Jalil Chaibderraine DAMS 5

Network Analysis Report

12/12/2025

Introduction

The goal of this project is to strengthen my understanding of network protocols by analyzing real traffic with Wireshark. I generated several types of traffic (DNS, ICMP, TCP, HTTP, and HTTPS) and inspected the corresponding packets to observe how each protocol behaves in practice.

After this Wireshark analysis, I plan to create small Python scripts to automate some checks or reproduce parts of the traffic, allowing me to explore network analysis from both a practical and a programmatic perspective.

Environment

OS: Ubuntu 24.04.3 LTS

Wireshark version: 4.2.2

Interface: Wi-Fi

Capture Duration:

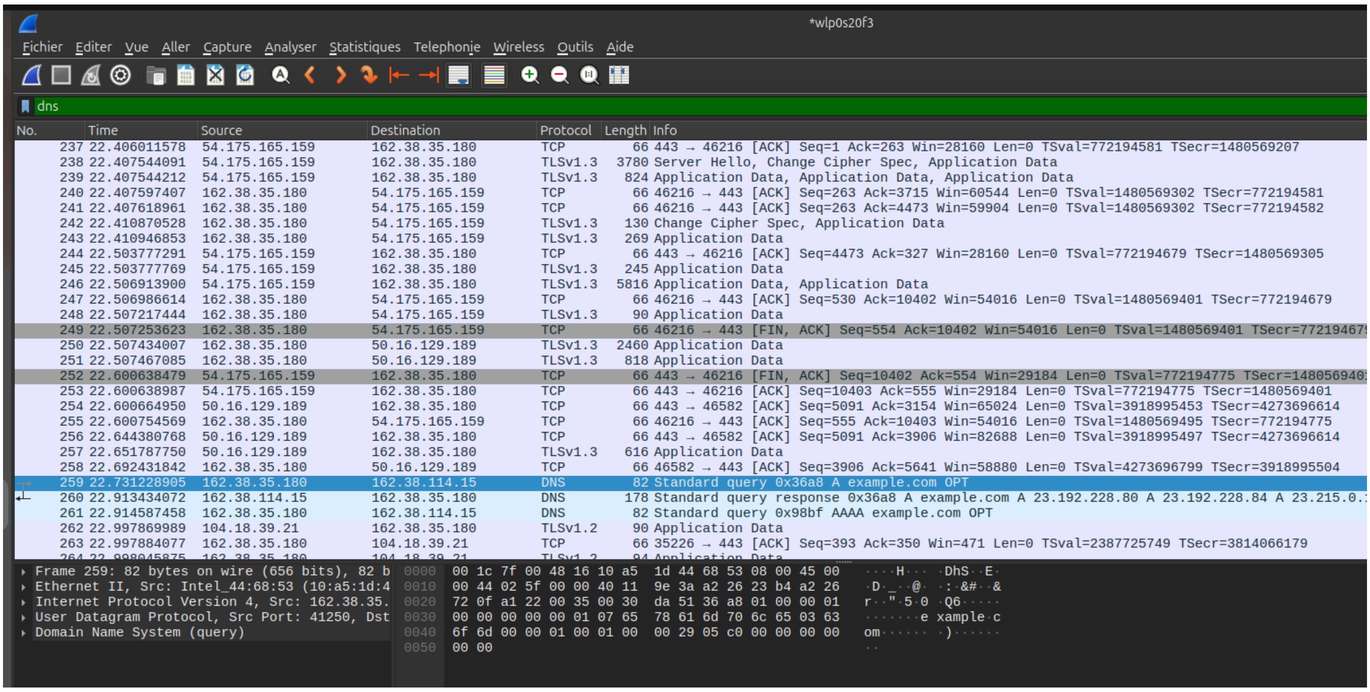
Methodology

1. Start a capture on the Wireshark interface
2. Generate network traDic with:
    a. Commands: ping, nslookup
    b. Browsing: example.com, neverssl.com, google.com, wikipedia.org
3. Sort the captured packets by protocol
4. Analyze each group of packets to identify the behavior of the corresponding protocol

Protocol analysis

DNS Analysis

To generate DNS traffic, you must use commands such as nslookup example.com.



*wlp0s20f3
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
dns

```
No.   Time         Source           Destination      Protocol Length Info
  237 22.406011578 54.175.165.159   162.38.35.180    TCP        66 443 → 46216 [ACK] Seq=1 Ack=263 Win=28160 Len=0 TSval=772194581 TSecr=1480569207
  238 22.407544091 54.175.165.159   162.38.35.180    TLSv1.3  3780 Server Hello, Change Cipher Spec, Application Data
  239 22.407544212 54.175.165.159   162.38.35.180    TLSv1.3   824 Application Data, Application Data, Application Data
  240 22.407597407 162.38.35.180    54.175.165.159   TCP        66 46216 → 443 [ACK] Seq=263 Ack=3715 Win=60544 Len=0 TSval=1480569302 TSecr=772194581
  241 22.407618961 162.38.35.180    54.175.165.159   TCP        66 46216 → 443 [ACK] Seq=263 Ack=4473 Win=59904 Len=0 TSval=1480569302 TSecr=772194582
  242 22.410870528 162.38.35.180    54.175.165.159   TLSv1.3   130 Change Cipher Spec, Application Data
  243 22.410946853 162.38.35.180    54.175.165.159   TLSv1.3   269 Application Data
  244 22.503777291 54.175.165.159   162.38.35.180    TCP        66 443 → 46216 [ACK] Seq=4473 Ack=327 Win=28160 Len=0 TSval=772194679 TSecr=1480569305
  245 22.503777769 54.175.165.159   162.38.35.180    TLSv1.3   245 Application Data
  246 22.506913900 54.175.165.159   162.38.35.180    TLSv1.3  5816 Application Data, Application Data
  247 22.506986614 162.38.35.180    54.175.165.159   TCP        66 46216 → 443 [ACK] Seq=530 Ack=10402 Win=54016 Len=0 TSval=1480569401 TSecr=772194679
  248 22.507217444 162.38.35.180    54.175.165.159   TLSv1.3    90 Application Data
  249 22.507253623 162.38.35.180    54.175.165.159   TCP        66 46216 → 443 [FIN, ACK] Seq=554 Ack=10402 Win=54016 Len=0 TSval=1480569401 TSecr=77219467
  250 22.507434007 162.38.35.180    50.16.129.189    TLSv1.3  2460 Application Data
  251 22.507467085 162.38.35.180    50.16.129.189    TLSv1.3   818 Application Data
  252 22.600638479 54.175.165.159   162.38.35.180    TCP        66 443 → 46216 [FIN, ACK] Seq=10402 Ack=554 Win=29184 Len=0 TSval=772194775 TSecr=148056940
  253 22.600638987 54.175.165.159   162.38.35.180    TCP        66 443 → 46216 [ACK] Seq=10403 Ack=555 Win=29184 Len=0 TSval=772194775 TSecr=1480569401
  254 22.600664950 50.16.129.189    162.38.35.180    TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3154 Win=65024 Len=0 TSval=3918995453 TSecr=4273696614
  255 22.600754569 162.38.35.180    54.175.165.159   TCP        66 46216 → 443 [ACK] Seq=555 Ack=10403 Win=54016 Len=0 TSval=1480569495 TSecr=772194775
  256 22.644380768 50.16.129.189    162.38.35.180    TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3906 Win=82688 Len=0 TSval=3918995497 TSecr=4273696614
  257 22.651787750 50.16.129.189    162.38.35.180    TLSv1.3   616 Application Data
  258 22.692431842 162.38.35.180    50.16.129.189    TCP        66 46582 → 443 [ACK] Seq=3906 Ack=5641 Win=58880 Len=0 TSval=4273696799 TSecr=3918995504
  259 22.731228905 162.38.35.180    162.38.114.15    DNS        82 Standard query 0x36a8 A example.com OPT
  260 22.913434072 162.38.114.15    162.38.35.180    DNS       178 Standard query response 0x36a8 A example.com A 23.192.228.80 A 23.192.228.84 A 23.215.0.
  261 22.914587458 162.38.35.180    162.38.114.15    DNS        82 Standard query 0x98bf AAAA example.com OPT
  262 22.997869989 104.18.39.21     162.38.35.180    TLSv1.2    90 Application Data
  263 22.997884077 162.38.35.180    104.18.39.21     TCP        66 35226 → 443 [ACK] Seq=393 Ack=350 Win=471 Len=0 TSval=2387725749 TSecr=3814066179
  264 22.998045875 162.38.35.180    104.18.39.21     TLSv1.2    94 Application Data
```

```
› Frame 259: 82 bytes on wire (656 bits), 82 b
› Ethernet II, Src: Intel_44:68:53 (10:a5:1d:4
› Internet Protocol Version 4, Src: 162.38.35.
› User Datagram Protocol, Src Port: 41250, Dst
› Domain Name System (query)
```

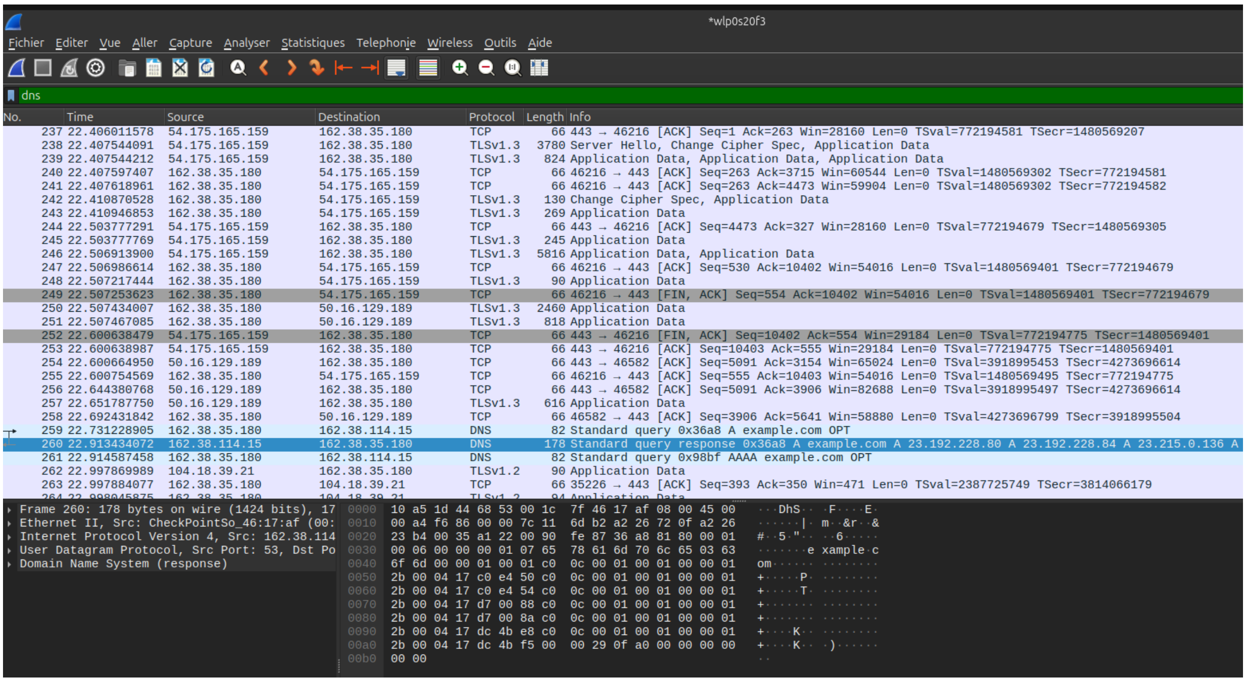
```
0000  00 1c 7f 00 48 16 10 a5  1d 44 68 53 08 00 45 00   ····H··· ·DhS··E·
0010  00 44 02 5f 00 00 40 11  9e 3a a2 26 23 b4 a2 26   ·D·_··@· ·:·&#··&
0020  72 0f a1 22 00 35 00 30  da 51 36 a8 01 00 00 01   r··"·5·0 ·Q6·····
0030  00 00 00 00 00 01 07 65  78 61 6d 70 6c 65 03 63   ·······e xample·c
0040  6f 6d 00 00 01 00 01 00  00 29 05 c0 00 00 00 00   om······ ·)······
0050  00 00                                              ··
```

1. DNS Request for example.com

This packet corresponds to the DNS request sent by the client.

Query Type: A (IPv4 address request)
Source IP: 162.38.35.180
Destination IP: 162.38.114.15
Transaction ID: 0x36a8
→ Used to match the request with its corresponding response

Flags: Standard query, no errors
Requested Domain: example.com
→ This packet represents the initial DNS query created by the client to resolve the IPv4 address of example.com.



