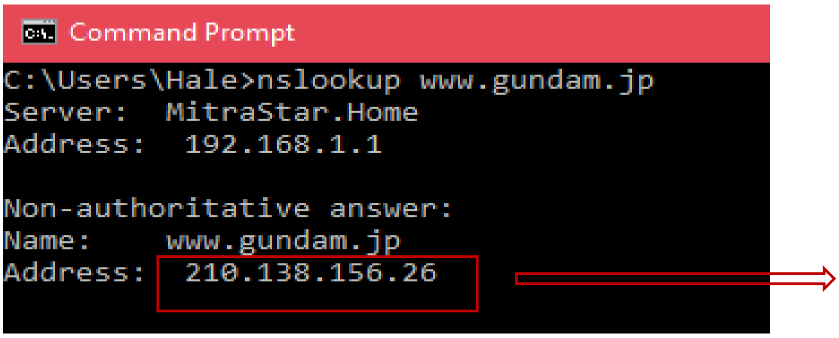
# HOMEWORK 2

**Hale Şahin – 150116841**

1. **Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**



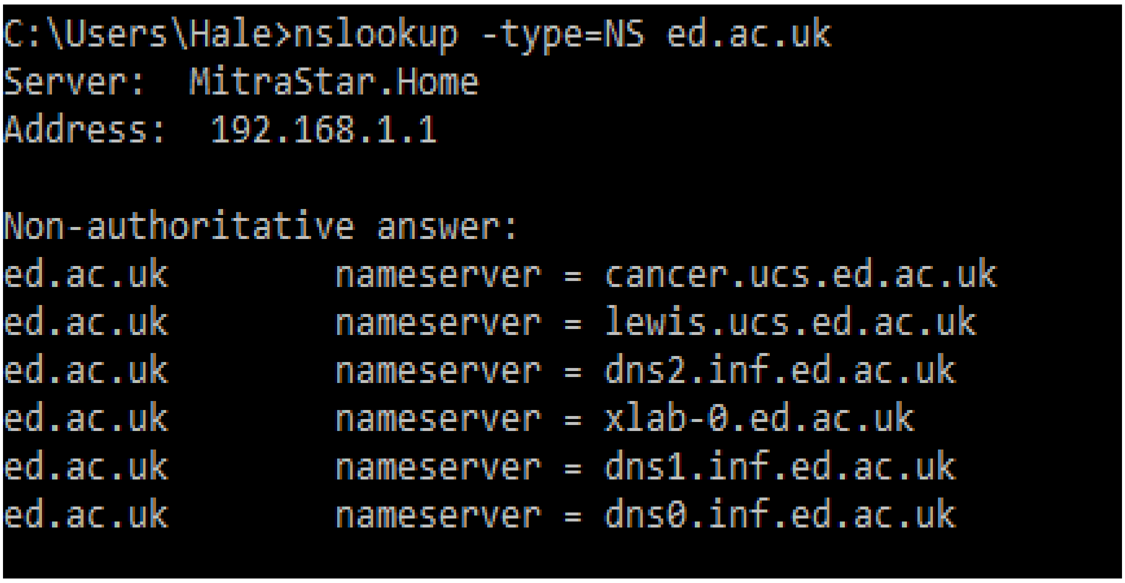
```
C:\Users\Hale>nslookup www.gundam.jp
Server:  MitraStar.Home
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.gundam.jp
Address:  210.138.156.26
```

