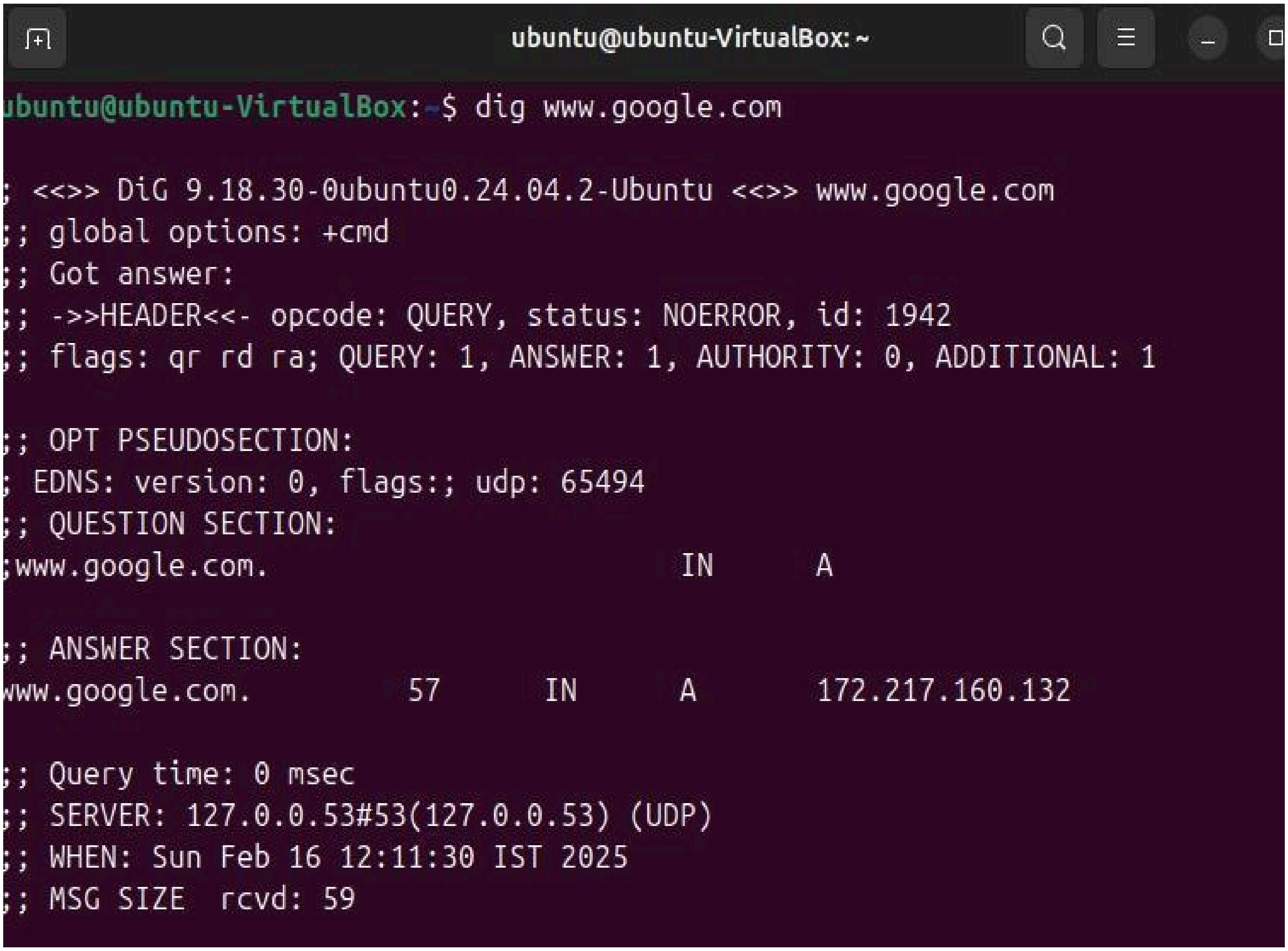
Computer Network: Lab 4

