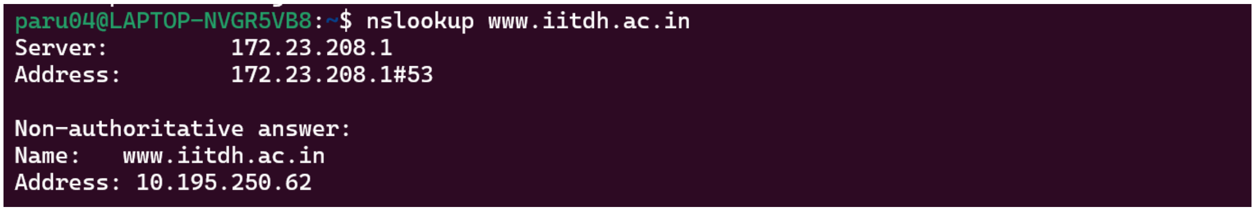
Assignment 4

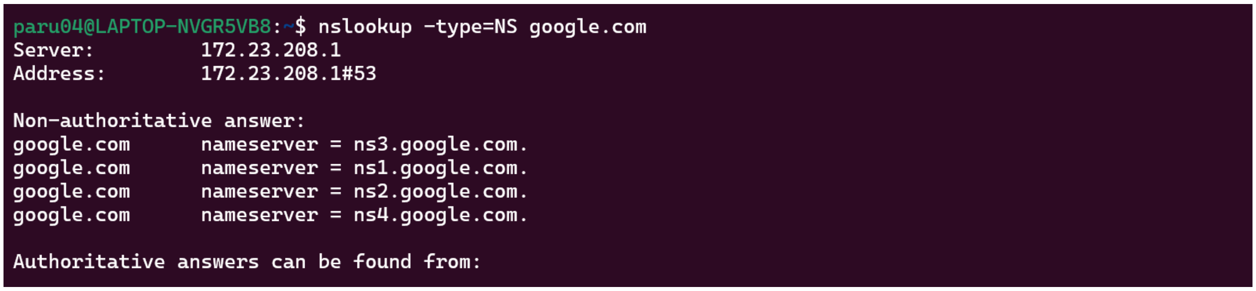
Part-1

1. The command used to obtain the IP address of www.iitdh.ac.in is: **nslookup www.iitdh.ac.in**
The IP address obtained of the web server for the Indian Institute of Technology, Dharwad is 10.195.250.62



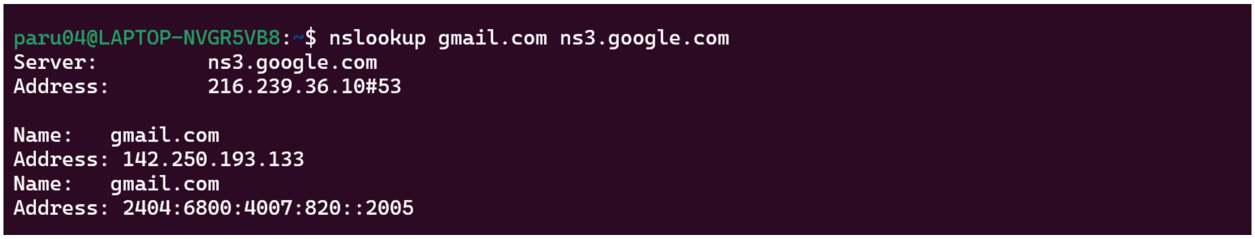
```
paru04@LAPTOP-NVGR5VB8:~$ nslookup www.iitdh.ac.in
Server:         172.23.208.1
Address:        172.23.208.1#53

Non-authoritative answer:
Name:   www.iitdh.ac.in
Address: 10.195.250.62
```

2. The DNS servers for google.com are: (ns4/ns3/ns2/ns1).google.com as shown in the figure



```
paru04@LAPTOP-NVGR5VB8:~$ nslookup -type=NS google.com
Server:         172.23.208.1
Address:        172.23.208.1#53

Non-authoritative answer:
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.

Authoritative answers can be found from:
```

3. The command is: **nslookup gmail.com ns1.google.com**
The IP address is: 142.250.193.133



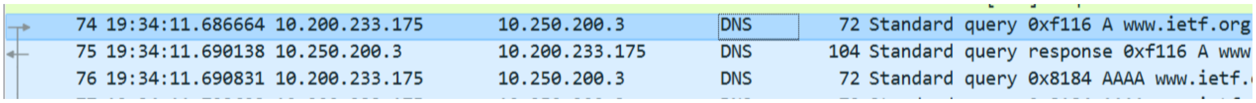
```
paru04@LAPTOP-NVGR5VB8:~$ nslookup gmail.com ns3.google.com
Server:         ns3.google.com
Address:        216.239.36.10#53

Name:   gmail.com
Address: 142.250.193.133
Name:   gmail.com
Address: 2404:6800:4007:820::2005
```

Part-3

1. The DNS query and response messages are sent over **UDP**

2. The Destination port for the DNS query message is: **53**
The Source port for the DNS response message is: **53**

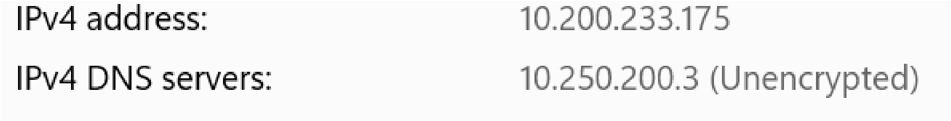
3. The IP address to which the DNS query is sent is: **10.250.200.3**



```
74 19:34:11.686664 10.200.233.175      10.250.200.3        DNS      72 Standard query 0xf116 A www.ietf.org
75 19:34:11.690138 10.250.200.3        10.200.233.175      DNS     104 Standard query response 0xf116 A www
76 19:34:11.690831 10.200.233.175      10.250.200.3        DNS      72 Standard query 0x8184 AAAA www.ietf.
```