IP address of the server

*Figure 1.Answer of the first question*

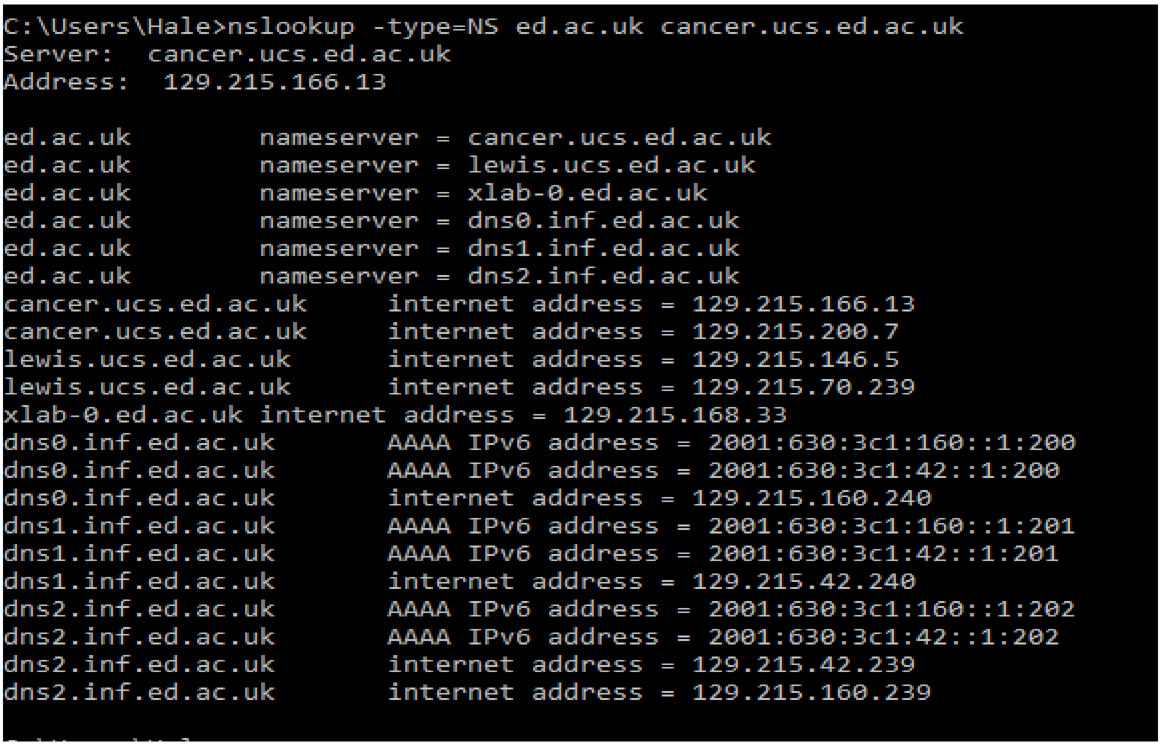
2. **Run nslookup to determine the authoritative DNS servers for a university in Europe.**

For the Edinburgh University the authoritative DNS server is cancer.ucs.ed.ac.uk.



```
C:\Users\Hale>nslookup -type=NS ed.ac.uk
Server:  MitraStar.Home
Address:  192.168.1.1

Non-authoritative answer:
ed.ac.uk        nameserver = cancer.ucs.ed.ac.uk
ed.ac.uk        nameserver = lewis.ucs.ed.ac.uk
ed.ac.uk        nameserver = dns2.inf.ed.ac.uk
ed.ac.uk        nameserver = xlab-0.ed.ac.uk
ed.ac.uk        nameserver = dns1.inf.ed.ac.uk
ed.ac.uk        nameserver = dns0.inf.ed.ac.uk
```

