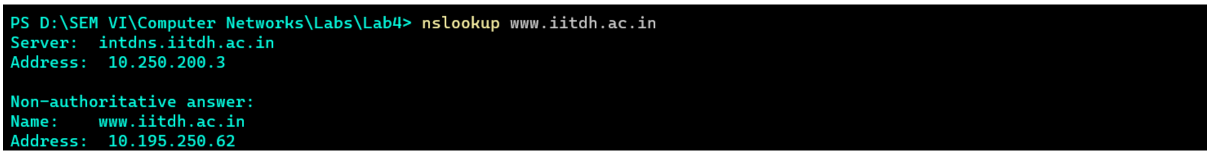
Assignment 4: DNS

Hrishikesh Ravindra Karande 210010020

Part1:

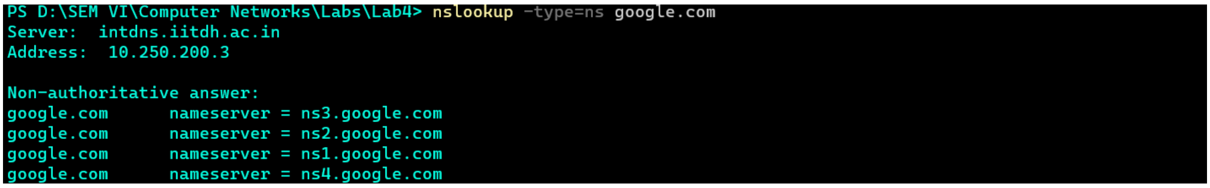
1. IP Address: 10.195.250.62



```
PS D:\SEM VI\Computer Networks\Labs\Lab4> nslookup www.iitdh.ac.in
Server:  intdns.iitdh.ac.in
Address:  10.250.200.3

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

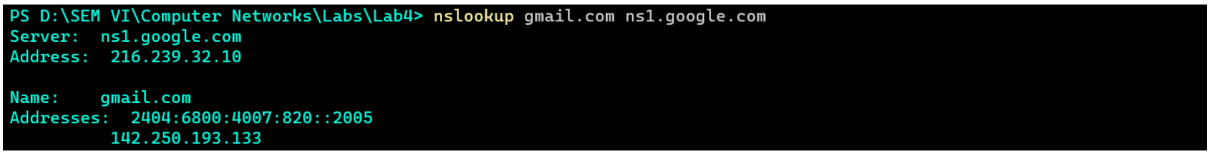
2. The servers for google.com can be found out using -ns option.



```
PS D:\SEM VI\Computer Networks\Labs\Lab4> nslookup -type=ns google.com
Server:  intdns.iitdh.ac.in
Address:  10.250.200.3

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

3. Queried server ns1.google.com instead of using server intdn.iitdh.ac.in obtained from Q2. The IP Address can be seen below.

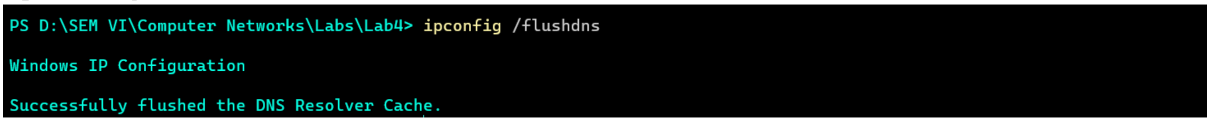


```
PS D:\SEM VI\Computer Networks\Labs\Lab4> nslookup gmail.com ns1.google.com
Server:  ns1.google.com
Address:  216.239.32.10

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

Part2

1. `ipconfig /flushdns`



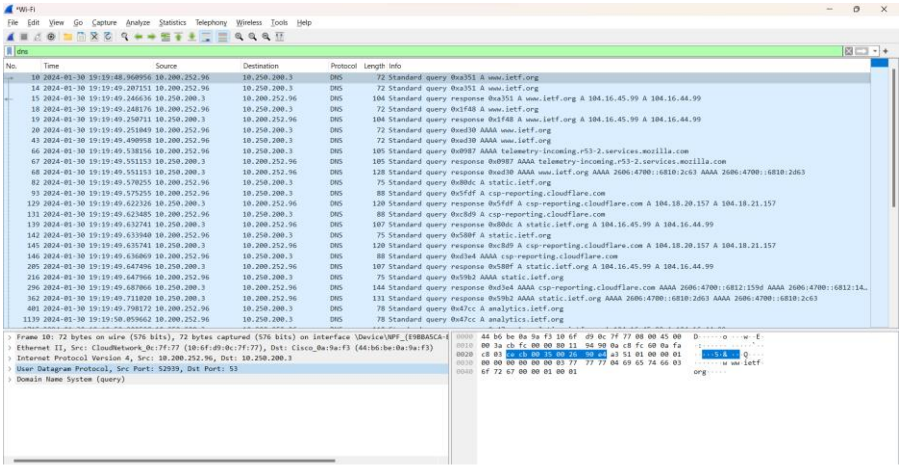
```
PS D:\SEM VI\Computer Networks\Labs\Lab4> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Part3