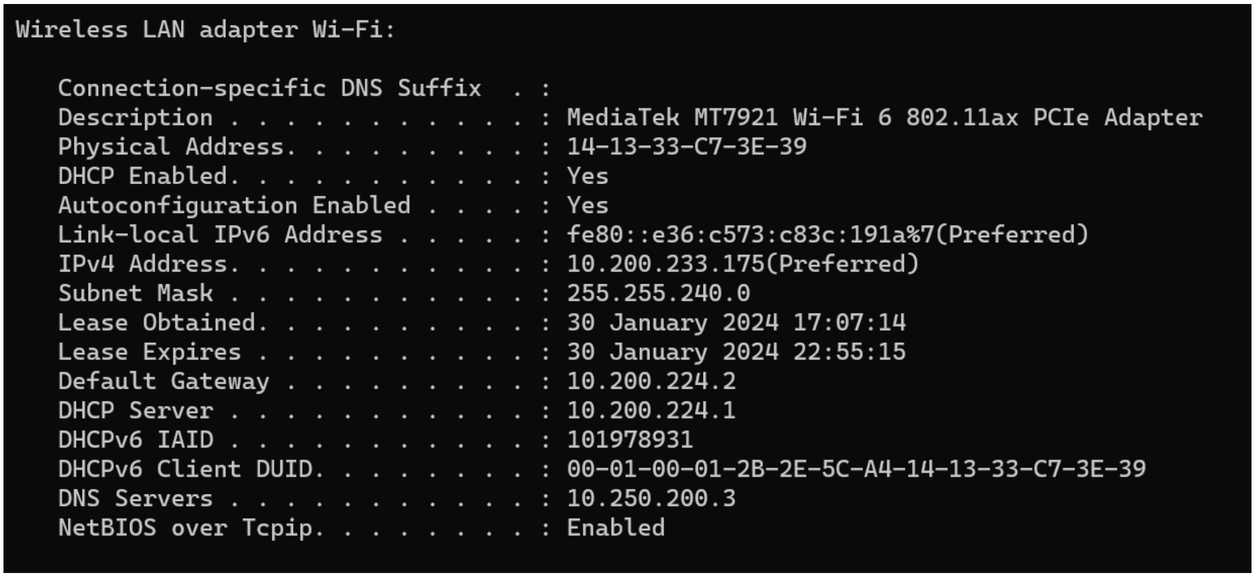
The IP address of local DNS server is:

a) 10.250.200.3 (for my windows system)



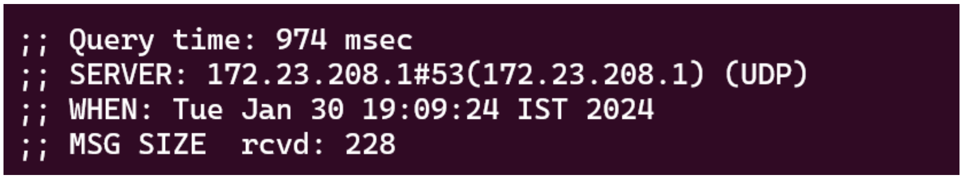
IPv4 address:	10.200.233.175
IPv4 DNS servers:	10.250.200.3 (Unencrypted)

With **“ipconfig -all”**



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe Adapter
   Physical Address. . . . . . . . . : 14-13-33-C7-3E-39
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e36:c573:c83c:191a%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.233.175(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : 30 January 2024 17:07:14
   Lease Expires . . . . . . . . . . : 30 January 2024 22:55:15
   Default Gateway . . . . . . . . . : 10.200.224.2
   DHCP Server . . . . . . . . . . . : 10.200.224.1
   DHCPv6 IAID . . . . . . . . . . . : 101978931
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-2E-5C-A4-14-13-33-C7-3E-39
   DNS Servers . . . . . . . . . . . : 10.250.200.3
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

b) 172.23.208.1 (for my wsl system)

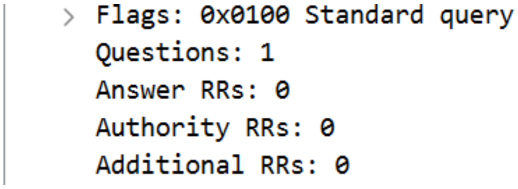


```
;; Query time: 974 msec
;; SERVER: 172.23.208.1#53(172.23.208.1) (UDP)
;; WHEN: Tue Jan 30 19:09:24 IST 2024
;; MSG SIZE  rcvd: 228
```

Yes, the IP address to which the DNS query message is sent is the same as one of my local DNS servers.

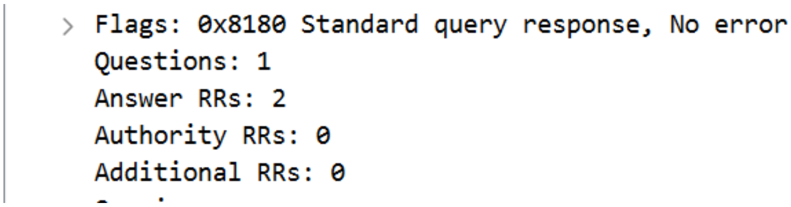
4. Type of the DNS query is: **A**

The query message has **No** answers.



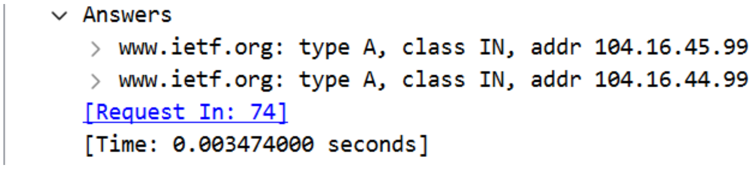
```
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
```

5. There are **2** answers.

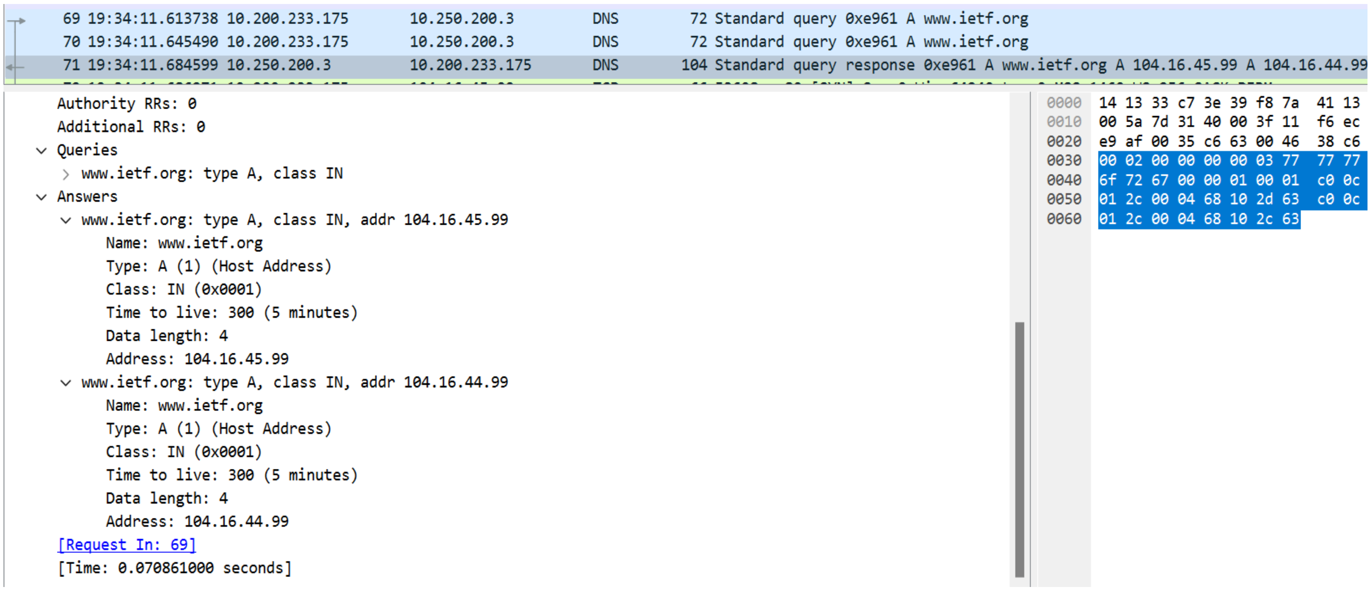


```
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
```

