VxLEARN Networks

Networking & Cybersecurity Track
Simulated Employment Program

Lab Report:
Exploring DNS Traffic

Prepared by:
Kudzaishe Majeza
Junior Network Engineer – VxLEARN Networks

Mentor:
Titus Majeza
Senior Network Engineer

Date: 17 December 2025

Table of Contents

1. Introduction

This lab explains how DNS traffic works by capturing and analyzing packets using Wireshark. The purpose is to understand how a computer resolves a website name into an IP address. All captures in this lab were done using a Wi-Fi network interface.

2. Objectives

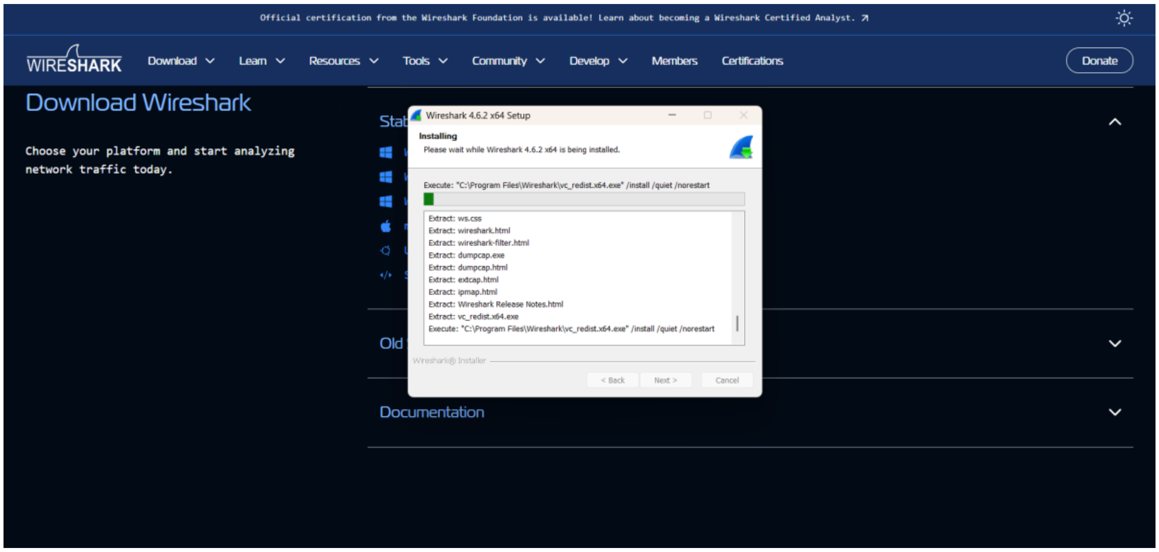
- Capture DNS traffic using Wireshark
- Analyze DNS query packets
- Analyze DNS response packets

3. Background / Scenario

Wireshark is a packet analysis tool used for troubleshooting and security investigations. Because it shows packet-level details, it can also be used by attackers to gather information. In this lab, Wireshark is used to observe DNS traffic.

4. Part 1: Capture DNS Traffic

Wireshark was installed and the active Wi-Fi interface was selected.



Choose your platform and start analyzing network traffic today.

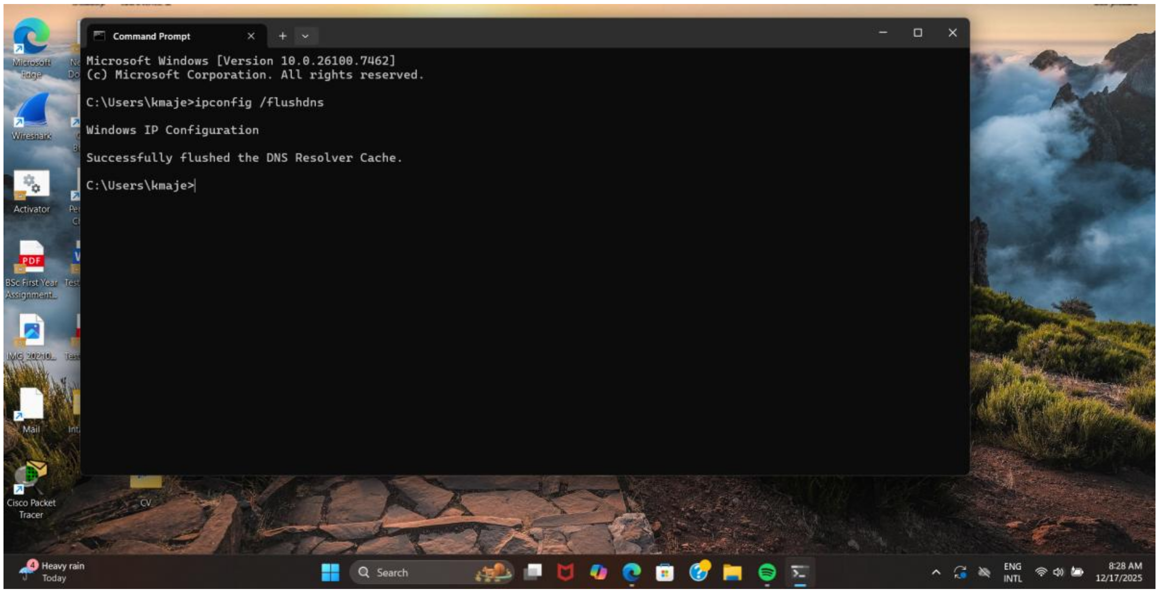
Installing

Please wait while Wireshark 4.6.2 x64 is being installed.

```
Execute: "C:\Program Files\Wireshark\vc_redist.x64.exe" /install /quiet /norestart
```

