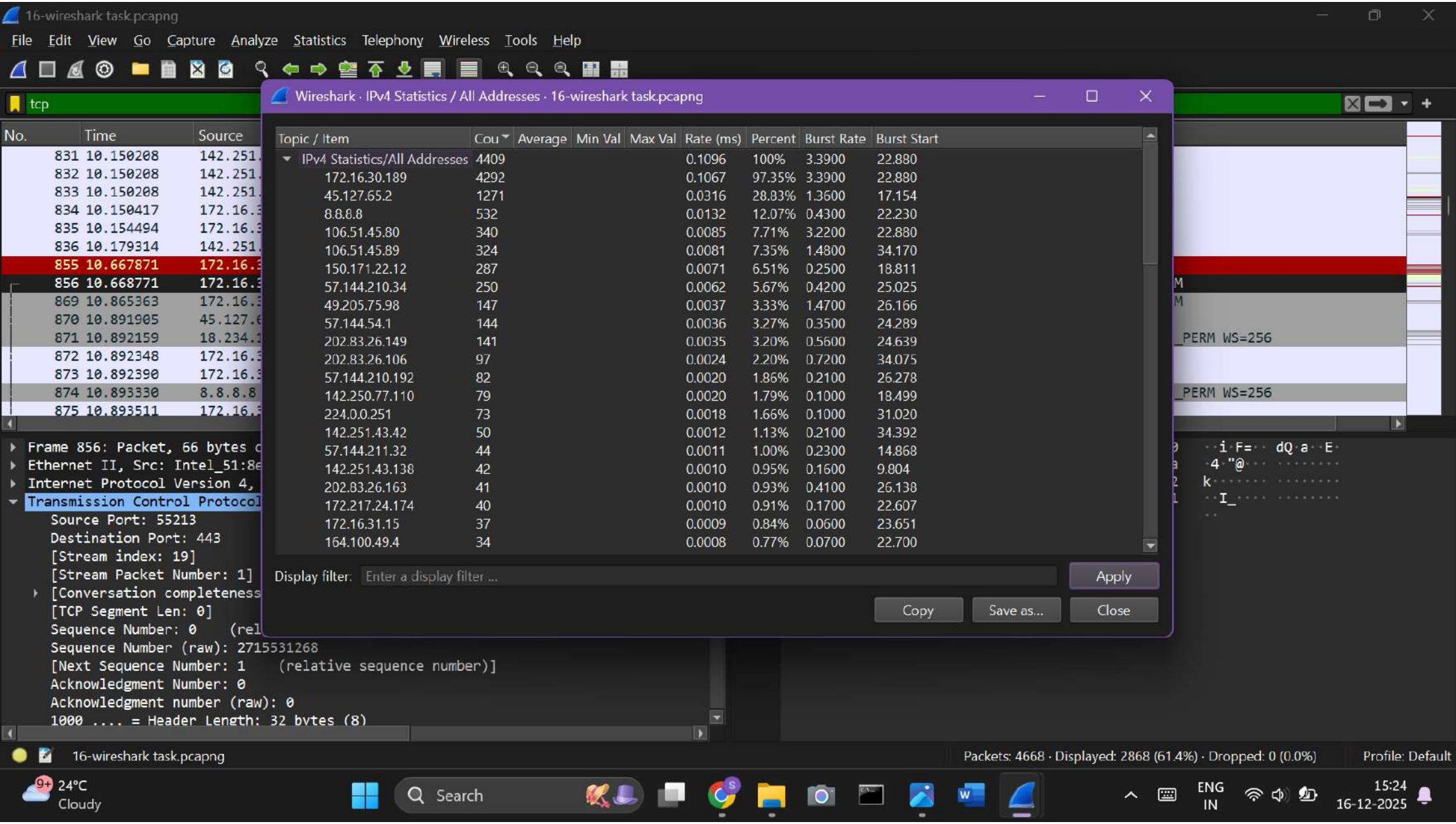
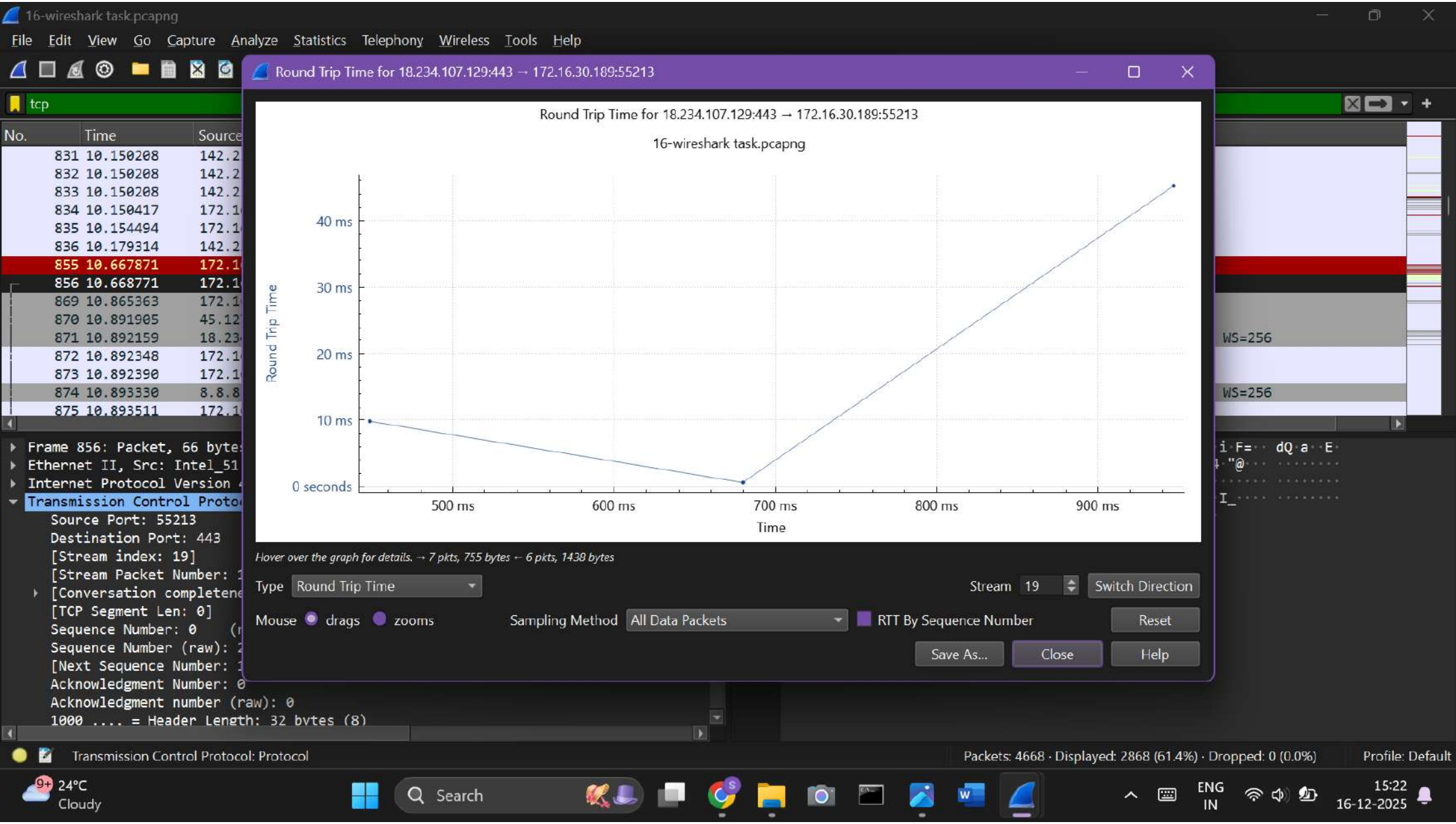
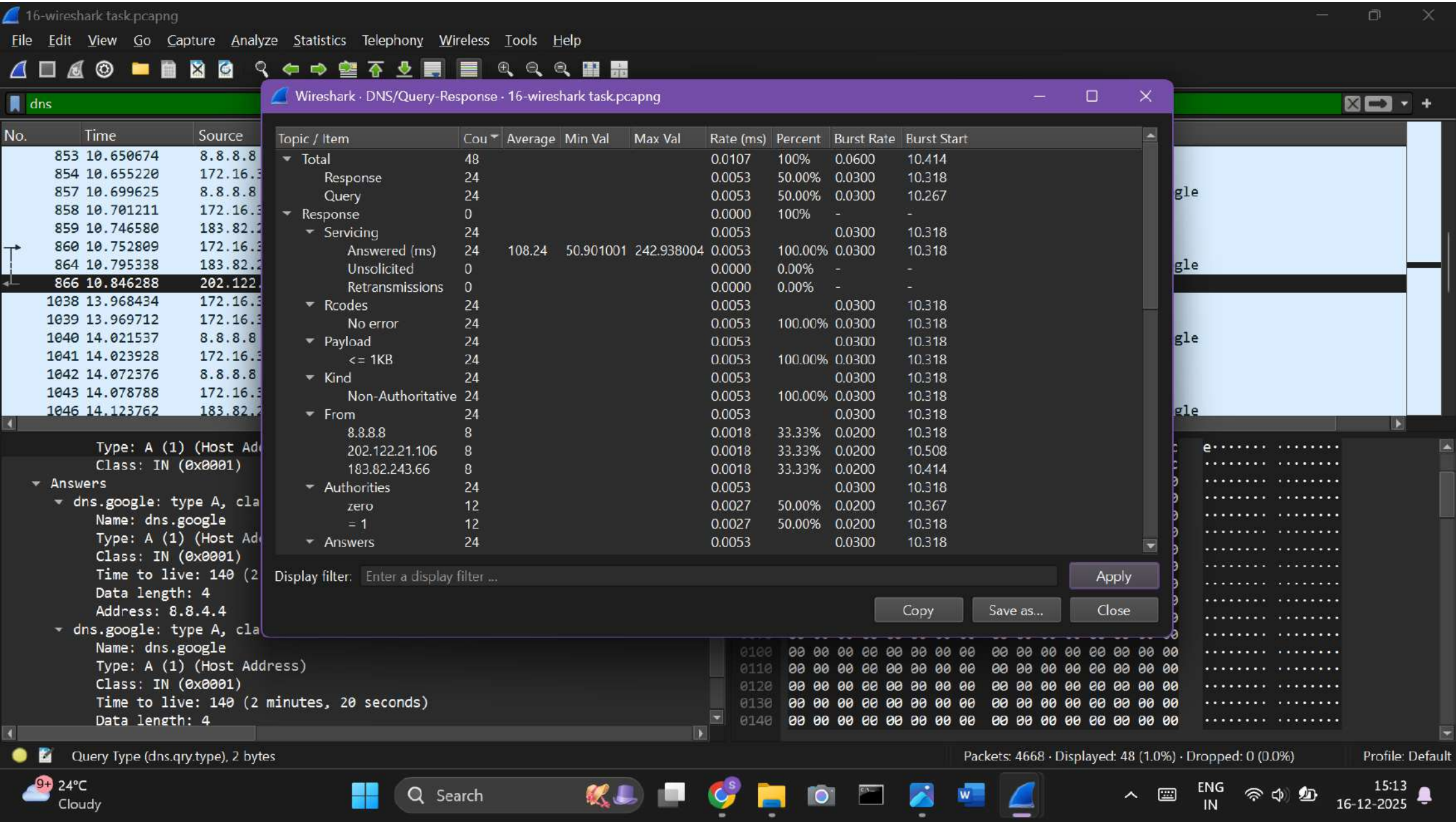
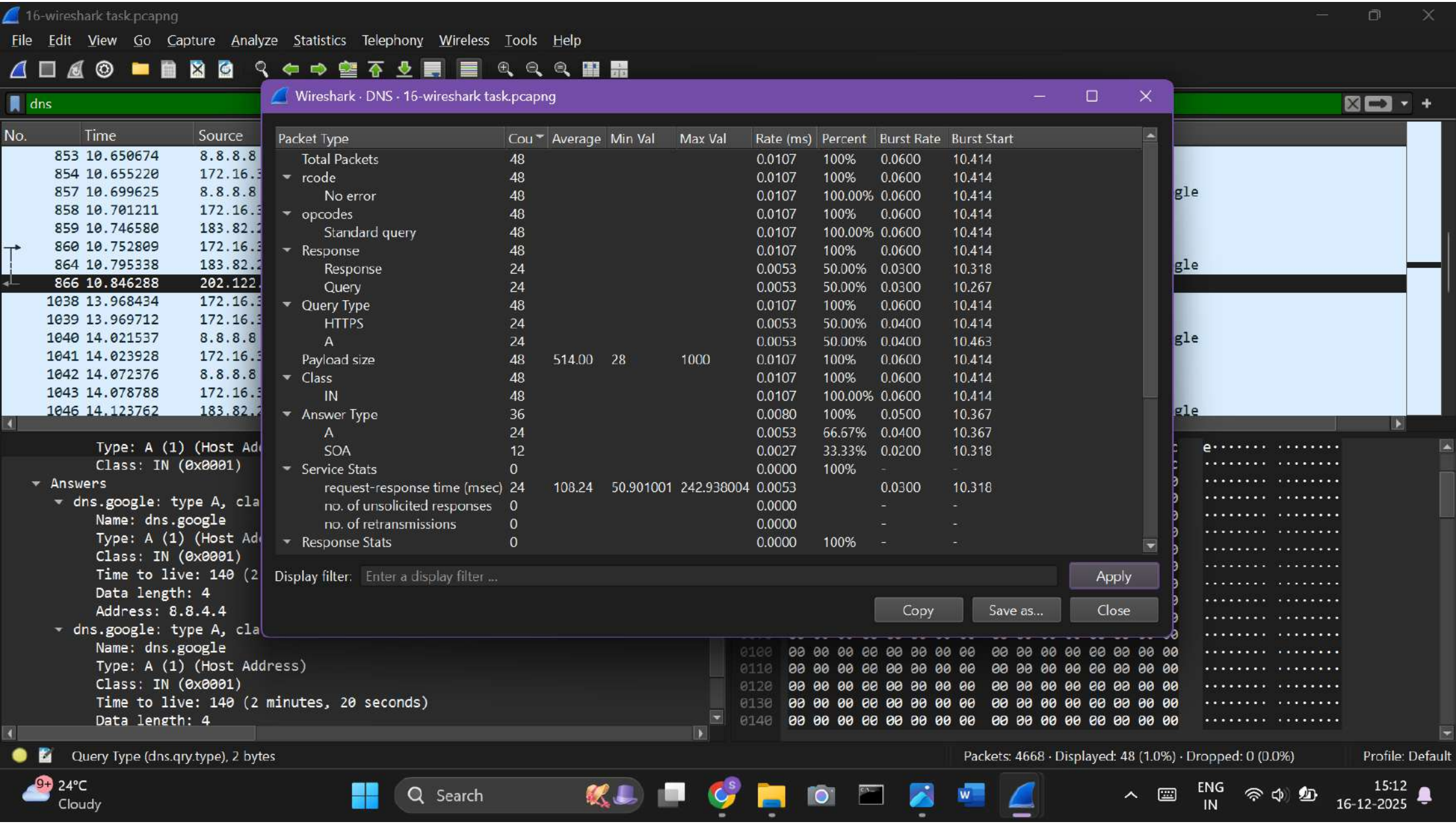
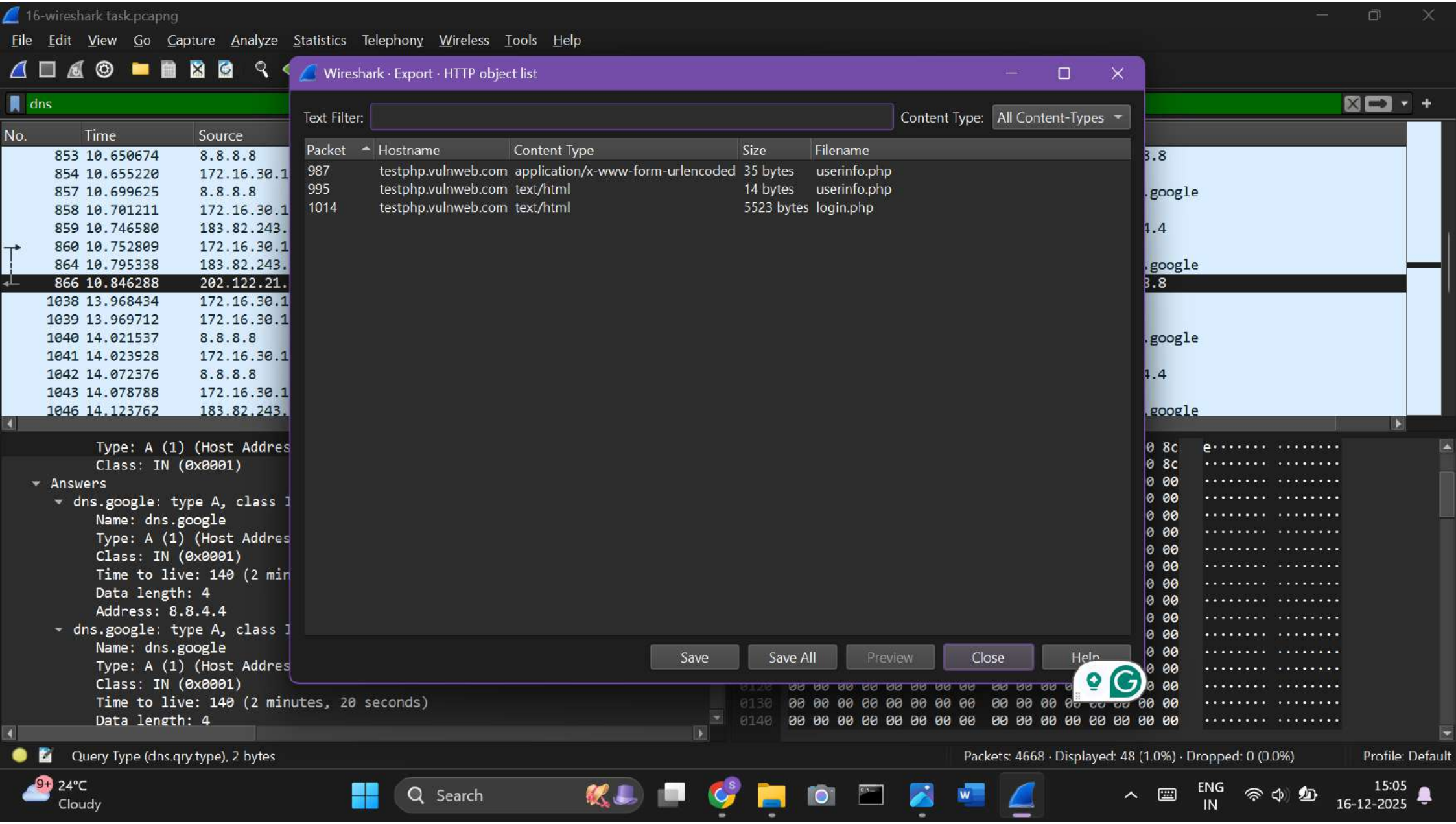
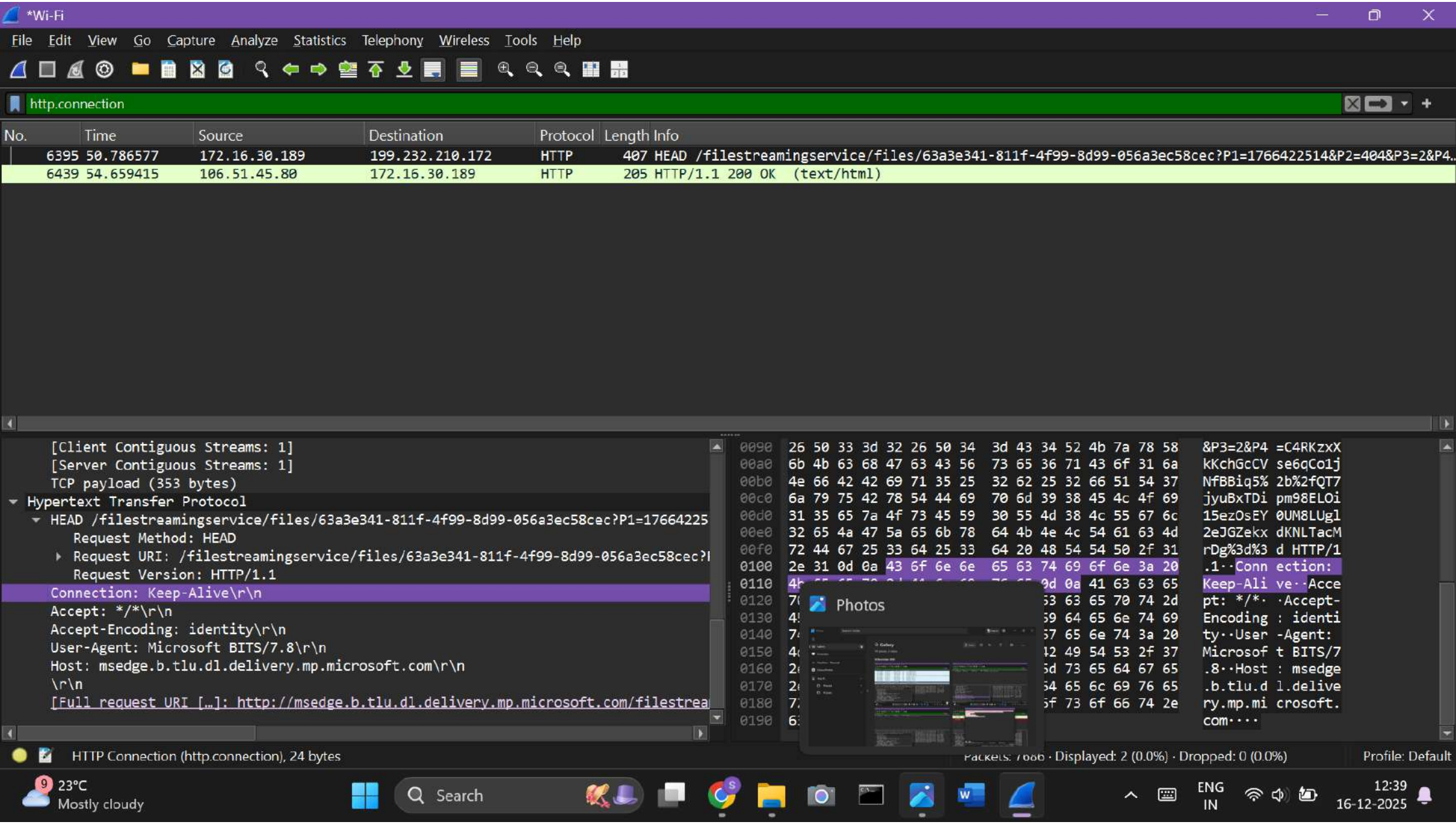

16-wireshark task.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source
831 10.150208 142.251.
832 10.150208 142.251.
833 10.150208 142.251.
834 10.150417 172.16.3
835 10.154494 172.16.3
836 10.179314 142.251.
855 10.667871 172.16.3
856 10.668771 172.16.3
869 10.865363 172.16.3
870 10.891905 45.127.6
871 10.892159 18.234.1
872 10.892348 172.16.3
873 10.892390 172.16.3