*wlp0s20f3
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
dns

```
No.   Time          Source          Destination     Protocol Length Info
  237 22.406011578  54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [ACK] Seq=1 Ack=263 Win=28160 Len=0 TSval=772194581 TSecr=1480569207
  238 22.407544091  54.175.165.159  162.38.35.180   TLSv1.3  3780 Server Hello, Change Cipher Spec, Application Data
  239 22.407544212  54.175.165.159  162.38.35.180   TLSv1.3   824 Application Data, Application Data, Application Data
  240 22.407597407  162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [ACK] Seq=263 Ack=3715 Win=60544 Len=0 TSval=1480569302 TSecr=772194581
  241 22.407618961  162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [ACK] Seq=263 Ack=4473 Win=59904 Len=0 TSval=1480569302 TSecr=772194582
  242 22.410870528  162.38.35.180   54.175.165.159  TLSv1.3   130 Change Cipher Spec, Application Data
  243 22.410946853  162.38.35.180   54.175.165.159  TLSv1.3   269 Application Data
  244 22.503777291  54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [ACK] Seq=4473 Ack=327 Win=28160 Len=0 TSval=772194679 TSecr=1480569305
  245 22.503777769  54.175.165.159  162.38.35.180   TLSv1.3   245 Application Data
  246 22.506913900  54.175.165.159  162.38.35.180   TLSv1.3  5816 Application Data, Application Data
  247 22.506986614  162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [ACK] Seq=530 Ack=10402 Win=54016 Len=0 TSval=1480569401 TSecr=772194679
  248 22.507217444  162.38.35.180   54.175.165.159  TLSv1.3    90 Application Data
  249 22.507253623  162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [FIN, ACK] Seq=554 Ack=10402 Win=54016 Len=0 TSval=1480569401 TSecr=772194679
  250 22.507434007  162.38.35.180   50.16.129.189   TLSv1.3  2460 Application Data
  251 22.507467085  162.38.35.180   50.16.129.189   TLSv1.3   818 Application Data
  252 22.600638479  54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [FIN, ACK] Seq=10402 Ack=554 Win=29184 Len=0 TSval=772194775 TSecr=1480569401
  253 22.600638987  54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [ACK] Seq=10403 Ack=555 Win=29184 Len=0 TSval=772194775 TSecr=1480569401
  254 22.600664950  50.16.129.189   162.38.35.180   TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3154 Win=65024 Len=0 TSval=3918995453 TSecr=4273696614
  255 22.600754569  162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [ACK] Seq=555 Ack=10403 Win=54016 Len=0 TSval=1480569495 TSecr=772194775
  256 22.644380768  50.16.129.189   162.38.35.180   TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3906 Win=82688 Len=0 TSval=3918995497 TSecr=4273696614
  257 22.651787750  50.16.129.189   162.38.35.180   TLSv1.3   616 Application Data
  258 22.692431842  162.38.35.180   50.16.129.189   TCP        66 46582 → 443 [ACK] Seq=3906 Ack=5641 Win=58880 Len=0 TSval=4273696799 TSecr=3918995504
  259 22.731228905  162.38.35.180   162.38.114.15   DNS        82 Standard query 0x36a8 A example.com OPT
  260 22.913434072  162.38.114.15   162.38.35.180   DNS       178 Standard query response 0x36a8 A example.com A 23.192.228.80 A 23.192.228.84 A 23.215.0.136 A
  261 22.914587458  162.38.35.180   162.38.114.15   DNS        82 Standard query 0x98bf AAAA example.com OPT
  262 22.997869989  104.18.39.21    162.38.35.180   TLSv1.2    90 Application Data
  263 22.997884077  162.38.35.180   104.18.39.21    TCP        66 35226 → 443 [ACK] Seq=393 Ack=350 Win=471 Len=0 TSval=2387725749 TSecr=3814066179
  264 22.998045875  162.38.35.180   104.18.39.21    TLSv1.2    94 Application Data
```

```
› Frame 260: 178 bytes on wire (1424 bits), 17
› Ethernet II, Src: CheckPointSo_46:17:af (00:
› Internet Protocol Version 4, Src: 162.38.114
› User Datagram Protocol, Src Port: 53, Dst Po
› Domain Name System (response)
```

```
0000  10 a5 1d 44 68 53 00 1c  7f 46 17 af 08 00 45 00   ···DhS·· ·F····E·
0010  00 a4 f6 86 00 00 7c 11  6d b2 a2 26 72 0f a2 26   ······|· m··&r··&
0020  23 b4 00 35 a1 22 00 90  fe 87 36 a8 81 80 00 01   #··5·"·· ··6·····
0030  00 06 00 00 00 01 07 65  78 61 6d 70 6c 65 03 63   ·······e xample·c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 01   om······ ········
0050  2b 00 04 17 c0 e4 50 c0  0c 00 01 00 01 00 00 01   +·····P· ········
0060  2b 00 04 17 c0 e4 54 c0  0c 00 01 00 01 00 00 01   +·····T· ········
0070  2b 00 04 17 d7 00 88 c0  0c 00 01 00 01 00 00 01   +······· ········
0080  2b 00 04 17 d7 00 8a c0  0c 00 01 00 01 00 00 01   +······· ········
0090  2b 00 04 17 dc 4b e8 c0  0c 00 01 00 01 00 00 01   +····K·· ········
00a0  2b 00 04 17 dc 4b f5 00  00 29 0f a0 00 00 00 00   +····K·· ·)······
00b0  00 00                                              ··
```

2. DNS Response for example.com

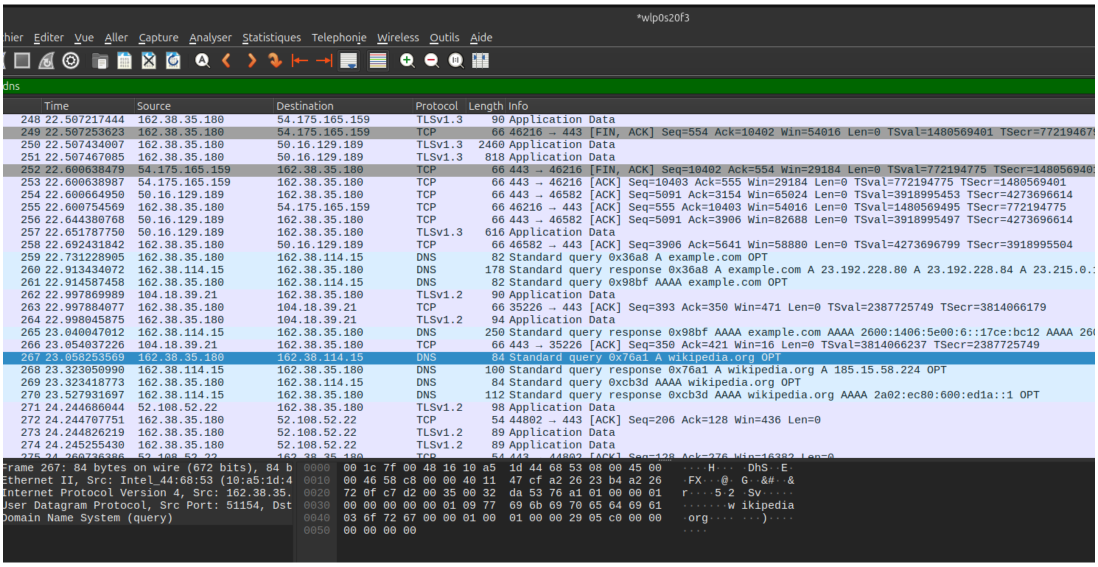
This packet is the DNS server's answer to the previous query.

Response Type: Standard query response (No error)
Source IP: 162.38.114.15 (DNS server)
Destination IP: 162.38.35.180 (local machine)
Transaction ID: 0x36a8 → Matches the request, confirming this response corresponds to the earlier query

Answer (A Records):

23.192.228.80
23.192.228.84
23.215.0.138
23.215.0.136
23.220.75.x (truncated but visible)

→ The DNS server returns multiple IPv4 addresses for example.com, as it is hosted behind a load-balancing infrastructure.


*wlp0s20f3
hier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
dns

```
    Time           Source          Destination     Protocol Length Info
248 22.507217444   162.38.35.180   54.175.165.159  TLSv1.3    90 Application Data
249 22.507253623   162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [FIN, ACK] Seq=554 Ack=10402 Win=54016 Len=0 TSval=1480569401 TSecr=77219467
250 22.507434007   162.38.35.180   50.16.129.189   TLSv1.3  2460 Application Data
251 22.507467085   162.38.35.180   50.16.129.189   TLSv1.3   818 Application Data
252 22.600638479   54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [FIN, ACK] Seq=10402 Ack=554 Win=29184 Len=0 TSval=772194775 TSecr=148056940
253 22.600638987   54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [ACK] Seq=10403 Ack=555 Win=29184 Len=0 TSval=772194775 TSecr=1480569401
254 22.600664950   50.16.129.189   162.38.35.180   TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3154 Win=65024 Len=0 TSval=3918995453 TSecr=4273696614
255 22.600754569   162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [ACK] Seq=555 Ack=10403 Win=54016 Len=0 TSval=1480569495 TSecr=772194775
256 22.644380768   50.16.129.189   162.38.35.180   TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3906 Win=82688 Len=0 TSval=3918995497 TSecr=4273696614
257 22.651787750   50.16.129.189   162.38.35.180   TLSv1.3   616 Application Data
258 22.692431842   162.38.35.180   50.16.129.189   TCP        66 46582 → 443 [ACK] Seq=3906 Ack=5641 Win=58880 Len=0 TSval=4273696799 TSecr=3918995504
259 22.731228905   162.38.35.180   162.38.114.15   DNS        82 Standard query 0x36a8 A example.com OPT
260 22.913434072   162.38.114.15   162.38.35.180   DNS       178 Standard query response 0x36a8 A example.com A 23.192.228.80 A 23.192.228.84 A 23.215.0.
261 22.914587458   162.38.35.180   162.38.114.15   DNS        82 Standard query 0x98bf AAAA example.com OPT
262 22.997869989   104.18.39.21    162.38.35.180   TLSv1.2    90 Application Data
263 22.997884077   162.38.35.180   104.18.39.21    TCP        66 35226 → 443 [ACK] Seq=393 Ack=350 Win=471 Len=0 TSval=2387725749 TSecr=3814066179
264 22.998045875   162.38.35.180   104.18.39.21    TLSv1.2    94 Application Data
265 23.040047012   162.38.114.15   162.38.35.180   DNS       250 Standard query response 0x98bf AAAA example.com AAAA 2600:1406:5e00:6::17ce:bc12 AAAA 26
266 23.054037226   104.18.39.21    162.38.35.180   TCP        66 443 → 35226 [ACK] Seq=350 Ack=421 Win=16 Len=0 TSval=3814066237 TSecr=2387725749
267 23.058253569   162.38.35.180   162.38.114.15   DNS        84 Standard query 0x76a1 A wikipedia.org OPT
268 23.323050990   162.38.114.15   162.38.35.180   DNS       100 Standard query response 0x76a1 A wikipedia.org A 185.15.58.224 OPT
269 23.323418773   162.38.35.180   162.38.114.15   DNS        84 Standard query 0xcb3d AAAA wikipedia.org OPT
270 23.527931697   162.38.114.15   162.38.35.180   DNS       112 Standard query response 0xcb3d AAAA wikipedia.org AAAA 2a02:ec80:600:ed1a::1 OPT
271 24.244686044   52.108.52.22    162.38.35.180   TLSv1.2    98 Application Data
272 24.244707751   162.38.35.180   52.108.52.22    TCP        54 44802 → 443 [ACK] Seq=206 Ack=128 Win=436 Len=0
273 24.244826219   162.38.35.180   52.108.52.22    TLSv1.2    89 Application Data
274 24.245255430   162.38.35.180   52.108.52.22    TLSv1.2    89 Application Data
275 24.260736386   52.108.52.22    162.38.35.180   TCP        54 443 → 44802 [ACK] Seq=128 Ack=276 Win=16382 Len=0
```