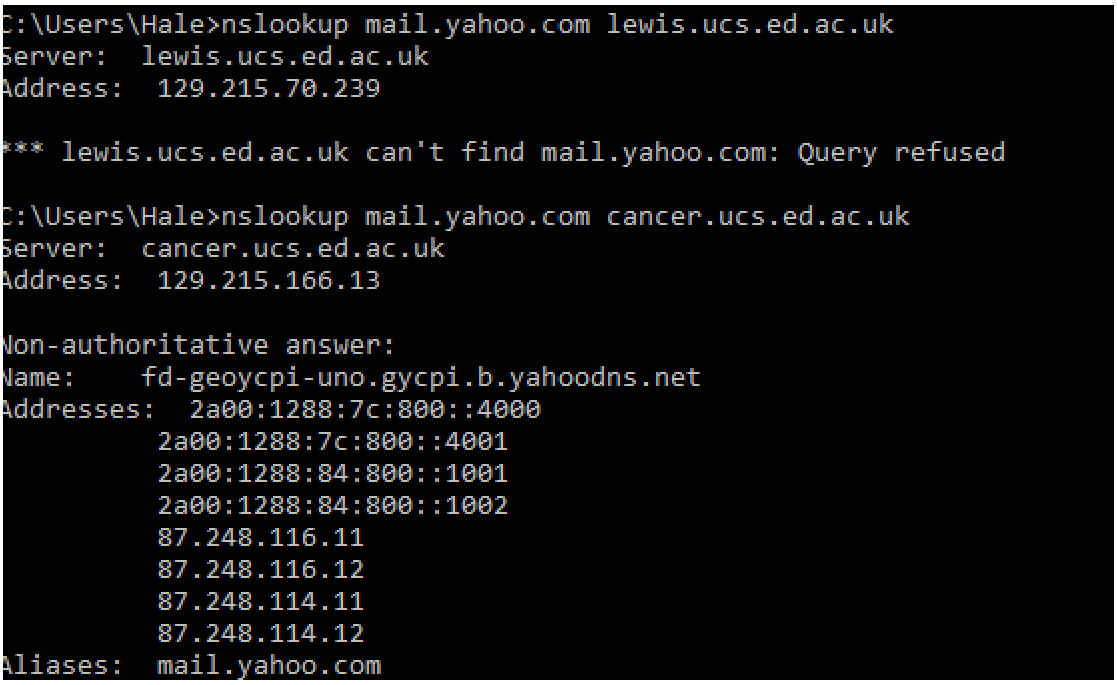
I can see that there can be more authoritative servers than one. The response we got back was from a cached record. To confirm the authoritative DNS servers, I perform the same DNS query of one of the servers that can provide authoritative answers.



```
C:\Users\Hale>nslookup -type=NS ed.ac.uk cancer.ucs.ed.ac.uk
Server:  cancer.ucs.ed.ac.uk
Address:  129.215.166.13

ed.ac.uk        nameserver = cancer.ucs.ed.ac.uk
ed.ac.uk        nameserver = lewis.ucs.ed.ac.uk
ed.ac.uk        nameserver = xlab-0.ed.ac.uk
ed.ac.uk        nameserver = dns0.inf.ed.ac.uk
ed.ac.uk        nameserver = dns1.inf.ed.ac.uk
ed.ac.uk        nameserver = dns2.inf.ed.ac.uk
cancer.ucs.ed.ac.uk     internet address = 129.215.166.13
cancer.ucs.ed.ac.uk     internet address = 129.215.200.7
lewis.ucs.ed.ac.uk      internet address = 129.215.146.5
lewis.ucs.ed.ac.uk      internet address = 129.215.70.239
xlab-0.ed.ac.uk internet address = 129.215.168.33
dns0.inf.ed.ac.uk       AAAA IPv6 address = 2001:630:3c1:160::1:200
dns0.inf.ed.ac.uk       AAAA IPv6 address = 2001:630:3c1:42::1:200
dns0.inf.ed.ac.uk       internet address = 129.215.160.240
dns1.inf.ed.ac.uk       AAAA IPv6 address = 2001:630:3c1:160::1:201
dns1.inf.ed.ac.uk       AAAA IPv6 address = 2001:630:3c1:42::1:201
dns1.inf.ed.ac.uk       internet address = 129.215.42.240
dns2.inf.ed.ac.uk       AAAA IPv6 address = 2001:630:3c1:160::1:202
dns2.inf.ed.ac.uk       AAAA IPv6 address = 2001:630:3c1:42::1:202
dns2.inf.ed.ac.uk       internet address = 129.215.42.239
dns2.inf.ed.ac.uk       internet address = 129.215.160.239
```

