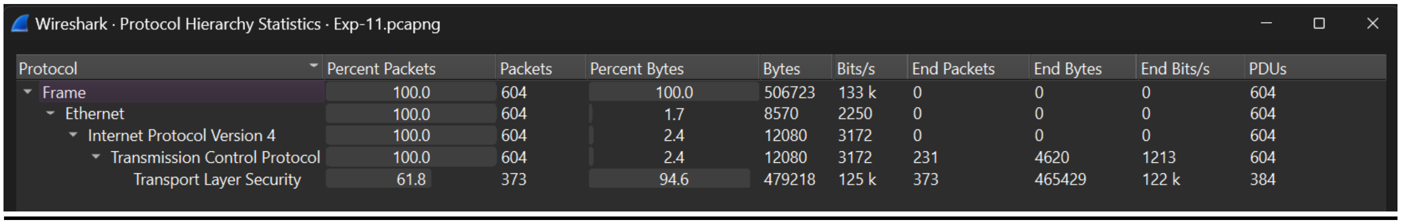




☐ Name resolution
☑ Absolute start time
☑ Display raw data
☑ Limit to display filter

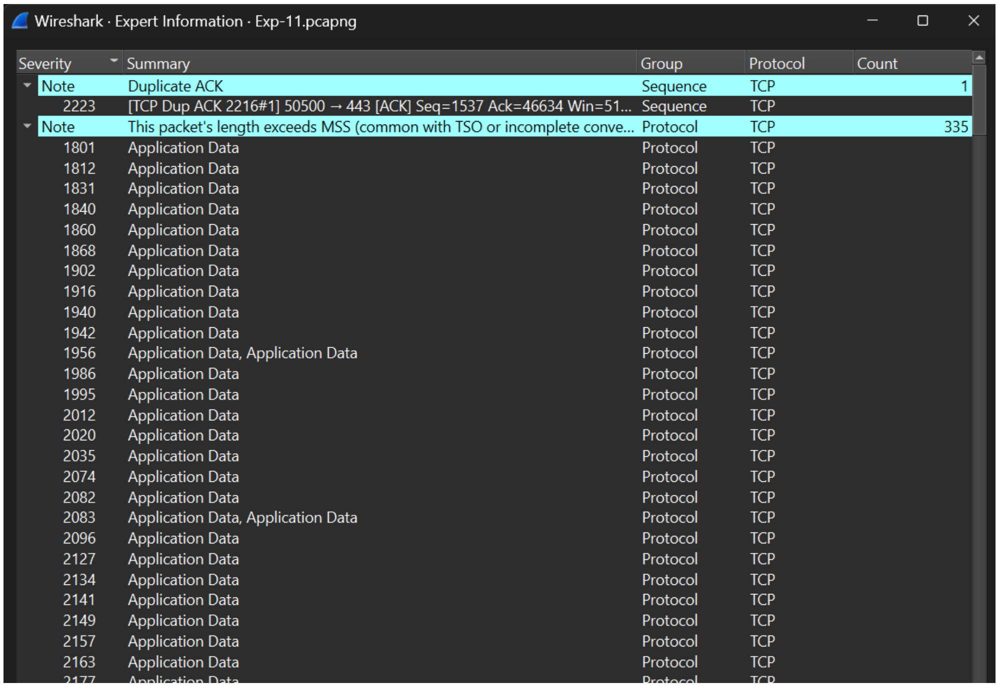
	Protocol
☐	SCTP
	SLL
✓	TCP
	Token-Ring
✓	UDP
	USB
☐	ZigBee

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes
10.80.12.131	50500	142.251.220.54	443	604	507 kB	27	604	100.00%	243	16 kB	361	4



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	604	100.0	506723	133 k	0	0	0	604
Ethernet	100.0	604	1.7	8570	2250	0	0	0	604
Internet Protocol Version 4	100.0	604	2.4	12080	3172	0	0	0	604
Transmission Control Protocol	100.0	604	2.4	12080	3172	231	4620	1213	604
Transport Layer Security	61.8	373	94.6	479218	125 k	373	465429	122 k	384