The two answers contain the name of the host, the type of address, class, the TTL, the data length and the IP address.



```
∨ Answers
    > www.ietf.org: type A, class IN, addr 104.16.45.99
    > www.ietf.org: type A, class IN, addr 104.16.44.99
  [Request In: 74]
  [Time: 0.003474000 seconds]
```



```
69 19:34:11.613738 10.200.233.175    10.250.200.3      DNS     72 Standard query 0xe961 A www.ietf.org
70 19:34:11.645490 10.200.233.175    10.250.200.3      DNS     72 Standard query 0xe961 A www.ietf.org
71 19:34:11.684599 10.250.200.3      10.200.233.175    DNS    104 Standard query response 0xe961 A www.ietf.org A 104.16.45.99 A 104.16.44.99
```

```
    Authority RRs: 0
    Additional RRs: 0
  ∨ Queries
    > www.ietf.org: type A, class IN
  ∨ Answers
    ∨ www.ietf.org: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.45.99
    ∨ www.ietf.org: type A, class IN, addr 104.16.44.99
        Name: www.ietf.org
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.44.99
    [Request In: 69]
    [Time: 0.070861000 seconds]
```

```
0000  14 13 33 c7 3e 39 f8 7a  41 13
0010  00 5a 7d 31 40 00 3f 11  f6 ec
0020  e9 af 00 35 c6 63 00 46  38 c6
0030  00 02 00 00 00 00 03 77  77 77
0040  6f 72 67 00 00 01 00 01  c0 0c
0050  01 2c 00 04 68 10 2d 63  c0 0c
0060  01 2c 00 04 68 10 2c 63
```

6. Yes, the DNS response message contains the IP address to which the TCP SYN packet was sent. The first SYN packet was sent to **104.16.45.99** which corresponds to the first IP address provided in the DNS response message.

7. No, The host doesn't issue new DNS queries.

Part-4

1)

1. The Destination port for the DNS query message is: **53**
The Source port for the DNS response message is: **53**

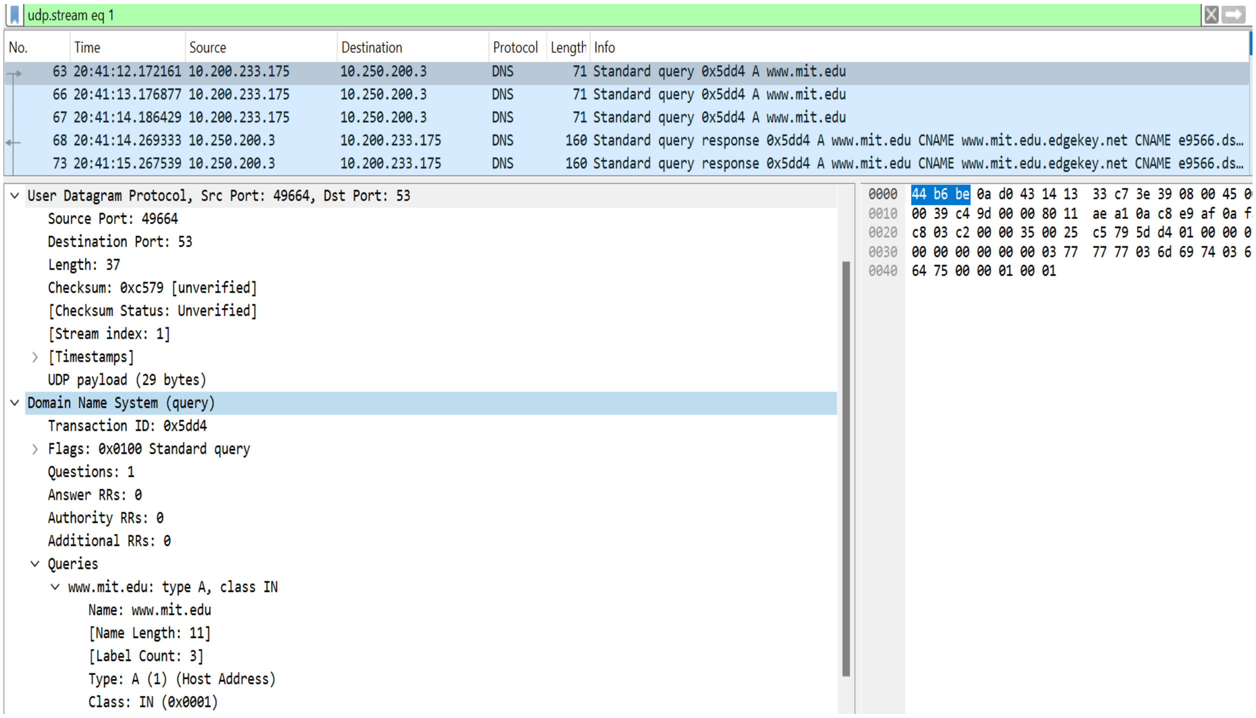
2. It's sent to **10.250.200.3** which as we can see from the "ipconfig –all screenshot", is the default local DNS server.

3. The query is of type **A** and it doesn't contain any answers.

4. The response DNS message contains 3 answers containing the name of the host, the type of address, the class, and the IP address. The first and second answers contain CNAME which is the alias of the Domain Name, while the third answer contains the IP address of the Domain Name.