*Figure 2.Answer of the second question*

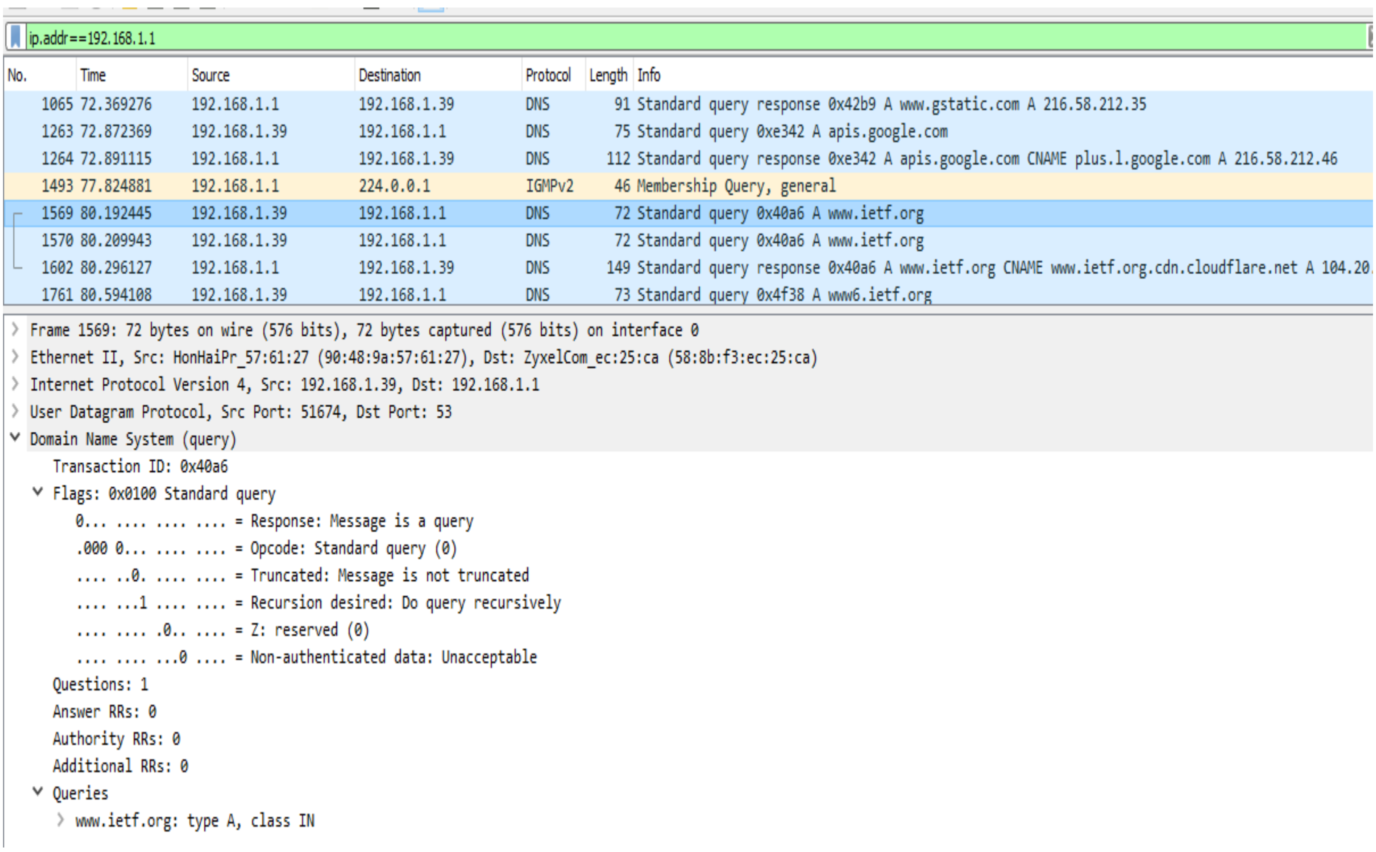
**3.** Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?



```
C:\Users\Hale>nslookup mail.yahoo.com lewis.ucs.ed.ac.uk
Server:  lewis.ucs.ed.ac.uk
Address:  129.215.70.239

*** lewis.ucs.ed.ac.uk can't find mail.yahoo.com: Query refused

C:\Users\Hale>nslookup mail.yahoo.com cancer.ucs.ed.ac.uk
Server:  cancer.ucs.ed.ac.uk
Address:  129.215.166.13

Non-authoritative answer:
Name:    fd-geoycpi-uno.gycpi.b.yahoodns.net
Addresses:  2a00:1288:7c:800::4000
          2a00:1288:7c:800::4001
          2a00:1288:84:800::1001
          2a00:1288:84:800::1002
          87.248.116.11
          87.248.116.12
          87.248.114.11
          87.248.114.12
Aliases:  mail.yahoo.com
```