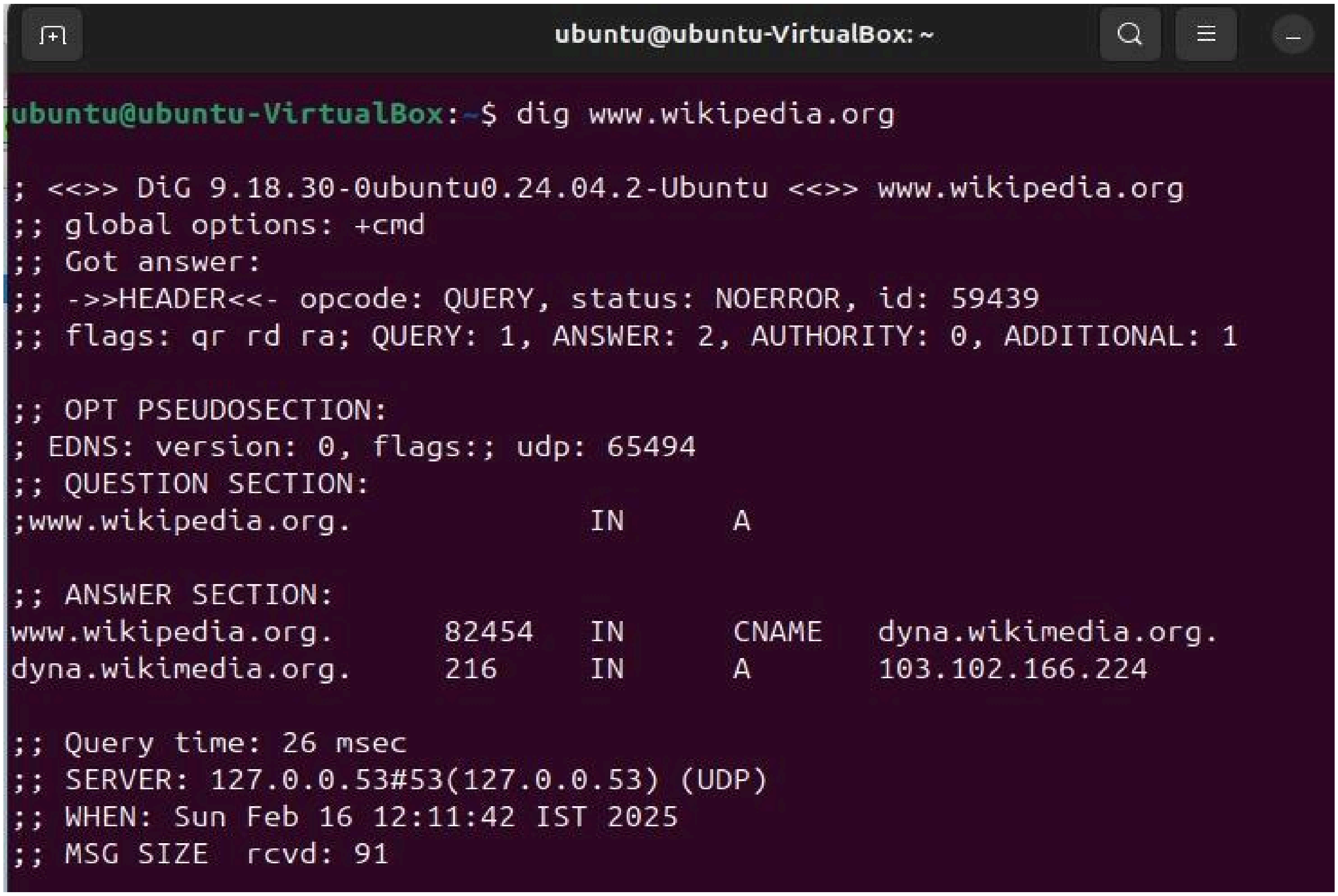
Name: Rithvik Rajesh Matta
SRN: PES2UG23CS485
Section: H