5. Screenshots are given below

DNS Query:

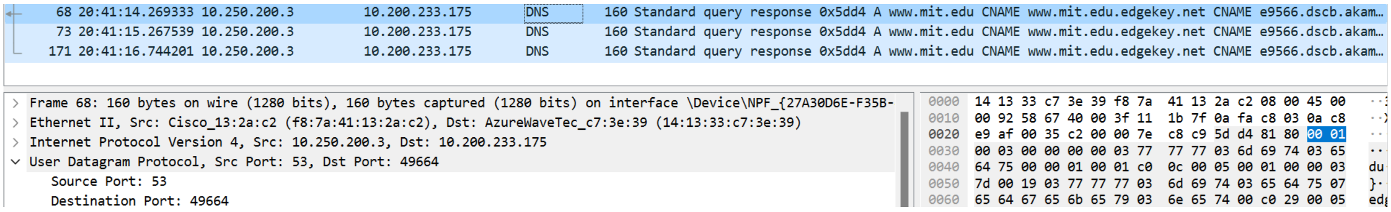


```
udp.stream eq 1

No.  Time             Source          Destination     Protocol Length Info
  63 20:41:12.172161 10.200.233.175 10.250.200.3    DNS        71 Standard query 0x5dd4 A www.mit.edu
  66 20:41:13.176877 10.200.233.175 10.250.200.3    DNS        71 Standard query 0x5dd4 A www.mit.edu
  67 20:41:14.186429 10.200.233.175 10.250.200.3    DNS        71 Standard query 0x5dd4 A www.mit.edu
  68 20:41:14.269333 10.250.200.3   10.200.233.175  DNS       160 Standard query response 0x5dd4 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.ds…
  73 20:41:15.267539 10.250.200.3   10.200.233.175  DNS       160 Standard query response 0x5dd4 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.ds…
```

```
v User Datagram Protocol, Src Port: 49664, Dst Port: 53
    Source Port: 49664
    Destination Port: 53
    Length: 37
    Checksum: 0xc579 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (29 bytes)
v Domain Name System (query)
    Transaction ID: 0x5dd4
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
```

```
0000  44 b6 be 0a d0 43 14 13  33 c7 3e 39 08 00 45 0
0010  00 39 c4 9d 00 00 80 11  ae a1 0a c8 e9 af 0a f
0020  c8 03 c2 00 00 35 00 25  c5 79 5d d4 01 00 00 0
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 6
0040  64 75 00 00 01 00 01
```

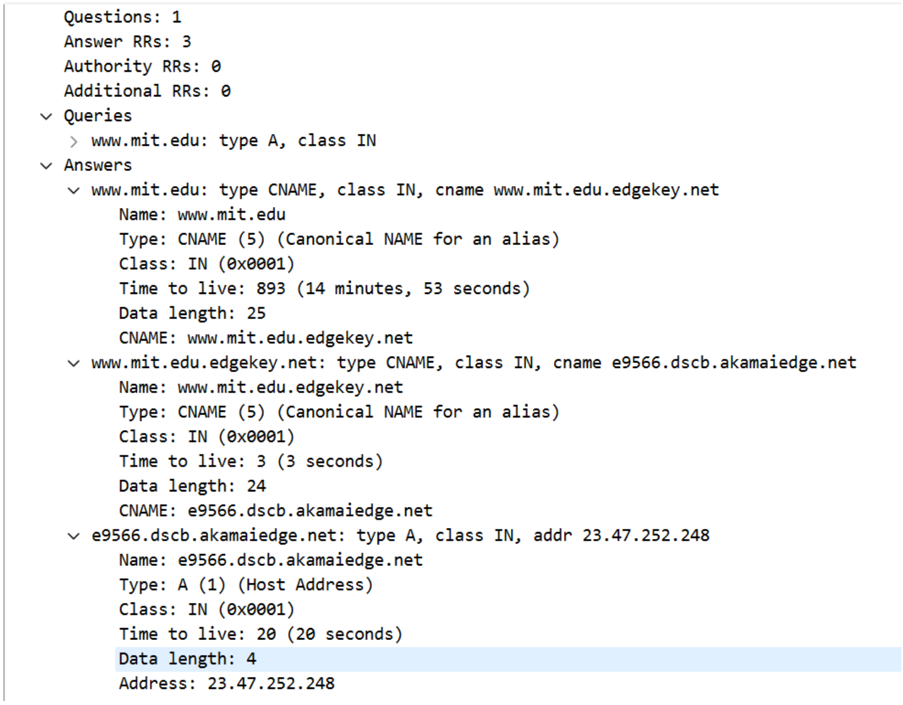
DNS Response:



```
   68 20:41:14.269333 10.250.200.3   10.200.233.175  DNS   160 Standard query response 0x5dd4 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akam…
   73 20:41:15.267539 10.250.200.3   10.200.233.175  DNS   160 Standard query response 0x5dd4 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akam…
  171 20:41:16.744201 10.250.200.3   10.200.233.175  DNS   160 Standard query response 0x5dd4 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akam…
```

```
> Frame 68: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{27A30D6E-F35B-
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39)
> Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.200.233.175
v User Datagram Protocol, Src Port: 53, Dst Port: 49664
    Source Port: 53
    Destination Port: 49664
```

```
0000  14 13 33 c7 3e 39 f8 7a  41 13 2a c2 08 00 45 00   ··
0010  00 92 58 67 40 00 3f 11  1b 7f 0a fa c8 03 0a c8   ··
0020  e9 af 00 35 c2 00 00 7e  c8 c9 5d d4 81 80 00 01   ··
0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ··
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 03   du
0050  7d 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   }·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edg
```

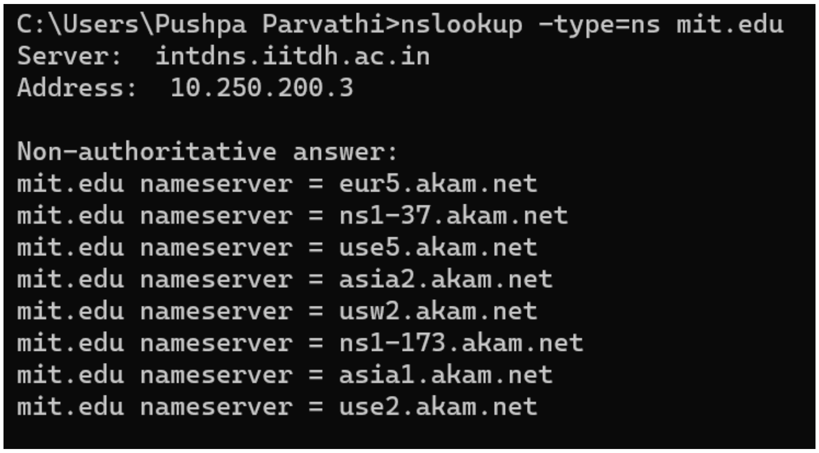


```
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
  v Answers
    v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 893 (14 minutes, 53 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 3 (3 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.47.252.248
        Name: e9566.dscb.akamaiedge.net
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 23.47.252.248
```