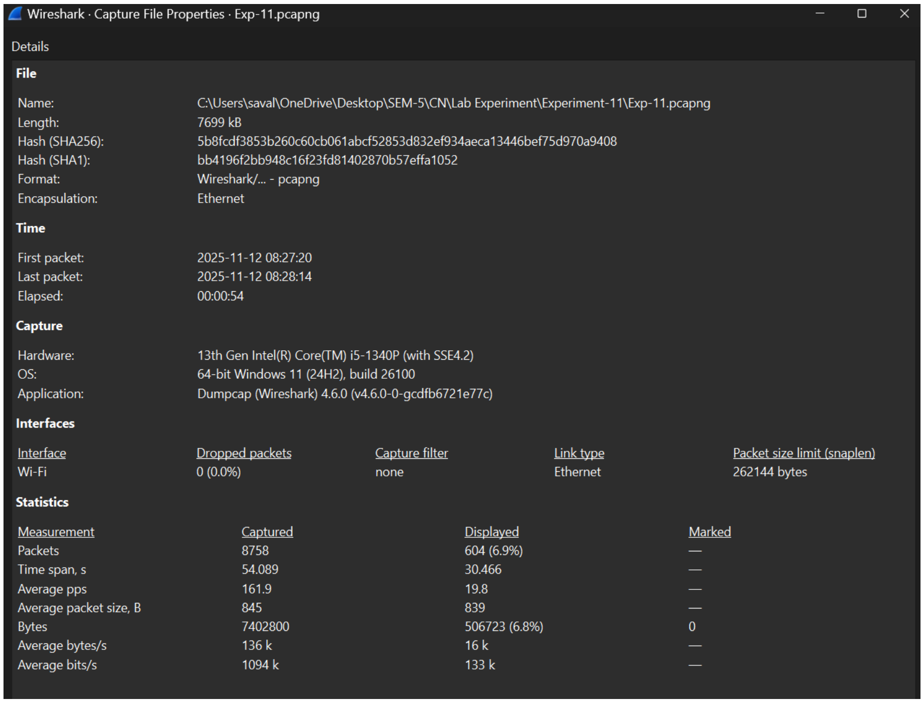
Step – 7 :- Check Expert Information for Anomalies.



Wireshark · Expert Information · Exp-11.pcapng

Severity	Summary	Group	Protocol	Count
Note	Duplicate ACK	Sequence	TCP	1
2223	[TCP Dup ACK 2216#1] 50500 → 443 [ACK] Seq=1537 Ack=46634 Win=51...	Sequence	TCP	
Note	This packet's length exceeds MSS (common with TSO or incomplete conve...	Protocol	TCP	335
1801	Application Data	Protocol	TCP	
1812	Application Data	Protocol	TCP	
1831	Application Data	Protocol	TCP	
1840	Application Data	Protocol	TCP	
1860	Application Data	Protocol	TCP	
1868	Application Data	Protocol	TCP	
1902	Application Data	Protocol	TCP	
1916	Application Data	Protocol	TCP	
1940	Application Data	Protocol	TCP	
1942	Application Data	Protocol	TCP	
1956	Application Data, Application Data	Protocol	TCP	
1986	Application Data	Protocol	TCP	
1995	Application Data	Protocol	TCP	
2012	Application Data	Protocol	TCP	
2020	Application Data	Protocol	TCP	
2035	Application Data	Protocol	TCP	
2074	Application Data	Protocol	TCP	
2082	Application Data	Protocol	TCP	
2083	Application Data, Application Data	Protocol	TCP	
2096	Application Data	Protocol	TCP	
2127	Application Data	Protocol	TCP	
2134	Application Data	Protocol	TCP	
2141	Application Data	Protocol	TCP	
2149	Application Data	Protocol	TCP	
2157	Application Data	Protocol	TCP	
2163	Application Data	Protocol	TCP	
2177	Application Data	Protocol	TCP	

Step – 8:- Export and Report Findings.



Wireshark · Capture File Properties · Exp-11.pcapng

Details

File

Name:	C:\Users\saval\OneDrive\Desktop\SEM-5\CN\Lab Experiment\Experiment-11\Exp-11.pcapng
Length:	7699 kB
Hash (SHA256):	5b8fcdf3853b260c60cb061abcf52853d832ef934aeca13446bef75d970a9408
Hash (SHA1):	bb4196f2bb948c16f23fd81402870b57effa1052
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2025-11-12 08:27:20
Last packet:	2025-11-12 08:28:14
Elapsed:	00:00:54

Capture

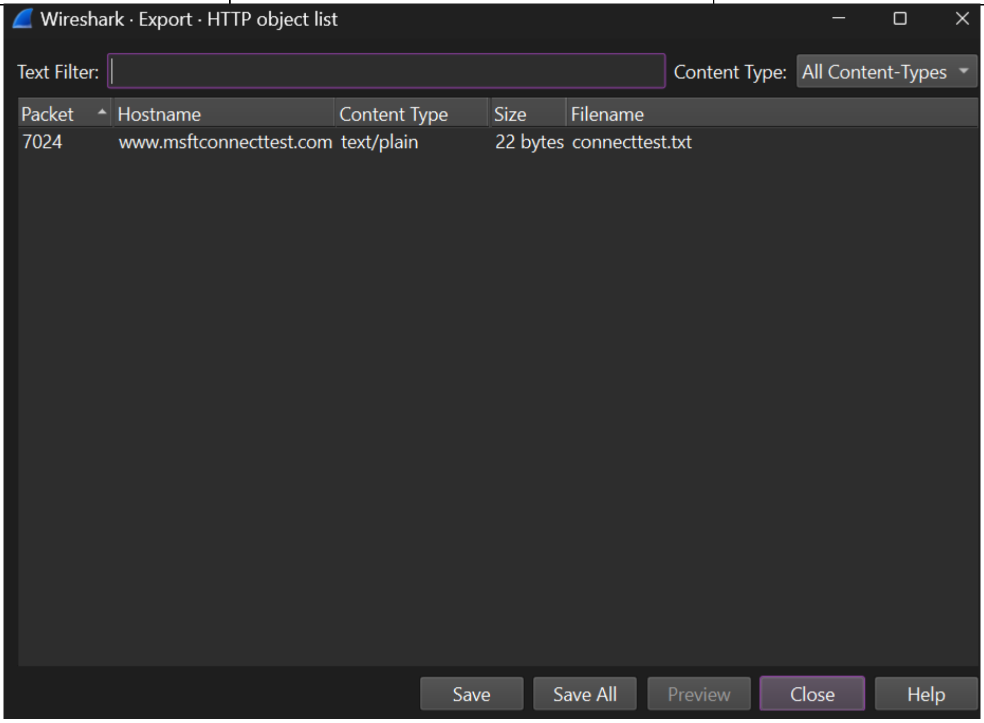
Hardware:	13th Gen Intel(R) Core(TM) i5-1340P (with SSE4.2)
OS:	64-bit Windows 11 (24H2), build 26100
Application:	Dumpcap (Wireshark) 4.6.0 (v4.6.0-0-gcdfb6721e77c)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	8758	604 (6.9%)	—
Time span, s	54.089	30.466	—
Average pps	161.9	19.8	—
Average packet size, B	845	839	—
Bytes	7402800	506723 (6.8%)	0
Average bytes/s	136 k	16 k	—
Average bits/s	1094 k	133 k	—