Problem Statement:
Exploring UDP with DNS - Wireshark

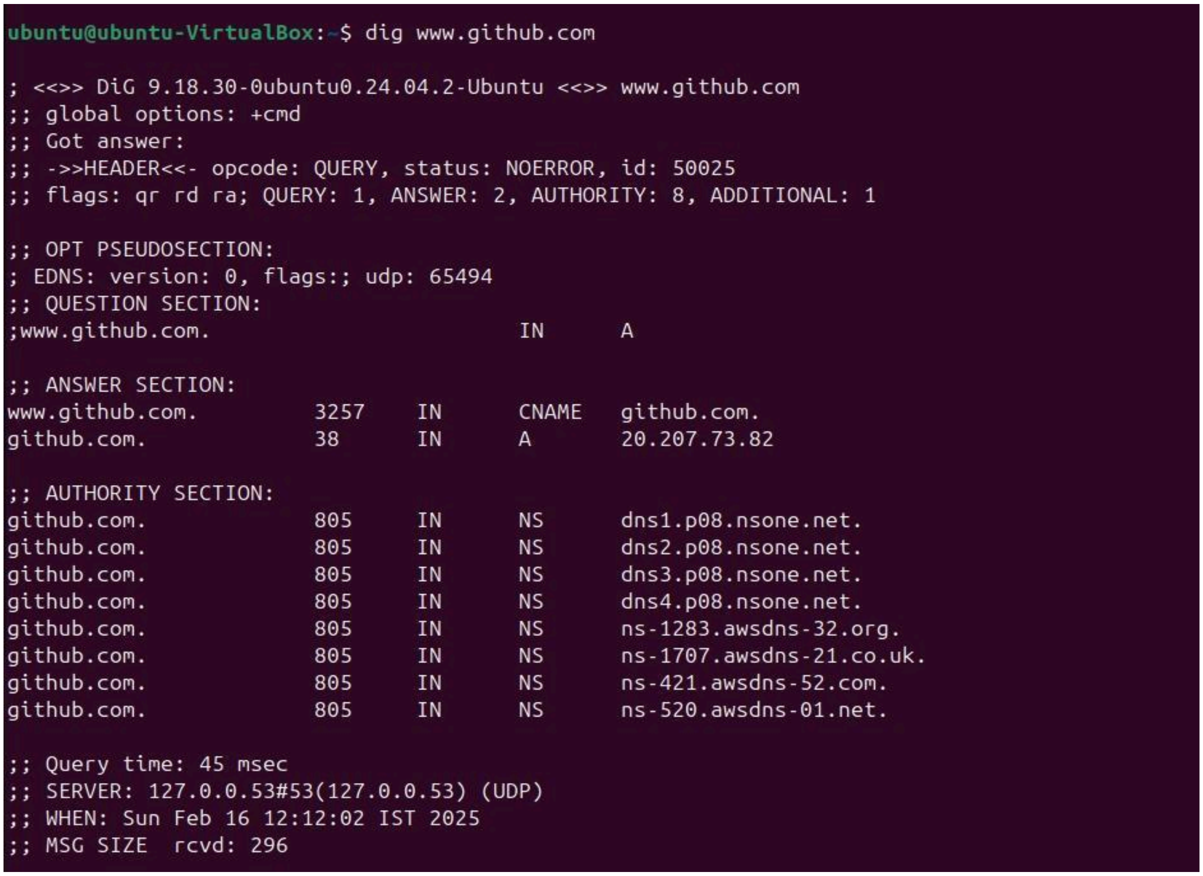
1) Generating dns traffic using dig command:



```
ubuntu@ubuntu-VirtualBox:~$ dig www.google.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1942
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         57      IN      A       172.217.160.132

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Feb 16 12:11:30 IST 2025
;; MSG SIZE  rcvd: 59
```