874 10.893330 8.8.8.8
875 10.893511 172.16.3
Frame 856: Packet, 66 bytes c
Ethernet II, Src: Intel_51:8e
Internet Protocol Version 4,
Transmission Control Protocol
Source Port: 55213
Destination Port: 443
[Stream index: 19]
[Stream Packet Number: 1]
[Conversation completeness
[TCP Segment Len: 0]
Sequence Number: 0 (rel
Sequence Number (raw): 2715531268
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Wireshark · IPv4 Statistics / All Addresses · 16-wireshark task.pcapng
Topic / Item Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
IPv4 Statistics/All Addresses 4409 0.1096 100% 3.3900 22.880
172.16.30.189 4292 0.1067 97.35% 3.3900 22.880
45.127.65.2 1271 0.0316 28.83% 1.3600 17.154
8.8.8.8 532 0.0132 12.07% 0.4300 22.230
106.51.45.80 340 0.0085 7.71% 3.2200 22.880
106.51.45.89 324 0.0081 7.35% 1.4800 34.170
150.171.22.12 287 0.0071 6.51% 0.2500 18.811
57.144.210.34 250 0.0062 5.67% 0.4200 25.025
49.205.75.98 147 0.0037 3.33% 1.4700 26.166
57.144.54.1 144 0.0036 3.27% 0.3500 24.289
202.83.26.149 141 0.0035 3.20% 0.5600 24.639
202.83.26.106 97 0.0024 2.20% 0.7200 34.075
57.144.210.192 82 0.0020 1.86% 0.2100 26.278
142.250.77.110 79 0.0020 1.79% 0.1000 18.499
224.0.0.251 73 0.0018 1.66% 0.1000 31.020