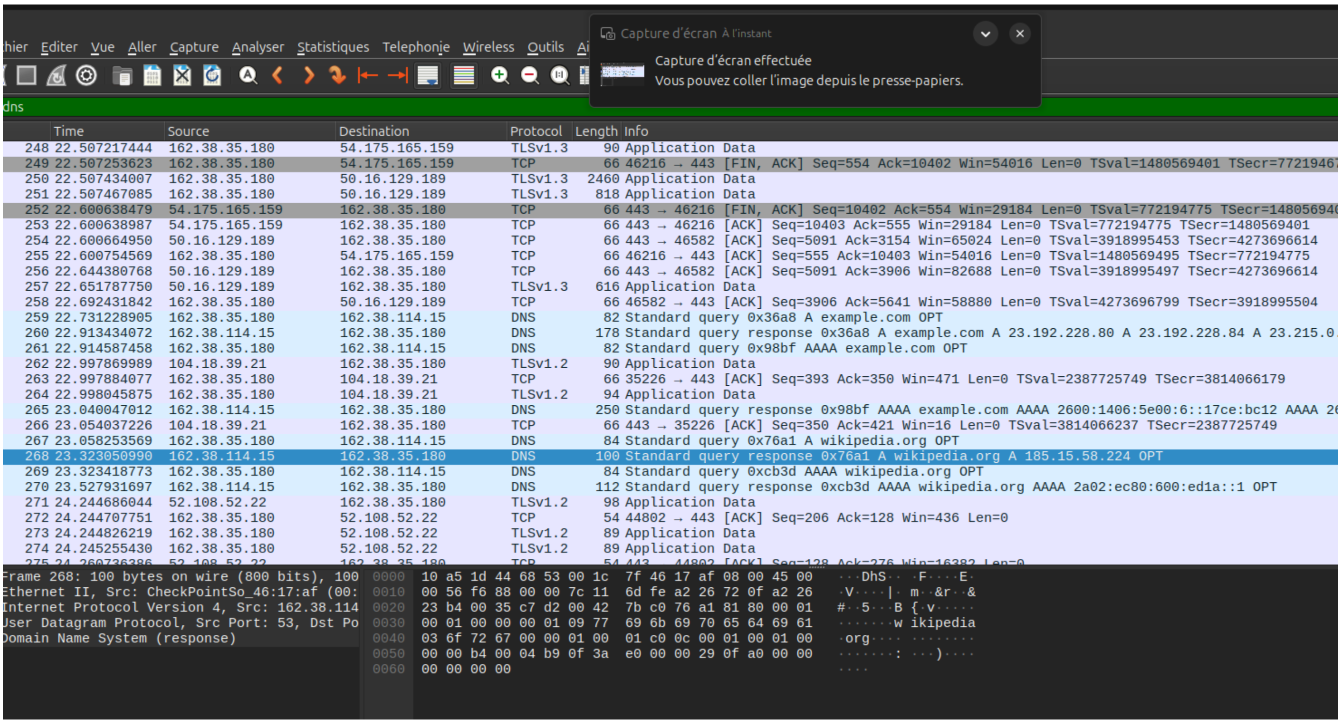
```
Frame 267: 84 bytes on wire (672 bits), 84 b    0000  00 1c 7f 00 48 16 10 a5  1d 44 68 53 08 00 45 00   ····H··· ·DhS··E·
Ethernet II, Src: Intel_44:68:53 (10:a5:1d:4    0010  00 46 58 c8 00 00 40 11  47 cf a2 26 23 b4 a2 26   ·FX···@· G··&#··&
Internet Protocol Version 4, Src: 162.38.35.    0020  72 0f c7 d2 00 35 00 32  da 53 76 a1 01 00 00 01   r····5·2 ·Sv·····
User Datagram Protocol, Src Port: 51154, Dst    0030  00 00 00 00 00 01 09 77  69 6b 69 70 65 64 69 61   ·······w ikipedia
Domain Name System (query)                      0040  03 6f 72 67 00 00 01 00  01 00 00 29 05 c0 00 00   ·org···· ···)····
                                                0050  00 00 00 00                                        ····
```

3. DNS Request for wikipedia.org

This packet corresponds to the DNS request sent by the client.

Query Type: A (IPv4 address request)
Source IP: 162.38.35.180
Destination IP: 162.38.114.15
Transaction ID: 0x67a1
→ Used to match the request with its corresponding response

Flags: Standard query, no errors
Requested Domain: wikipedia.org
→ This packet shows the client initiating DNS resolution for wikipedia.org.


hier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Ai
dns

Capture d'écran À l'instant
Capture d'écran effectuée
Vous pouvez coller l'image depuis le presse-papiers.

```
    Time           Source          Destination     Protocol Length Info
248 22.507217444   162.38.35.180   54.175.165.159  TLSv1.3    90 Application Data
249 22.507253623   162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [FIN, ACK] Seq=554 Ack=10402 Win=54016 Len=0 TSval=1480569401 TSecr=7721946
250 22.507434007   162.38.35.180   50.16.129.189   TLSv1.3  2460 Application Data
251 22.507467085   162.38.35.180   50.16.129.189   TLSv1.3   818 Application Data
252 22.600638479   54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [FIN, ACK] Seq=10402 Ack=554 Win=29184 Len=0 TSval=772194775 TSecr=14805694
253 22.600638987   54.175.165.159  162.38.35.180   TCP        66 443 → 46216 [ACK] Seq=10403 Ack=555 Win=29184 Len=0 TSval=772194775 TSecr=1480569401
254 22.600664950   50.16.129.189   162.38.35.180   TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3154 Win=65024 Len=0 TSval=3918995453 TSecr=4273696614
255 22.600754569   162.38.35.180   54.175.165.159  TCP        66 46216 → 443 [ACK] Seq=555 Ack=10403 Win=54016 Len=0 TSval=1480569495 TSecr=772194775
256 22.644380768   50.16.129.189   162.38.35.180   TCP        66 443 → 46582 [ACK] Seq=5091 Ack=3906 Win=82688 Len=0 TSval=3918995497 TSecr=4273696614
257 22.651787750   50.16.129.189   162.38.35.180   TLSv1.3   616 Application Data
258 22.692431842   162.38.35.180   50.16.129.189   TCP        66 46582 → 443 [ACK] Seq=3906 Ack=5641 Win=58880 Len=0 TSval=4273696799 TSecr=3918995504
259 22.731228905   162.38.35.180   162.38.114.15   DNS        82 Standard query 0x36a8 A example.com OPT
260 22.913434072   162.38.114.15   162.38.35.180   DNS       178 Standard query response 0x36a8 A example.com A 23.192.228.80 A 23.192.228.84 A 23.215.0
261 22.914587458   162.38.35.180   162.38.114.15   DNS        82 Standard query 0x98bf AAAA example.com OPT
262 22.997869989   104.18.39.21    162.38.35.180   TLSv1.2    90 Application Data
263 22.997884077   162.38.35.180   104.18.39.21    TCP        66 35226 → 443 [ACK] Seq=393 Ack=350 Win=471 Len=0 TSval=2387725749 TSecr=3814066179
264 22.998045875   162.38.35.180   104.18.39.21    TLSv1.2    94 Application Data
265 23.040047012   162.38.114.15   162.38.35.180   DNS       250 Standard query response 0x98bf AAAA example.com AAAA 2600:1406:5e00:6::17ce:bc12 AAAA 2
266 23.054037226   104.18.39.21    162.38.35.180   TCP        66 443 → 35226 [ACK] Seq=350 Ack=421 Win=16 Len=0 TSval=3814066237 TSecr=2387725749
267 23.058253569   162.38.35.180   162.38.114.15   DNS        84 Standard query 0x76a1 A wikipedia.org OPT
268 23.323050990   162.38.114.15   162.38.35.180   DNS       100 Standard query response 0x76a1 A wikipedia.org A 185.15.58.224 OPT
269 23.323418773   162.38.35.180   162.38.114.15   DNS        84 Standard query 0xcb3d AAAA wikipedia.org OPT
270 23.527931697   162.38.114.15   162.38.35.180   DNS       112 Standard query response 0xcb3d AAAA wikipedia.org AAAA 2a02:ec80:600:ed1a::1 OPT
271 24.244686044   52.108.52.22    162.38.35.180   TLSv1.2    98 Application Data
272 24.244707751   162.38.35.180   52.108.52.22    TCP        54 44802 → 443 [ACK] Seq=206 Ack=128 Win=436 Len=0
273 24.244826219   162.38.35.180   52.108.52.22    TLSv1.2    89 Application Data
274 24.245255430   162.38.35.180   52.108.52.22    TLSv1.2    89 Application Data
275 24.260736386   52.108.52.22    162.38.35.180   TCP        54 443 → 44802 [ACK] Seq=128 Ack=276 Win=16382 Len=0
```

```
Frame 268: 100 bytes on wire (800 bits), 100    0000  10 a5 1d 44 68 53 00 1c  7f 46 17 af 08 00 45 00   ···DhS·· ·F····E·
Ethernet II, Src: CheckPointSo_46:17:af (00:    0010  00 56 f6 88 00 00 7c 11  6d fe a2 26 72 0f a2 26   ·V····|· m··&r··&
Internet Protocol Version 4, Src: 162.38.114    0020  23 b4 00 35 c7 d2 00 42  7b c0 76 a1 81 80 00 01   #··5···B {·v·····
User Datagram Protocol, Src Port: 53, Dst Po    0030  00 01 00 00 00 01 09 77  69 6b 69 70 65 64 69 61   ·······w ikipedia
Domain Name System (response)                   0040  03 6f 72 67 00 00 01 00  01 c0 0c 00 01 00 01 00   ·org···· ········
                                                0050  00 00 b4 00 04 b9 0f 3a  e0 00 00 29 0f a0 00 00   ·······: ···)····
                                                0060  00 00 00 00                                        ····
```

4. DNS Response for wikipedia.org

This packet is the DNS server's answer to the previous query.

Response Type: Standard query response (No error)
Source IP: 162.38.114.15 (DNS server)
Destination IP: 162.38.35.180 (local machine)
Transaction ID: 0x67a1
→ Matches the request, confirming the correspondence

Answer (A Record): 185.15.58.224
→ The DNS server successfully resolves wikipedia.org and returns the corresponding IPv4 address.

The DNS captures show the complete resolution process for the domains example.com and wikipedia.org.

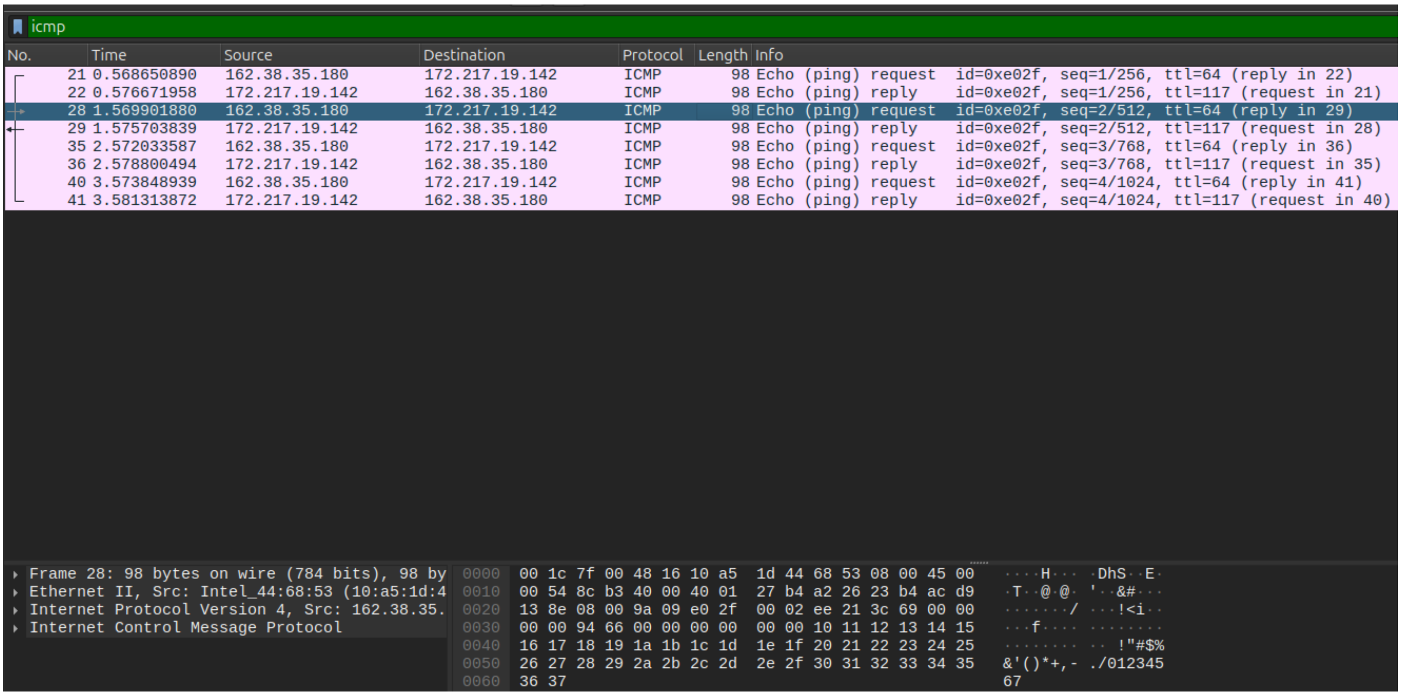
For each domain, the client sends a standard A-type query to the DNS server, and the server responds with the corresponding IPv4 address.

