

Computer Networks Lab

ASSIGNMENT – 4

Rahul Cheryala, 210010012

PART – 1

1.

```
PS C:\Users\Rahul\Documents\SEM-6\COMPUTER_NETWORKS\CN lab\Lab_4> 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
```

IP Address of **DNS** server – 10.250.200.3

IP Address of **Web** server – 10.195.250.62

2.

```
PS C:\Users\Rahul\Documents\SEM-6\COMPUTER_NETWORKS\CN lab\Lab_4> nslookup google.com
Server:   intdns.iitdh.ac.in
Address:  10.250.200.3

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:     google.com
Address:  172.217.27.206
```

3.

```
PS C:\Users\Rahul\Documents\SEM-6\COMPUTER_NETWORKS\CN lab\Lab_4> nslookup gmail.com
Server:   intdns.iitdh.ac.in
Address:  10.250.200.3

Non-authoritative answer:
Name:     gmail.com
Addresses: 2404:6800:4009:828::2005
          142.250.193.133
```

IPV4 – 142.250.193.133

IPV6 – 2404:6800:4809:828::2005

PART – 2

```
PS C:\Users\Rahul\Documents\SEM-6\COMPUTER_NETWORKS\CN lab\Lab_4> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

PART – 3

No.	dns	Source	Destination	Protocol	Length	Info
27	Standard query 0xc4a A www.ietf.org	10.250.200.3	10.240.117.85	DNS	72	Standard query 0xc4a A www.ietf.org
28	Standard query response 0xc4a A www.ietf.org	10.240.117.85	10.250.200.3	DNS	104	Standard query response 0xc4a A www.ietf.org A 104.16.45.99 A 104.16.44.99
29	Standard query 0xe78d A www.ietf.org	10.250.200.3	10.240.117.85	DNS	72	Standard query 0xe78d A www.ietf.org
30	Standard query response 0xe78d A www.ietf.org	10.240.117.85	10.250.200.3	DNS	104	Standard query response 0xe78d A www.ietf.org A 104.16.45.99 A 104.16.44.99
66	Standard query 0x5799 A incoming.telemetry.mozilla.org	10.240.117.85	10.250.200.3	DNS	90	Standard query 0x5799 A incoming.telemetry.mozilla.org
67	Standard query response 0x5799 A incoming.telemetry.mozilla.org	10.250.200.3	10.240.117.85	DNS	165	Standard query response 0x5799 A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com
69	Standard query 0x842b AAAA telemetry-incoming.r53-2.services.mozilla.com	10.240.117.85	10.250.200.3	DNS	105	Standard query 0x842b AAAA telemetry-incoming.r53-2.services.mozilla.com
70	Standard query response 0x842b AAAA telemetry-incoming.r53-2.services.mozilla.com	10.250.200.3	10.240.117.85	DNS	105	Standard query response 0x842b AAAA telemetry-incoming.r53-2.services.mozilla.com

1.

DNS query messages – 27, 29, 66, 69

DNS query response – 28, 30, 67, 70

```
Frame 27: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}, id 0
Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
Internet Protocol Version 4, Src: 10.240.117.85, Dst: 10.250.200.3
User Datagram Protocol, Src Port: 58218, Dst Port: 53
  Source Port: 58218
  Destination Port: 53
  Length: 38
  Checksum: 0xd72f [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
  UDP payload (30 bytes)
  Domain Name System (query)
```

All the DNS query messages and response are sent over **UDP**

2.

Destination Port – **53**

Source Port – **58218**

DNS query message - (frame 27)

```
▶ Frame 27: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}, id 0
▶ Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
▶ Internet Protocol Version 4, Src: 10.240.117.85, Dst: 10.250.200.3
▼ User Datagram Protocol, Src Port: 58218, Dst Port: 53
    Source Port: 58218
    Destination Port: 53
    Length: 38
    Checksum: 0xd72f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    ▶ [Timestamps]
    UDP payload (30 bytes)
▶ Domain Name System (query)
```

DNS query response - (frame 28)

```
▶ Frame 28: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}, id 0
▶ Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d)
▶ Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.117.85
▼ User Datagram Protocol, Src Port: 53, Dst Port: 58218
    Source Port: 53
    Destination Port: 58218
    Length: 70
    Checksum: 0xaa0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    ▶ [Timestamps]
    UDP payload (62 bytes)
▶ Domain Name System (response)
```

3.