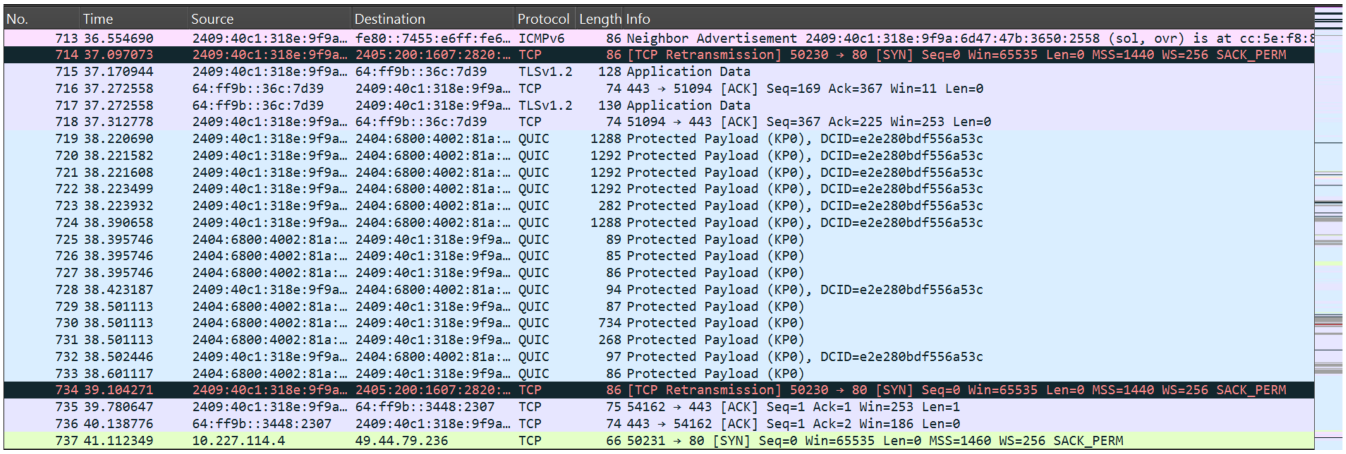
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Save
Save All
Preview
Close
Help

Packet	Hostname	Content Type	Size	Filename
7024	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

UDP (User Datagram Protocol) Analysis using Wireshark

Step-1: Start Capturing Packets

While capturing, perform a network activity to generate UDP traffic: Open Command Prompt (search "cmd" in Start menu), type "nslookup example.com" and press Enter. This sends a UDP DNS query to a server on port 53.