The matching Transaction IDs confirm the link between each request and response, and the flags indicate that all queries were processed without errors.

Overall, the DNS traffic behaves as expected and clearly illustrates how domain names are translated into IP addresses before any communication with remote servers can begin.

ICMP Analysis

To generate ICMP traTic, the command ping -c 4 google.com was executed. This command is used to test whether the remote machine (here google.com) is accessible. It generate 4 Echo requests and 4 Echo replies.



```
icmp
No.   Time         Source          Destination     Protocol Length Info
   21 0.568650890  162.38.35.180   172.217.19.142  ICMP        98 Echo (ping) request  id=0xe02f, seq=1/256, ttl=64 (reply in 22)
   22 0.576671958  172.217.19.142  162.38.35.180   ICMP        98 Echo (ping) reply    id=0xe02f, seq=1/256, ttl=117 (request in 21)
   28 1.569901880  162.38.35.180   172.217.19.142  ICMP        98 Echo (ping) request  id=0xe02f, seq=2/512, ttl=64 (reply in 29)
   29 1.575703839  172.217.19.142  162.38.35.180   ICMP        98 Echo (ping) reply    id=0xe02f, seq=2/512, ttl=117 (request in 28)
   35 2.572033587  162.38.35.180   172.217.19.142  ICMP        98 Echo (ping) request  id=0xe02f, seq=3/768, ttl=64 (reply in 36)
   36 2.578800494  172.217.19.142  162.38.35.180   ICMP        98 Echo (ping) reply    id=0xe02f, seq=3/768, ttl=117 (request in 35)
   40 3.573848939  162.38.35.180   172.217.19.142  ICMP        98 Echo (ping) request  id=0xe02f, seq=4/1024, ttl=64 (reply in 41)
   41 3.581313872  172.217.19.142  162.38.35.180   ICMP        98 Echo (ping) reply    id=0xe02f, seq=4/1024, ttl=117 (request in 40)
```

```
▸ Frame 28: 98 bytes on wire (784 bits), 98 by
▸ Ethernet II, Src: Intel_44:68:53 (10:a5:1d:4
▸ Internet Protocol Version 4, Src: 162.38.35.
▸ Internet Control Message Protocol
```

```
0000  00 1c 7f 00 48 16 10 a5  1d 44 68 53 08 00 45 00   ····H··· ·DhS··E·
0010  00 54 8c b3 40 00 40 01  27 b4 a2 26 23 b4 ac d9   ·T··@·@· '··&#···
0020  13 8e 08 00 9a 09 e0 2f  00 02 ee 21 3c 69 00 00   ·······/ ···!<i··
0030  00 00 94 66 00 00 00 00  00 00 10 11 12 13 14 15   ···f···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

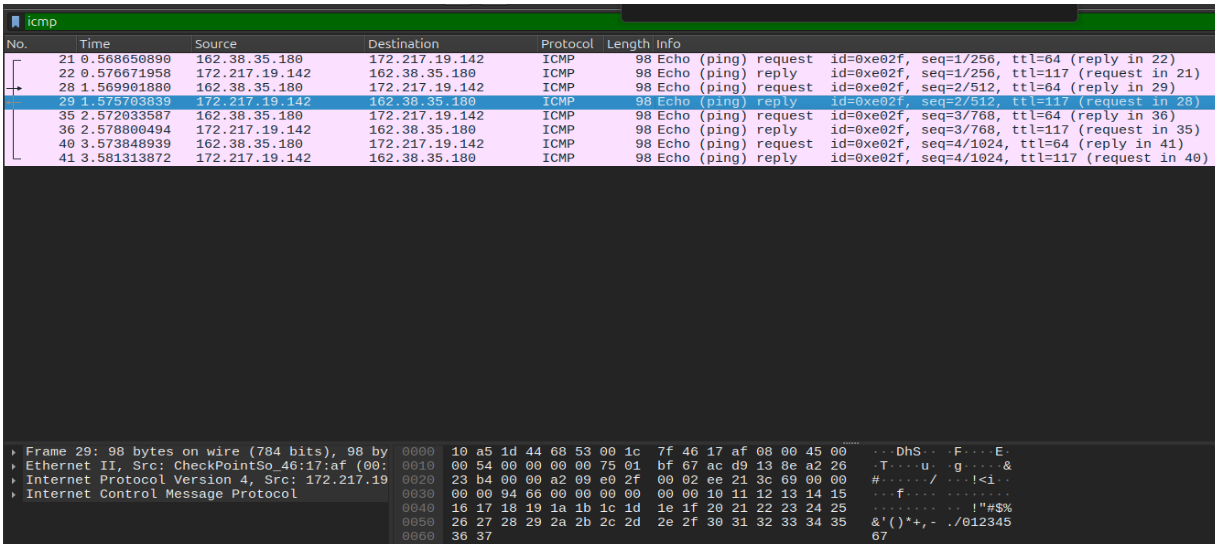
1. ICMP Echo Request (Packet 28)

This packet represents the ICMP Echo Request sent by the client as part of the ping command.

Type: 8 (Echo Request)
Source IP: 162.38.35.180 (local machine)
Destination IP: 172.217.19.142 (Google server)
Identifier: 0xe02f

Sequence Number: 2
→ Allows matching the request with the corresponding reply
TTL: 64
→ Typical for packets originating from a local host

Payload: Incremental byte pattern used to verify data integrity
→ This packet shows the client attempting to reach the remote host by sending an ICMP Echo Request.



```
No.     Time         Source          Destination     Protocol Length Info
   21 0.568650890  162.38.35.180   172.217.19.142  ICMP       98 Echo (ping) request  id=0xe02f, seq=1/256, ttl=64 (reply in 22)
   22 0.576671958  172.217.19.142  162.38.35.180   ICMP       98 Echo (ping) reply    id=0xe02f, seq=1/256, ttl=117 (request in 21)
   28 1.569901880  162.38.35.180   172.217.19.142  ICMP       98 Echo (ping) request  id=0xe02f, seq=2/512, ttl=64 (reply in 29)
   29 1.575703839  172.217.19.142  162.38.35.180   ICMP       98 Echo (ping) reply    id=0xe02f, seq=2/512, ttl=117 (request in 28)
   35 2.572033587  162.38.35.180   172.217.19.142  ICMP       98 Echo (ping) request  id=0xe02f, seq=3/768, ttl=64 (reply in 36)
   36 2.578800494  172.217.19.142  162.38.35.180   ICMP       98 Echo (ping) reply    id=0xe02f, seq=3/768, ttl=117 (request in 35)
   40 3.573848939  162.38.35.180   172.217.19.142  ICMP       98 Echo (ping) request  id=0xe02f, seq=4/1024, ttl=64 (reply in 41)
   41 3.581313872  172.217.19.142  162.38.35.180   ICMP       98 Echo (ping) reply    id=0xe02f, seq=4/1024, ttl=117 (request in 40)
```

```
› Frame 29: 98 bytes on wire (784 bits), 98 by
› Ethernet II, Src: CheckPointSo_46:17:af (00:
› Internet Protocol Version 4, Src: 172.217.19
› Internet Control Message Protocol
```

```
0000  10 a5 1d 44 68 53 00 1c  7f 46 17 af 08 00 45 00   ···DhS·· ·F····E·
0010  00 54 00 00 00 00 75 01  bf 67 ac d9 13 8e a2 26   ·T····u· ·g·····&
0020  23 b4 00 00 a2 09 e0 2f  00 02 ee 21 3c 69 00 00   #······/ ···!<i··
0030  00 00 94 66 00 00 00 00  00 00 10 11 12 13 14 15   ···f···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

2. ICMP Echo Reply (Packet 29)

This packet represents the reply sent by the remote host in response to the previous request.

Type: 0 (Echo Reply)
Source IP: 172.217.19.142 (Google server)
Destination IP: 162.38.35.180 (local machine)
Identifier: 0xe02f
→ Matches the identifier from the request

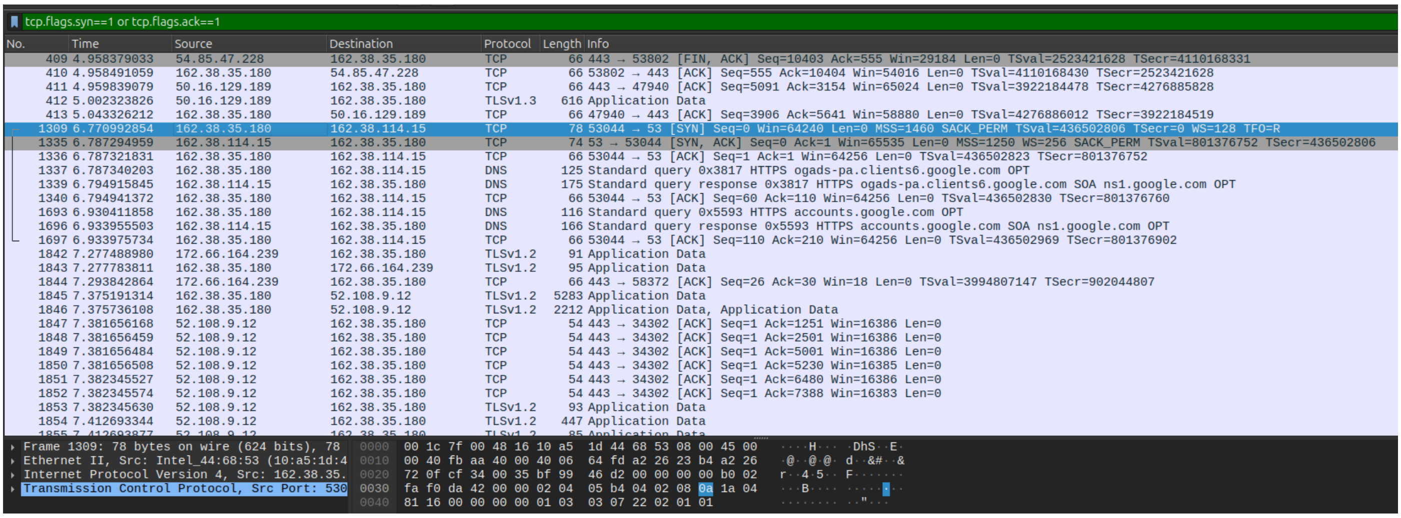
Sequence Number: 2
→ Same as the request, confirming the correspondence
TTL: 117
→ Indicates the packet traveled across an external network (Internet)

Round-Trip Time: Visible in the ping output, corresponds to the time between request and reply
→ This packet confirms that the remote host is reachable and responded successfully to the ICMP Echo Request.

The ICMP captures show a normal ping exchange between the client and Google's server.
Each Echo Request from the local machine receives a corresponding Echo Reply, confirmed by matching identifiers and sequence numbers.
The TTL values reflect the path differences between outgoing and incoming packets, and the successful replies demonstrate proper network connectivity.