1. DNS Follows UDP protocol.

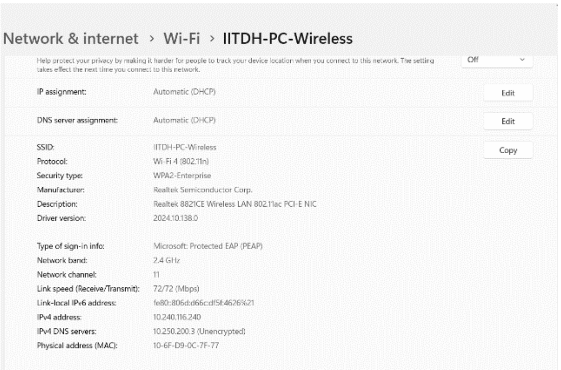

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time                       Source          Destination     Protocol Length Info
   10 2024-01-30 19:19:48.960956 10.200.252.96   10.250.200.3    DNS        72 Standard query 0xa351 A www.ietf.org
   14 2024-01-30 19:19:49.207151 10.200.252.96   10.250.200.3    DNS        72 Standard query 0xa351 A www.ietf.org
   15 2024-01-30 19:19:49.246636 10.250.200.3    10.200.252.96   DNS       104 Standard query response 0xa351 A www.ietf.org A 104.16.45.99 A 104.16.44.99
   18 2024-01-30 19:19:49.248176 10.200.252.96   10.250.200.3    DNS        72 Standard query 0x1f48 A www.ietf.org
   19 2024-01-30 19:19:49.250711 10.250.200.3    10.200.252.96   DNS       104 Standard query response 0x1f48 A www.ietf.org A 104.16.45.99 A 104.16.44.99
   20 2024-01-30 19:19:49.251049 10.200.252.96   10.250.200.3    DNS        72 Standard query 0xed30 AAAA www.ietf.org
   43 2024-01-30 19:19:49.490958 10.200.252.96   10.250.200.3    DNS        72 Standard query 0xed30 AAAA www.ietf.org
   66 2024-01-30 19:19:49.538156 10.200.252.96   10.250.200.3    DNS       105 Standard query 0x0987 AAAA telemetry-incoming.r53-2.services.mozilla.com
   67 2024-01-30 19:19:49.551153 10.250.200.3    10.200.252.96   DNS       105 Standard query response 0x0987 AAAA telemetry-incoming.r53-2.services.mozilla.com
   68 2024-01-30 19:19:49.551153 10.250.200.3    10.200.252.96   DNS       128 Standard query response 0xed30 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
   82 2024-01-30 19:19:49.570255 10.200.252.96   10.250.200.3    DNS        75 Standard query 0x80dc A static.ietf.org
   93 2024-01-30 19:19:49.575255 10.200.252.96   10.250.200.3    DNS        88 Standard query 0x5fdf A csp-reporting.cloudflare.com
  129 2024-01-30 19:19:49.622326 10.250.200.3    10.200.252.96   DNS       120 Standard query response 0x5fdf A csp-reporting.cloudflare.com A 104.18.20.157 A 104.18.21.157
  131 2024-01-30 19:19:49.623485 10.200.252.96   10.250.200.3    DNS        88 Standard query 0xc8d9 A csp-reporting.cloudflare.com
  139 2024-01-30 19:19:49.632741 10.250.200.3    10.200.252.96   DNS       107 Standard query response 0x80dc A static.ietf.org A 104.16.45.99 A 104.16.44.99
  142 2024-01-30 19:19:49.633940 10.200.252.96   10.250.200.3    DNS        75 Standard query 0x580f A static.ietf.org
  145 2024-01-30 19:19:49.635741 10.250.200.3    10.200.252.96   DNS       120 Standard query response 0xc8d9 A csp-reporting.cloudflare.com A 104.18.20.157 A 104.18.21.157
  146 2024-01-30 19:19:49.636069 10.200.252.96   10.250.200.3    DNS        88 Standard query 0xd3e4 AAAA csp-reporting.cloudflare.com
  205 2024-01-30 19:19:49.647496 10.250.200.3    10.200.252.96   DNS       107 Standard query response 0x580f A static.ietf.org A 104.16.45.99 A 104.16.44.99
  216 2024-01-30 19:19:49.647966 10.200.252.96   10.250.200.3    DNS        75 Standard query 0x59b2 AAAA static.ietf.org
  296 2024-01-30 19:19:49.687066 10.250.200.3    10.200.252.96   DNS       144 Standard query response 0xd3e4 AAAA csp-reporting.cloudflare.com AAAA 2606:4700::6812:159d AAAA 2606:4700::6812:14…
  362 2024-01-30 19:19:49.711020 10.250.200.3    10.200.252.96   DNS       131 Standard query response 0x59b2 AAAA static.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
  401 2024-01-30 19:19:49.798172 10.200.252.96   10.250.200.3    DNS        78 Standard query 0x47cc A analytics.ietf.org
 1139 2024-01-30 19:19:50.059662 10.200.252.96   10.250.200.3    DNS        78 Standard query 0x47cc A analytics.ietf.org
```

```
> Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{E9BBA5CA-E
> Ethernet II, Src: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77), Dst: Cisco_0a:9a:f3 (44:b6:be:0a:9a:f3)
> Internet Protocol Version 4, Src: 10.200.252.96, Dst: 10.250.200.3
> User Datagram Protocol, Src Port: 52939, Dst Port: 53
> Domain Name System (query)
```