```
▶ Frame 27: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}, id 0
▶ Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
▼ Internet Protocol Version 4, Src: 10.240.117.85, Dst: 10.250.200.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0xd9f4 (55796)
    ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xd7c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.240.117.85
    Destination Address: 10.250.200.3
▶ User Datagram Protocol, Src Port: 58218, Dst Port: 53
▶ Domain Name System (query)
```

The IP address of the DNS query message – **10.250.200.3**

IP address of the local DNS server – **10.250.200.3**

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . : 
Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Physical Address. . . . . : 48-E7-DA-0D-70-4D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c174:cf7e:9c49:6461%16(Preferred)
IPv4 Address. . . . . : 10.240.117.85(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Lease Obtained. . . . . : 25 January 2024 09:05:23
Lease Expires . . . . . : 25 January 2024 11:37:57
Default Gateway . . . . . : 10.240.116.2
DHCP Server . . . . . : 10.240.116.1
DHCPv6 IAID . . . . . : 172550106
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-BE-5E-DC-04-42-1A-02-43-CF
DNS Servers . . . . . : 10.250.200.3
NetBIOS over Tcpip. . . . . : Enabled

```

4. DNS query message - (frame 27)

```

> Frame 27: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}, id 0
> Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
> Internet Protocol Version 4, Src: 10.240.117.85, Dst: 10.250.200.3
> User Datagram Protocol, Src Port: 58218, Dst Port: 53
< Domain Name System (query)
  Transaction ID: 0xcf4a
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  < Queries
    > www.ietf.org: type A, class IN
    [Response in frame 28]

```

- The **Type** of DNS query message is “**A**”
- The query message does not contain any answers regarding itself

5. DNS query response- (frame 28)

```

> Frame 28: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}, id 0
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d)
> Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.117.85
> User Datagram Protocol, Src Port: 53, Dst Port: 58218
< Domain Name System (response)
  Transaction ID: 0xcf4a
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    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
    > www.ietf.org: type A, class IN, addr 104.16.44.99
    [Response in frame 27]
  [Time: 0.003083000 seconds]

```

DNS response message contains 2 answers.

```
▼ 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: 208 (3 minutes, 28 seconds)
    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: 208 (3 minutes, 28 seconds)
    Data length: 4
    Address: 104.16.44.99
  [Request In: 27]
  [Time: 0.003083000 seconds]
```

6.

```
▶ Frame 27: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}, id 0
▶ Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
▶ Internet Protocol Version 4, Src: 10.240.117.85, Dst: 10.250.200.3
▶ User Datagram Protocol, Src Port: 58218, Dst Port: 53
▶ Domain Name System (query)
```

- **Yes**, as seen in the prior screenshot, the destination address is **10.250.200.3** which is the address provided by the DNS server for www.ietf.org.

7. **No**, the images are all loaded from www.ietf.org. So, no additional DNS queries are necessary (the host uses a cached address).

PART – 4

nslookup www.mit.edu

No.	Time	Source	Destination	Protocol	Length	Info
15	2024-01-25 14:37:57.762042	10.240.17.76	10.250.200.3	DNS	85	Standard query 0x0001 PTR 3.200.250.10.in-addr.arpa
16	2024-01-25 14:37:57.762478	10.250.200.3	10.240.17.76	DNS	117	Standard query response 0x0001 PTR 3.200.250.10.in-addr.arpa PTR intdns.iitdh.ac.in
17	2024-01-25 14:37:57.763501	10.240.17.76	10.250.200.3	DNS	71	Standard query 0x0002 A www.mit.edu
40	2024-01-25 14:37:59.764392	10.240.17.76	10.250.200.3	DNS	71	Standard query 0x0003 AAAA www.mit.edu
42	2024-01-25 14:38:00.939951	10.250.200.3	10.240.17.76	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.47.252...
43	2024-01-25 14:38:01.774758	10.240.17.76	10.250.200.3	DNS	71	Standard query 0x0004 A www.mit.edu
44	2024-01-25 14:38:01.775252	10.250.200.3	10.240.17.76	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.47.252...
45	2024-01-25 14:38:01.778303	10.240.17.76	10.250.200.3	DNS	71	Standard query 0x0005 AAAA www.mit.edu
48	2024-01-25 14:38:01.849120	10.250.200.3	10.240.17.76	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 260...
69	2024-01-25 14:38:02.824088	10.250.200.3	10.240.17.76	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 260...