TCP analysis : 3-way handshake

To generate TCP traffic, several websites were visited using an Internet browser. This action creates multiple TCP connections, each beginning with the standard three-way handshake (SYN, SYN-ACK, ACK) between the client and the web server.



tcp.flags.syn==1 or tcp.flags.ack==1

```
No.    Time        Source          Destination     Protocol Length Info
   409 4.958379033 54.85.47.228    162.38.35.180   TCP        66 443 → 53802 [FIN, ACK] Seq=10403 Ack=555 Win=29184 Len=0 TSval=2523421628 TSecr=4110168331
   410 4.958491059 162.38.35.180   54.85.47.228    TCP        66 53802 → 443 [ACK] Seq=555 Ack=10404 Win=54016 Len=0 TSval=4110168430 TSecr=2523421628
   411 4.959839079 50.16.129.189   162.38.35.180   TCP        66 443 → 47940 [ACK] Seq=5091 Ack=3154 Win=65024 Len=0 TSval=3922184478 TSecr=4276885828
   412 5.002323826 50.16.129.189   162.38.35.180   TLSv1.3   616 Application Data
   413 5.043326212 162.38.35.180   50.16.129.189   TCP        66 47940 → 443 [ACK] Seq=3906 Ack=5641 Win=58880 Len=0 TSval=4276886012 TSecr=3922184519
  1309 6.770992854 162.38.35.180   162.38.114.15   TCP        78 53044 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=436502806 TSecr=0 WS=128 TFO=R
  1335 6.787294959 162.38.114.15   162.38.35.180   TCP        74 53 → 53044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 WS=256 SACK_PERM TSval=801376752 TSecr=436502806
  1336 6.787321831 162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=436502823 TSecr=801376752
  1337 6.787340203 162.38.35.180   162.38.114.15   DNS       125 Standard query 0x3817 HTTPS ogads-pa.clients6.google.com OPT
  1339 6.794915845 162.38.114.15   162.38.35.180   DNS       175 Standard query response 0x3817 HTTPS ogads-pa.clients6.google.com SOA ns1.google.com OPT
  1340 6.794941372 162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=60 Ack=110 Win=64256 Len=0 TSval=436502830 TSecr=801376760
  1693 6.930411858 162.38.35.180   162.38.114.15   DNS       116 Standard query 0x5593 HTTPS accounts.google.com OPT
  1696 6.933955503 162.38.114.15   162.38.35.180   DNS       166 Standard query response 0x5593 HTTPS accounts.google.com SOA ns1.google.com OPT
  1697 6.933975734 162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=110 Ack=210 Win=64256 Len=0 TSval=436502969 TSecr=801376902
  1842 7.277488980 172.66.164.239  162.38.35.180   TLSv1.2    91 Application Data
  1843 7.277783811 162.38.35.180   172.66.164.239  TLSv1.2    95 Application Data
  1844 7.293842864 172.66.164.239  162.38.35.180   TCP        66 443 → 58372 [ACK] Seq=26 Ack=30 Win=18 Len=0 TSval=3994807147 TSecr=902044807
  1845 7.375191314 162.38.35.180   52.108.9.12     TLSv1.2  5283 Application Data
  1846 7.375736108 162.38.35.180   52.108.9.12     TLSv1.2  2212 Application Data, Application Data
  1847 7.381656168 52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=1251 Win=16386 Len=0
  1848 7.381656459 52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=2501 Win=16386 Len=0
  1849 7.381656484 52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=5001 Win=16386 Len=0
  1850 7.381656508 52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=5230 Win=16385 Len=0
  1851 7.382345527 52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=6480 Win=16386 Len=0
  1852 7.382345574 52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=7388 Win=16383 Len=0
  1853 7.382345630 52.108.9.12     162.38.35.180   TLSv1.2    93 Application Data
  1854 7.412693344 52.108.9.12     162.38.35.180   TLSv1.2   447 Application Data
  1855 7.412693877 52.108.9.12     162.38.35.180   TLSv1.2    85 Application Data
```

```
› Frame 1309: 78 bytes on wire (624 bits), 78    0000  00 1c 7f 00 48 16 10 a5  1d 44 68 53 08 00 45 00   ····H··· ·DhS··E·
› Ethernet II, Src: Intel_44:68:53 (10:a5:1d:4   0010  00 40 fb aa 40 00 40 06  64 fd a2 26 23 b4 a2 26   ·@··@·@· d··&#··&
› Internet Protocol Version 4, Src: 162.38.35.   0020  72 0f cf 34 00 35 bf 99  46 d2 00 00 00 00 b0 02   r··4·5·· F·······
› Transmission Control Protocol, Src Port: 530   0030  fa f0 da 42 00 00 02 04  05 b4 04 02 08 0a 1a 04   ···B···· ········
                                                 0040  81 16 00 00 00 00 01 03  03 07 22 02 01 01         ········ ··"···
```

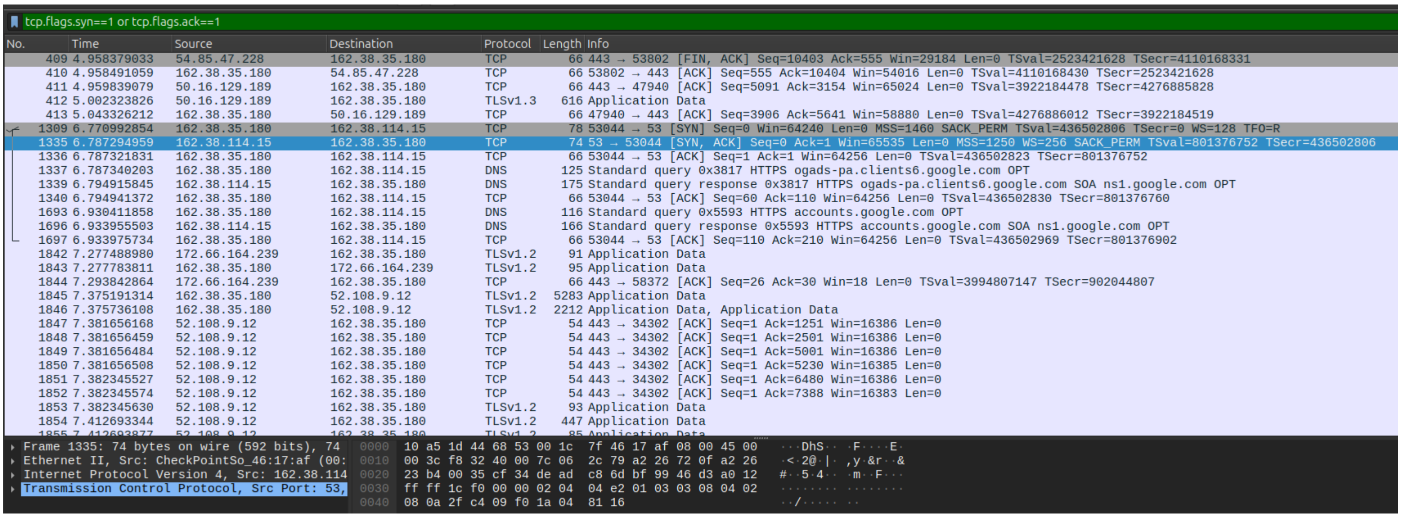
1. TCP SYN (Client → Server)

This packet is the TCP SYN sent by the client to initiate a connection with the server.

Source Port: 53044 (client)
Destination Port: 53 (server)
Flags: SYN
→ Indicates the beginning of a TCP connection.
Sequence Number: 0
→ First sequence number sent by the client.

Window Size: 64240
→ Advertised receive window of the client.

Options: MSS = 1460
→ This packet represents the client's attempt to establish a TCP session.



```
tcp.flags.syn==1 or tcp.flags.ack==1
No.    Time        Source          Destination     Protocol Length Info
  409 4.958379033  54.85.47.228    162.38.35.180   TCP        66 443 → 53802 [FIN, ACK] Seq=10403 Ack=555 Win=29184 Len=0 TSval=2523421628 TSecr=4110168331
  410 4.958491059  162.38.35.180   54.85.47.228    TCP        66 53802 → 443 [ACK] Seq=555 Ack=10404 Win=54016 Len=0 TSval=4110168430 TSecr=2523421628
  411 4.959839079  50.16.129.189   162.38.35.180   TCP        66 443 → 47940 [ACK] Seq=5091 Ack=3154 Win=65024 Len=0 TSval=3922184478 TSecr=4276885828
  412 5.002323826  50.16.129.189   162.38.35.180   TLSv1.3   616 Application Data
  413 5.043326212  162.38.35.180   50.16.129.189   TCP        66 47940 → 443 [ACK] Seq=3906 Ack=5641 Win=58880 Len=0 TSval=4276886012 TSecr=3922184519
 1309 6.770992854  162.38.35.180   162.38.114.15   TCP        78 53044 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=436502806 TSecr=0 WS=128 TFO=R
 1335 6.787294959  162.38.114.15   162.38.35.180   TCP        74 53 → 53044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 WS=256 SACK_PERM TSval=801376752 TSecr=436502806
 1336 6.787321831  162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=436502823 TSecr=801376752
 1337 6.787340203  162.38.35.180   162.38.114.15   DNS       125 Standard query 0x3817 HTTPS ogads-pa.clients6.google.com OPT
 1339 6.794915845  162.38.114.15   162.38.35.180   DNS       175 Standard query response 0x3817 HTTPS ogads-pa.clients6.google.com SOA ns1.google.com OPT
 1340 6.794941372  162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=60 Ack=110 Win=64256 Len=0 TSval=436502830 TSecr=801376760
 1693 6.930411858  162.38.35.180   162.38.114.15   DNS       116 Standard query 0x5593 HTTPS accounts.google.com OPT
 1696 6.933955503  162.38.114.15   162.38.35.180   DNS       166 Standard query response 0x5593 HTTPS accounts.google.com SOA ns1.google.com OPT
 1697 6.933975734  162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=110 Ack=210 Win=64256 Len=0 TSval=436502969 TSecr=801376902
 1842 7.277488980  172.66.164.239  162.38.35.180   TLSv1.2    91 Application Data
 1843 7.277783811  162.38.35.180   172.66.164.239  TLSv1.2    95 Application Data
 1844 7.293842864  172.66.164.239  162.38.35.180   TCP        66 443 → 58372 [ACK] Seq=26 Ack=30 Win=18 Len=0 TSval=3994807147 TSecr=902044807
 1845 7.375191314  162.38.35.180   52.108.9.12     TLSv1.2  5283 Application Data
 1846 7.375736108  162.38.35.180   52.108.9.12     TLSv1.2  2212 Application Data, Application Data
 1847 7.381656168  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=1251 Win=16386 Len=0
 1848 7.381656459  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=2501 Win=16386 Len=0
 1849 7.381656484  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=5001 Win=16386 Len=0
 1850 7.381656508  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=5230 Win=16385 Len=0
 1851 7.382345527  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=6480 Win=16386 Len=0
 1852 7.382345574  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=7388 Win=16383 Len=0
 1853 7.382345630  52.108.9.12     162.38.35.180   TLSv1.2    93 Application Data
 1854 7.412693344  52.108.9.12     162.38.35.180   TLSv1.2   447 Application Data
 1855 7.412693877  52.108.9.12     162.38.35.180   TLSv1.2    85 Application Data
```

```
› Frame 1335: 74 bytes on wire (592 bits), 74          0000  10 a5 1d 44 68 53 00 1c  7f 46 17 af 08 00 45 00   ···DhS·· ·F····E·
› Ethernet II, Src: CheckPointSo_46:17:af (00:         0010  00 3c f8 32 40 00 7c 06  2c 79 a2 26 72 0f a2 26   ·<·2@·|· ,y·&r··&
› Internet Protocol Version 4, Src: 162.38.114         0020  23 b4 00 35 cf 34 de ad  c8 6d bf 99 46 d3 a0 12   #··5·4·· ·m··F···
› Transmission Control Protocol, Src Port: 53,         0030  ff ff 1c f0 00 00 02 04  04 e2 01 03 03 08 04 02   ········ ········
                                                       0040  08 0a 2f c4 09 f0 1a 04  81 16                     ··/····· ··
```

2. TCP SYN-ACK (Server → Client)

This packet is the SYN-ACK response sent by the server as part of the handshake.

Source Port: 53 (server)

Destination Port: 53044 (client)

Flags: SYN, ACK

→ Confirms that the server received the client's SYN and agrees to establish the connection.

Sequence Number: 0

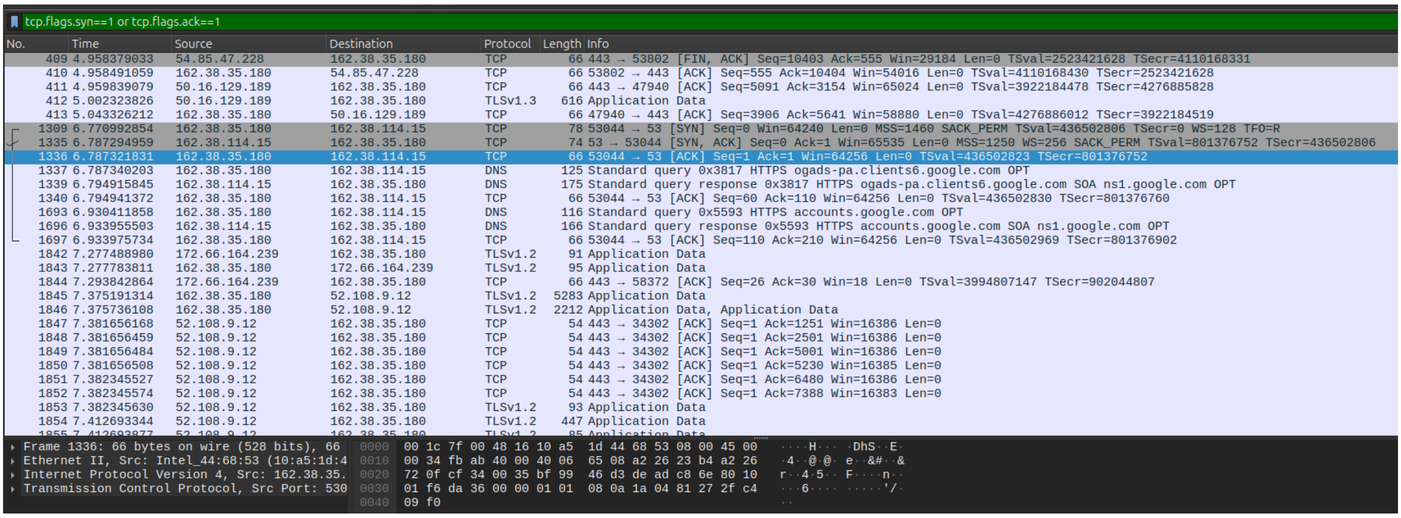
→ First sequence number sent by the server.