```
0000  44 b6 be 0a 9a f3 10 6f  d9 0c 7f 77 08 00 45 00   D······o ···w··E·
0010  00 3a cb fc 00 00 80 11  94 90 0a c8 fc 60 0a fa   ·:·······`··
0020  c8 03 ce cb 00 35 00 26  90 e4 a3 51 01 00 00 01   ·····5·&···Q····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····
```

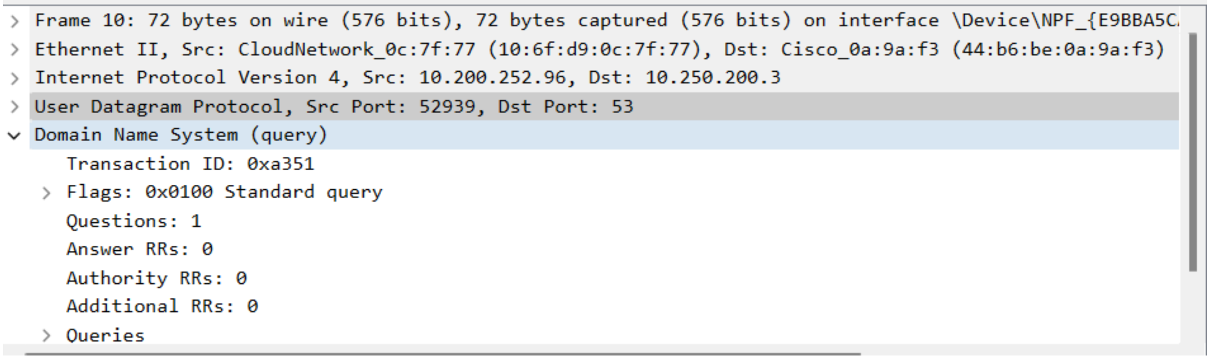
2. The source for DNS Query Message and destination for DNS response message is **port 53.**
3. The highlighted IPv4 address matches the destination address obtained by checking the wifi settings on local computer.


Network & internet › Wi-Fi › IITDH-PC-Wireless

Help protect your privacy by making it harder for people to track your device location when you connect to this network. The setting takes effect the next time you connect to this network. Off

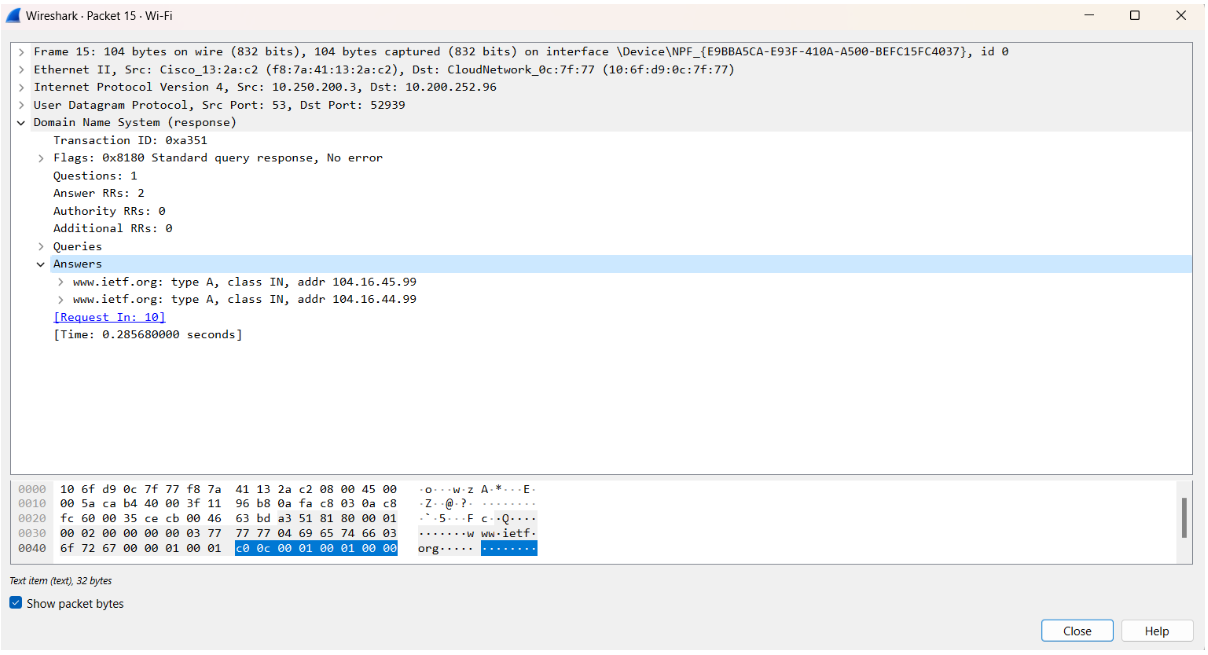
IP assignment:	Automatic (DHCP)	Edit
DNS server assignment:	Automatic (DHCP)	Edit
SSID:	IITDH-PC-Wireless	Copy
Protocol:	Wi-Fi 4 (802.11n)	
Security type:	WPA2-Enterprise	
Manufacturer:	Realtek Semiconductor Corp.	
Description:	Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC	
Driver version:	2024.10.138.0	
Type of sign-in info:	Microsoft: Protected EAP (PEAP)	
Network band:	2.4 GHz	
Network channel:	11	
Link speed (Receive/Transmit):	72/72 (Mbps)	
Link-local IPv6 address:	fe80::806d:d66c:df5f:4626%21	
IPv4 address:	10.240.116.240	
IPv4 DNS servers:	10.250.200.3 (Unencrypted)	
Physical address (MAC):	10-6F-D9-0C-7F-77	

4. The DNS Query is Type A Standard Query and contains 0 answers.



```
> Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{E9BBA5C
> Ethernet II, Src: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77), Dst: Cisco_0a:9a:f3 (44:b6:be:0a:9a:f3)
> Internet Protocol Version 4, Src: 10.200.252.96, Dst: 10.250.200.3
> User Datagram Protocol, Src Port: 52939, Dst Port: 53
v Domain Name System (query)
      Transaction ID: 0xa351
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    > Queries
```

5. Two answers is provided. Contents of answers are: Name, Type, Class, Time To Live(TTL) and Address.



```
> Frame 15: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{E9BBA5CA-E93F-410A-A500-BEFC15FC4037}, id 0
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77)
> Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.200.252.96
> User Datagram Protocol, Src Port: 53, Dst Port: 52939
v Domain Name System (response)
    Transaction ID: 0xa351
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v 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: 10]
    [Time: 0.285680000 seconds]
```

```
0000  10 6f d9 0c 7f 77 f8 7a  41 13 2a c2 08 00 45 00   ·o···w·z A·*···E·
0010  00 5a ca b4 40 00 3f 11  96 b8 0a fa c8 03 0a c8   ·Z··@·?· ········
0020  fc 60 00 35 ce cb 00 46  63 bd a3 51 81 80 00 01   ·`·5···F c··Q····
0030  00 02 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01  c0 0c 00 01 00 01 00 00   org····· ········
```

Text item (text), 32 bytes

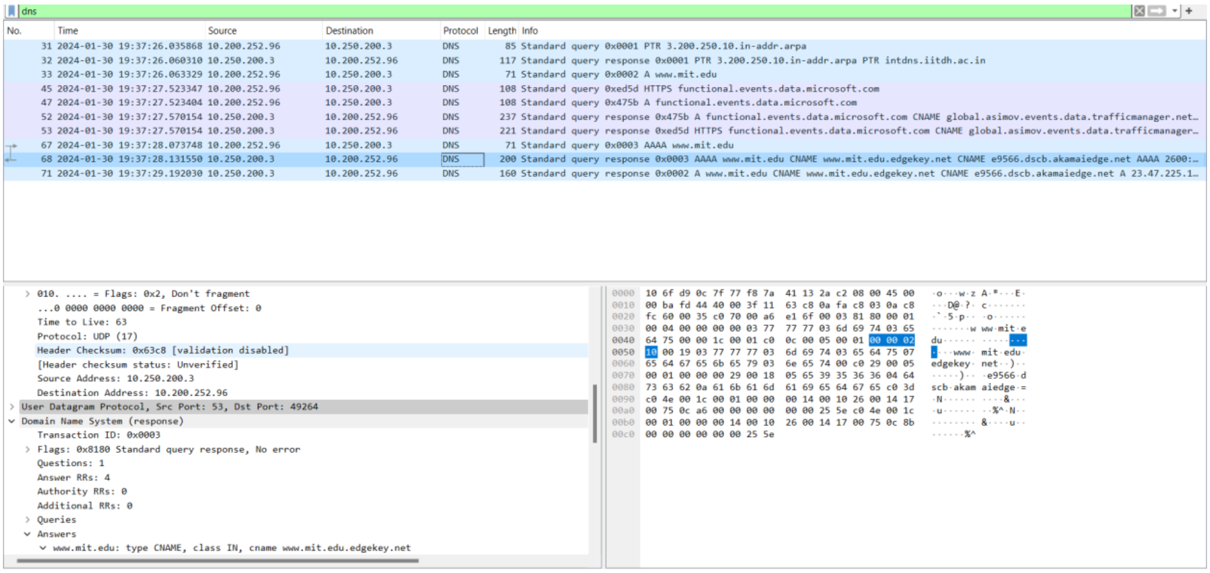
☑ Show packet bytes

6. The Destination IP address on first TCP-SYN packet 10.240.116.240 corresponds to first DNS response message.
7. No, the images are all loaded from www.ietf.org, so no additional DNS queries are necessary to fetch the request of objects.

Part4

1.

1. The Destination port for DNS = 53
   Query port for DNS Response=53



