CS-315 COMPUTER NETWORKS LAB-4

PART-1

1. IP address of web server: 10.250.200.3,
   IP address of www.iitdh.ac.in : 10.195.250.62

```
PS C:\Users\pavan> 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. There are 4 DNS servers for google

```
PS C:\Users\pavan> nslookup -type=NS google.com
Server:  intdns.iitdh.ac.in
Address:  10.250.200.3

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

3. IPv4 address: 142.250.193.133,
   IPv6 address: 2404:6800:4007:820::2005

```
PS C:\Users\pavan> 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
```

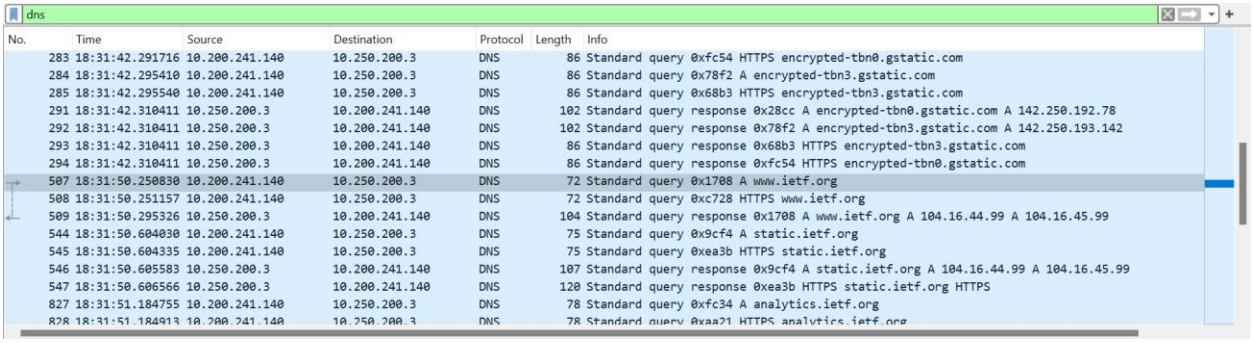
PART-2

```
PS C:\Users\pavan> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

PART-3



dns

No.	Time	Source	Destination	Protocol	Length	Info
283	18:31:42.291716	10.200.241.140	10.250.200.3	DNS	86	Standard query 0xfc54 HTTPS encrypted-tbn0.gstatic.com
284	18:31:42.295410	10.200.241.140	10.250.200.3	DNS	86	Standard query 0x78f2 A encrypted-tbn3.gstatic.com
285	18:31:42.295540	10.200.241.140	10.250.200.3	DNS	86	Standard query 0x68b3 HTTPS encrypted-tbn3.gstatic.com
291	18:31:42.310411	10.250.200.3	10.200.241.140	DNS	102	Standard query response 0x28cc A encrypted-tbn0.gstatic.com A 142.250.192.78
292	18:31:42.310411	10.250.200.3	10.200.241.140	DNS	102	Standard query response 0x78f2 A encrypted-tbn3.gstatic.com A 142.250.193.142
293	18:31:42.310411	10.250.200.3	10.200.241.140	DNS	86	Standard query response 0x68b3 HTTPS encrypted-tbn3.gstatic.com
294	18:31:42.310411	10.250.200.3	10.200.241.140	DNS	86	Standard query response 0xfc54 HTTPS encrypted-tbn0.gstatic.com
507	18:31:50.250830	10.200.241.140	10.250.200.3	DNS	72	Standard query 0x1708 A www.ietf.org
508	18:31:50.251157	10.200.241.140	10.250.200.3	DNS	72	Standard query 0xc728 HTTPS www.ietf.org