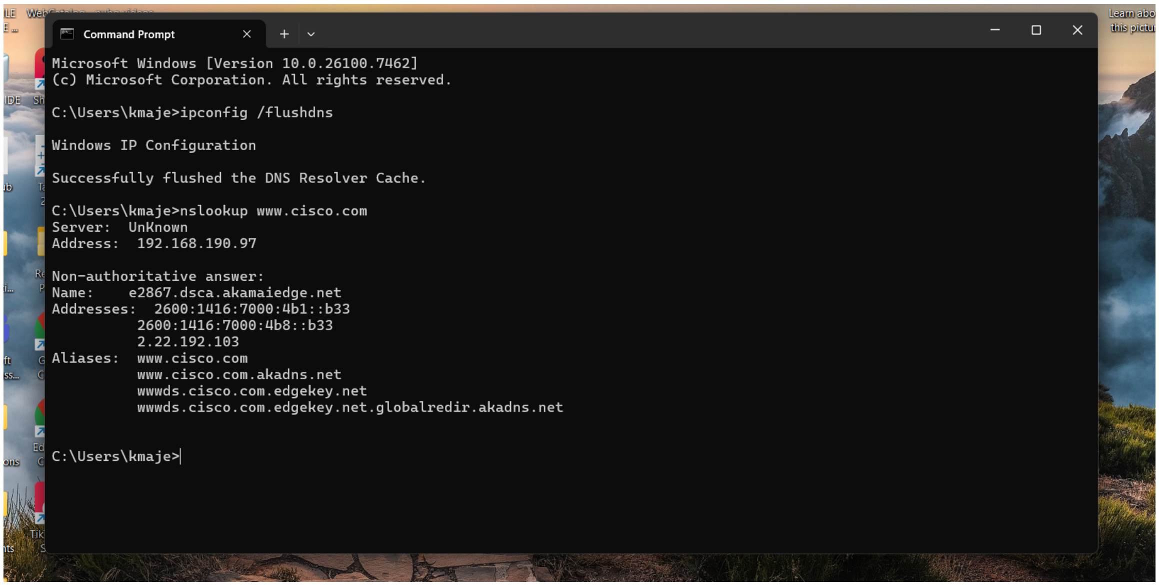
```
Extract: ws.css
Extract: wireshark.html
Extract: wireshark-filter.html
Extract: dumpcap.exe
Extract: dumpcap.html
Extract: extcap.html
Extract: ipmap.html
Extract: Wireshark Release Notes.html
Extract: vc_redist.x64.exe
Execute: "C:\Program Files\Wireshark\vc_redist.x64.exe" /install /quiet /norestart
```

The DNS cache was cleared using the ipconfig /flushdns command.

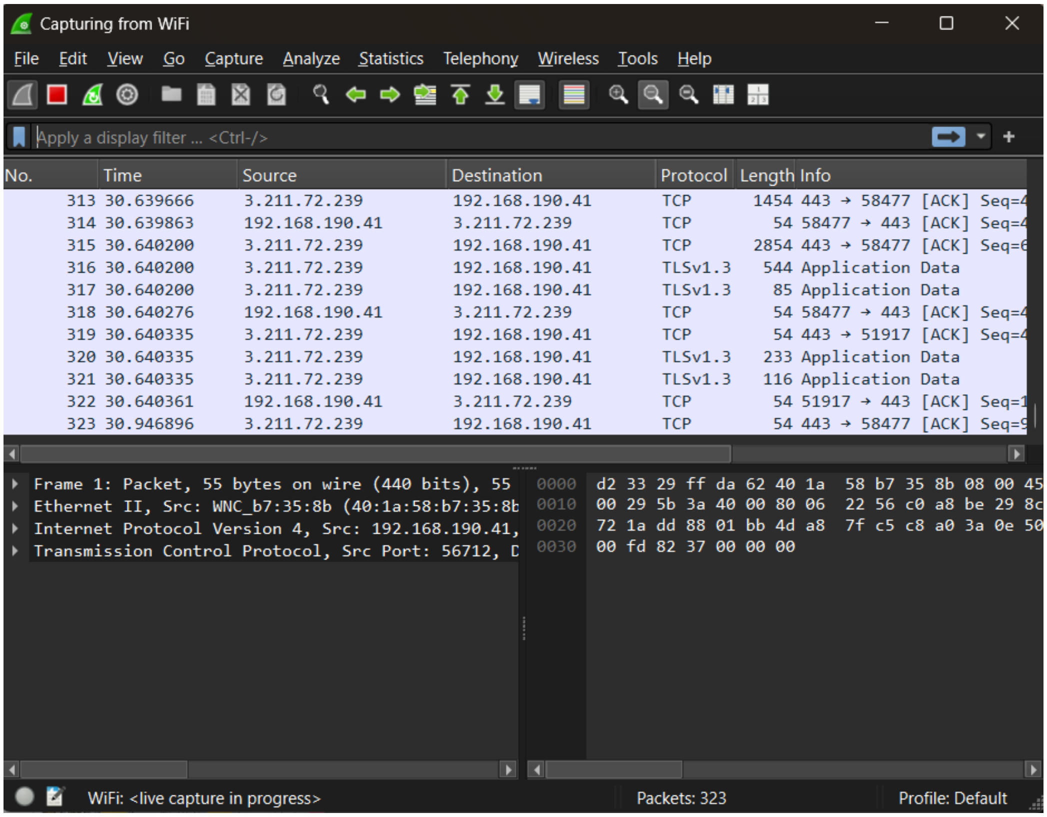


```
Microsoft Windows [Version 10.0.26100.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kmaje>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\kmaje>
```