```
dns
No.   Time                        Source          Destination     Protocol Length Info
   31 2024-01-30 19:37:26.035868 10.200.252.96   10.250.200.3    DNS        85 Standard query 0x0001 PTR 3.200.250.10.in-addr.arpa
   32 2024-01-30 19:37:26.060310 10.250.200.3    10.200.252.96   DNS       117 Standard query response 0x0001 PTR 3.200.250.10.in-addr.arpa PTR intdns.iitdh.ac.in
   33 2024-01-30 19:37:26.063329 10.200.252.96   10.250.200.3    DNS        71 Standard query 0x0002 A www.mit.edu
   45 2024-01-30 19:37:27.523347 10.200.252.96   10.250.200.3    DNS       108 Standard query 0xed5d HTTPS functional.events.data.microsoft.com
   47 2024-01-30 19:37:27.523404 10.200.252.96   10.250.200.3    DNS       108 Standard query 0x475b A functional.events.data.microsoft.com
   52 2024-01-30 19:37:27.570154 10.250.200.3    10.200.252.96   DNS       237 Standard query response 0x475b A functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net…
   53 2024-01-30 19:37:27.570154 10.250.200.3    10.200.252.96   DNS       221 Standard query response 0xed5d HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager…
   67 2024-01-30 19:37:28.073748 10.200.252.96   10.250.200.3    DNS        71 Standard query 0x0003 AAAA www.mit.edu
   68 2024-01-30 19:37:28.131550 10.250.200.3    10.200.252.96   DNS       200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:…
   71 2024-01-30 19:37:29.192030 10.250.200.3    10.200.252.96   DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.47.225.1…
```

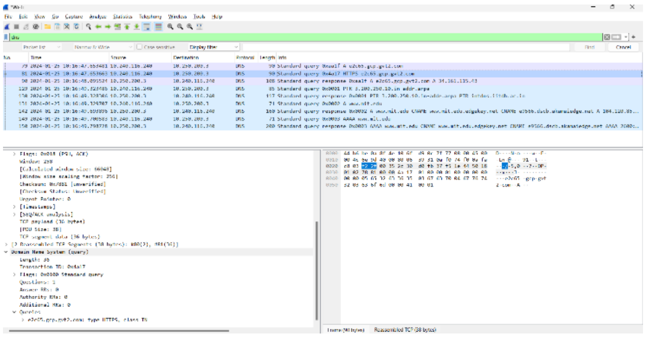
```
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: UDP (17)
    Header Checksum: 0x63c8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.250.200.3
    Destination Address: 10.200.252.96
> User Datagram Protocol, Src Port: 53, Dst Port: 49264
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
```

```
0000  10 6f d9 0c 7f 77 f8 7a  41 13 2a c2 08 00 45 00   ·o···w·z A·*···E·
0010  00 ba fd 44 40 00 3f 11  63 c8 0a fa c8 03 0a c8   ···D@·?· c·······
0020  fc 60 00 35 c0 70 00 a6  e1 6f 00 03 81 80 00 01   ·`·5·p·· ·o······
0030  00 04 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 1c 00 01 c0  0c 00 05 00 01 00 00 02   du······ ········
0050  10 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ····www· mit·edu·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey· net··)··
0070  00 01 00 00 00 29 00 18  05 65 39 35 36 36 04 64   ·····)·· ·e9566·d
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 c0 3d   scb·akam aiedge·=
0090  c0 4e 00 1c 00 01 00 00  00 14 00 10 26 00 14 17   ·N······ ····&···
00a0  00 75 0c a6 00 00 00 00  00 00 25 5e c0 4e 00 1c   ·u······ ··%^·N··
00b0  00 01 00 00 00 14 00 10  26 00 14 17 00 75 0c 8b   ········ &····u··
00c0  00 00 00 00 00 00 25 5e                            ······%^
```

2. Destination IP is 10.250.200.3 ,Yes this is the IP of my default local DNS server.

3. Destination Port for DNS Query Message: 10.240.200.3

4. This is Type A Query and the Query message contains no answers.



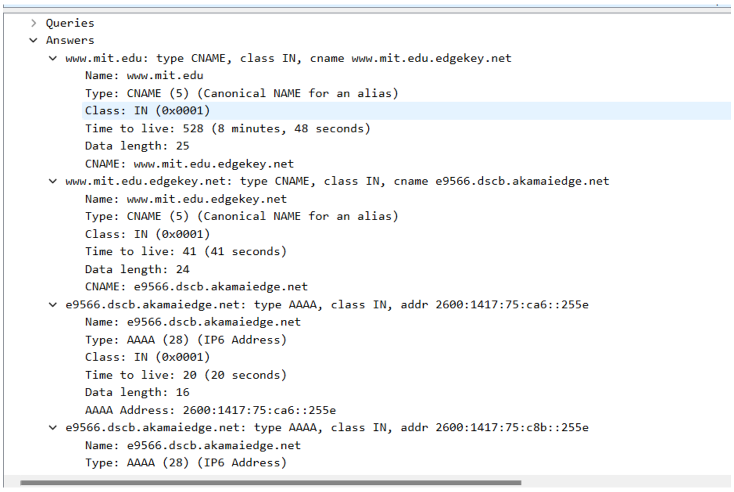
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