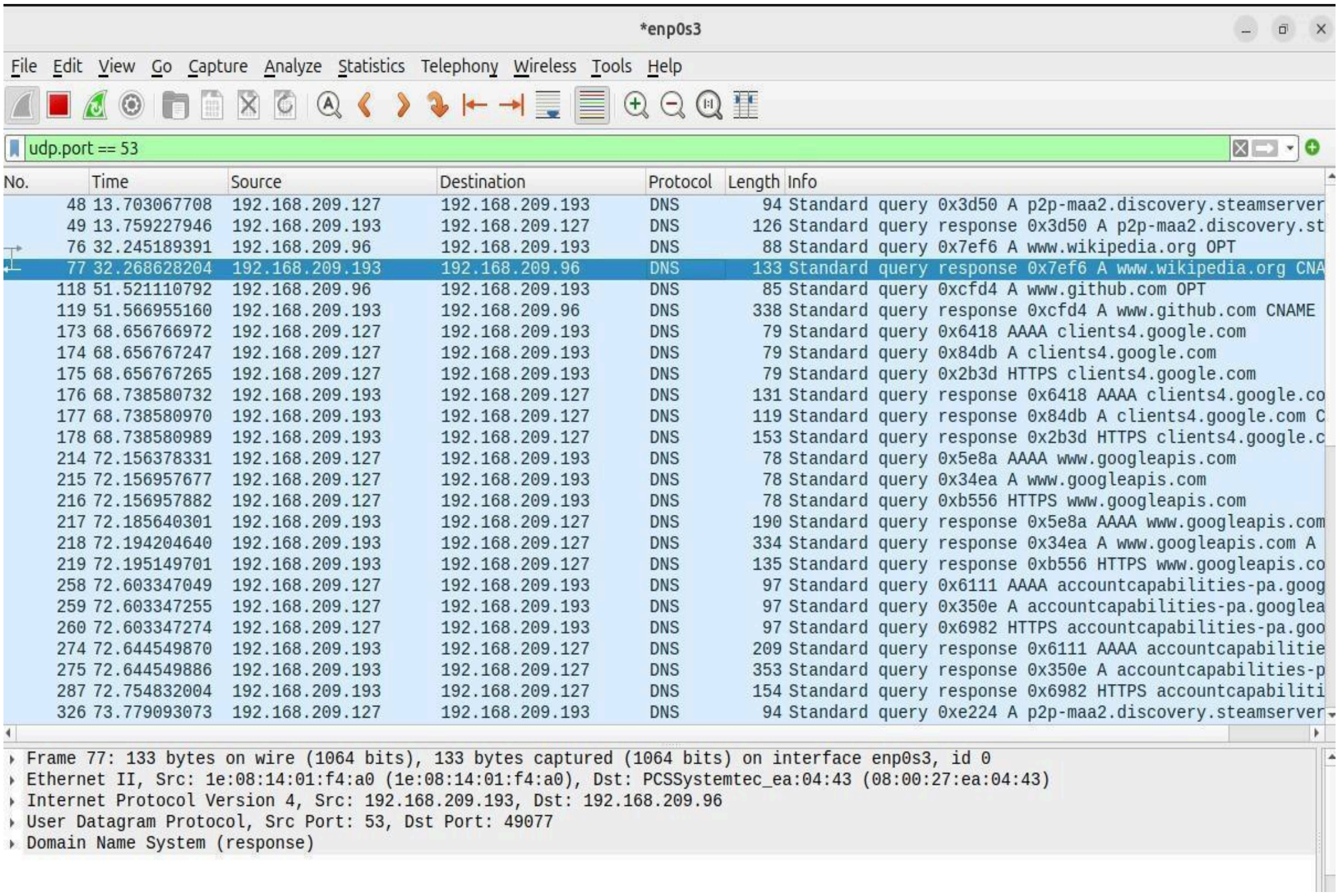


```
ubuntu@ubuntu-VirtualBox:~$ dig www.wikipedia.org

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.wikipedia.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59439
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.wikipedia.org.             IN      A

;; ANSWER SECTION:
www.wikipedia.org.      82454   IN      CNAME   dyna.wikimedia.org.
dyna.wikimedia.org.     216     IN      A       103.102.166.224

;; Query time: 26 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Feb 16 12:11:42 IST 2025
;; MSG SIZE  rcvd: 91
```



```
ubuntu@ubuntu-VirtualBox:~$ dig www.github.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.github.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50025
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.github.com.                        IN      A

;; ANSWER SECTION:
www.github.com.         3257    IN      CNAME   github.com.
github.com.             38      IN      A       20.207.73.82

;; AUTHORITY SECTION:
github.com.             805     IN      NS      dns1.p08.nsone.net.
github.com.             805     IN      NS      dns2.p08.nsone.net.
github.com.             805     IN      NS      dns3.p08.nsone.net.
github.com.             805     IN      NS      dns4.p08.nsone.net.
github.com.             805     IN      NS      ns-1283.awsdns-32.org.
github.com.             805     IN      NS      ns-1707.awsdns-21.co.uk.
github.com.             805     IN      NS      ns-421.awsdns-52.com.
github.com.             805     IN      NS      ns-520.awsdns-01.net.

;; Query time: 45 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Feb 16 12:12:02 IST 2025
;; MSG SIZE  rcvd: 296
```