2)

1. It was sent to 10.250.200.3 which is my default local DNS server.
2. It’s a type **NS** DNS query that doesn’t contain any answers.
3. The nameservers are:

   ns1-37.akam.net
   asia2.akam.net
   use5.akam.net
   asia1.akam.net
   ns1-173.akam.net
   use2.akam.net
   usw2.akam.net
   eur5.akam.net

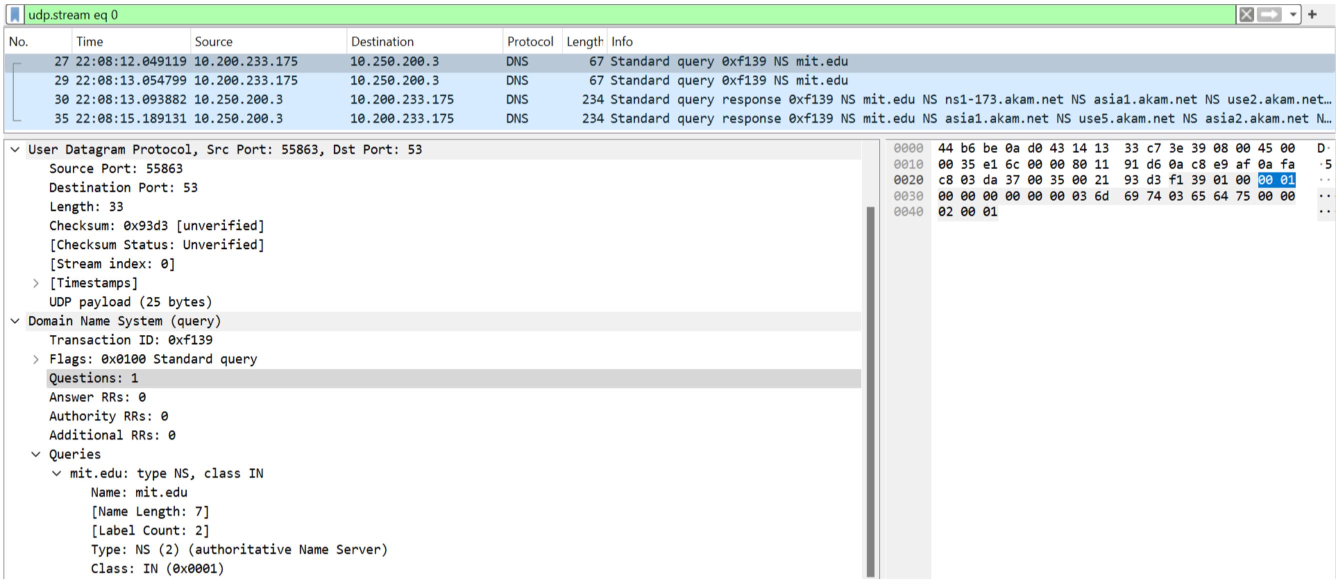


```
C:\Users\Pushpa Parvathi>nslookup -type=ns mit.edu
Server:  intdns.iitdh.ac.in
Address:  10.250.200.3

Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use2.akam.net
```

No, the response doesn’t provide an IP address(also, Additional RRs(Records)=0, in the DNS Response)

4. Screenshots are given below

DNS Query:

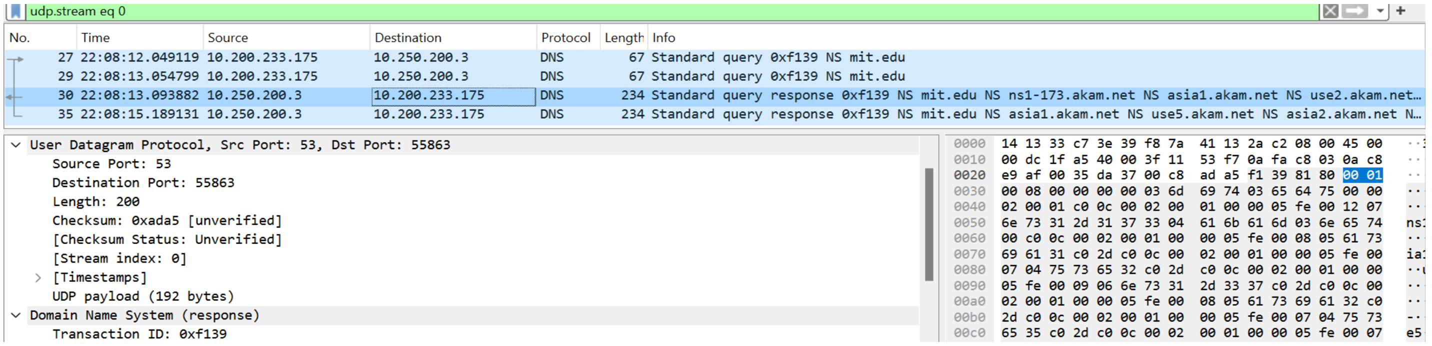


```
No.  Time             Source          Destination     Protocol Length Info
  27 22:08:12.049119 10.200.233.175  10.250.200.3    DNS        67 Standard query 0xf139 NS mit.edu
  29 22:08:13.054799 10.200.233.175  10.250.200.3    DNS        67 Standard query 0xf139 NS mit.edu
  30 22:08:13.093882 10.250.200.3    10.200.233.175  DNS       234 Standard query response 0xf139 NS mit.edu NS ns1-173.akam.net NS asia1.akam.net NS use2.akam.net…
  35 22:08:15.189131 10.250.200.3    10.200.233.175  DNS       234 Standard query response 0xf139 NS mit.edu NS asia1.akam.net NS use5.akam.net NS asia2.akam.net N…
```

```
∨ User Datagram Protocol, Src Port: 55863, Dst Port: 53
    Source Port: 55863
    Destination Port: 53
    Length: 33
    Checksum: 0x93d3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (25 bytes)
∨ Domain Name System (query)
    Transaction ID: 0xf139
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ∨ Queries
    ∨ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
```

```
0000  44 b6 be 0a d0 43 14 13  33 c7 3e 39 08 00 45 00   D·
0010  00 35 e1 6c 00 00 80 11  91 d6 0a c8 e9 af 0a fa   ·5
0020  c8 03 da 37 00 35 00 21  93 d3 f1 39 01 00 00 01   ··
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ··
0040  02 00 01                                           ··
```