The nslookup command was used to generate DNS traffic.



```
Microsoft Windows [Version 10.0.26100.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kmaje>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\kmaje>nslookup www.cisco.com
Server:  UnKnown
Address:  192.168.190.97

Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2600:1416:7000:4b1::b33
          2600:1416:7000:4b8::b33
          2.22.192.103
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net


C:\Users\kmaje>
```



```
No.    Time         Source            Destination       Protocol  Length Info
   313 30.639666    3.211.72.239      192.168.190.41    TCP       1454 443 → 58477 [ACK] Seq=4
   314 30.639863    192.168.190.41    3.211.72.239      TCP         54 58477 → 443 [ACK] Seq=4
   315 30.640200    3.211.72.239      192.168.190.41    TCP       2854 443 → 58477 [ACK] Seq=6
   316 30.640200    3.211.72.239      192.168.190.41    TLSv1.3    544 Application Data
   317 30.640200    3.211.72.239      192.168.190.41    TLSv1.3     85 Application Data
   318 30.640276    192.168.190.41    3.211.72.239      TCP         54 58477 → 443 [ACK] Seq=4
   319 30.640335    3.211.72.239      192.168.190.41    TCP         54 443 → 51917 [ACK] Seq=4
   320 30.640335    3.211.72.239      192.168.190.41    TLSv1.3    233 Application Data
   321 30.640335    3.211.72.239      192.168.190.41    TLSv1.3    116 Application Data
   322 30.640361    192.168.190.41    3.211.72.239      TCP         54 51917 → 443 [ACK] Seq=1
   323 30.946896    3.211.72.239      192.168.190.41    TCP         54 443 → 58477 [ACK] Seq=9
```

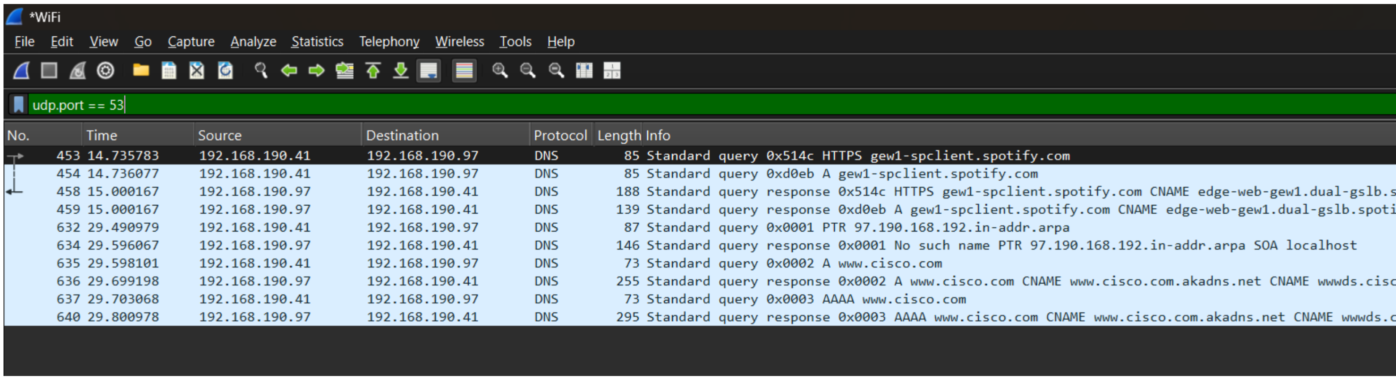
```
Frame 1: Packet, 55 bytes on wire (440 bits), 55
Ethernet II, Src: WNC_b7:35:8b (40:1a:58:b7:35:8b
Internet Protocol Version 4, Src: 192.168.190.41,
Transmission Control Protocol, Src Port: 56712, D
```

```
0000  d2 33 29 ff da 62 40 1a  58 b7 35 8b 08 00 45
0010  00 29 5b 3a 40 00 80 06  22 56 c0 a8 be 29 8c
0020  72 1a dd 88 01 bb 4d a8  7f c5 c8 a0 3a 0e 50
0030  00 fd 82 37 00 00 00
```

Wireshark capturing packets

5. Part 2: Explore DNS Query Traffic

The filter udp.port == 53 was applied to view DNS traffic only. The DNS query packet for www.cisco.com was analyzed.