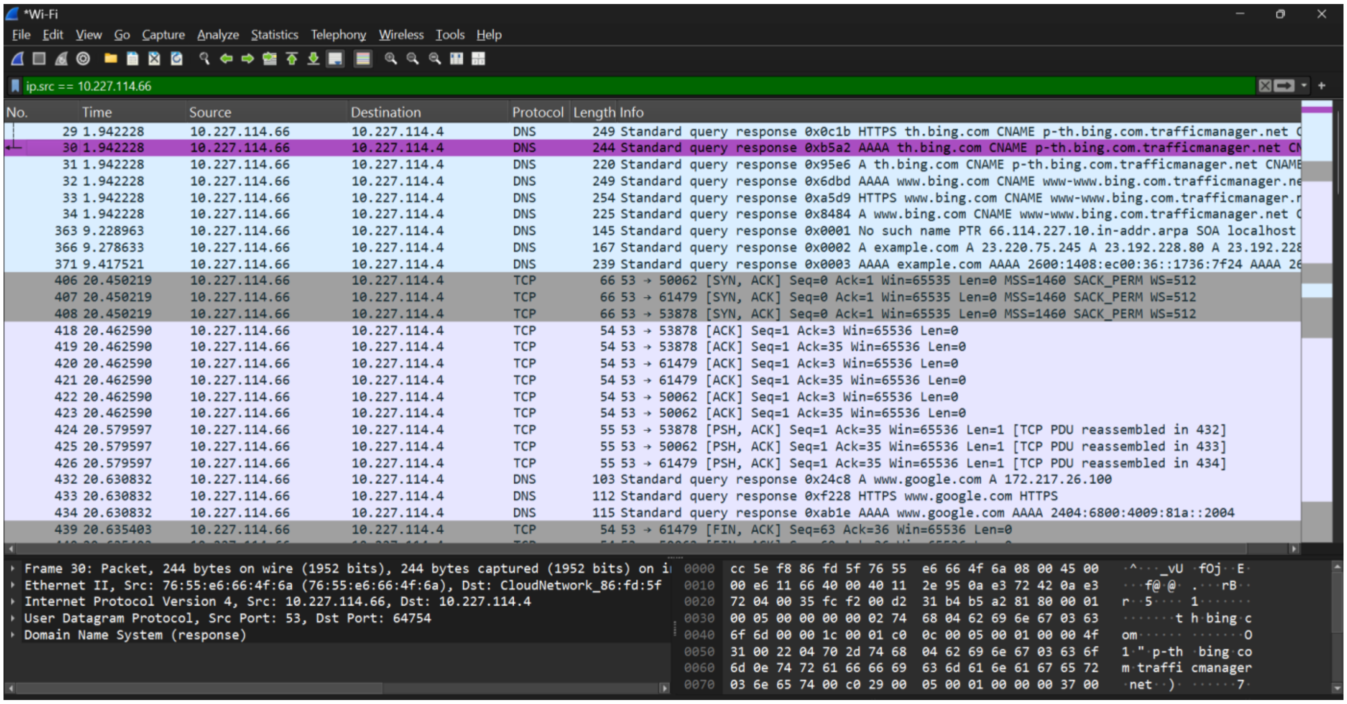
```
No.     Time        Source                   Destination              Protocol Length Info
    713 36.554690   2409:40c1:318e:9f9a…     fe80::7455:e6ff:fe6…     ICMPv6     86 Neighbor Advertisement 2409:40c1:318e:9f9a:6d47:47b:3650:2558 (sol, ovr) is at cc:5e:f8:8
    714 37.097073   2409:40c1:318e:9f9a…     2405:200:1607:2820:…     TCP        86 [TCP Retransmission] 50230 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
    715 37.170944   2409:40c1:318e:9f9a…     64:ff9b::36c:7d39        TLSv1.2   128 Application Data
    716 37.272558   64:ff9b::36c:7d39        2409:40c1:318e:9f9a…     TCP        74 443 → 51094 [ACK] Seq=169 Ack=367 Win=11 Len=0
    717 37.272558   64:ff9b::36c:7d39        2409:40c1:318e:9f9a…     TLSv1.2   130 Application Data
    718 37.312778   2409:40c1:318e:9f9a…     64:ff9b::36c:7d39        TCP        74 51094 → 443 [ACK] Seq=367 Ack=225 Win=253 Len=0
    719 38.220690   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC     1288 Protected Payload (KP0), DCID=e2e280bdf556a53c
    720 38.221582   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC     1292 Protected Payload (KP0), DCID=e2e280bdf556a53c
    721 38.221608   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC     1292 Protected Payload (KP0), DCID=e2e280bdf556a53c
    722 38.223499   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC     1292 Protected Payload (KP0), DCID=e2e280bdf556a53c
    723 38.223932   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC      282 Protected Payload (KP0), DCID=e2e280bdf556a53c
    724 38.390658   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC     1288 Protected Payload (KP0), DCID=e2e280bdf556a53c
    725 38.395746   2404:6800:4002:81a:…     2409:40c1:318e:9f9a…     QUIC       89 Protected Payload (KP0)
    726 38.395746   2404:6800:4002:81a:…     2409:40c1:318e:9f9a…     QUIC       85 Protected Payload (KP0)
    727 38.395746   2404:6800:4002:81a:…     2409:40c1:318e:9f9a…     QUIC       86 Protected Payload (KP0)
    728 38.423187   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC       94 Protected Payload (KP0), DCID=e2e280bdf556a53c
    729 38.501113   2404:6800:4002:81a:…     2409:40c1:318e:9f9a…     QUIC       87 Protected Payload (KP0)
    730 38.501113   2404:6800:4002:81a:…     2409:40c1:318e:9f9a…     QUIC      734 Protected Payload (KP0)
    731 38.501113   2404:6800:4002:81a:…     2409:40c1:318e:9f9a…     QUIC      268 Protected Payload (KP0)
    732 38.502446   2409:40c1:318e:9f9a…     2404:6800:4002:81a:…     QUIC       97 Protected Payload (KP0), DCID=e2e280bdf556a53c
    733 38.601117   2404:6800:4002:81a:…     2409:40c1:318e:9f9a…     QUIC       86 Protected Payload (KP0)
    734 39.104271   2409:40c1:318e:9f9a…     2405:200:1607:2820:…     TCP        86 [TCP Retransmission] 50230 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
    735 39.780647   2409:40c1:318e:9f9a…     64:ff9b::3448:2307       TCP        75 54162 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
    736 40.138776   64:ff9b::3448:2307       2409:40c1:318e:9f9a…     TCP        74 443 → 54162 [ACK] Seq=1 Ack=2 Win=186 Len=0
    737 41.112349   10.227.114.4             49.44.79.236             TCP        66 50231 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
```