142.251.43.42 50 0.0012 1.13% 0.2100 34.392
57.144.211.32 44 0.0011 1.00% 0.2300 14.868
142.251.43.138 42 0.0010 0.95% 0.1600 9.804
202.83.26.163 41 0.0010 0.93% 0.4100 26.138
172.217.24.174 40 0.0010 0.91% 0.1700 22.607
172.16.31.15 37 0.0009 0.84% 0.0600 23.651
164.100.49.4 34 0.0008 0.77% 0.0700 22.700
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close
16-wireshark task.pcapng
Packets: 4668 · Displayed: 2868 (61.4%) · Dropped: 0 (0.0%)
Profile: Default
24°C Cloudy
Search
ENG IN
15:24 16-12-2025

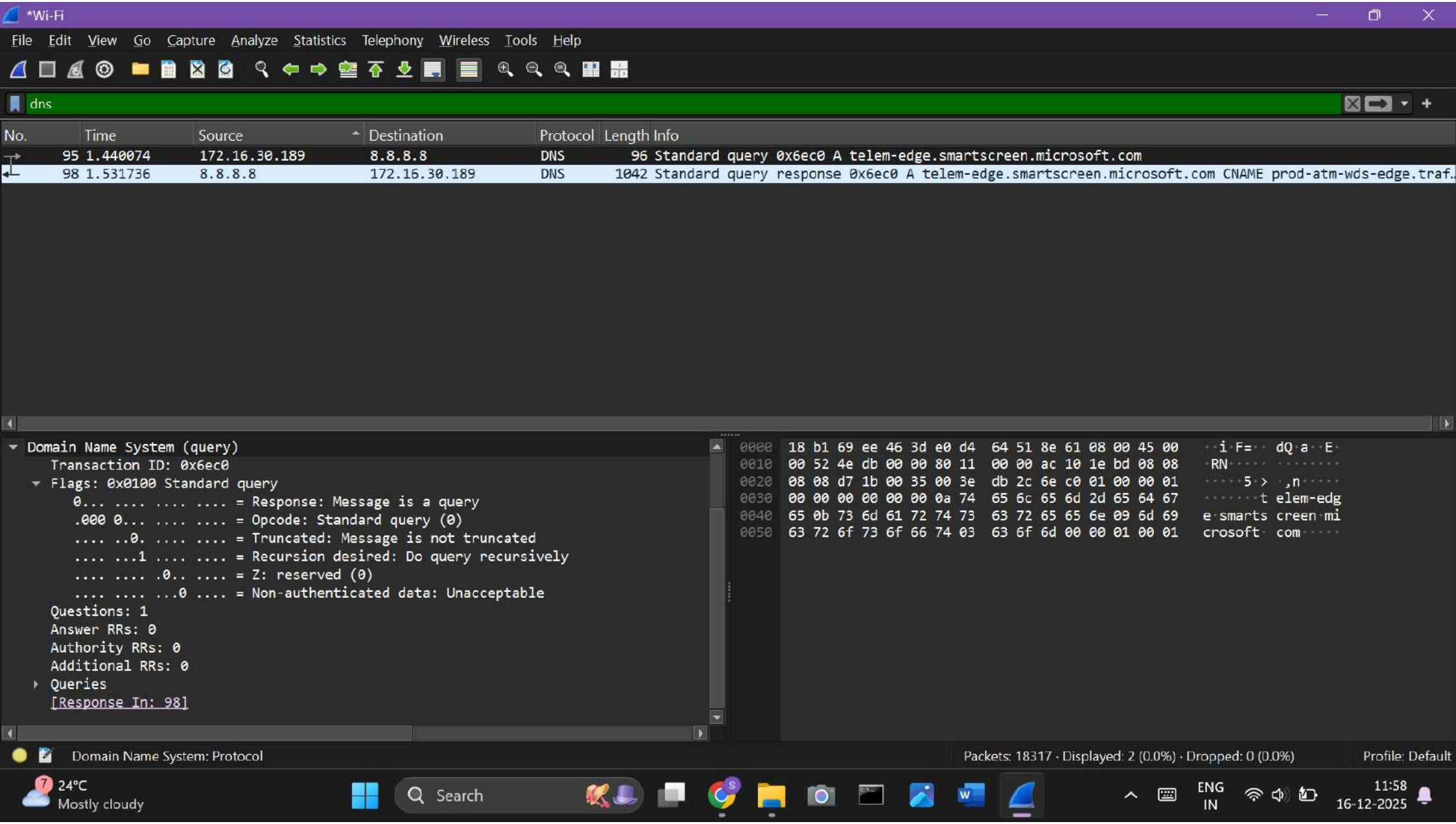

16-wireshark task.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source