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

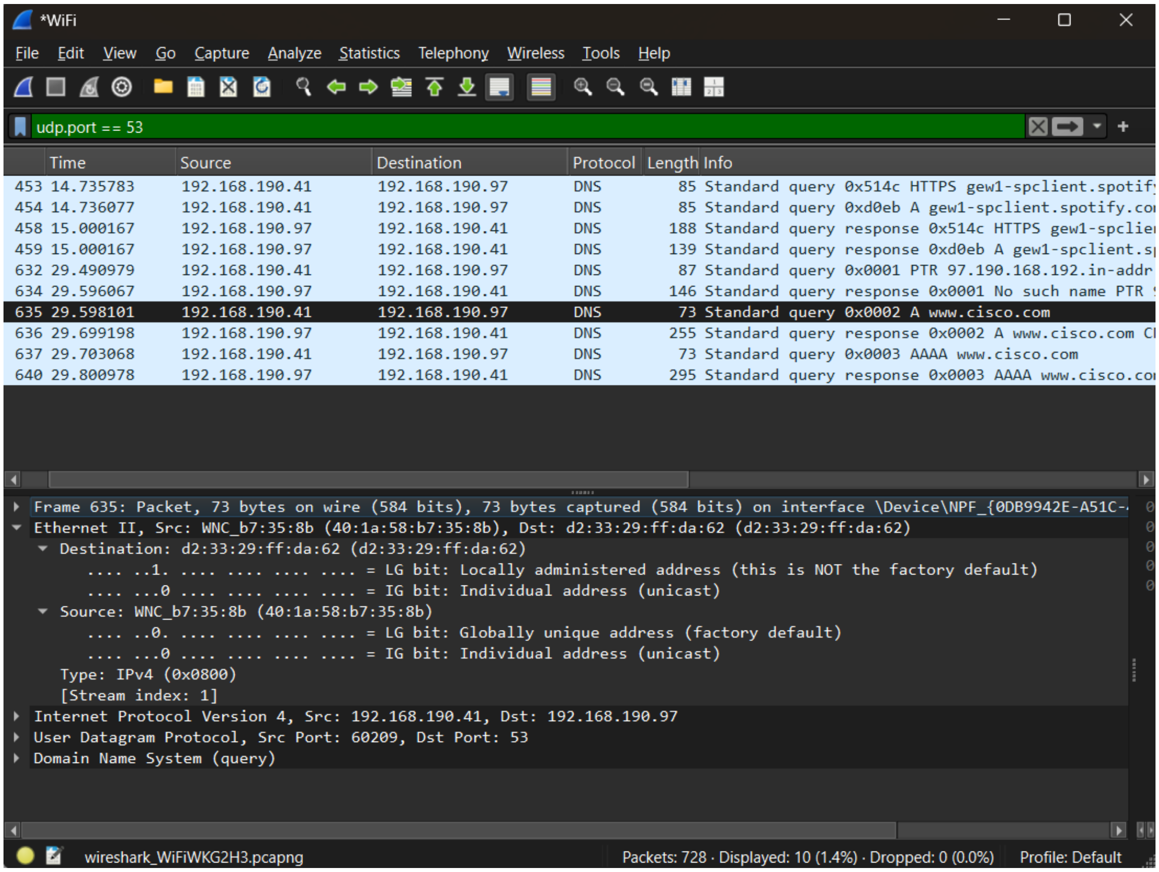
No.	Time	Source	Destination	Protocol	Length	Info
453	14.735783	192.168.190.41	192.168.190.97	DNS	85	Standard query 0x514c HTTPS gew1-spclient.spotify.com
454	14.736077	192.168.190.41	192.168.190.97	DNS	85	Standard query 0xd0eb A gew1-spclient.spotify.com
458	15.000167	192.168.190.97	192.168.190.41	DNS	188	Standard query response 0x514c HTTPS gew1-spclient.spotify.com CNAME edge-web-gew1.dual-gslb.s
459	15.000167	192.168.190.97	192.168.190.41	DNS	139	Standard query response 0xd0eb A gew1-spclient.spotify.com CNAME edge-web-gew1.dual-gslb.spoti
632	29.490979	192.168.190.41	192.168.190.97	DNS	87	Standard query 0x0001 PTR 97.190.168.192.in-addr.arpa
634	29.596067	192.168.190.97	192.168.190.41	DNS	146	Standard query response 0x0001 No such name PTR 97.190.168.192.in-addr.arpa SOA localhost
635	29.598101	192.168.190.41	192.168.190.97	DNS	73	Standard query 0x0002 A www.cisco.com
636	29.699198	192.168.190.97	192.168.190.41	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisc
637	29.703068	192.168.190.41	192.168.190.97	DNS	73	Standard query 0x0003 AAAA www.cisco.com
640	29.800978	192.168.190.97	192.168.190.41	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.c

The packet uses IEEE 802.11 (Wifi) because the connection is wireless. The destination port is 53, which is the default DNS port.

When examining the DNS query packet, the IEEE 802.11 (Wifi) header shows:

- **Source MAC Address:** 40:1a:58:b7:35:8b
- **Destination MAC Address:** d2:33:29:ff:da:62

This indicates that DNS queries are first sent to the router, not directly to the DNS server.



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

```
     Time         Source          Destination     Protocol Length Info
453 14.735783    192.168.190.41  192.168.190.97  DNS        85 Standard query 0x514c HTTPS gew1-spclient.spotif
454 14.736077    192.168.190.41  192.168.190.97  DNS        85 Standard query 0xd0eb A gew1-spclient.spotify.co
458 15.000167    192.168.190.97  192.168.190.41  DNS       188 Standard query response 0x514c HTTPS gew1-spclie
459 15.000167    192.168.190.97  192.168.190.41  DNS       139 Standard query response 0xd0eb A gew1-spclient.s
632 29.490979    192.168.190.41  192.168.190.97  DNS        87 Standard query 0x0001 PTR 97.190.168.192.in-addr
634 29.596067    192.168.190.97  192.168.190.41  DNS       146 Standard query response 0x0001 No such name PTR
635 29.598101    192.168.190.41  192.168.190.97  DNS        73 Standard query 0x0002 A www.cisco.com
636 29.699198    192.168.190.97  192.168.190.41  DNS       255 Standard query response 0x0002 A www.cisco.com C
637 29.703068    192.168.190.41  192.168.190.97  DNS        73 Standard query 0x0003 AAAA www.cisco.com
640 29.800978    192.168.190.97  192.168.190.41  DNS       295 Standard query response 0x0003 AAAA www.cisco.co
```

```
Frame 635: Packet, 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{0DB9942E-A51C-
Ethernet II, Src: WNC_b7:35:8b (40:1a:58:b7:35:8b), Dst: d2:33:29:ff:da:62 (d2:33:29:ff:da:62)
  Destination: d2:33:29:ff:da:62 (d2:33:29:ff:da:62)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: WNC_b7:35:8b (40:1a:58:b7:35:8b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
Internet Protocol Version 4, Src: 192.168.190.41, Dst: 192.168.190.97
User Datagram Protocol, Src Port: 60209, Dst Port: 53
Domain Name System (query)
```