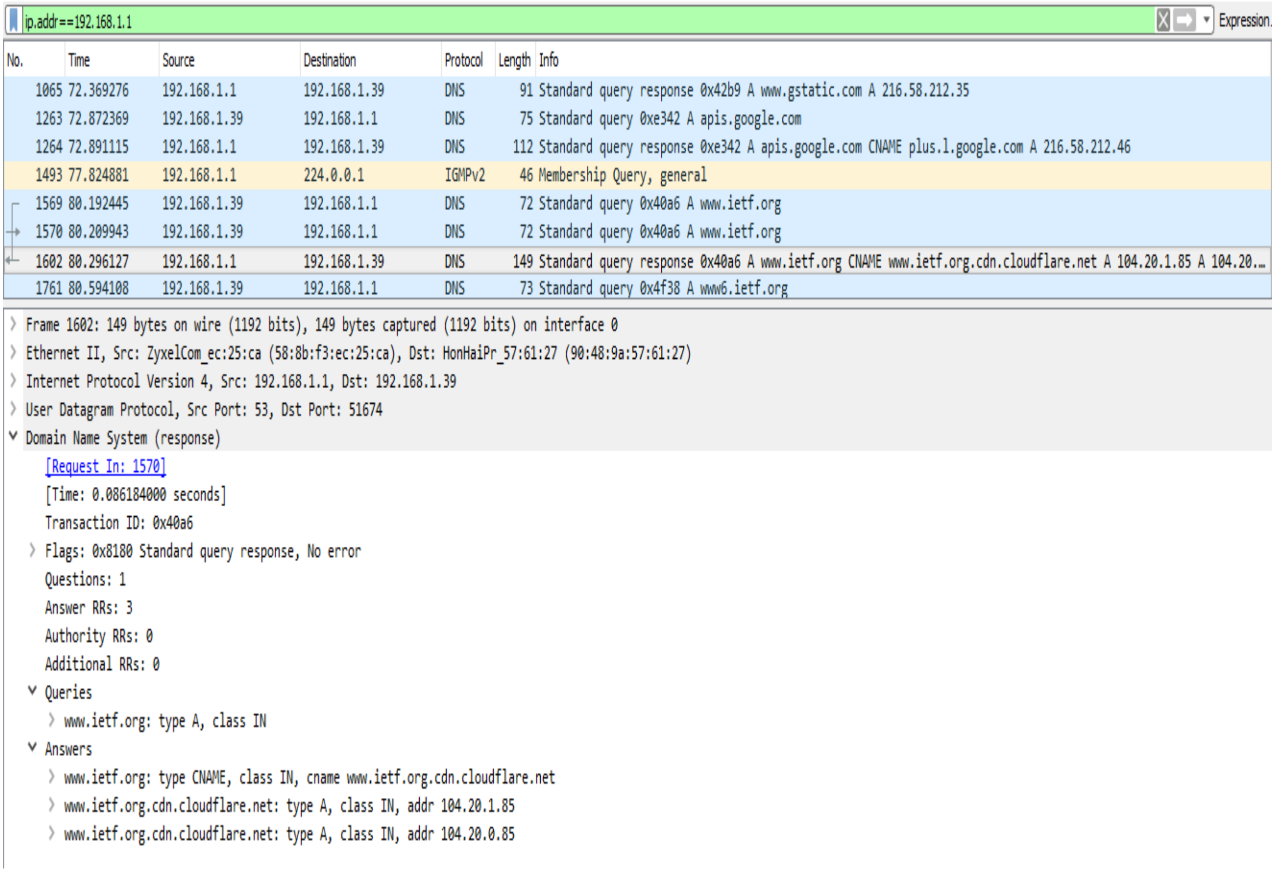
*Figure 3Answer of the third question*

**4.** Locate the DNS queury and response messages. Are then sent over UDP or TCP? They are sent over UDP, User Datagram Protocol.



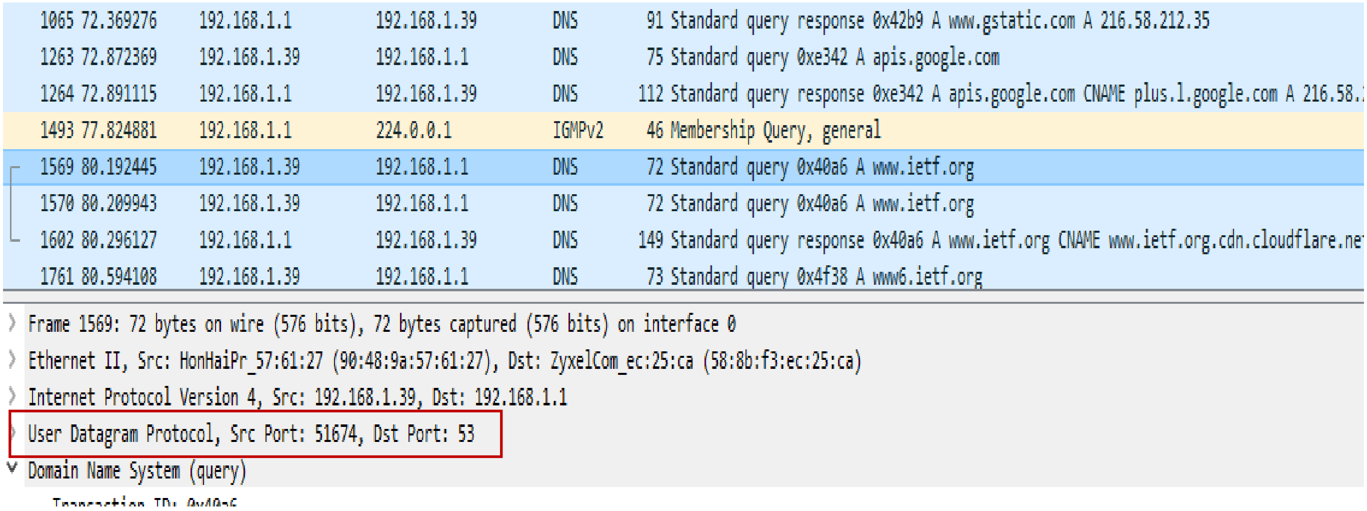
```
ip.addr==192.168.1.1

No.     Time        Source          Destination     Protocol  Length  Info
   1065 72.369276   192.168.1.1     192.168.1.39    DNS           91  Standard query response 0x42b9 A www.gstatic.com A 216.58.212.35
   1263 72.872369   192.168.1.39    192.168.1.1     DNS           75  Standard query 0xe342 A apis.google.com
   1264 72.891115   192.168.1.1     192.168.1.39    DNS          112  Standard query response 0xe342 A apis.google.com CNAME plus.l.google.com A 216.58.212.46
   1493 77.824881   192.168.1.1     224.0.0.1       IGMPv2        46  Membership Query, general
   1569 80.192445   192.168.1.39    192.168.1.1     DNS           72  Standard query 0x40a6 A www.ietf.org
   1570 80.209943   192.168.1.39    192.168.1.1     DNS           72  Standard query 0x40a6 A www.ietf.org
   1602 80.296127   192.168.1.1     192.168.1.39    DNS          149  Standard query response 0x40a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20
   1761 80.594108   192.168.1.39    192.168.1.1     DNS           73  Standard query 0x4f38 A www6.ietf.org

> Frame 1569: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: HonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
> Internet Protocol Version 4, Src: 192.168.1.39, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 51674, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x40a6
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
```