831 10.150208 142.2
832 10.150208 142.2
833 10.150208 142.2
834 10.150417 172.1
835 10.154494 172.1
836 10.179314 142.2
855 10.667871 172.1
856 10.668771 172.1
869 10.865363 172.1
870 10.891905 45.12
871 10.892159 18.23
872 10.892348 172.1
873 10.892390 172.1
874 10.893330 8.8.8
875 10.893511 172.1
Frame 856: Packet, 66 byte
Ethernet II, Src: Intel_51
Internet Protocol Version
Transmission Control Proto
Source Port: 55213
Destination Port: 443
[Stream index: 19]
[Stream Packet Number:
[Conversation completene
[TCP Segment Len: 0]
Sequence Number: 0
Sequence Number (raw):
[Next Sequence Number:
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
WS=256
WS=256
Transmission Control Protocol: Protocol
Packets: 4668 · Displayed: 2868 (61.4%) · Dropped: 0 (0.0%)
Profile: Default
Round Trip Time for 18.234.107.129:443 → 172.16.30.189:55213
Round Trip Time for 18.234.107.129:443 → 172.16.30.189:55213
16-wireshark task.pcapng
Round Trip Time
40 ms
30 ms
20 ms
10 ms
0 seconds
500 ms
600 ms
700 ms
800 ms
900 ms
Time
Hover over the graph for details. → 7 pkts, 755 bytes ← 6 pkts, 1438 bytes
Type Round Trip Time
Stream 19
Switch Direction
Mouse drags zooms
Sampling Method All Data Packets
RTT By Sequence Number
Reset
Save As...