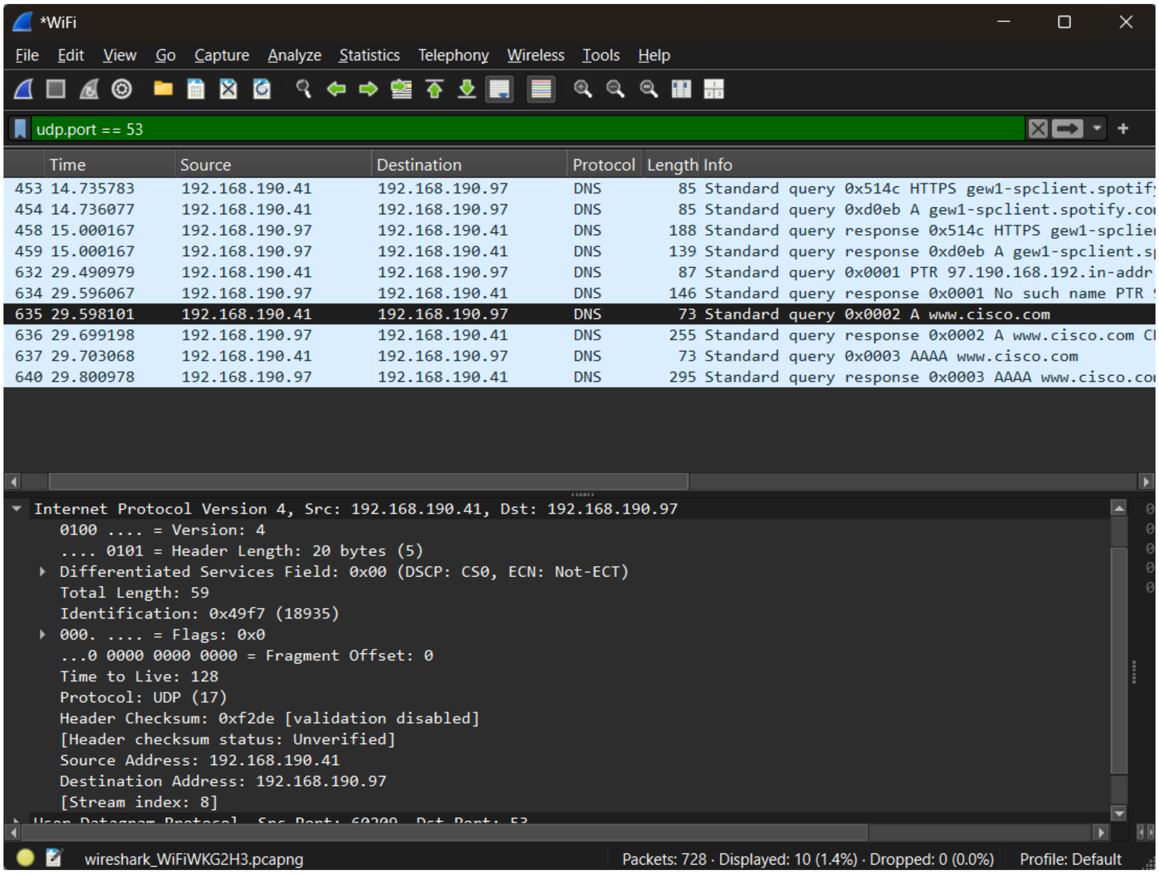
wireshark_WiFiWKG2H3.pcapng   Packets: 728 · Displayed: 10 (1.4%) · Dropped: 0 (0.0%)   Profile: Default

IEEE 802.11 header expanded

At the **IPv4 layer**, the packet shows:

- **Source IP Address:** 192.168.190.41
- **Destination IP Address:** 192.168.190.97

This confirms that IP addresses remain constant end-to-end, while MAC addresses change as packets move across the network.



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port == 53
```

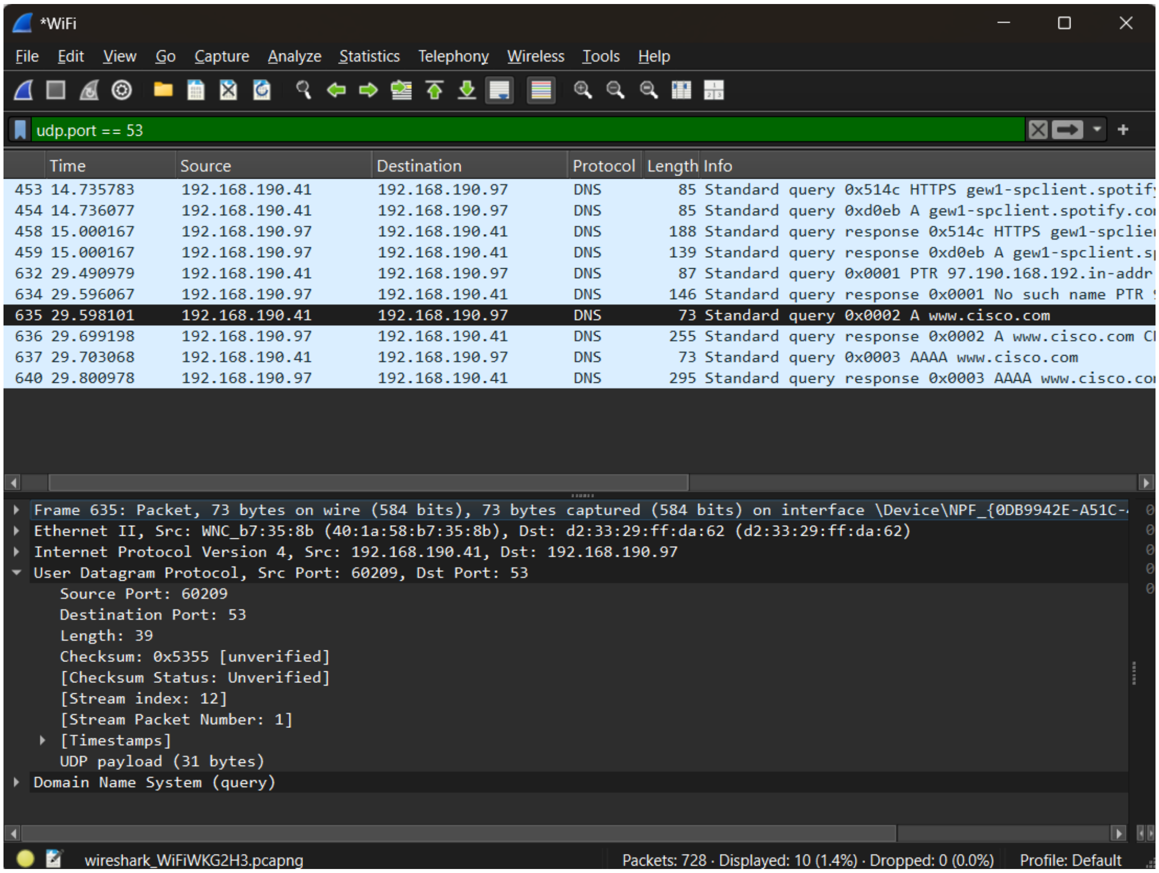
```
     Time       Source          Destination     Protocol Length Info
453 14.735783  192.168.190.41  192.168.190.97  DNS       85 Standard query 0x514c HTTPS gew1-spclient.spotif
454 14.736077  192.168.190.41  192.168.190.97  DNS       85 Standard query 0xd0eb A gew1-spclient.spotify.co
458 15.000167  192.168.190.97  192.168.190.41  DNS      188 Standard query response 0x514c HTTPS gew1-spclie
459 15.000167  192.168.190.97  192.168.190.41  DNS      139 Standard query response 0xd0eb A gew1-spclient.s
632 29.490979  192.168.190.41  192.168.190.97  DNS       87 Standard query 0x0001 PTR 97.190.168.192.in-addr
634 29.596067  192.168.190.97  192.168.190.41  DNS      146 Standard query response 0x0001 No such name PTR
635 29.598101  192.168.190.41  192.168.190.97  DNS       73 Standard query 0x0002 A www.cisco.com
636 29.699198  192.168.190.97  192.168.190.41  DNS      255 Standard query response 0x0002 A www.cisco.com C
637 29.703068  192.168.190.41  192.168.190.97  DNS       73 Standard query 0x0003 AAAA www.cisco.com
640 29.800978  192.168.190.97  192.168.190.41  DNS      295 Standard query response 0x0003 AAAA www.cisco.co
```