```
dns
No.   Time                        Source          Destination     Protocol Length Info
   79 2024-01-25 10:16:47.653481 10.240.116.240  10.250.200.3    DNS        90 Standard query 0xaa1f A e2c65.gcp.gvt2.com
   81 2024-01-25 10:16:47.653663 10.240.116.240  10.250.200.3    DNS        90 Standard query 0x4a17 HTTPS e2c65.gcp.gvt2.com
   90 2024-01-25 10:16:48.095524 10.250.200.3    10.240.116.240  DNS       106 Standard query response 0xaa1f A e2c65.gcp.gvt2.com A 34.161.115.43
  129 2024-01-25 10:16:49.323486 10.240.116.240  10.250.200.3    DNS        85 Standard query 0x0001 PTR 3.200.250.10.in-addr.arpa
  130 2024-01-25 10:16:49.328786 10.250.200.3    10.240.116.240  DNS       117 Standard query response 0x0001 PTR 3.200.250.10.in-addr.arpa PTR intdns.iitdh.ac.in
  131 2024-01-25 10:16:49.329787 10.240.116.240  10.250.200.3    DNS        71 Standard query 0x0002 A www.mit.edu
  142 2024-01-25 10:16:49.699896 10.250.200.3    10.240.116.240  DNS       160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.120.85…
  149 2024-01-25 10:16:49.700583 10.240.116.240  10.250.200.3    DNS        71 Standard query 0x0003 AAAA www.mit.edu
  150 2024-01-25 10:16:49.798726 10.250.200.3    10.240.116.240  DNS       200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:…
```

```
  > Flags: 0x018 (PSH, ACK)
    Window: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0x7881 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (36 bytes)
    [PDU Size: 38]
    TCP segment data (36 bytes)
> [2 Reassembled TCP Segments (38 bytes): #80(2), #81(36)]
v Domain Name System (query)
    Length: 36
    Transaction ID: 0x4a17
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > e2c65.gcp.gvt2.com: type HTTPS, class IN
```

Frame (90 bytes)   Reassembled TCP (38 bytes)

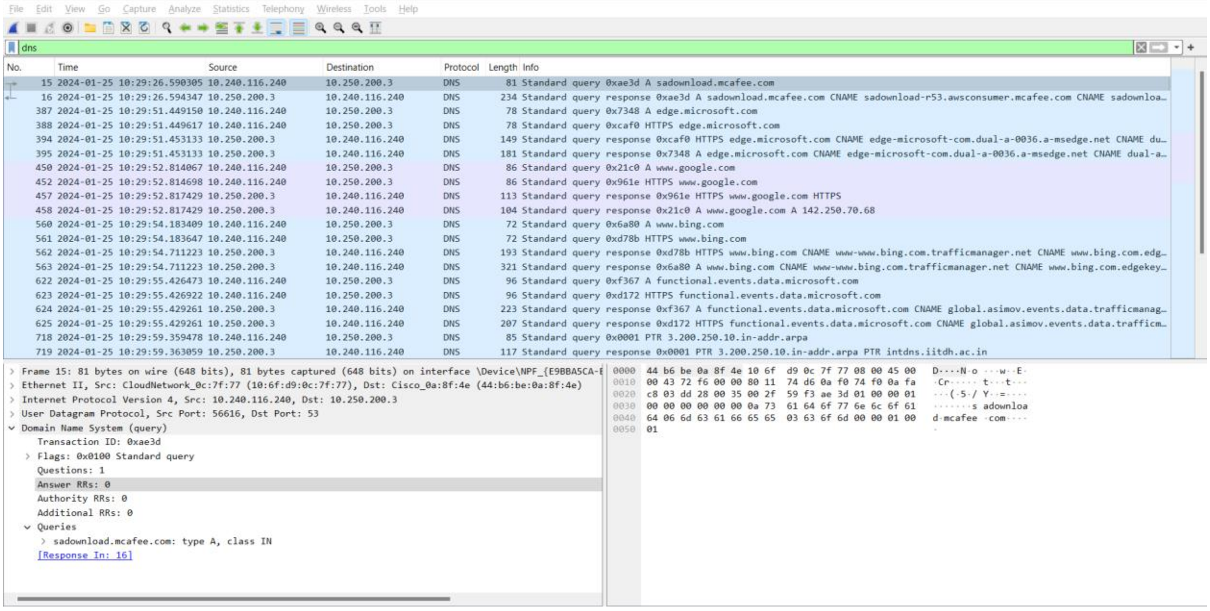
5. There are four answers two are Canonical and two are type A which is attached in screenshot below. Each contains name,type,class,TTL,Data Length and CNAME/AAAA Address as per the Type of packet.