Close
Help
24°C
Cloudy
Search
ENG
IN
15:22
16-12-2025


16-wireshark task.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source
853 10.650674 8.8.8.8
854 10.655220 172.16.3
857 10.699625 8.8.8.8
858 10.701211 172.16.3
859 10.746580 183.82.2
860 10.752809 172.16.3
864 10.795338 183.82.2
866 10.846288 202.122.
1038 13.968434 172.16.3
1039 13.969712 172.16.3
1040 14.021537 8.8.8.8
1041 14.023928 172.16.3
1042 14.072376 8.8.8.8
1043 14.078788 172.16.3
1046 14.123762 183.82.2
Type: A (1) (Host Ad
Class: IN (0x0001)
Answers
dns.google: type A, cla
Name: dns.google
Type: A (1) (Host Ad
Class: IN (0x0001)
Time to live: 140 (2
Data length: 4
Address: 8.8.4.4
dns.google: type A, cla
Name: dns.google
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 140 (2 minutes, 20 seconds)
Data length: 4
Wireshark · DNS/Query-Response · 16-wireshark task.pcapng
Topic / Item Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Total 48 0.0107 100% 0.0600 10.414
Response 24 0.0053 50.00% 0.0300 10.318
Query 24 0.0053 50.00% 0.0300 10.267
Response 0 0.0000 100% - -
Servicing 24 0.0053 0.0300 10.318
Answered (ms) 24 108.24 50.901001 242.938004 0.0053 100.00% 0.0300 10.318
Unsolicited 0 0.0000 0.00% - -
Retransmissions 0 0.0000 0.00% - -
Rcodes 24 0.0053 0.0300 10.318
No error 24 0.0053 100.00% 0.0300 10.318
Payload 24 0.0053 0.0300 10.318
<= 1KB 24 0.0053 100.00% 0.0300 10.318
Kind 24 0.0053 0.0300 10.318
Non-Authoritative 24 0.0053 100.00% 0.0300 10.318
From 24 0.0053 0.0300 10.318
8.8.8.8 8 0.0018 33.33% 0.0200 10.318
202.122.21.106 8 0.0018 33.33% 0.0200 10.508
183.82.243.66 8 0.0018 33.33% 0.0200 10.414
Authorities 24 0.0053 0.0300 10.318
zero 12 0.0027 50.00% 0.0200 10.367
= 1 12 0.0027 50.00% 0.0200 10.318
Answers 24 0.0053 0.0300 10.318
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close
Query Type (dns.qry.type), 2 bytes
Packets: 4668 · Displayed: 48 (1.0%) · Dropped: 0 (0.0%)
Profile: Default
24°C Cloudy
Search
ENG IN
15:13 16-12-2025


16-wireshark task.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source
853 10.650674 8.8.8.8
854 10.655220 172.16.3
857 10.699625 8.8.8.8
858 10.701211 172.16.3
859 10.746580 183.82.2
860 10.752809 172.16.3
864 10.795338 183.82.2
866 10.846288 202.122.
1038 13.968434 172.16.3
1039 13.969712 172.16.3
1040 14.021537 8.8.8.8
1041 14.023928 172.16.3
1042 14.072376 8.8.8.8
1043 14.078788 172.16.3
1046 14.123762 183.82.2
Type: A (1) (Host Ad
Class: IN (0x0001)
Answers
dns.google: type A, cla
Name: dns.google
Type: A (1) (Host Ad
Class: IN (0x0001)
Time to live: 140 (2
Data length: 4
Address: 8.8.4.4
dns.google: type A, cla
Name: dns.google
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 140 (2 minutes, 20 seconds)
Data length: 4
Wireshark · DNS · 16-wireshark task.pcapng
Packet Type Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Total Packets 48 0.0107 100% 0.0600 10.414
rcode 48 0.0107 100% 0.0600 10.414
No error 48 0.0107 100.00% 0.0600 10.414
opcodes 48 0.0107 100% 0.0600 10.414
Standard query 48 0.0107 100.00% 0.0600 10.414
Response 48 0.0107 100% 0.0600 10.414
Response 24 0.0053 50.00% 0.0300 10.318
Query 24 0.0053 50.00% 0.0300 10.267
Query Type 48 0.0107 100% 0.0600 10.414
HTTPS 24 0.0053 50.00% 0.0400 10.414
A 24 0.0053 50.00% 0.0400 10.463
Payload size 48 514.00 28 1000 0.0107 100% 0.0600 10.414
Class 48 0.0107 100% 0.0600 10.414
IN 48 0.0107 100.00% 0.0600 10.414
Answer Type 36 0.0080 100% 0.0500 10.367
A 24 0.0053 66.67% 0.0400 10.367
SOA 12 0.0027 33.33% 0.0200 10.318
Service Stats 0 0.0000 100%
request-response time (msec) 24 108.24 50.901001 242.938004 0.0053 0.0300 10.318
no. of unsolicited responses 0 0.0000
no. of retransmissions 0 0.0000
Response Stats 0 0.0000 100%
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Query Type (dns.qry.type), 2 bytes
Packets: 4668 · Displayed: 48 (1.0%) · Dropped: 0 (0.0%)
Profile: Default
24°C Cloudy
Search
ENG IN
15:12 16-12-2025


16-wireshark task.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source
853 10.650674 8.8.8.8
854 10.655220 172.16.30.1
857 10.699625 8.8.8.8
858 10.701211 172.16.30.1
859 10.746580 183.82.243.