Acknowledgment Number: 1

→ Acknowledges the client's SYN (Seq=0 → Ack=1).

Window Size: 65535

→ This packet completes the second step of the TCP 3-way handshake.



```
tcp.flags.syn==1 or tcp.flags.ack==1
No.    Time        Source          Destination     Protocol Length Info
  409 4.958379033  54.85.47.228    162.38.35.180   TCP        66 443 → 53802 [FIN, ACK] Seq=10403 Ack=555 Win=29184 Len=0 TSval=2523421628 TSecr=4110168331
  410 4.958491059  162.38.35.180   54.85.47.228    TCP        66 53802 → 443 [ACK] Seq=555 Ack=10404 Win=54016 Len=0 TSval=4110168430 TSecr=2523421628
  411 4.959839079  50.16.129.189   162.38.35.180   TCP        66 443 → 47940 [ACK] Seq=5091 Ack=3154 Win=65024 Len=0 TSval=3922184478 TSecr=4276885828
  412 5.002323826  50.16.129.189   162.38.35.180   TLSv1.3   616 Application Data
  413 5.043326212  162.38.35.180   50.16.129.189   TCP        66 47940 → 443 [ACK] Seq=3906 Ack=5641 Win=58880 Len=0 TSval=4276886012 TSecr=3922184519
 1309 6.770992854  162.38.35.180   162.38.114.15   TCP        78 53044 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=436502806 TSecr=0 WS=128 TFO=R
 1335 6.787294959  162.38.114.15   162.38.35.180   TCP        74 53 → 53044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 WS=256 SACK_PERM TSval=801376752 TSecr=436502806
 1336 6.787321831  162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=436502823 TSecr=801376752
 1337 6.787340203  162.38.35.180   162.38.114.15   DNS       125 Standard query 0x3817 HTTPS ogads-pa.clients6.google.com OPT
 1339 6.794915845  162.38.114.15   162.38.35.180   DNS       175 Standard query response 0x3817 HTTPS ogads-pa.clients6.google.com SOA ns1.google.com OPT
 1340 6.794941372  162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=60 Ack=110 Win=64256 Len=0 TSval=436502830 TSecr=801376760
 1693 6.930411858  162.38.35.180   162.38.114.15   DNS       116 Standard query 0x5593 HTTPS accounts.google.com OPT
 1696 6.933955503  162.38.114.15   162.38.35.180   DNS       166 Standard query response 0x5593 HTTPS accounts.google.com SOA ns1.google.com OPT
 1697 6.933975734  162.38.35.180   162.38.114.15   TCP        66 53044 → 53 [ACK] Seq=110 Ack=210 Win=64256 Len=0 TSval=436502969 TSecr=801376902
 1842 7.277488980  172.66.164.239  162.38.35.180   TLSv1.2    91 Application Data
 1843 7.277783811  162.38.35.180   172.66.164.239  TLSv1.2    95 Application Data
 1844 7.293842864  172.66.164.239  162.38.35.180   TCP        66 443 → 58372 [ACK] Seq=26 Ack=30 Win=18 Len=0 TSval=3994807147 TSecr=902044807
 1845 7.375191314  162.38.35.180   52.108.9.12     TLSv1.2  5283 Application Data
 1846 7.375736108  162.38.35.180   52.108.9.12     TLSv1.2  2212 Application Data, Application Data
 1847 7.381656168  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=1251 Win=16386 Len=0
 1848 7.381656459  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=2501 Win=16386 Len=0
 1849 7.381656484  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=5001 Win=16386 Len=0
 1850 7.381656508  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=5230 Win=16385 Len=0
 1851 7.382345527  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=6480 Win=16386 Len=0
 1852 7.382345574  52.108.9.12     162.38.35.180   TCP        54 443 → 34302 [ACK] Seq=1 Ack=7388 Win=16383 Len=0
 1853 7.382345630  52.108.9.12     162.38.35.180   TLSv1.2    93 Application Data
 1854 7.412693344  52.108.9.12     162.38.35.180   TLSv1.2   447 Application Data
 1855 7.412693877  52.108.9.12     162.38.35.180   TLSv1.2    85 Application Data
```

```
› Frame 1336: 66 bytes on wire (528 bits), 66          0000  00 1c 7f 00 48 16 10 a5  1d 44 68 53 08 00 45 00   ····H··· ·DhS··E·
› Ethernet II, Src: Intel_44:68:53 (10:a5:1d:4         0010  00 34 fb ab 40 00 40 06  65 08 a2 26 23 b4 a2 26   ·4··@·@· e··&#··&
› Internet Protocol Version 4, Src: 162.38.35.         0020  72 0f cf 34 00 35 bf 99  46 d3 de ad c8 6e 80 10   r··4·5·· F····n··
› Transmission Control Protocol, Src Port: 530         0030  01 f6 da 36 00 00 01 01  08 0a 1a 04 81 27 2f c4   ···6···· ·····'/·
                                                       0040  09 f0                                              ··
```

3. TCP ACK (Client → Server)

This packet is the final ACK completing the handshake.

Source Port: 53044 (client)
Destination Port: 53 (server)
Flags: ACK
→ Final step confirming connection establishment.

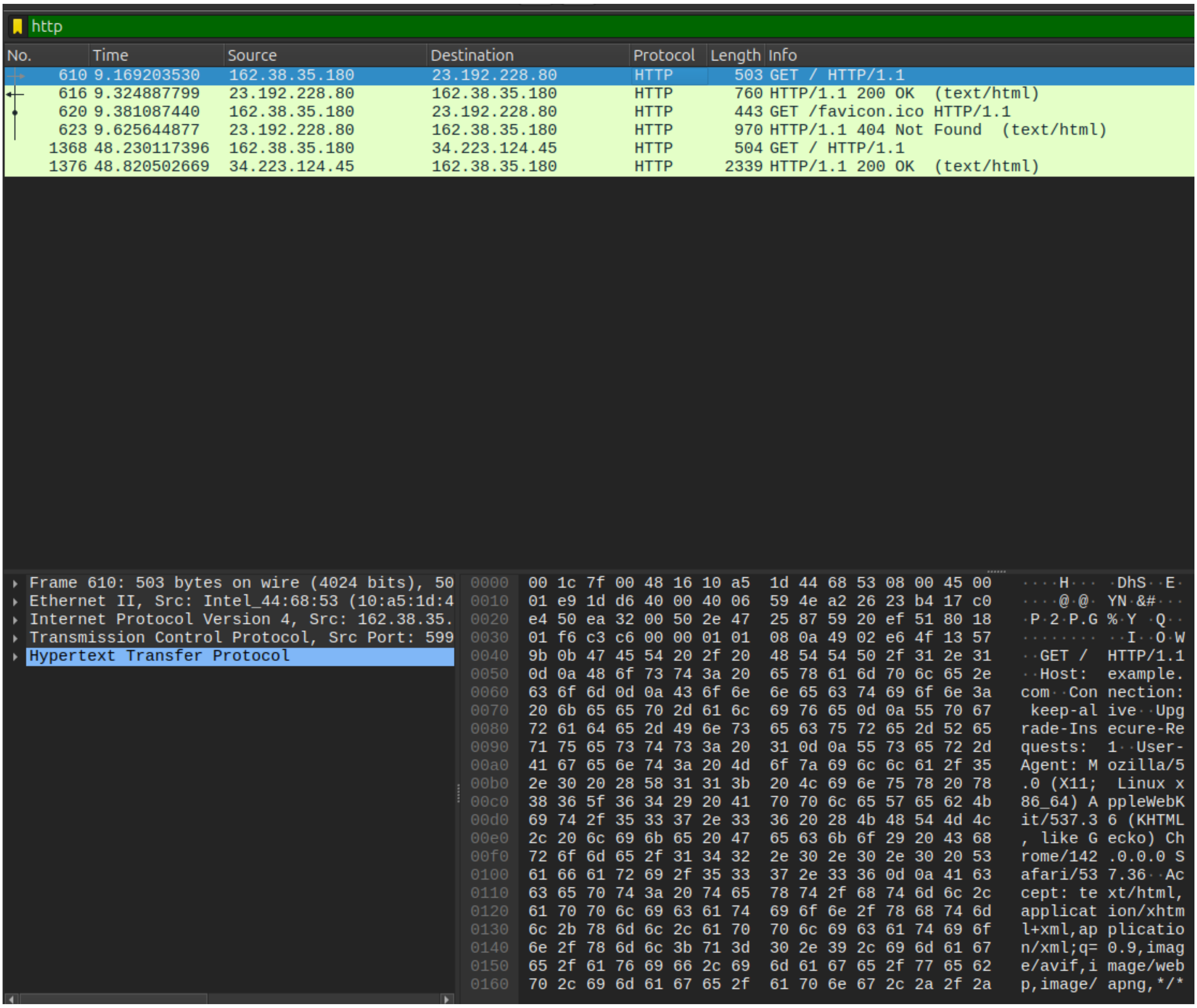
Sequence Number: 1
→ Next byte after the SYN.
Acknowledgment Number: 1
→ Confirms receipt of the server's SYN-ACK.

→ This packet finalizes the TCP handshake and establishes a reliable TCP connection between client and server.

The three packets (SYN → SYN-ACK → ACK) clearly show a complete and valid TCP 3-way handshake.
Sequence and acknowledgment numbers match, and both endpoints successfully negotiate the connection parameters.
This confirms that a reliable TCP session was successfully established between the client and the server.

HTTP analysis

To generate HTTP traffic, the browser was used to visit the websites http://example.com and http://neverssl.com. These actions produce HTTP GET requests sent from the client to the web servers, followed by HTTP responses containing the requested webpage content.



```
http
No.     Time            Source          Destination     Protocol Length Info
    610 9.169203530     162.38.35.180   23.192.228.80   HTTP      503 GET / HTTP/1.1
    616 9.324887799     23.192.228.80   162.38.35.180   HTTP      760 HTTP/1.1 200 OK  (text/html)
    620 9.381087440     162.38.35.180   23.192.228.80   HTTP      443 GET /favicon.ico HTTP/1.1
    623 9.625644877     23.192.228.80   162.38.35.180   HTTP      970 HTTP/1.1 404 Not Found  (text/html)
   1368 48.230117396    162.38.35.180   34.223.124.45   HTTP      504 GET / HTTP/1.1
   1376 48.820502669    34.223.124.45   162.38.35.180   HTTP     2339 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 610: 503 bytes on wire (4024 bits), 50
▸ Ethernet II, Src: Intel_44:68:53 (10:a5:1d:4
▸ Internet Protocol Version 4, Src: 162.38.35.
▸ Transmission Control Protocol, Src Port: 599
▸ Hypertext Transfer Protocol
```

```
0000  00 1c 7f 00 48 16 10 a5  1d 44 68 53 08 00 45 00   ····H··· ·DhS··E·
0010  01 e9 1d d6 40 00 40 06  59 4e a2 26 23 b4 17 c0   ····@·@· YN·&#···
0020  e4 50 ea 32 00 50 2e 47  25 87 59 20 ef 51 80 18   ·P·2·P.G %·Y ·Q··
0030  01 f6 c3 c6 00 00 01 01  08 0a 49 02 e6 4f 13 57   ········ ··I··O·W
0040  9b 0b 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  65 78 61 6d 70 6c 65 2e   ··Host:  example.
0060  63 6f 6d 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   com··Con nection:
0070  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 55 70 67    keep-al ive··Upg
0080  72 61 64 65 2d 49 6e 73  65 63 75 72 65 2d 52 65   rade-Ins ecure-Re
0090  71 75 65 73 74 73 3a 20  31 0d 0a 55 73 65 72 2d   quests:  1··User-
00a0  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
00b0  2e 30 20 28 58 31 31 3b  20 4c 69 6e 75 78 20 78   .0 (X11;  Linux x
00c0  38 36 5f 36 34 29 20 41  70 70 6c 65 57 65 62 4b   86_64) A ppleWebK
00d0  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
00e0  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
00f0  72 6f 6d 65 2f 31 34 32  2e 30 2e 30 2e 30 20 53   rome/142 .0.0.0 S
0100  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0110  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0120  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0130  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0140  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0150  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
0160  70 2c 69 6d 61 67 65 2f  61 70 6e 67 2c 2a 2f 2a   p,image/ apng,*/*
```

1. HTTP GET Request (Packet 610)

This packet is the HTTP GET request sent by the client to retrieve a webpage hosted on the remote server.