2) Capturing packet in wireshark:



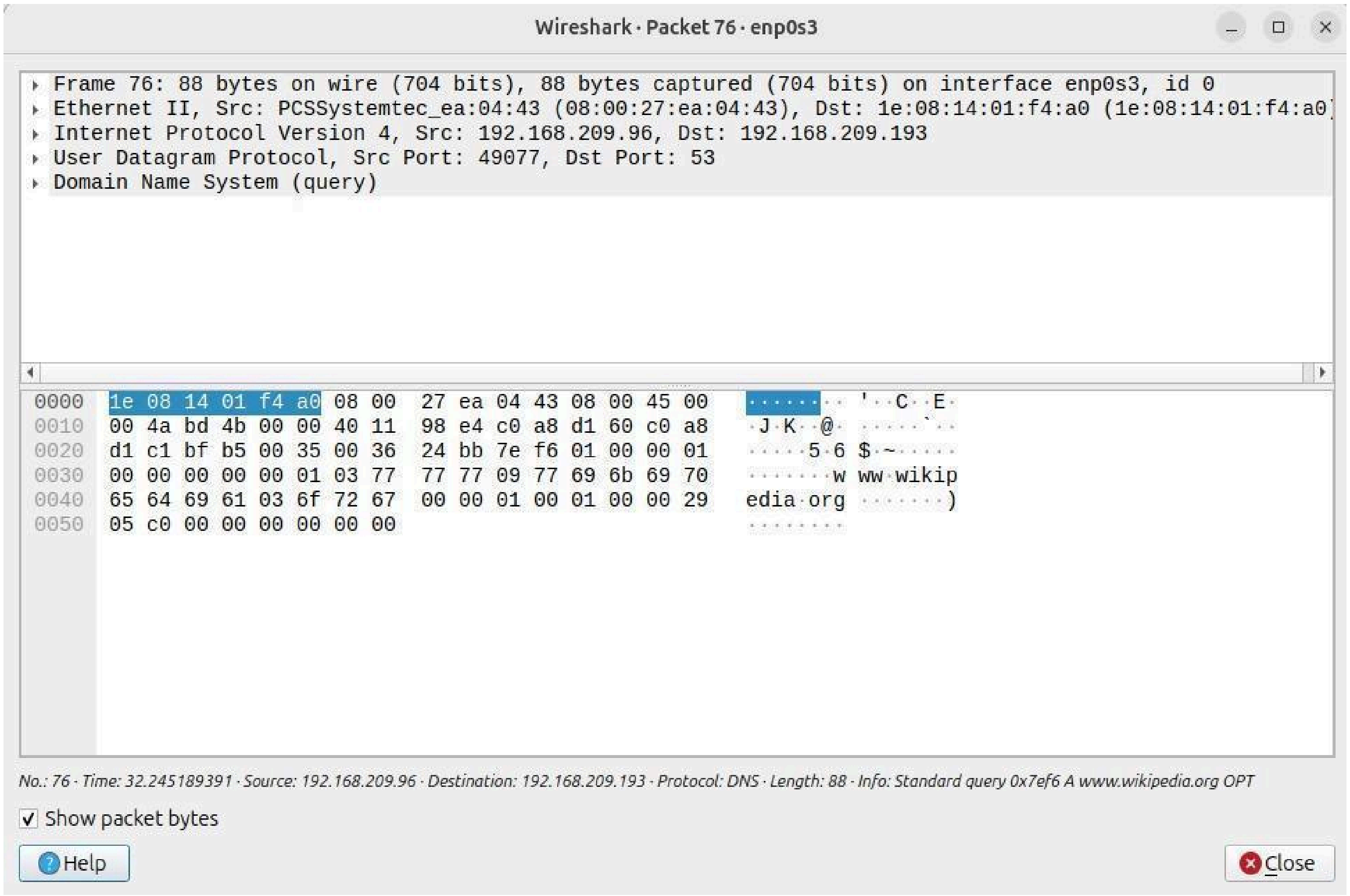
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

```
No.   Time          Source            Destination       Protocol  Length Info
   48 13.703067708  192.168.209.127   192.168.209.193   DNS        94 Standard query 0x3d50 A p2p-maa2.discovery.steamserver
   49 13.759227946  192.168.209.193   192.168.209.127   DNS       126 Standard query response 0x3d50 A p2p-maa2.discovery.st
   76 32.245189391  192.168.209.96    192.168.209.193   DNS        88 Standard query 0x7ef6 A www.wikipedia.org OPT
   77 32.268628204  192.168.209.193   192.168.209.96    DNS       133 Standard query response 0x7ef6 A www.wikipedia.org CNA
  118 51.521110792  192.168.209.96    192.168.209.193   DNS        85 Standard query 0xcfd4 A www.github.com OPT
  119 51.566955160  192.168.209.193   192.168.209.96    DNS       338 Standard query response 0xcfd4 A www.github.com CNAME
  173 68.656766972  192.168.209.127   192.168.209.193   DNS        79 Standard query 0x6418 AAAA clients4.google.com
  174 68.656767247  192.168.209.127   192.168.209.193   DNS        79 Standard query 0x84db A clients4.google.com
  175 68.656767265  192.168.209.127   192.168.209.193   DNS        79 Standard query 0x2b3d HTTPS clients4.google.com
  176 68.738580732  192.168.209.193   192.168.209.127   DNS       131 Standard query response 0x6418 AAAA clients4.google.co
  177 68.738580970  192.168.209.193   192.168.209.127   DNS       119 Standard query response 0x84db A clients4.google.com C
  178 68.738580989  192.168.209.193   192.168.209.127   DNS       153 Standard query response 0x2b3d HTTPS clients4.google.c
  214 72.156378331  192.168.209.127   192.168.209.193   DNS        78 Standard query 0x5e8a AAAA www.googleapis.com