509	18:31:50.295326	10.250.200.3	10.200.241.140	DNS	104	Standard query response 0x1708 A www.ietf.org A 104.16.44.99 A 104.16.45.99
544	18:31:50.604030	10.200.241.140	10.250.200.3	DNS	75	Standard query 0x9cf4 A static.ietf.org
545	18:31:50.604335	10.200.241.140	10.250.200.3	DNS	75	Standard query 0xea3b HTTPS static.ietf.org
546	18:31:50.605583	10.250.200.3	10.200.241.140	DNS	107	Standard query response 0x9cf4 A static.ietf.org A 104.16.44.99 A 104.16.45.99
547	18:31:50.606566	10.250.200.3	10.200.241.140	DNS	120	Standard query response 0xea3b HTTPS static.ietf.org HTTPS
827	18:31:51.184755	10.200.241.140	10.250.200.3	DNS	78	Standard query 0xfc34 A analytics.ietf.org
828	18:31:51.184913	10.200.241.140	10.250.200.3	DNS	78	Standard query 0xaa21 HTTPS analytics.ietf.org

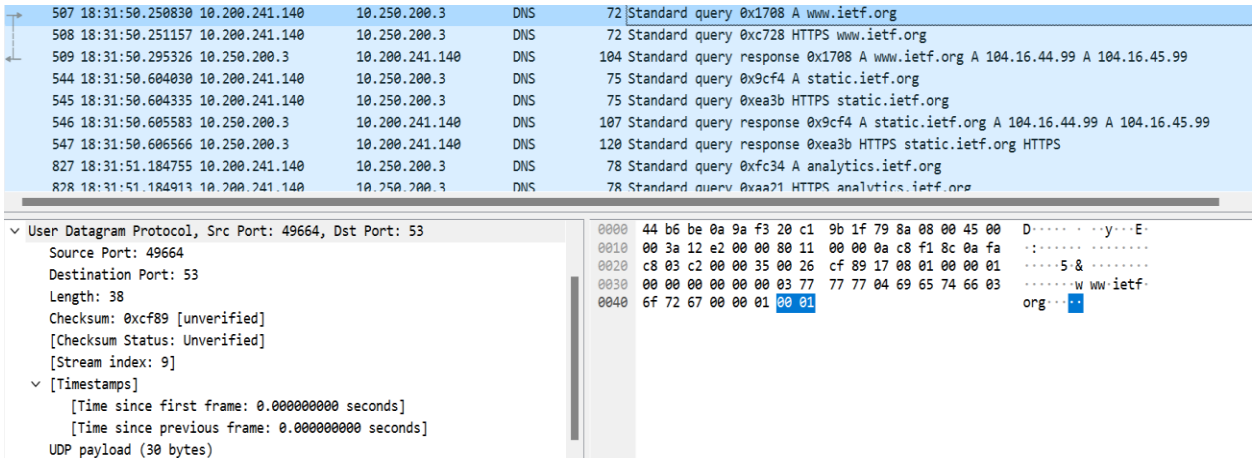
1. Packet No. : 283, 284, 285, 507, 508, 544, 545 are Query messages

   Packet No. : 291, 292, 293, 294, 509, 546, 547 are Response messages

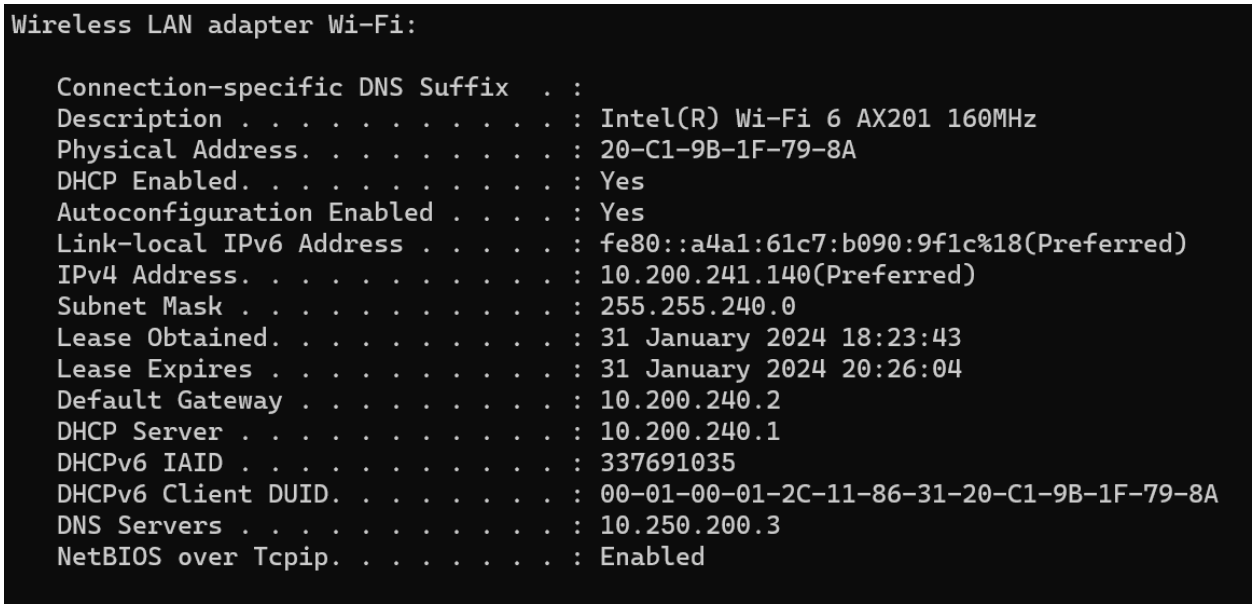
   ```
   ▾ User Datagram Protocol, Src Port: 58186, Dst Port: 53
       Source Port: 58186
       Destination Port: 53
       Length: 54
       Checksum: 0xcf99 [unverified]
       [Checksum Status: Unverified]
       [Stream index: 0]
     ▾ [Timestamps]
           [Time since first frame: 0.000000000 seconds]
           [Time since previous frame: 0.000000000 seconds]
       UDP payload (46 bytes)
   ```

   The packets are sent over UDP
2. Destination port: 53(& Source port: 49664) for Query message,

Source port: 53(& Destination port: 49664) for Response message



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



We can see DNS server as 10.250.200.3 from above. So, Yes, these two IP addresses are same.

4. DNS query Type : A, It does not contain any answers

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  [Response In: 509]
```