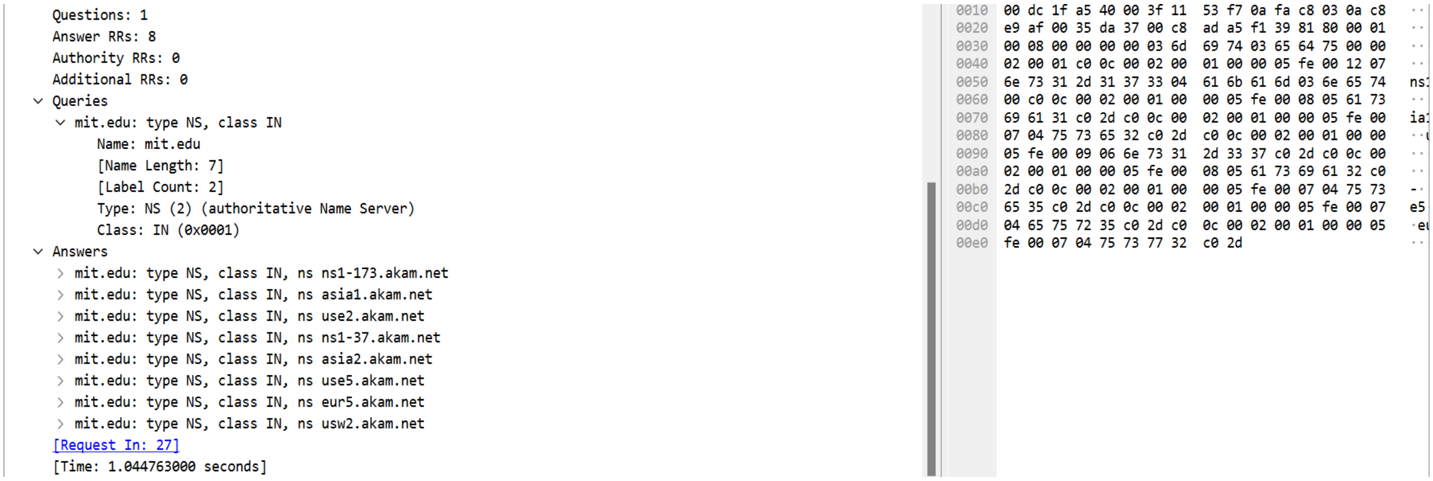
DNS Response:



```
udp.stream eq 0
No.  Time             Source          Destination     Protocol Length Info
  27 22:08:12.049119 10.200.233.175  10.250.200.3    DNS        67 Standard query 0xf139 NS mit.edu
  29 22:08:13.054799 10.200.233.175  10.250.200.3    DNS        67 Standard query 0xf139 NS mit.edu
  30 22:08:13.093882 10.250.200.3    10.200.233.175  DNS       234 Standard query response 0xf139 NS mit.edu NS ns1-173.akam.net NS asia1.akam.net NS use2.akam.net…
  35 22:08:15.189131 10.250.200.3    10.200.233.175  DNS       234 Standard query response 0xf139 NS mit.edu NS asia1.akam.net NS use5.akam.net NS asia2.akam.net N…
```

```
∨ User Datagram Protocol, Src Port: 53, Dst Port: 55863
    Source Port: 53
    Destination Port: 55863
    Length: 200
    Checksum: 0xada5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (192 bytes)
∨ Domain Name System (response)
    Transaction ID: 0xf139
```

```
0000  14 13 33 c7 3e 39 f8 7a  41 13 2a c2 08 00 45 00   ··
0010  00 dc 1f a5 40 00 3f 11  53 f7 0a fa c8 03 0a c8   ··
0020  e9 af 00 35 da 37 00 c8  ad a5 f1 39 81 80 00 01   ··
0030  00 08 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ··
0040  02 00 01 c0 0c 00 02 00  01 00 00 05 fe 00 12 07   ··
0050  6e 73 31 2d 31 37 33 04  61 6b 61 6d 03 6e 65 74   ns
0060  00 c0 0c 00 02 00 01 00  00 05 fe 00 08 05 61 73   ··
0070  69 61 31 c0 2d c0 0c 00  02 00 01 00 00 05 fe 00   ia
0080  07 04 75 73 65 32 c0 2d  c0 0c 00 02 00 01 00 00   ··u
0090  05 fe 00 09 06 6e 73 31  2d 33 37 c0 2d c0 0c 00   ··
00a0  02 00 01 00 00 05 fe 00  08 05 61 73 69 61 32 c0   ··
00b0  2d c0 0c 00 02 00 01 00  00 05 fe 00 07 04 75 73   -·
00c0  65 35 c0 2d c0 0c 00 02  00 01 00 00 05 fe 00 07   e5
```

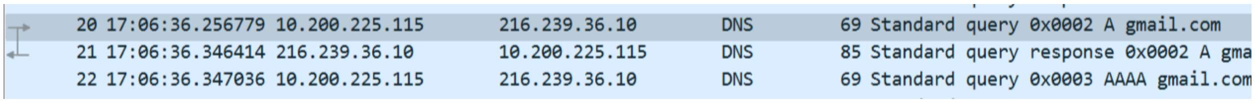


```
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ∨ Queries
    ∨ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
  ∨ Answers
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    [Request In: 27]
    [Time: 1.044763000 seconds]
```

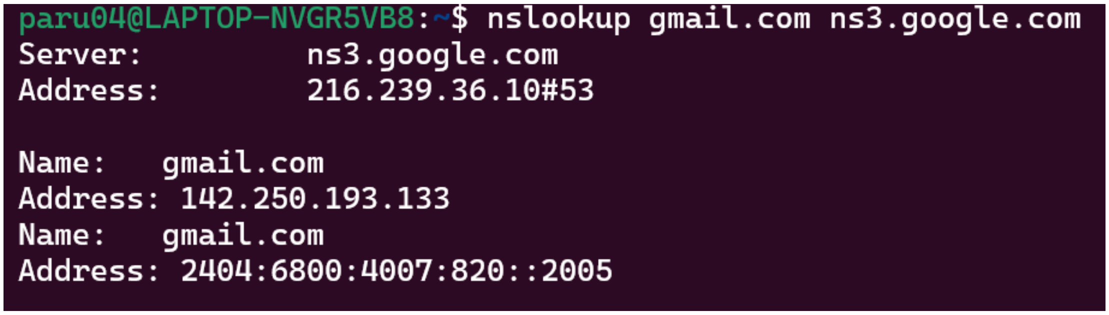
```
0010  00 dc 1f a5 40 00 3f 11  53 f7 0a fa c8 03 0a c8   ··
0020  e9 af 00 35 da 37 00 c8  ad a5 f1 39 81 80 00 01   ··
0030  00 08 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ··
0040  02 00 01 c0 0c 00 02 00  01 00 00 05 fe 00 12 07   ··
0050  6e 73 31 2d 31 37 33 04  61 6b 61 6d 03 6e 65 74   ns
0060  00 c0 0c 00 02 00 01 00  00 05 fe 00 08 05 61 73   ··
0070  69 61 31 c0 2d c0 0c 00  02 00 01 00 00 05 fe 00   ia
0080  07 04 75 73 65 32 c0 2d  c0 0c 00 02 00 01 00 00   ··u
0090  05 fe 00 09 06 6e 73 31  2d 33 37 c0 2d c0 0c 00   ··
00a0  02 00 01 00 00 05 fe 00  08 05 61 73 69 61 32 c0   ··
00b0  2d c0 0c 00 02 00 01 00  00 05 fe 00 07 04 75 73   -·
00c0  65 35 c0 2d c0 0c 00 02  00 01 00 00 05 fe 00 07   e5
00d0  04 65 75 72 35 c0 2d c0  0c 00 02 00 01 00 00 05   ·eu
00e0  fe 00 07 04 75 73 77 32  c0 2d                     ··
```