  215 72.156957677  192.168.209.127   192.168.209.193   DNS        78 Standard query 0x34ea A www.googleapis.com
  216 72.156957882  192.168.209.127   192.168.209.193   DNS        78 Standard query 0xb556 HTTPS www.googleapis.com
  217 72.185640301  192.168.209.193   192.168.209.127   DNS       190 Standard query response 0x5e8a AAAA www.googleapis.com
  218 72.194204640  192.168.209.193   192.168.209.127   DNS       334 Standard query response 0x34ea A www.googleapis.com A
  219 72.195149701  192.168.209.193   192.168.209.127   DNS       135 Standard query response 0xb556 HTTPS www.googleapis.co
  258 72.603347049  192.168.209.127   192.168.209.193   DNS        97 Standard query 0x6111 AAAA accountcapabilities-pa.goog
  259 72.603347255  192.168.209.127   192.168.209.193   DNS        97 Standard query 0x350e A accountcapabilities-pa.googlea
  260 72.603347274  192.168.209.127   192.168.209.193   DNS        97 Standard query 0x6982 HTTPS accountcapabilities-pa.goo
  274 72.644549870  192.168.209.193   192.168.209.127   DNS       209 Standard query response 0x6111 AAAA accountcapabilitie
  275 72.644549886  192.168.209.193   192.168.209.127   DNS       353 Standard query response 0x350e A accountcapabilities-p
  287 72.754832004  192.168.209.193   192.168.209.127   DNS       154 Standard query response 0x6982 HTTPS accountcapabiliti
  326 73.779093073  192.168.209.127   192.168.209.193   DNS        94 Standard query 0xe224 A p2p-maa2.discovery.steamserver
```

```
▸ Frame 77: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: 1e:08:14:01:f4:a0 (1e:08:14:01:f4:a0), Dst: PCSSystemtec_ea:04:43 (08:00:27:ea:04:43)
▸ Internet Protocol Version 4, Src: 192.168.209.193, Dst: 192.168.209.96
▸ User Datagram Protocol, Src Port: 53, Dst Port: 49077
▸ Domain Name System (response)
```