5. Two answers are provided. The answers contain: Name(www.ietf.org), Type(A), Class(IN), Time to live(300), Data length(4), Address(104.16.44.99)

```
Answers
  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
  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
  [Request In: 507]
  [Time: 0.044496000 seconds]
```

6. The destination address of the TCP SYN packet sent by the host is 104.16.44.99 . This address corresponds to the address in the Answers field in DNS message (from above screenshot).

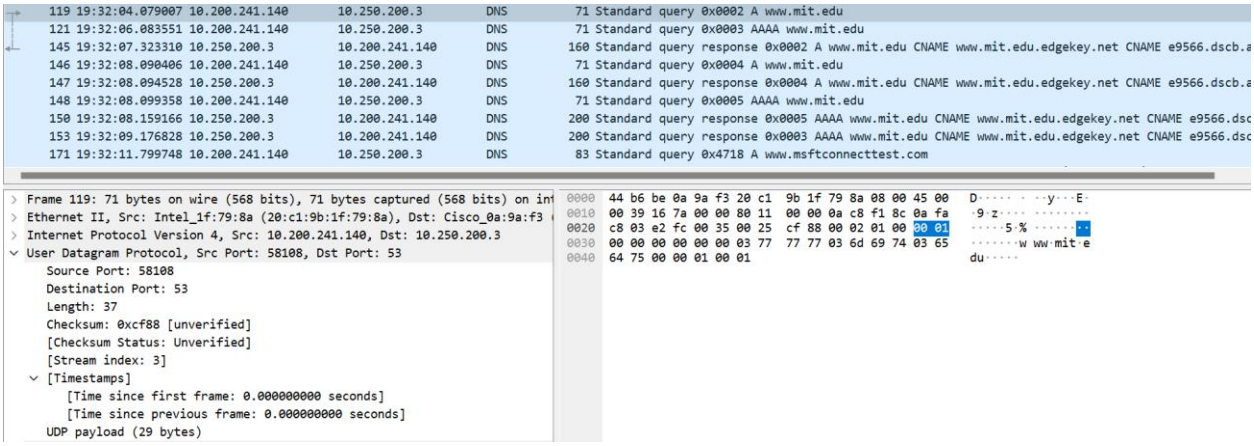
832 18:31:51.186100 10.200.241.140	104.16.44.99	TCP	66 50413 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