```
  > Queries
  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: 528 (8 minutes, 48 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: 41 (41 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    v e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:75:ca6::255e
        Name: e9566.dscb.akamaiedge.net
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 16
        AAAA Address: 2600:1417:75:ca6::255e
    v e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:75:c8b::255e
        Name: e9566.dscb.akamaiedge.net
        Type: AAAA (28) (IP6 Address)
```

2.

1. The DNS Query message is sent to 10.250.200.3, same as my local server address.

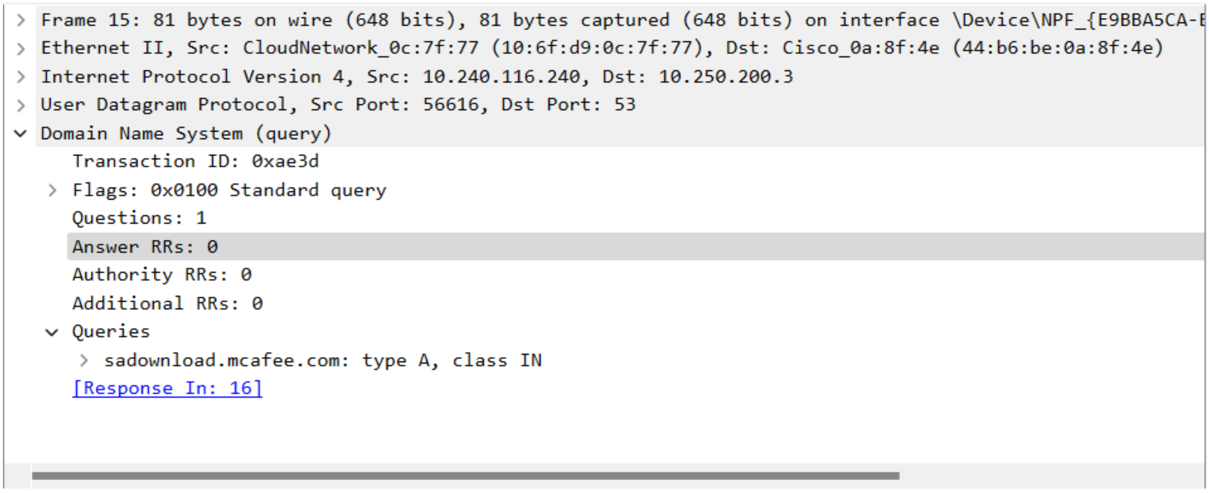

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

No.	Time	Source	Destination	Protocol	Length	Info
15	2024-01-25 10:29:26.590305	10.240.116.240	10.250.200.3	DNS	81	Standard query 0xae3d A sadownload.mcafee.com
16	2024-01-25 10:29:26.594347	10.250.200.3	10.240.116.240	DNS	234	Standard query response 0xae3d A sadownload.mcafee.com CNAME sadownload-r53.awsconsumer.mcafee.com CNAME sadownloa…
387	2024-01-25 10:29:51.449150	10.240.116.240	10.250.200.3	DNS	78	Standard query 0x7348 A edge.microsoft.com
388	2024-01-25 10:29:51.449617	10.240.116.240	10.250.200.3	DNS	78	Standard query 0xcaf0 HTTPS edge.microsoft.com
394	2024-01-25 10:29:51.453133	10.250.200.3	10.240.116.240	DNS	149	Standard query response 0xcaf0 HTTPS edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME du…
395	2024-01-25 10:29:51.453133	10.250.200.3	10.240.116.240	DNS	181	Standard query response 0x7348 A edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a…
450	2024-01-25 10:29:52.814067	10.240.116.240	10.250.200.3	DNS	86	Standard query 0x21c0 A www.google.com
452	2024-01-25 10:29:52.814698	10.240.116.240	10.250.200.3	DNS	86	Standard query 0x961e HTTPS www.google.com
457	2024-01-25 10:29:52.817429	10.250.200.3	10.240.116.240	DNS	113	Standard query response 0x961e HTTPS www.google.com HTTPS
458	2024-01-25 10:29:52.817429	10.250.200.3	10.240.116.240	DNS	104	Standard query response 0x21c0 A www.google.com A 142.250.70.68
560	2024-01-25 10:29:54.183409	10.240.116.240	10.250.200.3	DNS	72	Standard query 0x6a80 A www.bing.com
561	2024-01-25 10:29:54.183647	10.240.116.240	10.250.200.3	DNS	72	Standard query 0xd78b HTTPS www.bing.com
562	2024-01-25 10:29:54.711223	10.250.200.3	10.240.116.240	DNS	193	Standard query response 0xd78b HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edg…
563	2024-01-25 10:29:54.711223	10.250.200.3	10.240.116.240	DNS	321	Standard query response 0x6a80 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey…
622	2024-01-25 10:29:55.426473	10.240.116.240	10.250.200.3	DNS	96	Standard query 0xf367 A functional.events.data.microsoft.com
623	2024-01-25 10:29:55.426922	10.240.116.240	10.250.200.3	DNS	96	Standard query 0xd172 HTTPS functional.events.data.microsoft.com
624	2024-01-25 10:29:55.429261	10.250.200.3	10.240.116.240	DNS	223	Standard query response 0xf367 A functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanag…
625	2024-01-25 10:29:55.429261	10.250.200.3	10.240.116.240	DNS	207	Standard query response 0xd172 HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficm…
718	2024-01-25 10:29:59.359478	10.240.116.240	10.250.200.3	DNS	85	Standard query 0x0001 PTR 3.200.250.10.in-addr.arpa
719	2024-01-25 10:29:59.363059	10.250.200.3	10.240.116.240	DNS	117	Standard query response 0x0001 PTR 3.200.250.10.in-addr.arpa PTR intdns.iitdh.ac.in