*Figure 4DNS query in Wireshark*



```
ip.addr==192.168.1.1                                                                    Expression.

No.     Time        Source          Destination     Protocol  Length  Info
   1065 72.369276   192.168.1.1     192.168.1.39    DNS           91  Standard query response 0x42b9 A www.gstatic.com A 216.58.212.35
   1263 72.872369   192.168.1.39    192.168.1.1     DNS           75  Standard query 0xe342 A apis.google.com
   1264 72.891115   192.168.1.1     192.168.1.39    DNS          112  Standard query response 0xe342 A apis.google.com CNAME plus.l.google.com A 216.58.212.46
   1493 77.824881   192.168.1.1     224.0.0.1       IGMPv2        46  Membership Query, general
   1569 80.192445   192.168.1.39    192.168.1.1     DNS           72  Standard query 0x40a6 A www.ietf.org
   1570 80.209943   192.168.1.39    192.168.1.1     DNS           72  Standard query 0x40a6 A www.ietf.org
   1602 80.296127   192.168.1.1     192.168.1.39    DNS          149  Standard query response 0x40a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20...
   1761 80.594108   192.168.1.39    192.168.1.1     DNS           73  Standard query 0x4f38 A www6.ietf.org

> Frame 1602: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
> Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.39
> User Datagram Protocol, Src Port: 53, Dst Port: 51674
v Domain Name System (response)
    [Request In: 1570]
    [Time: 0.086184000 seconds]
    Transaction ID: 0x40a6
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
  v Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
```

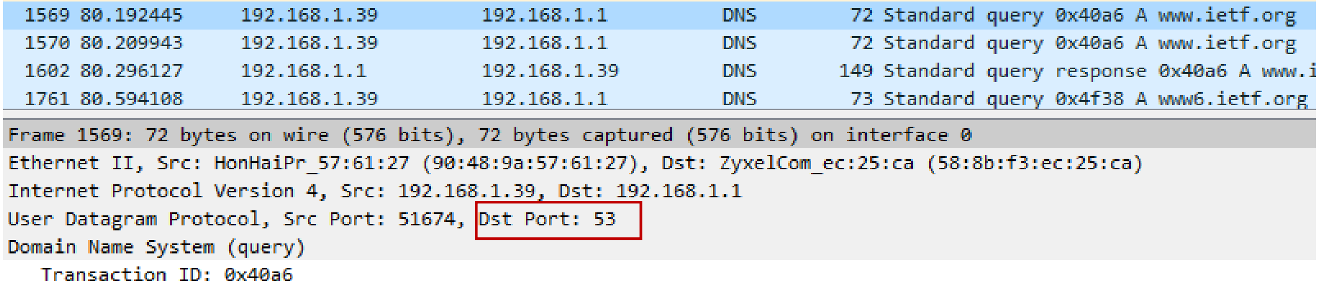
*Figure 5. DNS response*



```
1065 72.369276   192.168.1.1    192.168.1.39   DNS     91 Standard query response 0x42b9 A www.gstatic.com A 216.58.212.35
1263 72.872369   192.168.1.39   192.168.1.1    DNS     75 Standard query 0xe342 A apis.google.com
1264 72.891115   192.168.1.1    192.168.1.39   DNS    112 Standard query response 0xe342 A apis.google.com CNAME plus.l.google.com A 216.58.
1493 77.824881   192.168.1.1    224.0.0.1      IGMPv2  46 Membership Query, general
1569 80.192445   192.168.1.39   192.168.1.1    DNS     72 Standard query 0x40a6 A www.ietf.org
1570 80.209943   192.168.1.39   192.168.1.1    DNS     72 Standard query 0x40a6 A www.ietf.org
1602 80.296127   192.168.1.1    192.168.1.39   DNS    149 Standard query response 0x40a6 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.ne
1761 80.594108   192.168.1.39   192.168.1.1    DNS     73 Standard query 0x4f38 A www6.ietf.org

> Frame 1569: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: HonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
> Internet Protocol Version 4, Src: 192.168.1.39, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 51674, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x40a6
```