860 10.752809 172.16.30.1
864 10.795338 183.82.243.
866 10.846288 202.122.21.
1038 13.968434 172.16.30.1
1039 13.969712 172.16.30.1
1040 14.021537 8.8.8.8
1041 14.023928 172.16.30.1
1042 14.072376 8.8.8.8
1043 14.078788 172.16.30.1
1046 14.123762 183.82.243.
Type: A (1) (Host Addres
Class: IN (0x0001)
Answers
dns.google: type A, class I
Name: dns.google
Type: A (1) (Host Addres
Class: IN (0x0001)
Time to live: 140 (2 min
Data length: 4
Address: 8.8.4.4
dns.google: type A, class I
Name: dns.google
Type: A (1) (Host Addres
Class: IN (0x0001)
Time to live: 140 (2 minutes, 20 seconds)
Data length: 4
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
987 testphp.vulnweb.com application/x-www-form-urlencoded 35 bytes userinfo.php
995 testphp.vulnweb.com text/html 14 bytes userinfo.php
1014 testphp.vulnweb.com text/html 5523 bytes login.php
Save
Save All
Preview
Close
Help
Query Type (dns.qry.type), 2 bytes
Packets: 4668 · Displayed: 48 (1.0%) · Dropped: 0 (0.0%)
Profile: Default
24°C
Cloudy
Search
ENG
IN
15:05
16-12-2025


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.connection
No. Time Source Destination Protocol Length Info
6395 50.786577 172.16.30.189 199.232.210.172 HTTP 407 HEAD /filestreamingservice/files/63a3e341-811f-4f99-8d99-056a3ec58cec?P1=1766422514&P2=404&P3=2&P4..
6439 54.659415 106.51.45.80 172.16.30.189 HTTP 205 HTTP/1.1 200 OK (text/html)
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
TCP payload (353 bytes)
Hypertext Transfer Protocol
HEAD /filestreamingservice/files/63a3e341-811f-4f99-8d99-056a3ec58cec?P1=17664225
Request Method: HEAD
Request URI: /filestreamingservice/files/63a3e341-811f-4f99-8d99-056a3ec58cec?
Request Version: HTTP/1.1
Connection: Keep-Alive\r\n
Accept: */*\r\n
Accept-Encoding: identity\r\n
User-Agent: Microsoft BITS/7.8\r\n
Host: msedge.b.tlu.dl.delivery.mp.microsoft.com\r\n
\r\n
[Full request URI [...]: http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestrea
0090 26 50 33 3d 32 26 50 34 3d 43 34 52 4b 7a 78 58 &P3=2&P4 =C4RKzxX
00a0 6b 4b 63 68 47 63 43 56 73 65 36 71 43 6f 31 6a kKchGcCV se6qCo1j
00b0 4e 66 42 42 69 71 35 25 32 62 25 32 66 51 54 37 NfBBiq5% 2b%2fQT7
00c0 6a 79 75 42 78 54 44 69 70 6d 39 38 45 4c 4f 69 jyuBxTDi pm98ELOi
00d0 31 35 65 7a 4f 73 45 59 30 55 4d 38 4c 55 67 6c 15ezOsEY 0UM8LUgl
00e0 32 65 4a 47 5a 65 6b 78 64 4b 4e 4c 54 61 63 4d 2eJGZekx dKNLTacM
00f0 72 44 67 25 33 64 25 33 64 20 48 54 54 50 2f 31 rDg%3d%3 d HTTP/1
0100 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 .1··Conn ection:
0110 4b Keep-Ali ve··Acce
0120 pt: */*· ·Accept-
0130 Encoding : identi
0140 ty··User -Agent:
0150 Microsof t BITS/7
0160 .8··Host : msedge
0170 .b.tlu.d l.delive
0180 ry.mp.mi crosoft.
0190 com····
Photos
HTTP Connection (http.connection), 24 bytes
Packets: 7866 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
23°C
Mostly cloudy
Search
ENG
IN
12:39
16-12-2025


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
95 1.440074 172.16.30.189 8.8.8.8 DNS 96 Standard query 0x6ec0 A telem-edge.smartscreen.microsoft.com
98 1.531736 8.8.8.8 172.16.30.189 DNS 1042 Standard query response 0x6ec0 A telem-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.traf
Domain Name System (query)
Transaction ID: 0x6ec0
Flags: 0x0100 Standard query
0... .... .... .... = Response: Message is a query
.000 0... .... .... = Opcode: Standard query (0)
.... ..0. .... .... = Truncated: Message is not truncated
.... ...1 .... .... = Recursion desired: Do query recursively
.... .... .0.. .... = Z: reserved (0)
.... .... ...0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 98]
0000 18 b1 69 ee 46 3d e0 d4 64 51 8e 61 08 00 45 00
0010 00 52 4e db 00 00 80 11 00 00 ac 10 1e bd 08 08
0020 08 08 d7 1b 00 35 00 3e db 2c 6e c0 01 00 00 01
0030 00 00 00 00 00 00 0a 74 65 6c 65 6d 2d 65 64 67
0040 65 0b 73 6d 61 72 74 73 63 72 65 65 6e 09 6d 69
0050 63 72 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01
Domain Name System: Protocol
Packets: 18317 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
24°C
Mostly cloudy
Search
ENG
IN
11:58
16-12-2025