```
> Frame 15: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{E9BBA5CA-E
> Ethernet II, Src: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
> Internet Protocol Version 4, Src: 10.240.116.240, Dst: 10.250.200.3
> User Datagram Protocol, Src Port: 56616, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xae3d
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > sadownload.mcafee.com: type A, class IN
    [Response In: 16]
```

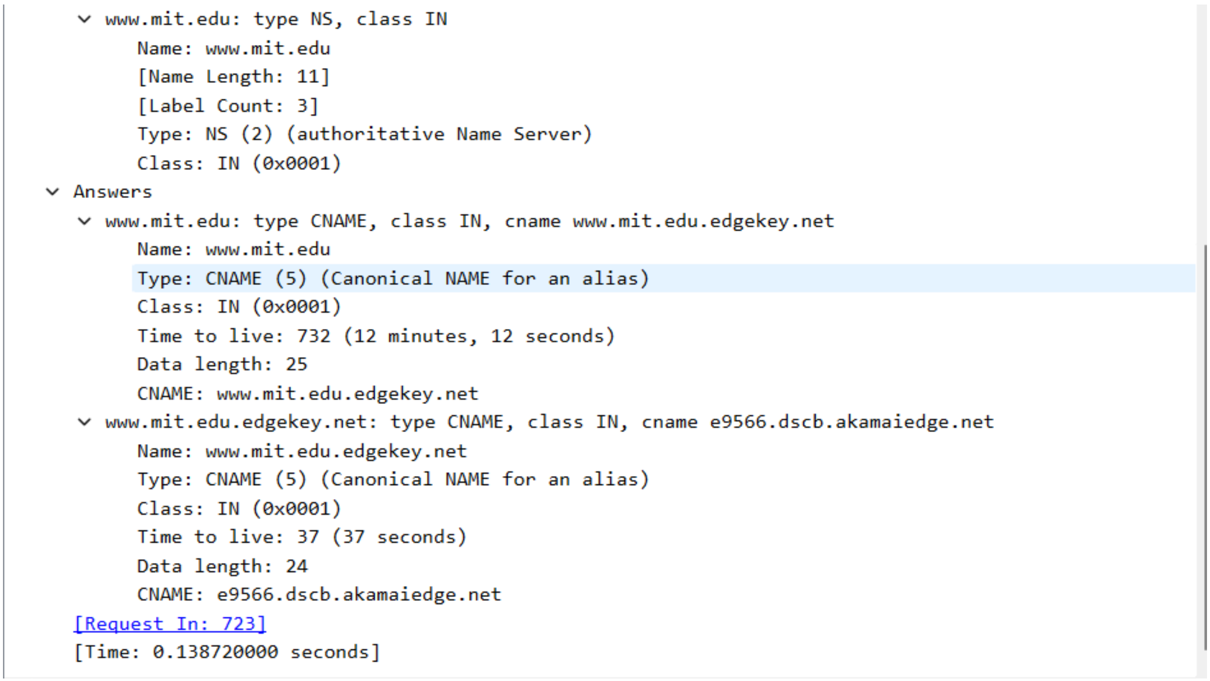
```
0000  44 b6 be 0a 8f 4e 10 6f  d9 0c 7f 77 08 00 45 00   D····N·o ···w··E·
0010  00 43 72 f6 00 00 80 11  74 d6 0a f0 74 f0 0a fa   ·Cr····· t···t···
0020  c8 03 dd 28 00 35 00 2f  59 f3 ae 3d 01 00 00 01   ···(·5·/ Y··=····
0030  00 00 00 00 00 00 0a 73  61 64 6f 77 6e 6c 6f 61   ·······s adownloa
0040  64 06 6d 63 61 66 65 65  03 63 6f 6d 00 00 01 00   d·mcafee ·com····
0050  01                                                 ·
```

2. The type of query is A. There are no answers in query message.

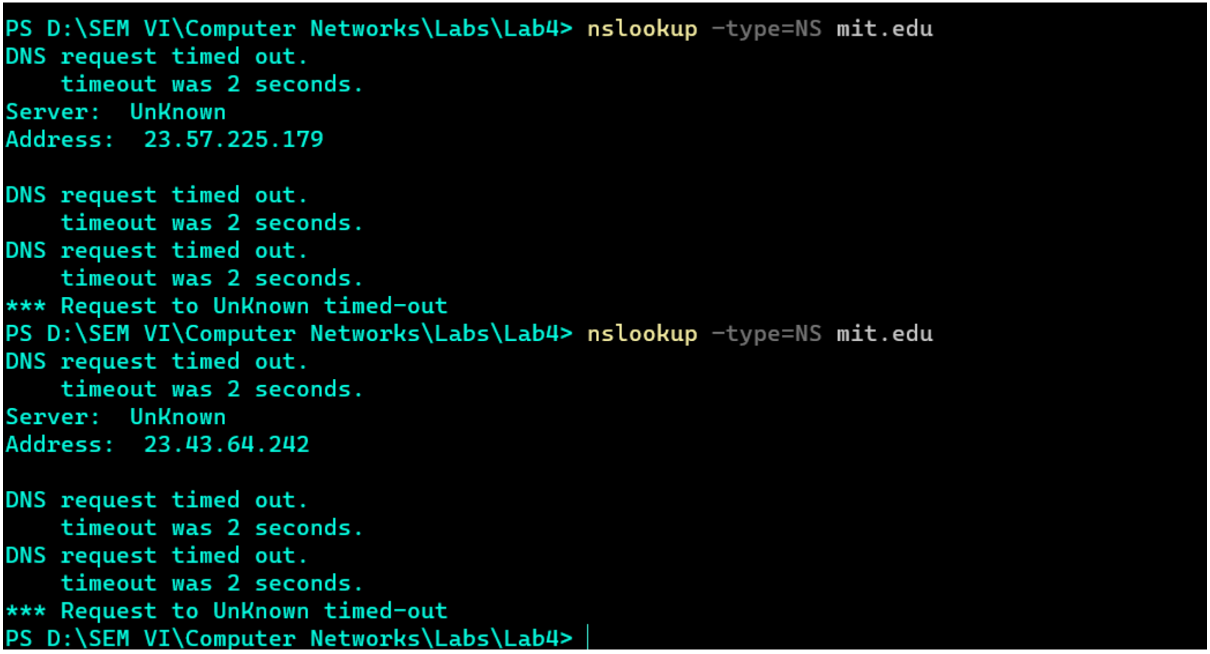


```
> Frame 15: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{E9BBA5CA-E
> Ethernet II, Src: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
> Internet Protocol Version 4, Src: 10.240.116.240, Dst: 10.250.200.3
> User Datagram Protocol, Src Port: 56616, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xae3d
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > sadownload.mcafee.com: type A, class IN
    [Response In: 16]
```

3. I could not find any MIT nameservers here, to verify this I have attached the screenshots also.



```
    ⌄ www.mit.edu: type NS, class IN
          Name: www.mit.edu
          [Name Length: 11]
          [Label Count: 3]
          Type: NS (2) (authoritative Name Server)
          Class: IN (0x0001)
  ⌄ Answers
    ⌄ 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: 732 (12 minutes, 12 seconds)
          Data length: 25
          CNAME: www.mit.edu.edgekey.net
    ⌄ 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: 37 (37 seconds)
          Data length: 24
          CNAME: e9566.dscb.akamaiedge.net
  [Request In: 723]
  [Time: 0.138720000 seconds]
```



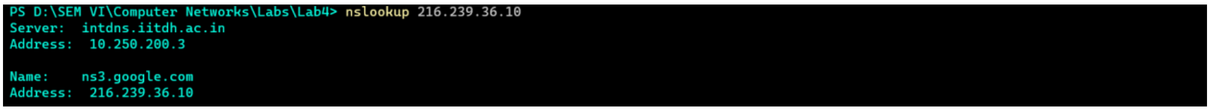
```
PS D:\SEM VI\Computer Networks\Labs\Lab4> nslookup -type=NS mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  23.57.225.179

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS D:\SEM VI\Computer Networks\Labs\Lab4> nslookup -type=NS mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  23.43.64.242