7. No, as we can see no DNS packets for retrieving images in the packet viewing list.

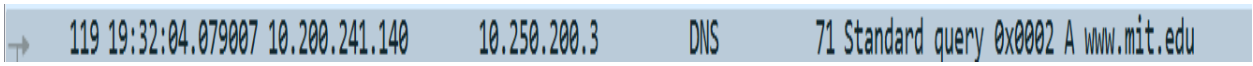
PART-4

(1)

1. Destination port: 53(& Source port: 58108) for Query message,
   Source port: 53(& Destination port: 58108) for Response message



2. The DNS query is sent to IP address : 10.250.200.3




```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 20-C1-9B-1F-79-8A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4a1:61c7:b090:9f1c%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.241.140(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : 31 January 2024 18:23:43
   Lease Expires . . . . . . . . . . : 31 January 2024 20:26:04
   Default Gateway . . . . . . . . . : 10.200.240.2
   DHCP Server . . . . . . . . . . . : 10.200.240.1
   DHCPv6 IAID . . . . . . . . . . . : 337691035
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-11-86-31-20-C1-9B-1F-79-8A
   DNS Servers . . . . . . . . . . . : 10.250.200.3
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

We can see DNS server as 10.250.200.3 from above. So, Yes, these two IP addresses are same.

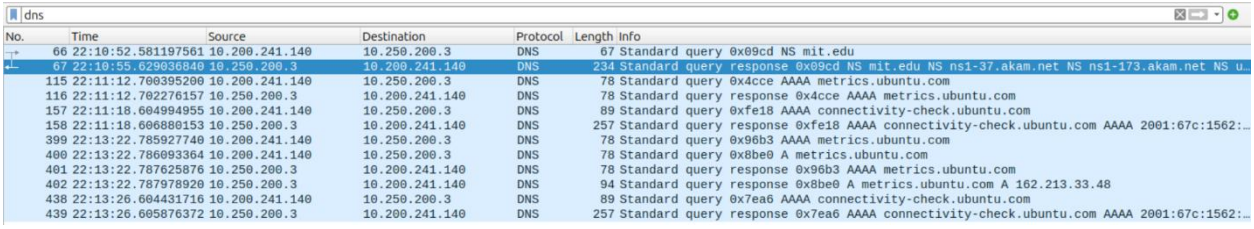
3. DNS Query Type : A, Does not contain any answers.

```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    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)
    [Response In: 145]
```

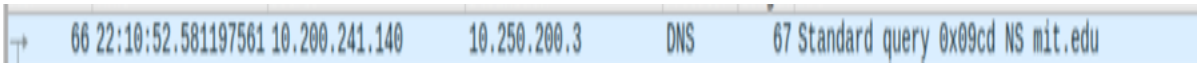
4. Three answers are provided. The answers contain: Name, Type, Class, Time to live, Data length, CNAME/Address
5. Screenshot:

```
        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: 1741 (29 minutes, 1 second)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.aka
      Name: www.mit.edu.edgekey.net
      Type: CNAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 1 (1 second)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 23.47.225.154
      Name: e9566.dscb.akamaiedge.net
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 23.47.225.154
  [Request In: 119]
  [Time: 3.244303000 seconds]
```

(2)



1. IP address: 10.250.200.3

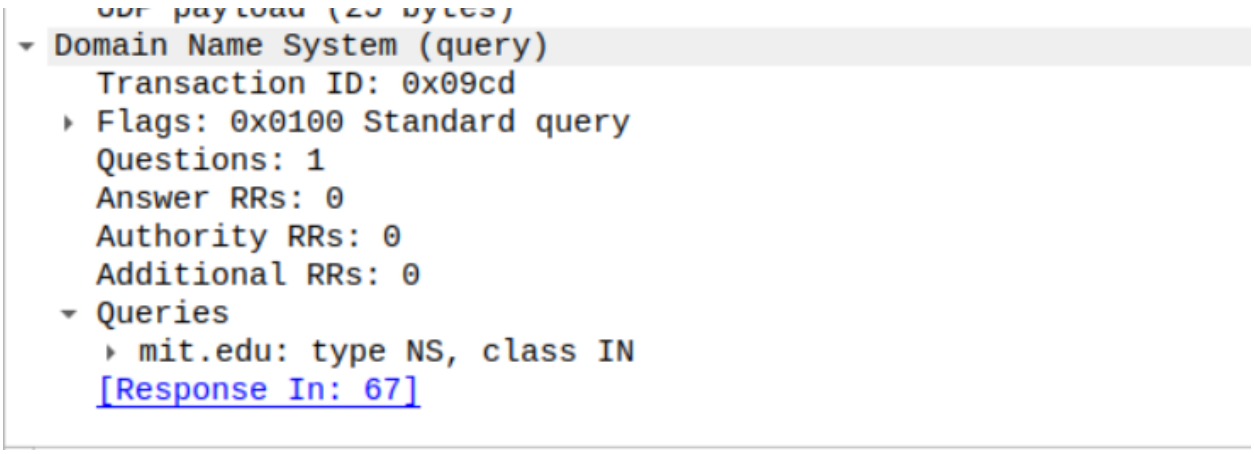



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 20-C1-9B-1F-79-8A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4a1:61c7:b090:9f1c%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.241.140(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : 31 January 2024 18:23:43
   Lease Expires . . . . . . . . . . : 31 January 2024 20:26:04
   Default Gateway . . . . . . . . . : 10.200.240.2
   DHCP Server . . . . . . . . . . . : 10.200.240.1
   DHCPv6 IAID . . . . . . . . . . . : 337691035
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-11-86-31-20-C1-9B-1F-79-8A
   DNS Servers . . . . . . . . . . . : 10.250.200.3
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

We can see DNS server as 10.250.200.3 from above. So, Yes, these two IP addresses are same.

2. DNS query Type: NS, It does not contain any answers



3. The response message provided 8 MIT nameservers – ns1-173.akam.net, use5.akam.net, asia2.akam.net, eur5.akam.net, usw2.akam.net, asia1.akam.net, use2.akam.net; No the response message does not provide the IP addresses of the MIT nameservers.

4. Screenshot:

```
▾ Queries
  ▸ mit.edu: type NS, class IN
▾ Answers
  ▾ mit.edu: type NS, class IN, ns ns1-37.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1505 (25 minutes, 5 seconds)
      Data length: 17
      Name Server: ns1-37.akam.net
  ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
  ▸ mit.edu: type NS, class IN, ns use5.akam.net
  ▸ mit.edu: type NS, class IN, ns asia2.akam.net
  ▸ mit.edu: type NS, class IN, ns eur5.akam.net
  ▸ mit.edu: type NS, class IN, ns usw2.akam.net
  ▸ mit.edu: type NS, class IN, ns asia1.akam.net
  ▸ mit.edu: type NS, class IN, ns use2.akam.net
  [Request In: 66]
  [Time: 3.047839279 seconds]
```

(3)

dns

No.	Time	Source	Destination	Protocol	Length	Info
26	20:01:19.245770	10.250.200.3	10.200.241.140	DNS	192	Standard query response 0xf166 A win-extension.femetrics.grammarly.io A 3.208.125.211 A 54.83
72	20:01:21.175201	10.200.241.140	10.250.200.3	DNS	74	Standard query 0x2a8b A ns3.google.com
73	20:01:21.208072	10.200.241.140	10.250.200.3	DNS	74	Standard query 0x2a8b A ns3.google.com
74	20:01:21.222431	10.250.200.3	10.200.241.140	DNS	90	Standard query response 0x2a8b A ns3.google.com A 216.239.36.10
75	20:01:21.223524	10.250.200.3	10.200.241.140	DNS	90	Standard query response 0x2a8b A ns3.google.com A 216.239.36.10
76	20:01:21.224821	10.200.241.140	216.239.36.10	DNS	86	Standard query 0x0001 PTR 10.36.239.216.in-addr.arpa
77	20:01:21.316203	216.239.36.10	10.200.241.140	DNS	114	Standard query response 0x0001 PTR 10.36.239.216.in-addr.arpa PTR ns3.google.com
78	20:01:21.316777	10.200.241.140	216.239.36.10	DNS	69	Standard query 0x0002 A gmail.com
79	20:01:21.408714	216.239.36.10	10.200.241.140	DNS	85	Standard query response 0x0002 A gmail.com A 142.250.193.133
80	20:01:21.409301	10.200.241.140	216.239.36.10	DNS	69	Standard query 0x0003 AAAA gmail.com
81	20:01:21.499896	216.239.36.10	10.200.241.140	DNS	97	Standard query response 0x0003 AAAA gmail.com AAAA 2404:6800:4007:820::2005
89	20:01:22.242382	10.250.200.3	10.200.241.140	DNS	192	Standard query response 0xf166 A win-extension.femetrics.grammarly.io A 52.201.207.25 A 54.83
240	20:01:32.470310	10.200.241.140	10.250.200.3	DNS	83	Standard query 0x042d A www.msftconnecttest.com
241	20:01:32.474129	10.250.200.3	10.200.241.140	DNS	227	Standard query response 0x042d A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CN

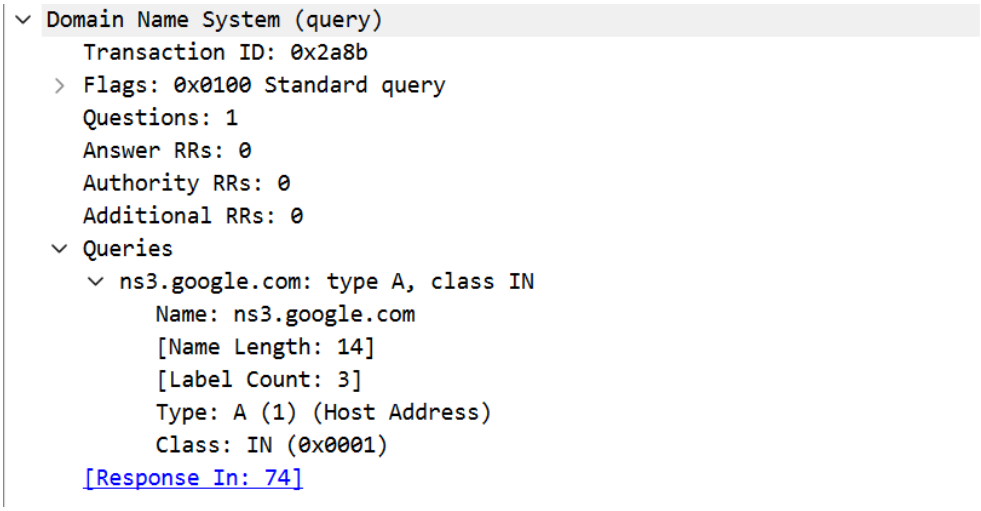
1. 72 20:01:21.175201 10.200.241.140 10.250.200.3 DNS 74 Standard query 0x2a8b A ns3.google.com

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 20-C1-9B-1F-79-8A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4a1:61c7:b090:9f1c%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.241.140(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : 31 January 2024 18:23:43
   Lease Expires . . . . . . . . . . : 31 January 2024 20:26:04
   Default Gateway . . . . . . . . . : 10.200.240.2
   DHCP Server . . . . . . . . . . . : 10.200.240.1
   DHCPv6 IAID . . . . . . . . . . . : 337691035
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-11-86-31-20-C1-9B-1F-79-8A
   DNS Servers . . . . . . . . . . . : 10.250.200.3
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

We can see DNS server as 10.250.200.3 from above. So, Yes, these two IP addresses are same.

2. DNS Query Type: A, Does not contain any answers



3. 1 answer is provided. It contains Name, Type, Class, Time to live, Data length, Address.
4. Screenshot:

```
Queries
    ns3.google.com: type A, class IN
        Name: ns3.google.com
        [Name Length: 14]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
Answers
    ns3.google.com: type A, class IN, addr 216.239.36.10
        Name: ns3.google.com
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 339414 (3 days, 22 hours, 16 minutes, 54 seconds)
        Data length: 4
        Address: 216.239.36.10
    [Request In: 72]
    [Time: 0.047230000 seconds]
```