Method: GET
Request URI: /

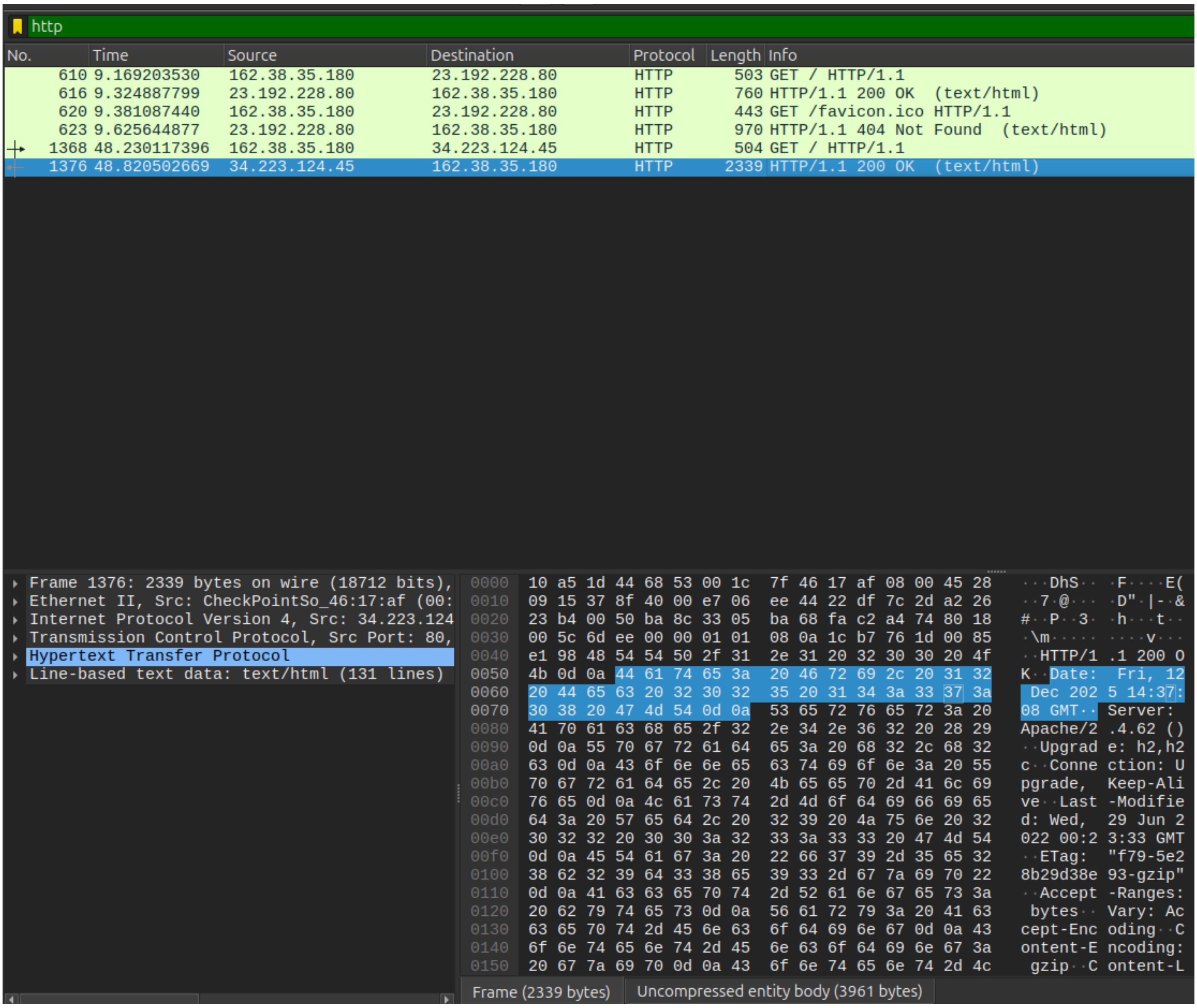
Host: example.com
→ The client requests the main web page from the server.

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/142.0.0.0 Safari/537.36
→ Identifies the browser and operating system.

Source IP: 162.38.35.180 (local machine)
Destination IP: 23.192.228.80 (web server)
Source Port: 599xx

Destination Port: 80 (HTTP)
TCP Info: Seq=47, Ack=45, Len=468

→ This packet represents the browser’s initial request for loading the webpage over an unencrypted HTTP connection.



```
http
No.   Time         Source          Destination     Protocol Length Info
  610 9.169203530  162.38.35.180   23.192.228.80   HTTP      503 GET / HTTP/1.1
  616 9.324887799  23.192.228.80   162.38.35.180   HTTP      760 HTTP/1.1 200 OK  (text/html)
  620 9.381087440  162.38.35.180   23.192.228.80   HTTP      443 GET /favicon.ico HTTP/1.1
  623 9.625644877  23.192.228.80   162.38.35.180   HTTP      970 HTTP/1.1 404 Not Found  (text/html)
 1368 48.230117396 162.38.35.180   34.223.124.45   HTTP      504 GET / HTTP/1.1
 1376 48.820502669 34.223.124.45   162.38.35.180   HTTP     2339 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 1376: 2339 bytes on wire (18712 bits),
▸ Ethernet II, Src: CheckPointSo_46:17:af (00:
▸ Internet Protocol Version 4, Src: 34.223.124
▸ Transmission Control Protocol, Src Port: 80,
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (131 lines)
```

```
0000  10 a5 1d 44 68 53 00 1c  7f 46 17 af 08 00 45 28   ···DhS·· ·F····E(
0010  09 15 37 8f 40 00 e7 06  ee 44 22 df 7c 2d a2 26   ··7·@··· ·D"·|-·&
0020  23 b4 00 50 ba 8c 33 05  ba 68 fa c2 a4 74 80 18   #··P··3· ·h···t··
0030  00 5c 6d ee 00 00 01 01  08 0a 1c b7 76 1d 00 85   ·\m····· ····v···
0040  e1 98 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ··HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 46 72 69 2c 20 31 32   K··Date:  Fri, 12
0060  20 44 65 63 20 32 30 32  35 20 31 34 3a 33 37 3a    Dec 202 5 14:37:
0070  30 38 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   08 GMT·· Server: 
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 32 20 28 29   Apache/2 .4.62 ()
0090  0d 0a 55 70 67 72 61 64  65 3a 20 68 32 2c 68 32   ··Upgrad e: h2,h2
00a0  63 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 55   c··Conne ction: U
00b0  70 67 72 61 64 65 2c 20  4b 65 65 70 2d 41 6c 69   pgrade,  Keep-Ali
00c0  76 65 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65   ve··Last -Modifie
00d0  64 3a 20 57 65 64 2c 20  32 39 20 4a 75 6e 20 32   d: Wed,  29 Jun 2
00e0  30 32 32 20 30 30 3a 32  33 3a 33 33 20 47 4d 54   022 00:2 3:33 GMT
00f0  0d 0a 45 54 61 67 3a 20  22 66 37 39 2d 35 65 32   ··ETag:  "f79-5e2
0100  38 62 32 39 64 33 38 65  39 33 2d 67 7a 69 70 22   8b29d38e 93-gzip"
0110  0d 0a 41 63 63 65 70 74  2d 52 61 6e 67 65 73 3a   ··Accept -Ranges:
0120  20 62 79 74 65 73 0d 0a  56 61 72 79 3a 20 41 63    bytes·· Vary: Ac
0130  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 0d 0a 43   cept-Enc oding··C
0140  6f 6e 74 65 6e 74 2d 45  6e 63 6f 64 69 6e 67 3a   ontent-E ncoding:
0150  20 67 7a 69 70 0d 0a 43  6f 6e 74 65 6e 74 2d 4c    gzip··C ontent-L
```

2. HTTP 200 OK Response (Packet 1376)

This packet is the server’s response to the previous GET request.

Status: HTTP/1.1 200 OK
→ Indicates that the request was successful.

Content-Type: text/html
Content-Length: 3961 bytes (uncompressed entity body)

Server: Apache/2.4.62
Date: Fri, 12 Dec 2025 14:37 GMT

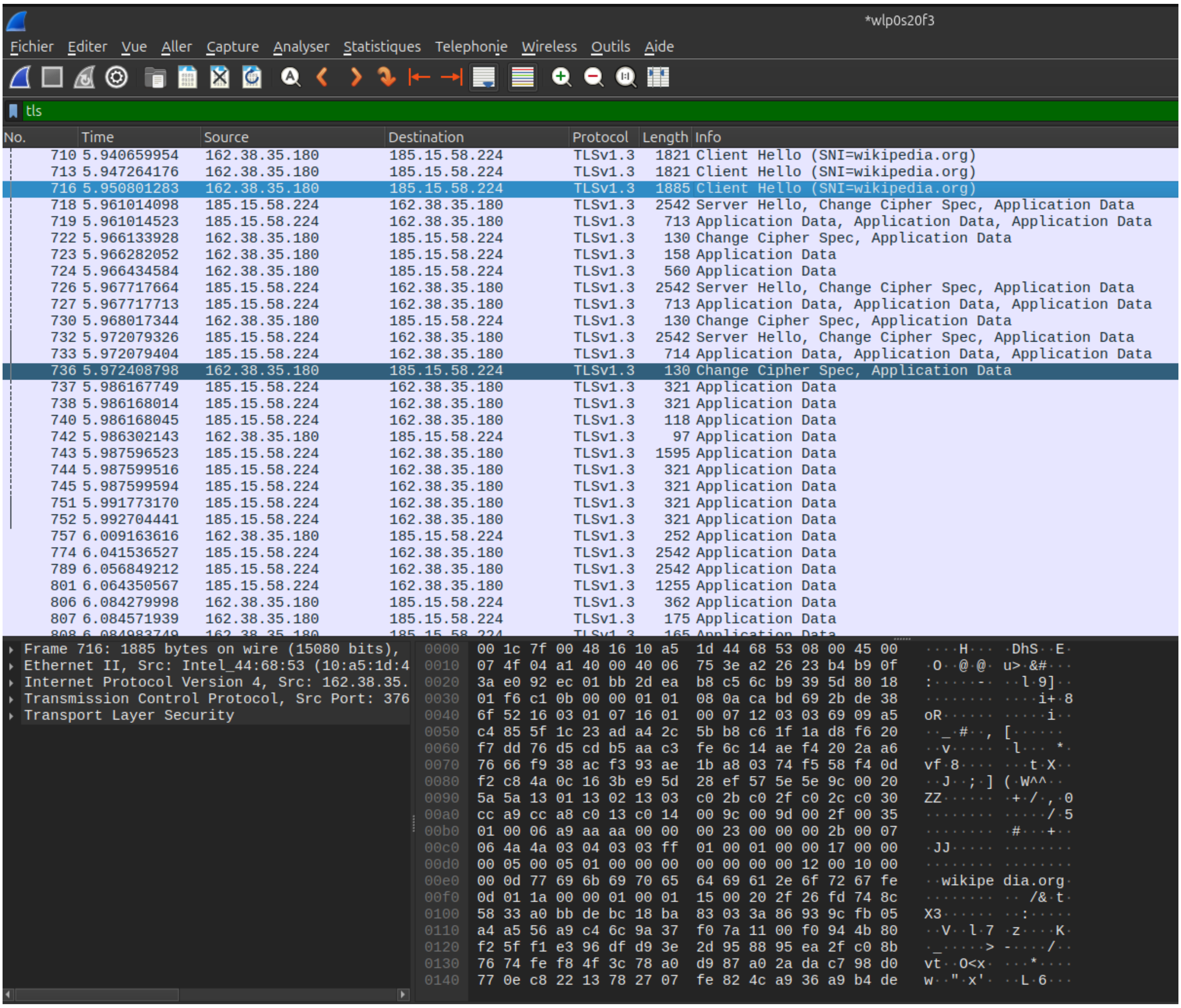
Headers:
Connection: keep-alive
Last-Modified: Wed, 29 Jun 2022
ETag: "f79-5e2bd438e93-gzip"
Accept-Ranges: bytes

In addition, the packet contains the HTML content of the page in clear text, since HTTP does not provide any encryption. The payload section shows readable HTML, making it easy to inspect the structure of the returned webpage.