Step-2: Stop the Capture and Save the File

Go to File > Save As, choose a location (e.g., Desktop), name it (e.g., "udp_capture.pcapng"), and save in .pcapng format for full metadata.

Step-3: Apply Display Filters for UDP Traffic

- In the filter bar (green box above the packet list), type "udp" and press Enter (or Apply).
- For specifics: "udp.port == 53" for DNS, or "udp.length > 100" for larger datagrams.
- Right-click a packet > Apply as Filter > Selected to quickly filter based on a field (e.g., source IP).


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

ip.src == 10.227.114.66

```
No.  Time         Source          Destination    Protocol Length Info
  29 1.942228     10.227.114.66   10.227.114.4   DNS      249 Standard query response 0x0c1b HTTPS th.bing.com CNAME p-th.bing.com.trafficmanager.net C
  30 1.942228     10.227.114.66   10.227.114.4   DNS      244 Standard query response 0xb5a2 AAAA th.bing.com CNAME p-th.bing.com.trafficmanager.net CN
  31 1.942228     10.227.114.66   10.227.114.4   DNS      220 Standard query response 0x95e6 A th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME
  32 1.942228     10.227.114.66   10.227.114.4   DNS      249 Standard query response 0x6dbd AAAA www.bing.com CNAME www-www.bing.com.trafficmanager.ne
  33 1.942228     10.227.114.66   10.227.114.4   DNS      254 Standard query response 0xa5d9 HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.r
  34 1.942228     10.227.114.66   10.227.114.4   DNS      225 Standard query response 0x8484 A www.bing.com CNAME www-www.bing.com.trafficmanager.net C
 363 9.228963     10.227.114.66   10.227.114.4   DNS      145 Standard query response 0x0001 No such name PTR 66.114.227.10.in-addr.arpa SOA localhost
 366 9.278633     10.227.114.66   10.227.114.4   DNS      167 Standard query response 0x0002 A example.com A 23.220.75.245 A 23.192.228.80 A 23.192.228
 371 9.417521     10.227.114.66   10.227.114.4   DNS      239 Standard query response 0x0003 AAAA example.com AAAA 2600:1408:ec00:36::1736:7f24 AAAA 26
 406 20.450219    10.227.114.66   10.227.114.4   TCP       66 53 → 50062 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
 407 20.450219    10.227.114.66   10.227.114.4   TCP       66 53 → 61479 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
 408 20.450219    10.227.114.66   10.227.114.4   TCP       66 53 → 53878 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
 418 20.462590    10.227.114.66   10.227.114.4   TCP       54 53 → 53878 [ACK] Seq=1 Ack=3 Win=65536 Len=0
 419 20.462590    10.227.114.66   10.227.114.4   TCP       54 53 → 53878 [ACK] Seq=1 Ack=35 Win=65536 Len=0
 420 20.462590    10.227.114.66   10.227.114.4   TCP       54 53 → 61479 [ACK] Seq=1 Ack=3 Win=65536 Len=0
 421 20.462590    10.227.114.66   10.227.114.4   TCP       54 53 → 61479 [ACK] Seq=1 Ack=35 Win=65536 Len=0
 422 20.462590    10.227.114.66   10.227.114.4   TCP       54 53 → 50062 [ACK] Seq=1 Ack=3 Win=65536 Len=0
 423 20.462590    10.227.114.66   10.227.114.4   TCP       54 53 → 50062 [ACK] Seq=1 Ack=35 Win=65536 Len=0
 424 20.579597    10.227.114.66   10.227.114.4   TCP       55 53 → 53878 [PSH, ACK] Seq=1 Ack=35 Win=65536 Len=1 [TCP PDU reassembled in 432]
 425 20.579597    10.227.114.66   10.227.114.4   TCP       55 53 → 50062 [PSH, ACK] Seq=1 Ack=35 Win=65536 Len=1 [TCP PDU reassembled in 433]
 426 20.579597    10.227.114.66   10.227.114.4   TCP       55 53 → 61479 [PSH, ACK] Seq=1 Ack=35 Win=65536 Len=1 [TCP PDU reassembled in 434]
 432 20.630832    10.227.114.66   10.227.114.4   DNS      103 Standard query response 0x24c8 A www.google.com A 172.217.26.100
 433 20.630832    10.227.114.66   10.227.114.4   DNS      112 Standard query response 0xf228 HTTPS www.google.com HTTPS
 434 20.630832    10.227.114.66   10.227.114.4   DNS      115 Standard query response 0xab1e AAAA www.google.com AAAA 2404:6800:4009:81a::2004
 439 20.635403    10.227.114.66   10.227.114.4   TCP       54 53 → 61479 [FIN, ACK] Seq=63 Ack=36 Win=65536 Len=0
```