1. DNS query message - (frame 17)

```
▶ Frame 17: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id 0
▶ Ethernet II, Src: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf), Dst: Cisco_0a:9a:e1 (44:b6:be:0a:9a:e1)
▶ Internet Protocol Version 4, Src: 10.240.17.76, Dst: 10.250.200.3
▼ User Datagram Protocol, Src Port: 49810, Dst Port: 53
  Source Port: 49810
  Destination Port: 53
  Length: 37
  Checksum: 0xef6f [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2]
  ▶ [Timestamps]
  UDP payload (29 bytes)
▶ Domain Name System (query)
```

DNS query response - (frame 42)

```
▶ Frame 42: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id 0
▶ Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf)
▶ Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.17.76
▼ User Datagram Protocol, Src Port: 53, Dst Port: 49810
  Source Port: 53
  Destination Port: 49810
  Length: 126
  Checksum: 0xf80f [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2]
  ▶ [Timestamps]
  UDP payload (118 bytes)
▶ Domain Name System (response)
```

Source port – **49810**

Destination port – **53**

2. From the prior screenshot we can see

IP address to which the query message is sent – **10.250.200.3**

IP address of the local DNS server – **10.250.200.3**

```
PS C:\Users\Rahul\Documents\SEM-6\COMPUTER_NETWORKS\CN lab\lab_4\Screenshots\part-4\1> nslookup www.mit.edu
Server:   intdns.iitdh.ac.in
Address:  10.250.200.3

Non-authoritative answer:
Name:     e9566.dscb.akamaiedge.net
Addresses: 2600:1417:75:ca6::255e
          2600:1417:75:c8b::255e
          23.47.252.248
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

3. DNS query message - (frame 17)

```
> Frame 17: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id 0
> Ethernet II, Src: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf), Dst: Cisco_0a:9a:e1 (44:b6:be:0a:9a:e1)
> Internet Protocol Version 4, Src: 10.240.17.76, Dst: 10.250.200.3
> User Datagram Protocol, Src Port: 49810, Dst Port: 53
< 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 4s)]
```

- The **Type** of DNS query message is “A”
- The query message does not contain any answers regarding itself

4. DNS query response - (frame 42)

```
> Frame 42: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id 0
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf)
> Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.17.76
> User Datagram Protocol, Src Port: 53, Dst Port: 49810
< Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  < Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.47.252.248
  [Time: 3.176450000 seconds]
```

```
▼ 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: 131 (2 minutes, 11 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: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  ▼ 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
[Request ID: 171]
[Time: 3.176450000 seconds]
```

Three answers (resource records) were produced in the query response, two corresponding to CNAME's and one host address.

nslookup -type=NS mit.edu

No.	Time	Source	Destination	Protocol	Length	Info
13	2024-01-31 13:34:20.667104	10.240.17.76	10.250.200.3	DNS	85	Standard query 0x0001 PTR 3.200.250.10.in-addr.arpa
15	2024-01-31 13:34:20.667926	10.240.17.76	10.250.200.3	DNS	71	Standard query 0x0002 NS www.mit.edu
14	2024-01-31 13:34:20.667277	10.250.200.3	10.240.17.76	DNS	117	Standard query response 0x0001 PTR 3.200.250.10.in-addr.arpa PTR intdns.iitdh.ac.in
16	2024-01-31 13:34:20.668094	10.250.200.3	10.240.17.76	DNS	144	Standard query response 0x0002 NS www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net

1. From the above screenshot we can see

IP address to which the query message is sent – **10.250.200.3**

IP address of the local DNS server – **10.250.200.3**