→ This packet corresponds to the server delivering the requested webpage to the client.

The HTTP exchange clearly shows how unencrypted web traffic operates.
The client sends a GET request, and the server responds with a valid 200 OK message containing the full HTML page. Because HTTP is not encrypted, all headers and the body content are visible in plain text within the packet capture.
This highlights the lack of confidentiality in HTTP communications and explains why HTTPS is preferred for secure browsing.

TLS analysis (HTTPS)


*wlp0s20f3
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
tls
```

```
No.  Time         Source          Destination     Protocol Length Info
 710 5.940659954  162.38.35.180   185.15.58.224   TLSv1.3  1821 Client Hello (SNI=wikipedia.org)
 713 5.947264176  162.38.35.180   185.15.58.224   TLSv1.3  1821 Client Hello (SNI=wikipedia.org)
 716 5.950801283  162.38.35.180   185.15.58.224   TLSv1.3  1885 Client Hello (SNI=wikipedia.org)
 718 5.961014098  185.15.58.224   162.38.35.180   TLSv1.3  2542 Server Hello, Change Cipher Spec, Application Data
 719 5.961014523  185.15.58.224   162.38.35.180   TLSv1.3   713 Application Data, Application Data, Application Data
 722 5.966133928  162.38.35.180   185.15.58.224   TLSv1.3   130 Change Cipher Spec, Application Data
 723 5.966282052  162.38.35.180   185.15.58.224   TLSv1.3   158 Application Data
 724 5.966434584  162.38.35.180   185.15.58.224   TLSv1.3   560 Application Data
 726 5.967717664  185.15.58.224   162.38.35.180   TLSv1.3  2542 Server Hello, Change Cipher Spec, Application Data
 727 5.967717713  185.15.58.224   162.38.35.180   TLSv1.3   713 Application Data, Application Data, Application Data
 730 5.968017344  162.38.35.180   185.15.58.224   TLSv1.3   130 Change Cipher Spec, Application Data
 732 5.972079326  185.15.58.224   162.38.35.180   TLSv1.3  2542 Server Hello, Change Cipher Spec, Application Data
 733 5.972079404  185.15.58.224   162.38.35.180   TLSv1.3   714 Application Data, Application Data, Application Data
 736 5.972408798  162.38.35.180   185.15.58.224   TLSv1.3   130 Change Cipher Spec, Application Data
 737 5.986167749  185.15.58.224   162.38.35.180   TLSv1.3   321 Application Data
 738 5.986168014  185.15.58.224   162.38.35.180   TLSv1.3   321 Application Data
 740 5.986168045  185.15.58.224   162.38.35.180   TLSv1.3   118 Application Data
 742 5.986302143  162.38.35.180   185.15.58.224   TLSv1.3    97 Application Data
 743 5.987596523  185.15.58.224   162.38.35.180   TLSv1.3  1595 Application Data
 744 5.987599516  185.15.58.224   162.38.35.180   TLSv1.3   321 Application Data
 745 5.987599594  185.15.58.224   162.38.35.180   TLSv1.3   321 Application Data
 751 5.991773170  185.15.58.224   162.38.35.180   TLSv1.3   321 Application Data
 752 5.992704441  185.15.58.224   162.38.35.180   TLSv1.3   321 Application Data
 757 6.009163616  162.38.35.180   185.15.58.224   TLSv1.3   252 Application Data
 774 6.041536527  185.15.58.224   162.38.35.180   TLSv1.3  2542 Application Data
 789 6.056849212  185.15.58.224   162.38.35.180   TLSv1.3  2542 Application Data
 801 6.064350567  185.15.58.224   162.38.35.180   TLSv1.3  1255 Application Data
 806 6.084279998  162.38.35.180   185.15.58.224   TLSv1.3   362 Application Data
 807 6.084571939  162.38.35.180   185.15.58.224   TLSv1.3   175 Application Data
 808 6.084983749  162.38.35.180   185.15.58.224   TLSv1.3   165 Application Data
```

```
› Frame 716: 1885 bytes on wire (15080 bits),
› Ethernet II, Src: Intel_44:68:53 (10:a5:1d:4
› Internet Protocol Version 4, Src: 162.38.35.
› Transmission Control Protocol, Src Port: 376
› Transport Layer Security
```

```
0000  00 1c 7f 00 48 16 10 a5  1d 44 68 53 08 00 45 00   ····H··· ·DhS··E·
0010  07 4f 04 a1 40 00 40 06  75 3e a2 26 23 b4 b9 0f   ·O··@·@· u>·&#···
0020  3a e0 92 ec 01 bb 2d ea  b8 c5 6c b9 39 5d 80 18   :·····-· ··l·9]··
0030  01 f6 c1 0b 00 00 01 01  08 0a ca bd 69 2b de 38   ········ ····i+·8
0040  6f 52 16 03 01 07 16 01  00 07 12 03 03 69 09 a5   oR······ ·····i··
0050  c4 85 5f 1c 23 ad a4 2c  5b b8 c6 1f 1a d8 f6 20   ··_·#··, [·······
0060  f7 dd 76 d5 cd b5 aa c3  fe 6c 14 ae f4 20 2a a6   ··v····· ·l··· *·
0070  76 66 f9 38 ac f3 93 ae  1b a8 03 74 f5 58 f4 0d   vf·8···· ···t·X··
0080  f2 c8 4a 0c 16 3b e9 5d  28 ef 57 5e 5e 9c 00 20   ··J··;·] (·W^^··
0090  5a 5a 13 01 13 02 13 03  c0 2b c0 2f c0 2c c0 30   ZZ······ ·+·/·,·0
00a0  cc a9 cc a8 c0 13 c0 14  00 9c 00 9d 00 2f 00 35   ········ ·····/·5
00b0  01 00 06 a9 aa aa 00 00  00 23 00 00 00 2b 00 07   ········ ·#···+··
00c0  06 4a 4a 03 04 03 03 ff  01 00 01 00 00 17 00 00   ·JJ····· ········
00d0  00 05 00 05 01 00 00 00  00 00 00 00 12 00 10 00   ········ ········
00e0  00 0d 77 69 6b 69 70 65  64 69 61 2e 6f 72 67 fe   ··wikipe dia.org·
00f0  0d 01 1a 00 00 01 00 01  15 00 20 2f 26 fd 74 8c   ········ ·· /&·t·
0100  58 33 a0 bb de bc 18 ba  83 03 3a 86 93 9c fb 05   X3······ ··:·····
0110  a4 a5 56 a9 c4 6c 9a 37  f0 7a 11 00 f0 94 4b 80   ··V··l·7 ·z····K·
0120  f2 5f f1 e3 96 df d9 3e  2d 95 88 95 ea 2f c0 8b   ·_·····> -····/··
0130  76 74 fe f8 4f 3c 78 a0  d9 87 a0 2a da c7 98 d0   vt··O<x· ···*····
0140  77 0e c8 22 13 78 27 07  fe 82 4c a9 36 a9 b4 de   w··"·x'· ··L·6···
```

1. Client Hello (Packet ~717)

This packet corresponds to the TLS Client Hello message sent by the client to initiate the TLS 1.3 handshake.

TLS Version: TLS 1.3
Random Value: Client-generated random value used during key derivation
Session ID: Present (indicates support for session resumption)

Cipher Suites:

The client proposes a list of supported cipher suites, typically including modern and secure options such as AES-GCM and ChaCha20-based suites (TLS 1.3 suites do not appear individually in Wireshark but are negotiated internally).

Extensions:

server_name (SNI): wikipedia.org
→ Indicates the domain the client intends to reach
supported_versions: Includes TLS 1.3
key_share: Used during ephemeral Diffie–Hellman key exchange
supported_groups: Lists supported elliptic curve groups
signature_algorithms: Allowed signature algorithms for certificate validation

→ This packet is the first step of the TLS handshake. The client proposes security parameters and announces support for TLS 1.3 while specifying the website it wants to reach through SNI.

2. Server Hello (Packet ~723 / 725)

This packet corresponds to the Server Hello message, sent by the server in response to the Client Hello.

TLS Version: TLS 1.3
Random Value: Server-generated random value
Session ID: Matches the one sent by the client
→ Confirms session establishment

Selected Cipher Suite:

(TLS 1.3 cipher suite negotiated internally, e.g., TLS_AES_128_GCM_SHA256 or TLS_CHACHA20_POLY1305_SHA256)

Extensions:
key_share: Server's contribution to the elliptic-curve key exchange
supported_versions: Confirms TLS 1.3 is chosen
ALPN: May include “h2” (HTTP/2) or “http/1.1”

Following the Server Hello, the server sends:
Change Cipher Spec
Encrypted handshake messages
Certificate (encrypted under TLS 1.3)
→ In TLS 1.3, most handshake messages after Server Hello are encrypted, which is why Wireshark displays them as Application Data rather than clear handshake fields.

The TLS capture shows a complete and modern TLS 1.3 handshake between the client and *wikipedia.org*.
The client sends a Client Hello advertising its supported cipher suites and TLS extensions, including the SNI extension specifying the target domain.
The server responds with a Server Hello selecting TLS 1.3 and negotiating cryptographic parameters.
Because TLS 1.3 encrypts most handshake messages after Server Hello, Wireshark displays the remaining exchange as encrypted application data.

Overall, the TLS traffic demonstrates a secure and up-to-date HTTPS session, ensuring confidentiality and integrity of all subsequent communication between the client and the server.

Summary of Observations

Protocol	Observations
DNS	DNS queries for *example.com* and *wikipedia.org* were successfully resolved. Each query (Transaction IDs 0x36a8 and 0x67a1) matched its corresponding response. The DNS server returned multiple A records for *example.com* and a single IPv4 address for *wikipedia.org*. All exchanges were processed without errors, demonstrating proper DNS resolution.
ICMP	The ICMP ping exchange with 172.217.19.142 (Google) shows normal network behavior. Each Echo Request was matched with an Echo Reply using identical identifiers (0xe02f) and sequence numbers. TTL values differ between outgoing (64) and incoming (117) packets, indicating traversal through external networks. Connectivity was stable with no packet loss.
TCP	A complete TCP 3-way handshake was observed: SYN → SYN-ACK → ACK. The client initiated the connection from port 53044, and the server responded from port 53. Sequence and acknowledgment numbers aligned correctly, and window sizes were properly negotiated. This confirms reliable establishment of a TCP connection.
HTTP	Unencrypted HTTP traffic clearly exposes all protocol details. The client sent a GET request to *example.com*, and the server responded with a 200 OK message containing the full HTML page. All headers, metadata, and content were visible in plaintext, highlighting the lack of confidentiality in HTTP communications.
TLS	The TLS 1.3 handshake with *wikipedia.org* showed secure negotiation of cryptographic parameters. The Client Hello included SNI (wikipedia.org), supported_versions, key_share, and signature_algorithms. The Server Hello confirmed TLS 1.3 and selected a cipher suite. Most handshake messages appeared encrypted, consistent with TLS 1.3 behavior. The exchange ensures confidentiality and integrity of all subsequent traffic.

Conclusion

This network analysis provided a clear and structured view of how fundamental Internet protocols operate in real conditions.
By capturing and examining DNS, ICMP, TCP, HTTP, and TLS traffic, each layer of communication revealed its role and behavior within the network stack.

DNS queries demonstrated how domain names are resolved into IP addresses through request–response exchanges.
ICMP traffic showed reliable host reachability, with each Echo Request receiving a matching Echo Reply.
The TCP 3-way handshake confirmed the proper establishment of reliable connections using sequence and acknowledgment numbers.
HTTP communication highlighted the lack of confidentiality in unencrypted traffic, exposing full requests, responses, and webpage content in plaintext.
Finally, the TLS 1.3 handshake illustrated how modern HTTPS connections negotiate cryptographic parameters to secure data exchanges, ensuring confidentiality and integrity.

Overall, this project reinforced practical understanding of key networking mechanisms and demonstrated how Wireshark can be used to visualize and interpret protocol behavior.
The observations made throughout the analysis reflect real-world interactions between clients and servers and underline the importance of secure communication protocols in today’s Internet.