3)

1. The DNS message is sent to the IP address: 216.239.36.10



```
20 17:06:36.256779 10.200.225.115  216.239.36.10   DNS   69 Standard query 0x0002 A gmail.com
21 17:06:36.346414 216.239.36.10   10.200.225.115  DNS   85 Standard query response 0x0002 A gma
22 17:06:36.347036 10.200.225.115  216.239.36.10   DNS   69 Standard query 0x0003 AAAA gmail.com
```

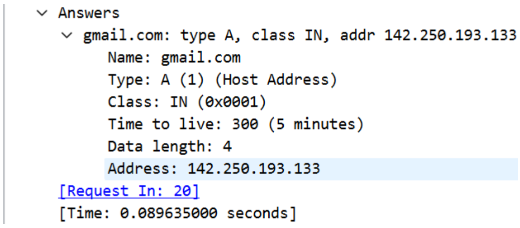


```
paru04@LAPTOP-NVGR5VB8:~$ nslookup gmail.com ns3.google.com
Server:         ns3.google.com
Address:        216.239.36.10#53

Name:   gmail.com
Address: 142.250.193.133
Name:   gmail.com
Address: 2404:6800:4007:820::2005
```

No, the IP address doesn't match the IP address of our Local DNS Server because the request is sent to the ns3.google.com

2. It's a type **A** DNS query that doesn't contain any answers.

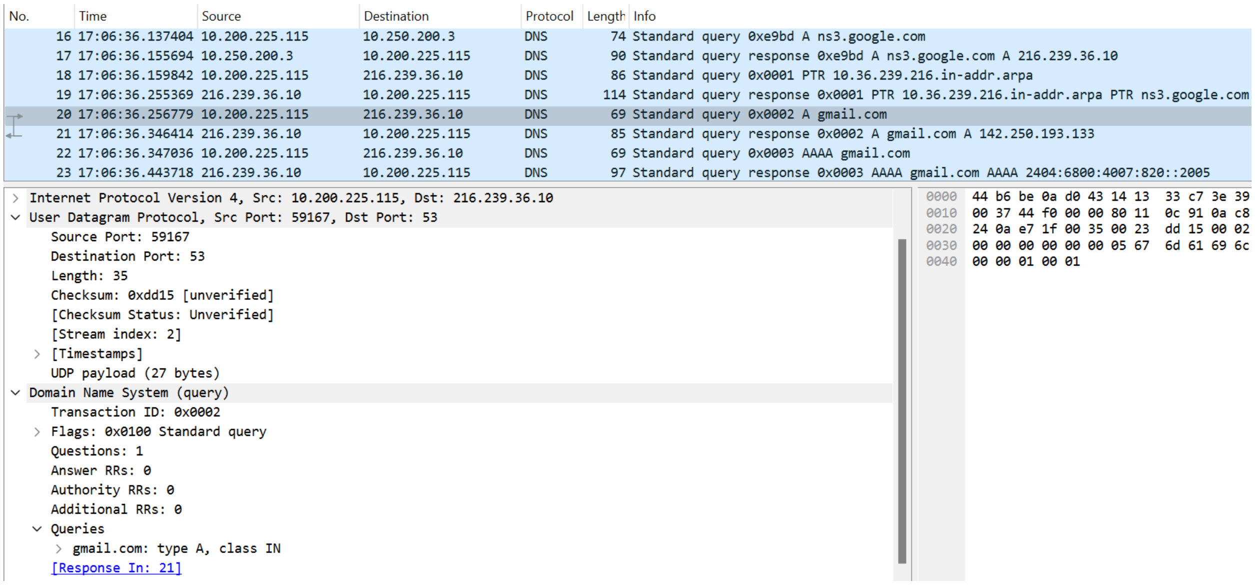
3. There is 1 answer. The answer contain the following



```
  ⌄ Answers
    ⌄ gmail.com: type A, class IN, addr 142.250.193.133
        Name: gmail.com
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 142.250.193.133
    [Request In: 20]
    [Time: 0.089635000 seconds]
```

4. Screenshots are given below

DNS Query:

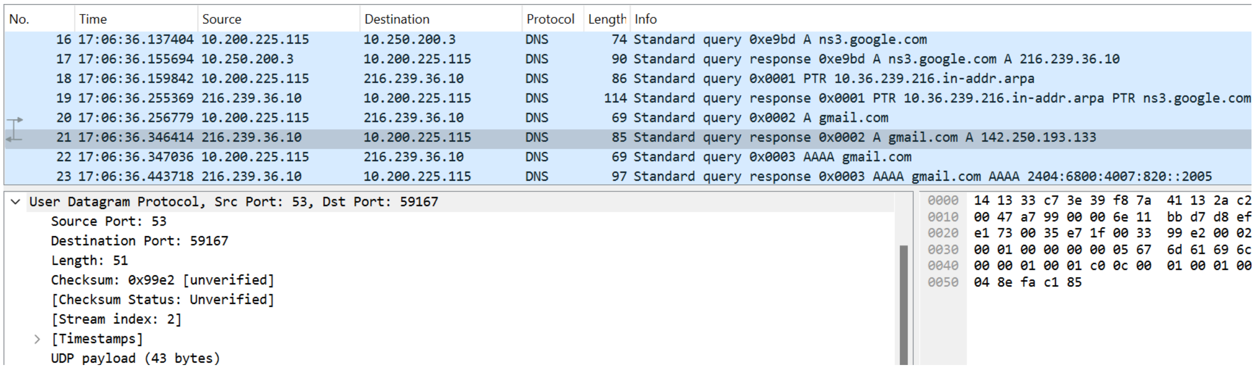


```
No.  Time            Source          Destination     Protocol Length Info
  16 17:06:36.137404 10.200.225.115  10.250.200.3    DNS       74 Standard query 0xe9bd A ns3.google.com
  17 17:06:36.155694 10.250.200.3    10.200.225.115  DNS       90 Standard query response 0xe9bd A ns3.google.com A 216.239.36.10
  18 17:06:36.159842 10.200.225.115  216.239.36.10   DNS       86 Standard query 0x0001 PTR 10.36.239.216.in-addr.arpa
  19 17:06:36.255369 216.239.36.10   10.200.225.115  DNS      114 Standard query response 0x0001 PTR 10.36.239.216.in-addr.arpa PTR ns3.google.com
  20 17:06:36.256779 10.200.225.115  216.239.36.10   DNS       69 Standard query 0x0002 A gmail.com
  21 17:06:36.346414 216.239.36.10   10.200.225.115  DNS       85 Standard query response 0x0002 A gmail.com A 142.250.193.133
  22 17:06:36.347036 10.200.225.115  216.239.36.10   DNS       69 Standard query 0x0003 AAAA gmail.com
  23 17:06:36.443718 216.239.36.10   10.200.225.115  DNS       97 Standard query response 0x0003 AAAA gmail.com AAAA 2404:6800:4007:820::2005
```

```
› Internet Protocol Version 4, Src: 10.200.225.115, Dst: 216.239.36.10
⌄ User Datagram Protocol, Src Port: 59167, Dst Port: 53
    Source Port: 59167
    Destination Port: 53
    Length: 35
    Checksum: 0xdd15 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  › [Timestamps]
    UDP payload (27 bytes)
⌄ Domain Name System (query)
    Transaction ID: 0x0002
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    › gmail.com: type A, class IN
    [Response In: 21]
```

```
0000  44 b6 be 0a d0 43 14 13  33 c7 3e 39
0010  00 37 44 f0 00 00 80 11  0c 91 0a c8
0020  24 0a e7 1f 00 35 00 23  dd 15 00 02
0030  00 00 00 00 00 00 05 67  6d 61 69 6c
0040  00 00 01 00 01
```

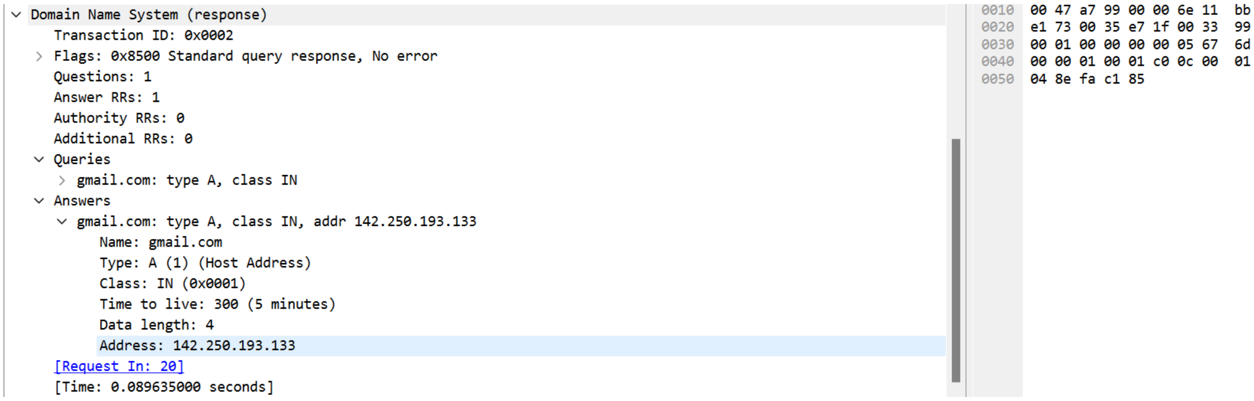
DNS Response:



```
No.  Time            Source          Destination     Protocol Length Info
  16 17:06:36.137404 10.200.225.115  10.250.200.3    DNS       74 Standard query 0xe9bd A ns3.google.com
  17 17:06:36.155694 10.250.200.3    10.200.225.115  DNS       90 Standard query response 0xe9bd A ns3.google.com A 216.239.36.10
  18 17:06:36.159842 10.200.225.115  216.239.36.10   DNS       86 Standard query 0x0001 PTR 10.36.239.216.in-addr.arpa
  19 17:06:36.255369 216.239.36.10   10.200.225.115  DNS      114 Standard query response 0x0001 PTR 10.36.239.216.in-addr.arpa PTR ns3.google.com
  20 17:06:36.256779 10.200.225.115  216.239.36.10   DNS       69 Standard query 0x0002 A gmail.com
  21 17:06:36.346414 216.239.36.10   10.200.225.115  DNS       85 Standard query response 0x0002 A gmail.com A 142.250.193.133
  22 17:06:36.347036 10.200.225.115  216.239.36.10   DNS       69 Standard query 0x0003 AAAA gmail.com
  23 17:06:36.443718 216.239.36.10   10.200.225.115  DNS       97 Standard query response 0x0003 AAAA gmail.com AAAA 2404:6800:4007:820::2005
```

```
⌄ User Datagram Protocol, Src Port: 53, Dst Port: 59167
    Source Port: 53
    Destination Port: 59167
    Length: 51
    Checksum: 0x99e2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  › [Timestamps]
    UDP payload (43 bytes)
```

```
0000  14 13 33 c7 3e 39 f8 7a  41 13 2a c2
0010  00 47 a7 99 00 00 6e 11  bb d7 d8 ef
0020  e1 73 00 35 e7 1f 00 33  99 e2 00 02
0030  00 01 00 00 00 00 05 67  6d 61 69 6c
0040  00 00 01 00 01 c0 0c 00  01 00 01 00
0050  04 8e fa c1 85
```



```
⌄ Domain Name System (response)
    Transaction ID: 0x0002
  › Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    › gmail.com: type A, class IN
  ⌄ Answers
    ⌄ gmail.com: type A, class IN, addr 142.250.193.133
        Name: gmail.com
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 142.250.193.133
    [Request In: 20]
    [Time: 0.089635000 seconds]
```

```
0010  00 47 a7 99 00 00 6e 11  bb
0020  e1 73 00 35 e7 1f 00 33  99
0030  00 01 00 00 00 00 05 67  6d
0040  00 00 01 00 01 c0 0c 00  01
0050  04 8e fa c1 85
```