```
Connection-specific DNS Suffix . : 
Description . . . . . : Realtek Gaming GbE Family Controller
Physical Address. . . . . : 04-42-1A-02-43-CF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::9cb4:15a2:d16e:7d6b%13(Preferred)
IPv4 Address. . . . . : 10.240.17.76(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Lease Obtained. . . . . : 31 January 2024 11:54:07
Lease Expires . . . . . : 31 January 2024 15:06:04
Default Gateway . . . . . : 10.240.16.2
DHCP Server . . . . . : 10.240.16.1
DHCPv6 IAID . . . . . : 352600602
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-BE-5E-DC-04-42-1A-02-43-CF
DNS Servers . . . . . : 10.250.200.3
NetBIOS over Tcpip. . . . . : Enabled
```


2. DNS query message - (frame number 7)

```
Frame 7: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id 0
Ethernet II, Src: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf), Dst: Cisco_0a:9a:e1 (44:b6:be:0a:9a:e1)
Internet Protocol Version 4, Src: 10.240.17.76, Dst: 10.250.200.3
User Datagram Protocol, Src Port: 56703, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0001
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    3.200.250.10.in-addr.arpa: type PTR, class IN
    [Response in 8]
```

- The **Type** of DNS query message is “**PTR**”
- The query message does not contain any answers regarding itself

3.

```
PS C:\Users\Rahul\Documents\SEM-6\COMPUTER_NETWORKS\CN lab\lab_4> nslookup -type=NS mit.edu
Server: intdns.iitdh.ac.in
Address: 10.250.200.3

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

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

4.

```
▶ Frame 10: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
▶ Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: ASUSTekCOMPU_
▶ Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.17.76
▶ User Datagram Protocol, Src Port: 53, Dst Port: 56704
▼ Domain Name System (response)
  Transaction ID: 0x0002
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ mit.edu: type NS, class IN
  ▼ Answers
    ▶ mit.edu: type NS, class IN, ns ns1-37.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 asia2.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 usw2.akam.net
    ▶ mit.edu: type NS, class IN, ns eur5.akam.net
  [Request In: 9]
  [Time: 0.000228000 seconds]
```

```
▼ Answers
  ▼ mit.edu: type NS, class IN, ns ns1-37.akam.net
    Name: mit.edu
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 1761 (29 minutes, 21 seconds)
    Data length: 17
    Name Server: ns1-37.akam.net
  ▼ mit.edu: type NS, class IN, ns asia1.akam.net
    Name: mit.edu
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 1761 (29 minutes, 21 seconds)
    Data length: 8
    Name Server: asia1.akam.net
  ▼ mit.edu: type NS, class IN, ns use2.akam.net
    Name: mit.edu
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 1761 (29 minutes, 21 seconds)
    Data length: 7
    Name Server: use2.akam.net
  ▼ mit.edu: type NS, class IN, ns asia2.akam.net
    Name: mit.edu
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 1761 (29 minutes, 21 seconds)
    Data length: 8
    Name Server: asia2.akam.net
```

```
▼ mit.edu: type NS, class IN, ns ns1-173.akam.net
  Name: mit.edu
  Type: NS (2) (authoritative Name Server)
  Class: IN (0x0001)
  Time to live: 1761 (29 minutes, 21 seconds)
  Data length: 10
  Name Server: ns1-173.akam.net
▼ mit.edu: type NS, class IN, ns use5.akam.net
  Name: mit.edu
  Type: NS (2) (authoritative Name Server)
  Class: IN (0x0001)
  Time to live: 1761 (29 minutes, 21 seconds)
  Data length: 7
  Name Server: use5.akam.net
▼ mit.edu: type NS, class IN, ns usw2.akam.net
  Name: mit.edu
  Type: NS (2) (authoritative Name Server)
  Class: IN (0x0001)
  Time to live: 1761 (29 minutes, 21 seconds)
  Data length: 7
  Name Server: usw2.akam.net
▼ mit.edu: type NS, class IN, ns eur5.akam.net
  Name: mit.edu
  Type: NS (2) (authoritative Name Server)
  Class: IN (0x0001)
  Time to live: 1761 (29 minutes, 21 seconds)
  Data length: 7
  Name Server: eur5.akam.net
[Request In: 9]
[Time: 0.000228000 seconds]
```