```
▾ Internet Protocol Version 4, Src: 192.168.190.41, Dst: 192.168.190.97
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x49f7 (18935)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xf2de [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.190.41
    Destination Address: 192.168.190.97
    [Stream index: 8]
▸ User Datagram Protocol, Src Port: 60209, Dst Port: 53
```

```
wireshark_WiFiWKG2H3.pcapng    Packets: 728 · Displayed: 10 (1.4%) · Dropped: 0 (0.0%)    Profile: Default
```

IPv4 header expanded

In the **UDP header**, the source port is a random high numbered port selected by the PC, while the destination port is **53**, confirming the packet is a DNS query.


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

```
    Time          Source            Destination       Protocol Length Info
453 14.735783     192.168.190.41    192.168.190.97    DNS       85 Standard query 0x514c HTTPS gew1-spclient.spotif
454 14.736077     192.168.190.41    192.168.190.97    DNS       85 Standard query 0xd0eb A gew1-spclient.spotify.co
458 15.000167     192.168.190.97    192.168.190.41    DNS      188 Standard query response 0x514c HTTPS gew1-spclie
459 15.000167     192.168.190.97    192.168.190.41    DNS      139 Standard query response 0xd0eb A gew1-spclient.s
632 29.490979     192.168.190.41    192.168.190.97    DNS       87 Standard query 0x0001 PTR 97.190.168.192.in-addr
634 29.596067     192.168.190.97    192.168.190.41    DNS      146 Standard query response 0x0001 No such name PTR
635 29.598101     192.168.190.41    192.168.190.97    DNS       73 Standard query 0x0002 A www.cisco.com
636 29.699198     192.168.190.97    192.168.190.41    DNS      255 Standard query response 0x0002 A www.cisco.com C
637 29.703068     192.168.190.41    192.168.190.97    DNS       73 Standard query 0x0003 AAAA www.cisco.com
640 29.800978     192.168.190.97    192.168.190.41    DNS      295 Standard query response 0x0003 AAAA www.cisco.co
```