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
PS D:\SEM VI\Computer Networks\Labs\Lab4>
```

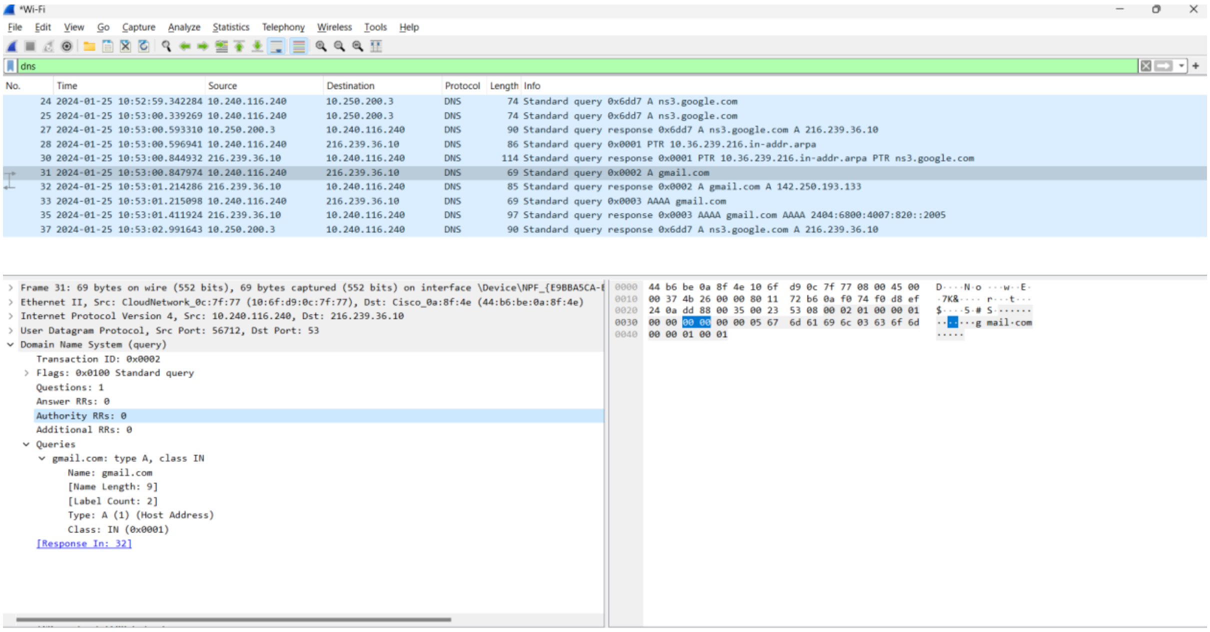
3.

1. Destination IP Address = 216.239.36.10 This is not the IP Address of my default DNS nameserver. This is because we have queried for specific DNS server given in question. After using nslookup to look for server name using this ip we get the server name as ns3.google.com itself this verifies our onservation.



```
PS D:\SEM VI\Computer Networks\Labs\Lab4> nslookup 216.239.36.10
Server:  intdns.iitdh.ac.in
Address:  10.250.200.3

Name:    ns3.google.com
Address:  216.239.36.10
```



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

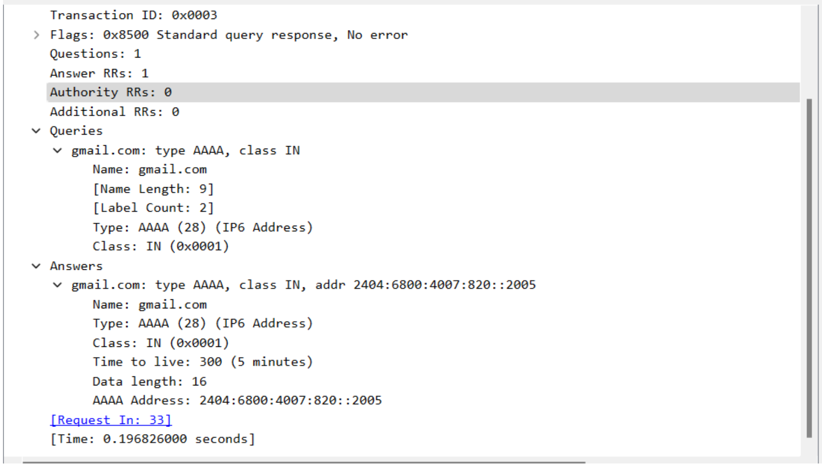
```
No.  Time                        Source          Destination     Protocol Length Info
  24 2024-01-25 10:52:59.342284 10.240.116.240  10.250.200.3    DNS       74 Standard query 0x6dd7 A ns3.google.com
  25 2024-01-25 10:53:00.339269 10.240.116.240  10.250.200.3    DNS       74 Standard query 0x6dd7 A ns3.google.com
  27 2024-01-25 10:53:00.593310 10.250.200.3    10.240.116.240  DNS       90 Standard query response 0x6dd7 A ns3.google.com A 216.239.36.10
  28 2024-01-25 10:53:00.596941 10.240.116.240  216.239.36.10   DNS       86 Standard query 0x0001 PTR 10.36.239.216.in-addr.arpa
  30 2024-01-25 10:53:00.844932 216.239.36.10   10.240.116.240  DNS      114 Standard query response 0x0001 PTR 10.36.239.216.in-addr.arpa PTR ns3.google.com
  31 2024-01-25 10:53:00.847974 10.240.116.240  216.239.36.10   DNS       69 Standard query 0x0002 A gmail.com
  32 2024-01-25 10:53:01.214286 216.239.36.10   10.240.116.240  DNS       85 Standard query response 0x0002 A gmail.com A 142.250.193.133
  33 2024-01-25 10:53:01.215098 10.240.116.240  216.239.36.10   DNS       69 Standard query 0x0003 AAAA gmail.com
  35 2024-01-25 10:53:01.411924 216.239.36.10   10.240.116.240  DNS       97 Standard query response 0x0003 AAAA gmail.com AAAA 2404:6800:4007:820::2005
  37 2024-01-25 10:53:02.991643 10.250.200.3    10.240.116.240  DNS       90 Standard query response 0x6dd7 A ns3.google.com A 216.239.36.10
```

```
> Frame 31: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{E9BBA5CA-E
> Ethernet II, Src: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
> Internet Protocol Version 4, Src: 10.240.116.240, Dst: 216.239.36.10
> User Datagram Protocol, Src Port: 56712, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v gmail.com: type A, class IN
        Name: gmail.com
        [Name Length: 9]
        [Label Count: 2]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 32]
```

```
0000  44 b6 be 0a 8f 4e 10 6f  d9 0c 7f 77 08 00 45 00   D····N·o ···w··E·
0010  00 37 4b 26 00 00 80 11  72 b6 0a f0 74 f0 d8 ef   ·7K&···· r···t···
0020  24 0a dd 88 00 35 00 23  53 08 00 02 01 00 00 01   $····5·# S·······
0030  00 00 00 00 00 00 05 67  6d 61 69 6c 03 63 6f 6d   ·······g mail·com
0040  00 00 01 00 01                                     ·····
```

2. Type is Type A Query and it contains no answers.

3. There is one answer with the following fields(Name,Type,Class,TTL,Data, AAAA Address) as per the screenshot below.



```
    Transaction ID: 0x0003
  > Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v gmail.com: type AAAA, class IN
        Name: gmail.com
        [Name Length: 9]
        [Label Count: 2]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  v Answers
    v gmail.com: type AAAA, class IN, addr 2404:6800:4007:820::2005
        Name: gmail.com
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 16
        AAAA Address: 2404:6800:4007:820::2005
    [Request In: 33]
    [Time: 0.196826000 seconds]
```

I have attached screenshots for questions separately so the questions which ask to add screenshots I have no written(not repeated the screenshots.)