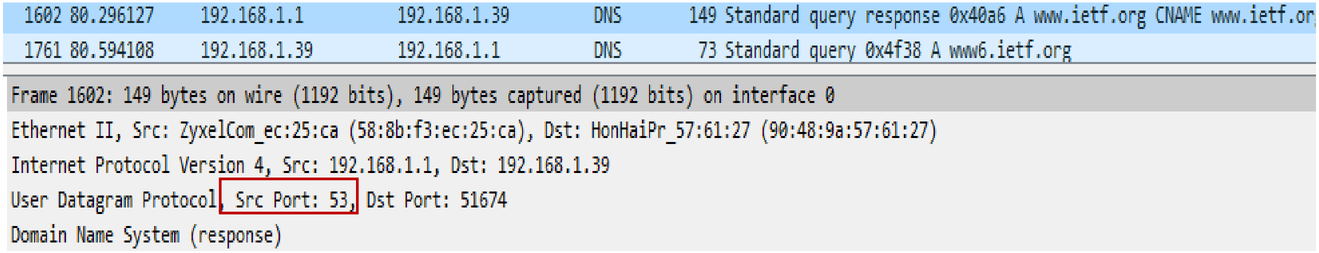
**5.** What is the destination port for the DNS query message? What is the source port of DNS response message?

They are both 53.



```
1569 80.192445   192.168.1.39   192.168.1.1    DNS    72 Standard query 0x40a6 A www.ietf.org
1570 80.209943   192.168.1.39   192.168.1.1    DNS    72 Standard query 0x40a6 A www.ietf.org
1602 80.296127   192.168.1.1    192.168.1.39   DNS   149 Standard query response 0x40a6 A www.i
1761 80.594108   192.168.1.39   192.168.1.1    DNS    73 Standard query 0x4f38 A www6.ietf.org
Frame 1569: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
Ethernet II, Src: HonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
Internet Protocol Version 4, Src: 192.168.1.39, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 51674, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x40a6
```

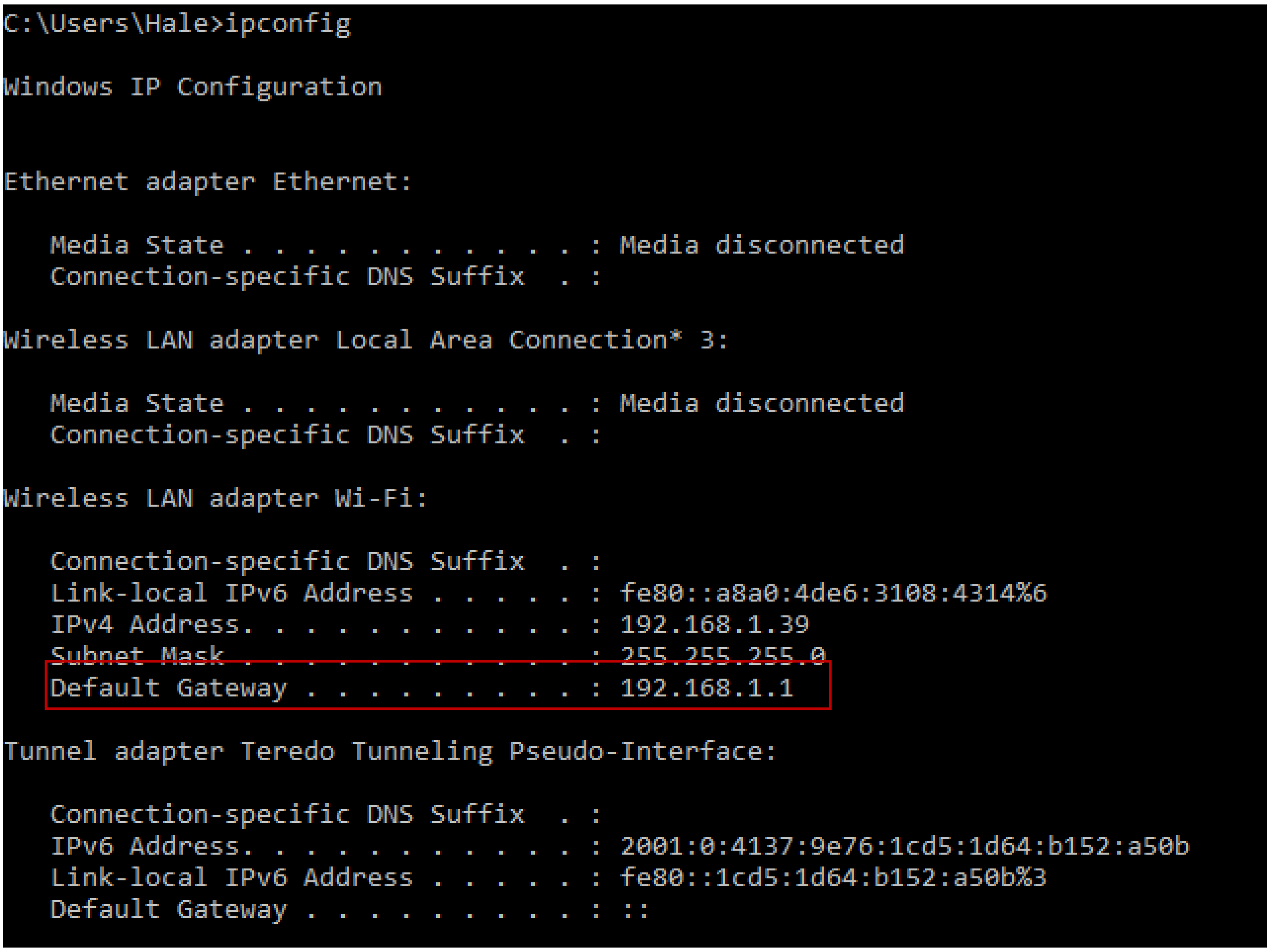
*Figure 6 Destination port for the DNS query message*



```
1602 80.296127   192.168.1.1    192.168.1.39   DNS   149 Standard query response 0x40a6 A www.ietf.org CNAME www.ietf.or
1761 80.594108   192.168.1.39   192.168.1.1    DNS    73 Standard query 0x4f38 A www6.ietf.org
Frame 1602: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.39
User Datagram Protocol, Src Port: 53, Dst Port: 51674
Domain Name System (response)
```