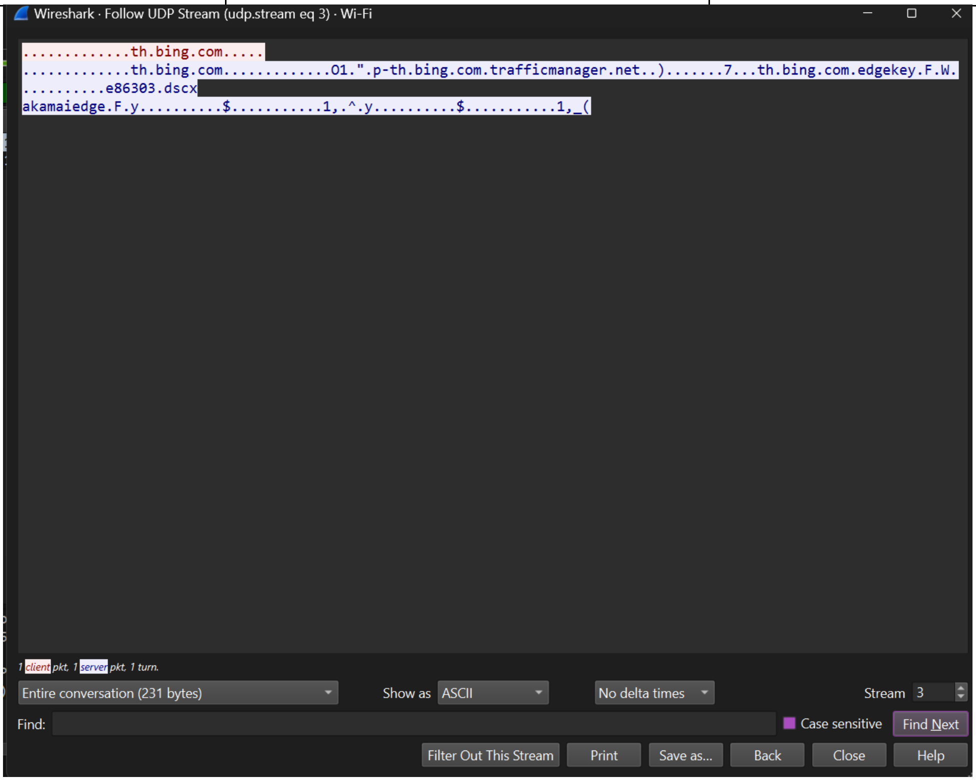
```
› Frame 30: Packet, 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits) on i
› Ethernet II, Src: 76:55:e6:66:4f:6a (76:55:e6:66:4f:6a), Dst: CloudNetwork_86:fd:5f
› Internet Protocol Version 4, Src: 10.227.114.66, Dst: 10.227.114.4
› User Datagram Protocol, Src Port: 53, Dst Port: 64754
› Domain Name System (response)
```

```
0000  cc 5e f8 86 fd 5f 76 55  e6 66 4f 6a 08 00 45 00   ·^···_vU ·fOj··E·
0010  00 e6 11 66 40 00 40 11  2e 95 0a e3 72 42 0a e3   ···f@·@· .···rB··
0020  72 04 00 35 fc f2 00 d2  31 b4 b5 a2 81 80 00 01   r··5···· 1·······
0030  00 05 00 00 00 00 02 74  68 04 62 69 6e 67 03 63   ·······t h·bing·c
0040  6f 6d 00 00 1c 00 01 c0  0c 00 05 00 01 00 00 4f   om······ ·······O
0050  31 00 22 04 70 2d 74 68  04 62 69 6e 67 03 63 6f   1·"·p-th ·bing·co
0060  6d 0e 74 72 61 66 66 69  63 6d 61 6e 61 67 65 72   m·traffi cmanager
0070  03 6e 65 74 00 c0 29 00  05 00 01 00 00 00 37 00   ·net··)· ······7·
```

Step-4: Follow a UDP Stream

- Select a UDP packet in the list (e.g., one with DNS data).
- Right-click > Follow > UDP Stream (or Analyze > Follow > UDP Stream).
- In the stream window, switch views: "Entire conversation," "ASCII," or "Hex Dump." Click "Save As" to export the stream.