```
> Frame 635: Packet, 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{0DB9942E-A51C-
> Ethernet II, Src: WNC_b7:35:8b (40:1a:58:b7:35:8b), Dst: d2:33:29:ff:da:62 (d2:33:29:ff:da:62)
> Internet Protocol Version 4, Src: 192.168.190.41, Dst: 192.168.190.97
v User Datagram Protocol, Src Port: 60209, Dst Port: 53
    Source Port: 60209
    Destination Port: 53
    Length: 39
    Checksum: 0x5355 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 12]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (31 bytes)
> Domain Name System (query)
```

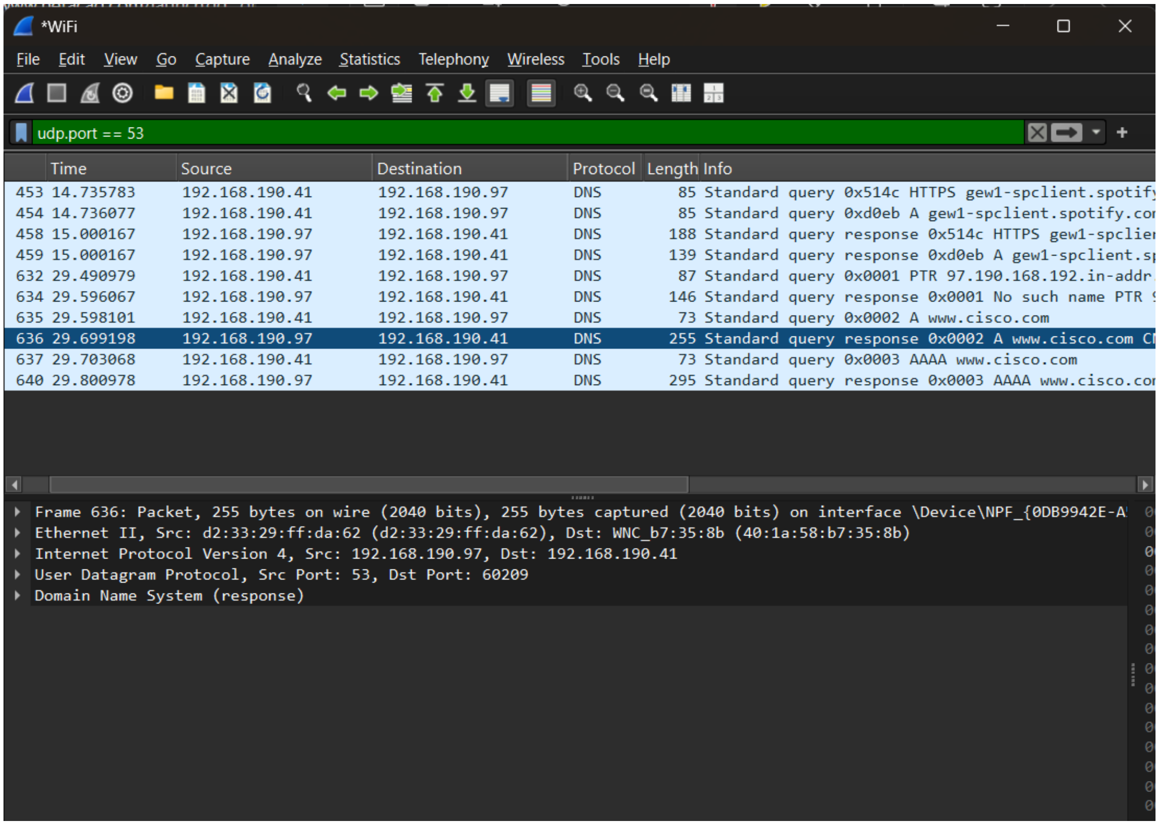
wireshark_WiFiWKG2H3.pcapng   Packets: 728 · Displayed: 10 (1.4%) · Dropped: 0 (0.0%)   Profile: Default

UDP header expanded

6. Part 3: Explore DNS Response Traffic

The DNS response packet represents the answer sent back by the DNS server. Compared to the DNS query, the source and destination information is reversed:

- The DNS server is now the source
- The PC is the destination


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

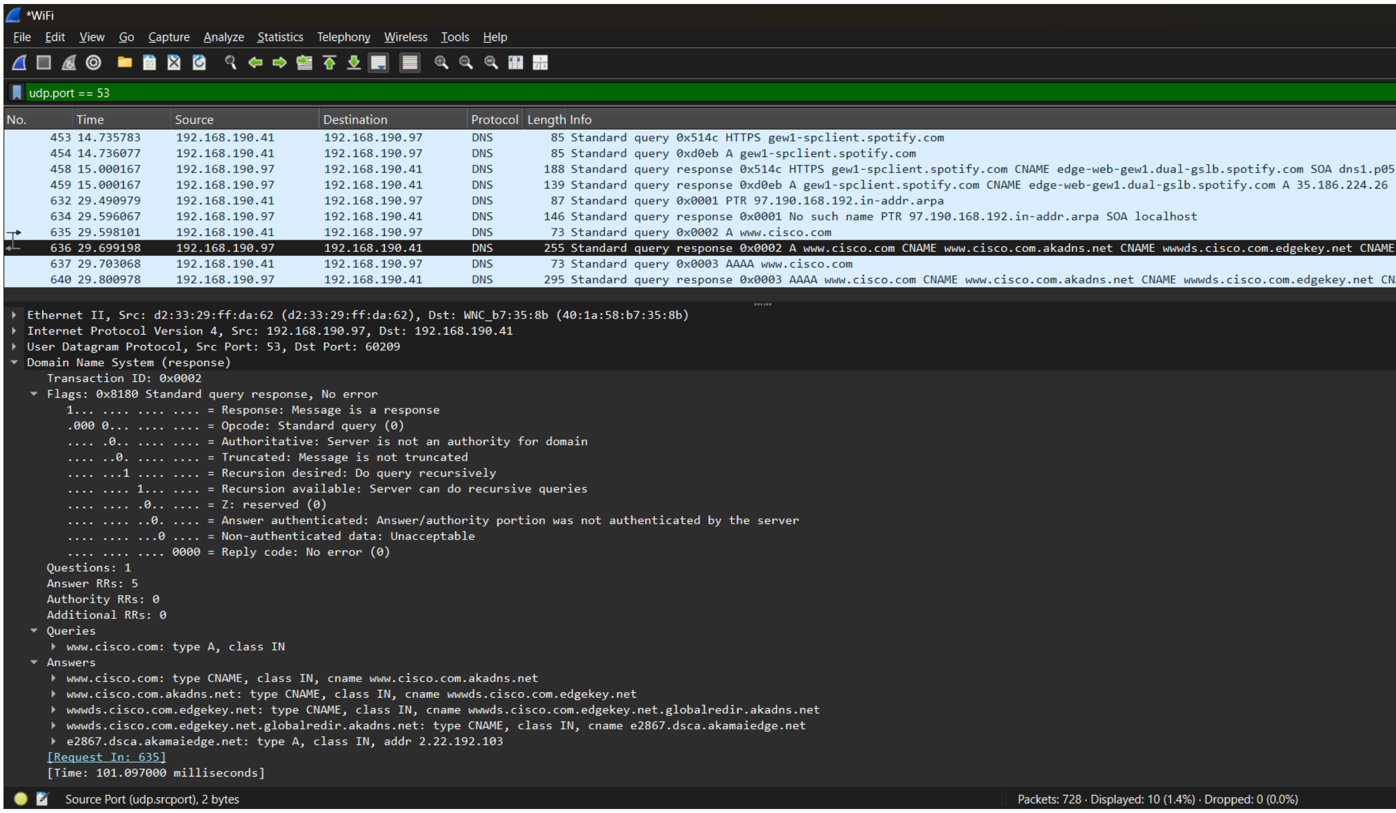
udp.port == 53