3) DNS Query:



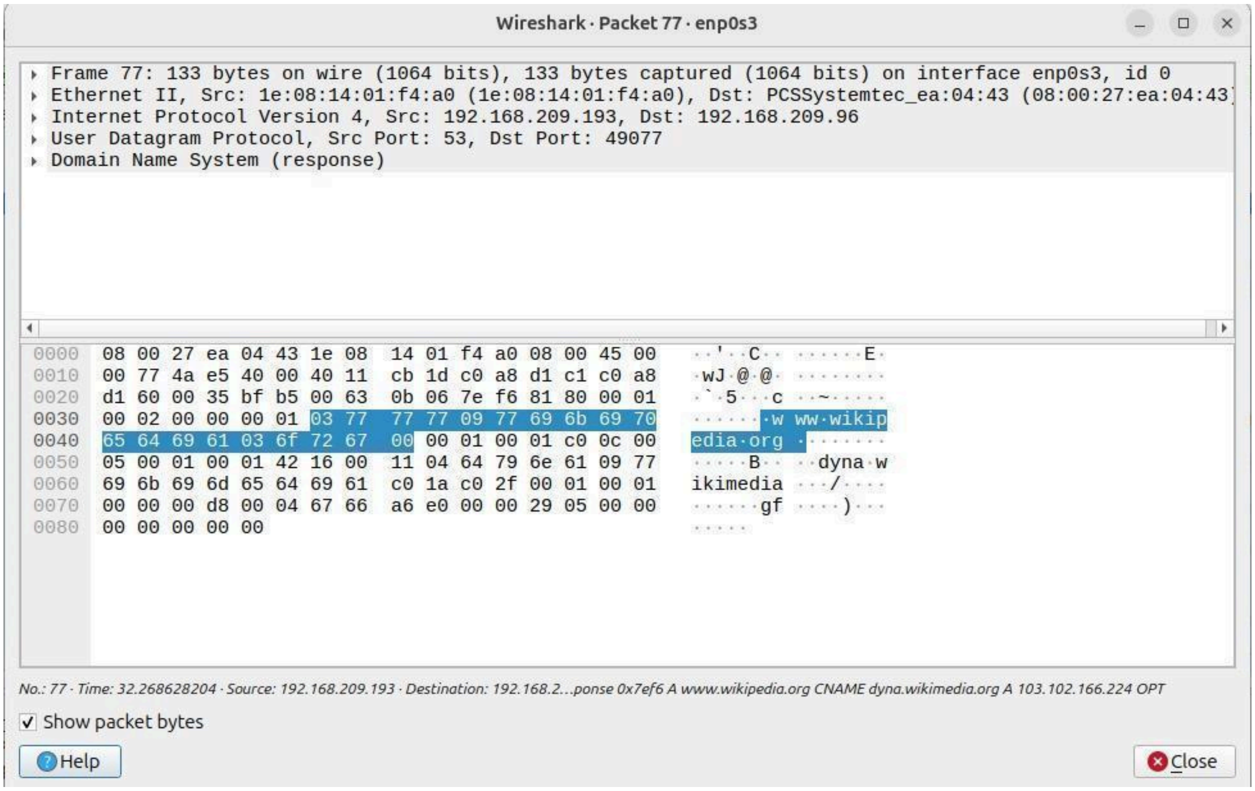
```
▸ Frame 76: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PCSSystemtec_ea:04:43 (08:00:27:ea:04:43), Dst: 1e:08:14:01:f4:a0 (1e:08:14:01:f4:a0
▸ Internet Protocol Version 4, Src: 192.168.209.96, Dst: 192.168.209.193
▸ User Datagram Protocol, Src Port: 49077, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  1e 08 14 01 f4 a0 08 00  27 ea 04 43 08 00 45 00   ········ '··C··E·
0010  00 4a bd 4b 00 00 40 11  98 e4 c0 a8 d1 60 c0 a8   ·J·K··@· ·····`··
0020  d1 c1 bf b5 00 35 00 36  24 bb 7e f6 01 00 00 01   ·····5·6 $·~·····
0030  00 00 00 00 00 01 03 77  77 77 09 77 69 6b 69 70   ·······w ww·wikip
0040  65 64 69 61 03 6f 72 67  00 00 01 00 01 00 00 29   edia·org ·······)
0050  05 c0 00 00 00 00 00 00                            ········
```