Step 7: View UDP Statistics and Graphs



Wireshark · Follow UDP Stream (udp.stream eq 3) · Wi-Fi

```
.............th.bing.com.....
.............th.bing.com.............01.".p-th.bing.com.trafficmanager.net..).......7...th.bing.com.edgekey.F.W.
..........e86303.dscx
akamaiedge.F.y.........$..........1,.^.y.........$..........1,_(
```

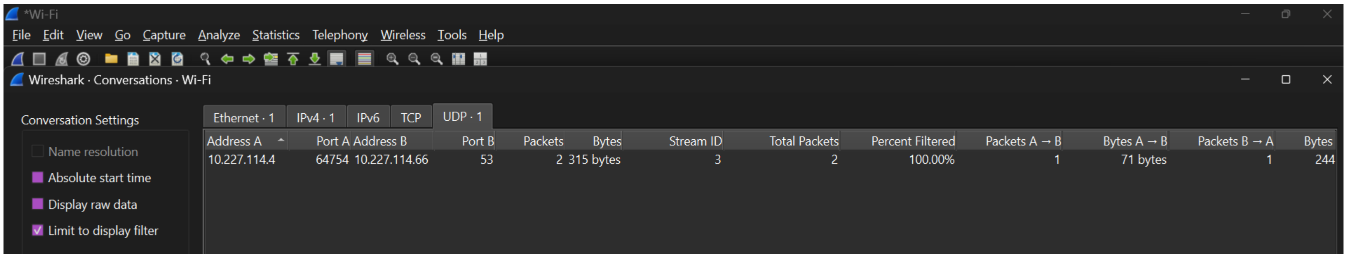
1 client pkt, 1 server pkt, 1 turn.

Entire conversation (231 bytes) · Show as: ASCII · No delta times · Stream: 3

Find: · ■ Case sensitive

Step-5: View UDP Statistics and Graphs

- Go to Statistics > Conversations > UDP tab for endpoint summaries.
- Or Statistics > Protocol Hierarchy to see UDP percentage.
- For graphs: Statistics > IO Graphs, filter for "udp" to plot packet rates over time (no dedicated UDP stream graphs like TCP).

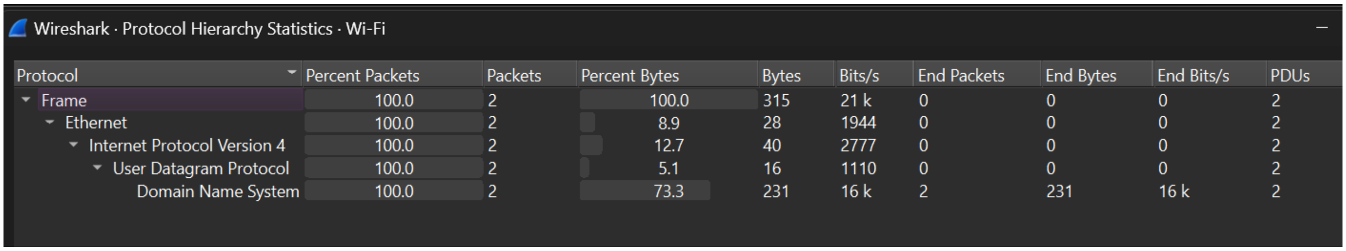


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · Wi-Fi
Ethernet · 1
IPv4 · 1
IPv6
TCP
UDP · 1

Conversation Settings

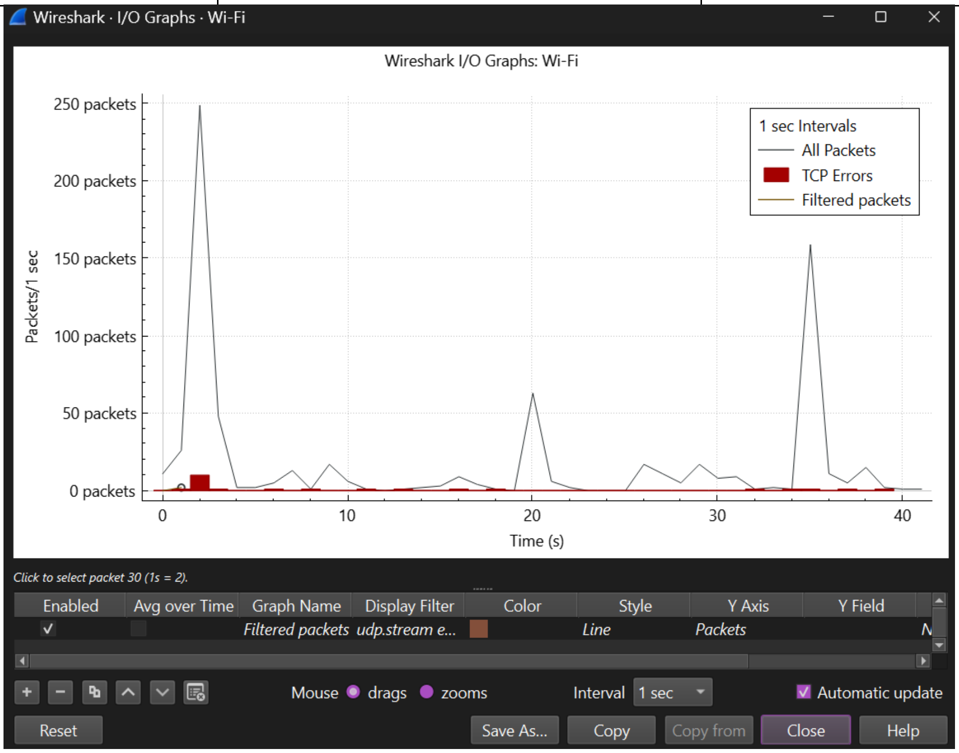
- □ Name resolution
- ■ Absolute start time
- ■ Display raw data
- ☑ Limit to display filter