```
     Time          Source            Destination       Protocol Length Info
 453 14.735783     192.168.190.41    192.168.190.97    DNS        85 Standard query 0x514c HTTPS gew1-spclient.spotif
 454 14.736077     192.168.190.41    192.168.190.97    DNS        85 Standard query 0xd0eb A gew1-spclient.spotify.co
 458 15.000167     192.168.190.97    192.168.190.41    DNS       188 Standard query response 0x514c HTTPS gew1-spclie
 459 15.000167     192.168.190.97    192.168.190.41    DNS       139 Standard query response 0xd0eb A gew1-spclient.s
 632 29.490979     192.168.190.41    192.168.190.97    DNS        87 Standard query 0x0001 PTR 97.190.168.192.in-addr
 634 29.596067     192.168.190.97    192.168.190.41    DNS       146 Standard query response 0x0001 No such name PTR
 635 29.598101     192.168.190.41    192.168.190.97    DNS        73 Standard query 0x0002 A www.cisco.com
 636 29.699198     192.168.190.97    192.168.190.41    DNS       255 Standard query response 0x0002 A www.cisco.com C
 637 29.703068     192.168.190.41    192.168.190.97    DNS        73 Standard query 0x0003 AAAA www.cisco.com
 640 29.800978     192.168.190.97    192.168.190.41    DNS       295 Standard query response 0x0003 AAAA www.cisco.co
```

```
▸ Frame 636: Packet, 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface \Device\NPF_{0DB9942E-A
▸ Ethernet II, Src: d2:33:29:ff:da:62 (d2:33:29:ff:da:62), Dst: WNC_b7:35:8b (40:1a:58:b7:35:8b)
▸ Internet Protocol Version 4, Src: 192.168.190.97, Dst: 192.168.190.41
▸ User Datagram Protocol, Src Port: 53, Dst Port: 60209
▸ Domain Name System (response)
```

DNS response packet selected

The response packet includes DNS flags that indicate recursive queries are supported. This means the DNS server performs the necessary lookups on behalf of the client and returns the final result.



```
udp.port == 53
```

```
No.      Time        Source          Destination     Protocol Length Info
     453 14.735783   192.168.190.41  192.168.190.97  DNS        85 Standard query 0x514c HTTPS gew1-spclient.spotify.com
     454 14.736077   192.168.190.41  192.168.190.97  DNS        85 Standard query 0xd0eb A gew1-spclient.spotify.com
     458 15.000167   192.168.190.97  192.168.190.41  DNS       188 Standard query response 0x514c HTTPS gew1-spclient.spotify.com CNAME edge-web-gew1.dual-gslb.spotify.com SOA dns1.p05
     459 15.000167   192.168.190.97  192.168.190.41  DNS       139 Standard query response 0xd0eb A gew1-spclient.spotify.com CNAME edge-web-gew1.dual-gslb.spotify.com A 35.186.224.26
     632 29.490979   192.168.190.41  192.168.190.97  DNS        87 Standard query 0x0001 PTR 97.190.168.192.in-addr.arpa
     634 29.596067   192.168.190.97  192.168.190.41  DNS       146 Standard query response 0x0001 No such name PTR 97.190.168.192.in-addr.arpa SOA localhost
     635 29.598101   192.168.190.41  192.168.190.97  DNS        73 Standard query 0x0002 A www.cisco.com
     636 29.699198   192.168.190.97  192.168.190.41  DNS       255 Standard query response 0x0002 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME
     637 29.703068   192.168.190.41  192.168.190.97  DNS        73 Standard query 0x0003 AAAA www.cisco.com
     640 29.800978   192.168.190.97  192.168.190.41  DNS       295 Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CN
```

```
› Ethernet II, Src: d2:33:29:ff:da:62 (d2:33:29:ff:da:62), Dst: WNC_b7:35:8b (40:1a:58:b7:35:8b)
› Internet Protocol Version 4, Src: 192.168.190.97, Dst: 192.168.190.41
› User Datagram Protocol, Src Port: 53, Dst Port: 60209
˅ Domain Name System (response)
    Transaction ID: 0x0002
  ˅ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    › www.cisco.com: type A, class IN
  ˅ Answers
    › www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
    › www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
    › wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
    › wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
    › e2867.dsca.akamaiedge.net: type A, class IN, addr 2.22.192.103
    [Request In: 635]
    [Time: 101.097000 milliseconds]
```

```
Source Port (udp.srcport), 2 bytes                Packets: 728 · Displayed: 10 (1.4%) · Dropped: 0 (0.0%)
```

DNS flags, queries, and answers expanded

In the **Answers** section, the DNS response includes:

- **CNAME records**, which show aliases used by DNS
- **A records**, which provide the final IPv4 address for the requested domain

These values match the results produced by the nslookup command, confirming the accuracy of the DNS resolution.

7. Reflection

When viewing all captured traffic without filters, it becomes clear how much information can be exposed on a network. DNS traffic reveals which websites users access and which DNS servers are in use. Attackers can use packet capture tools like Wireshark to perform reconnaissance, monitor user activity, and carry out attacks such as DNS spoofing or man-in-the-middle attacks.

This highlights the importance of securing DNS traffic using encryption technologies such as **DNS over HTTPS (DoH)** or **DNS over TLS (DoT)**.

8. Conclusion

This lab demonstrated how DNS queries and responses operate by analyzing real network traffic with Wireshark. By examining packet headers and DNS records, the lab provided a deeper understanding of DNS functionality and emphasized the security risks associated with unprotected DNS traffic.