No.: 76 · Time: 32.245189391 · Source: 192.168.209.96 · Destination: 192.168.209.193 · Protocol: DNS · Length: 88 · Info: Standard query 0x7ef6 A www.wikipedia.org OPT

☑ Show packet bytes

4) DNS Response:



```
▸ Frame 77: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: 1e:08:14:01:f4:a0 (1e:08:14:01:f4:a0), Dst: PCSSystemtec_ea:04:43 (08:00:27:ea:04:43
▸ Internet Protocol Version 4, Src: 192.168.209.193, Dst: 192.168.209.96
▸ User Datagram Protocol, Src Port: 53, Dst Port: 49077
▸ Domain Name System (response)
```

```
0000  08 00 27 ea 04 43 1e 08  14 01 f4 a0 08 00 45 00   ··'··C·· ······E·
0010  00 77 4a e5 40 00 40 11  cb 1d c0 a8 d1 c1 c0 a8   ·wJ·@·@· ········
0020  d1 60 00 35 bf b5 00 63  0b 06 7e f6 81 80 00 01   ·`·5···c ··~·····
0030  00 02 00 00 00 01 03 77  77 77 09 77 69 6b 69 70   ·······w ww·wikip
0040  65 64 69 61 03 6f 72 67  00 00 01 00 01 c0 0c 00   edia·org ········
0050  05 00 01 00 01 42 16 00  11 04 64 79 6e 61 09 77   ·····B·· ··dyna·w
0060  69 6b 69 6d 65 64 69 61  c0 1a c0 2f 00 01 00 01   ikimedia ···/····
0070  00 00 00 d8 00 04 67 66  a6 e0 00 00 29 05 00 00   ······gf ····)···
0080  00 00 00 00 00                                     ·····
```

No.: 77 · Time: 32.268628204 · Source: 192.168.209.193 · Destination: 192.168.2...ponse 0x7ef6 A www.wikipedia.org CNAME dyna.wikimedia.org A 103.102.166.224 OPT

☑ Show packet bytes

How does UDP differ from TCP?

UDP is faster because it just sends data without setting up a connection first.

But there's no guarantee the data will arrive or be in order.

TCP, on the other hand, ensures reliability by establishing a connection first (three-way handshake) and making sure data is received correctly, but it's slower due to this extra processing.

Why is UDP used for DNS? DNS needs to be fast, and UDP helps by sending requests without waiting for a connection.

Since DNS queries are small, UDP works perfectly. TCP is used only when the response is too big or extra security is needed.

What did I see in Wireshark?

DNS requests used UDP on port 53, with random high-numbered source ports. There was no handshake, making it faster but with no packet recovery if something gets lost.