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes
10.227.114.4	64754	10.227.114.66	53	2	315 bytes	3	2	100.00%	1	71 bytes	1	244



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	2	100.0	315	21 k	0	0	0	2
Ethernet	100.0	2	8.9	28	1944	0	0	0	2
Internet Protocol Version 4	100.0	2	12.7	40	2777	0	0	0	2
User Datagram Protocol	100.0	2	5.1	16	1110	0	0	0	2
Domain Name System	100.0	2	73.3	231	16 k	2	231	16 k	2



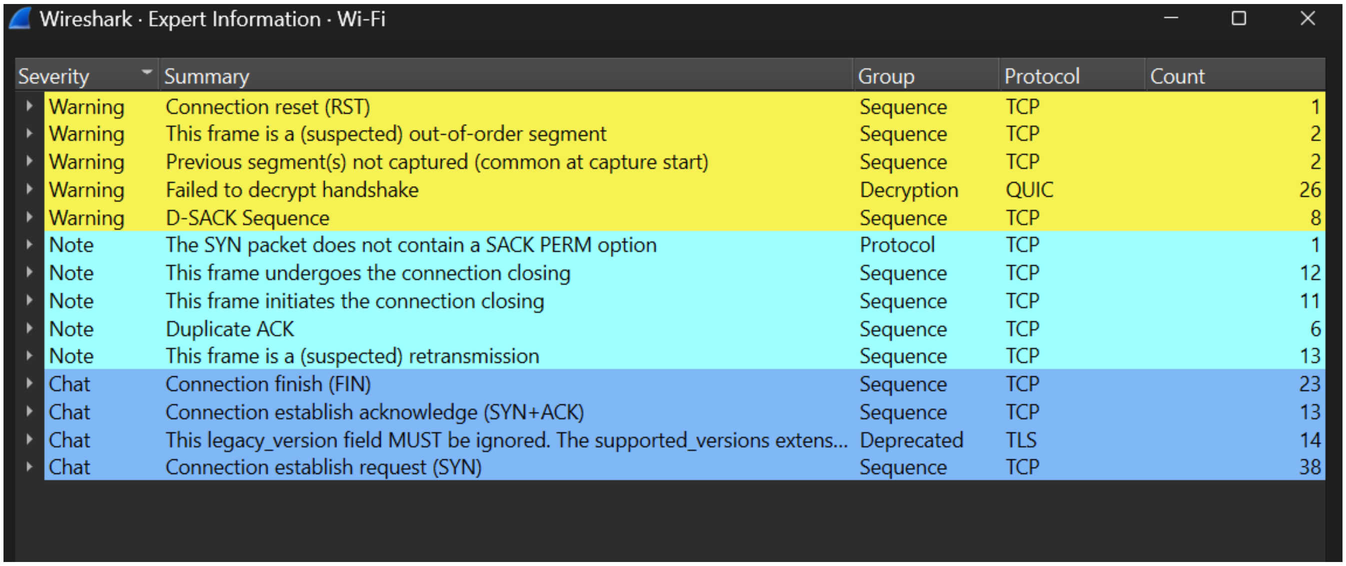
Enabled	Avg over Time	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
✓	□	Filtered packets	udp.stream e...	■	Line	Packets	N

Interval 1 sec

☑ Automatic update

Step-6: Check Expert Information for Anomalies

- Go to Analyze > Expert Information.
- Filter by severity: Errors (red), Warnings (yellow), Notes (cyan), Chats (blue).
- Click entries to jump to packets



Severity	Summary	Group	Protocol	Count
Warning	Connection reset (RST)	Sequence	TCP	1
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	2
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	2
Warning	Failed to decrypt handshake	Decryption	QUIC	26
Warning	D-SACK Sequence	Sequence	TCP	8
Note	The SYN packet does not contain a SACK PERM option	Protocol	TCP	1
Note	This frame undergoes the connection closing	Sequence	TCP	12
Note	This frame initiates the connection closing	Sequence	TCP	11
Note	Duplicate ACK	Sequence	TCP	6
Note	This frame is a (suspected) retransmission	Sequence	TCP	13
Chat	Connection finish (FIN)	Sequence	TCP	23
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	13
Chat	This legacy_version field MUST be ignored. The supported_versions extens...	Deprecated	TLS	14
Chat	Connection establish request (SYN)	Sequence	TCP	38

Step-7: Export and Report Findings

- For reports: Statistics > Capture File Properties > Copy to clipboard.
- Export objects: File > Export Objects > HTTP (if UDP carries HTTP-like data) or general packet bytes.
- Close Wireshark or File > Quit.