nslookup gmail.com ns3.google.com

dns							
No.	Time	Source	Destination	Protocol	Length	Info	
260	2024-01-31 14:03:18.857120	10.240.17.76	10.250.200.3	DNS	74	Standard query 0xe470 A ns3.google.com	
261	2024-01-31 14:03:18.896627	10.240.17.76	10.250.200.3	DNS	74	Standard query 0xe470 A ns3.google.com	
262	2024-01-31 14:03:19.899836	10.240.17.76	10.250.200.3	DNS	74	Standard query 0xe470 A ns3.google.com	
263	2024-01-31 14:03:19.948264	10.250.200.3	10.240.17.76	DNS	90	Standard query response 0xe470 A ns3.google.com A 216.239.36.10	
264	2024-01-31 14:03:19.950063	10.240.17.76	216.239.36.10	DNS	86	Standard query 0x0001 PTR 10.36.239.216.in-addr.arpa	
265	2024-01-31 14:03:20.042186	216.239.36.10	10.240.17.76	DNS	114	Standard query response 0x0001 PTR 10.36.239.216.in-addr.arpa PTR ns3.google.com	
266	2024-01-31 14:03:20.043072	10.240.17.76	216.239.36.10	DNS	69	Standard query 0x0002 A gmail.com	
267	2024-01-31 14:03:20.135168	216.239.36.10	10.240.17.76	DNS	85	Standard query response 0x0002 A gmail.com A 142.250.193.133	
268	2024-01-31 14:03:20.135516	10.240.17.76	216.239.36.10	DNS	69	Standard query 0x0003 AAAA gmail.com	
269	2024-01-31 14:03:20.228510	216.239.36.10	10.240.17.76	DNS	97	Standard query response 0x0003 AAAA gmail.com AAAA 2404:6800:4007:820::2005	

1. From the above screenshot we can see

IP address to which the query message is sent – **10.250.200.3**

IP address of the local DNS server – **10.250.200.3**

```
Connection-specific DNS Suffix . : 
Description . . . . . : Realtek Gaming GbE Family Controller
Physical Address. . . . . : 04-42-1A-02-43-CF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::9cb4:15a2:d16e:7d6b%13(Preferred)
IPv4 Address. . . . . : 10.240.17.76(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Lease Obtained. . . . . : 31 January 2024 11:54:07
Lease Expires . . . . . : 31 January 2024 15:06:04
Default Gateway . . . . . : 10.240.16.2
DHCP Server . . . . . : 10.240.16.1
DHCPv6 IAID . . . . . : 352600602
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-BE-5E-DC-04-42-1A-02-43-CF
DNS Servers . . . . . : 10.250.200.3
NetBIOS over Tcpip. . . . . : Enabled
```

2. DNS query message - (frame number 260)

```
▶ Frame 260: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf), Dst: Cisc
▶ Internet Protocol Version 4, Src: 10.240.17.76, Dst: 10.250.200.3
▶ User Datagram Protocol, Src Port: 62957, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0xe470
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ ns3.google.com: type A, class IN
    [Response in: 263]
```

- The **Type** of DNS query message is “**PTR**”

- The query message does not contain any answers regarding itself

3,4 . DNS query response - (frame number 263)

```
▶ Frame 263: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface
▶ Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: ASUSTekCOMPU_02:43:cf
▶ Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.240.17.76
▶ User Datagram Protocol, Src Port: 53, Dst Port: 62957
▼ Domain Name System (response)
  Transaction ID: 0xe470
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▶ Queries
  ▼ 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: 341083 (3 days, 22 hours, 44 minutes, 43 seconds)
      Data length: 4
      Address: 216.239.36.10
    [Request in: 260]
    [Time: 1.091144000 seconds]
```

One answer is produced in the query response, contains Name, Type, Class, Expiry, Data Length, Address.