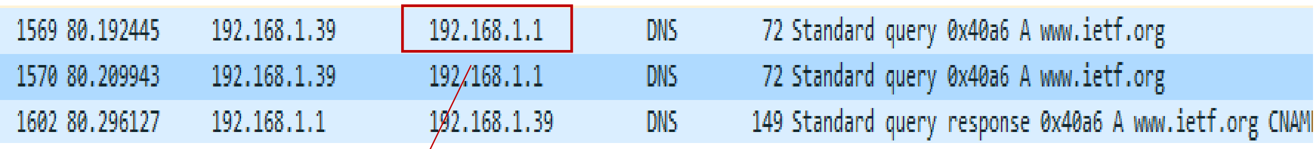
*Figure 7 Source port of DNS response message*

**6.** To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?



```
C:\Users\Hale>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a8a0:4de6:3108:4314%6
   IPv4 Address. . . . . . . . . . . : 192.168.1.39
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e76:1cd5:1d64:b152:a50b
   Link-local IPv6 Address . . . . . : fe80::1cd5:1d64:b152:a50b%3
   Default Gateway . . . . . . . . . : ::
```

*Figure 8. Result of the ipconfig command*



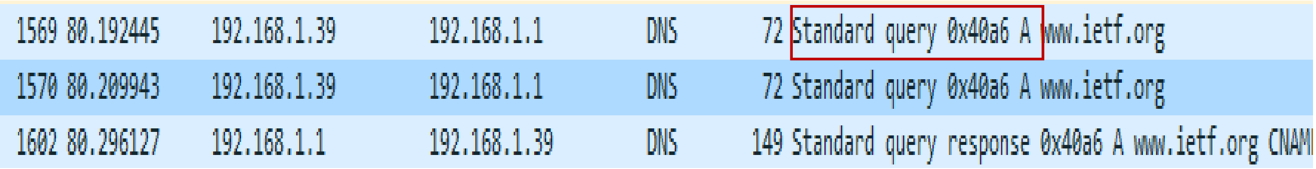
```
1569 80.192445    192.168.1.39    192.168.1.1     DNS    72 Standard query 0x40a6 A www.ietf.org
1570 80.209943    192.168.1.39    192.168.1.1     DNS    72 Standard query 0x40a6 A www.ietf.org
1602 80.296127    192.168.1.1     192.168.1.39    DNS   149 Standard query response 0x40a6 A www.ietf.org CNAM
```

*Figure 9. Answer of the sixth question*

DNS query message sent to this IP address and also it is the IP address of one of my local DNS servers according to the Figure 8.

**7.** Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

It is a Type A standard query. And it does not contain any answers.

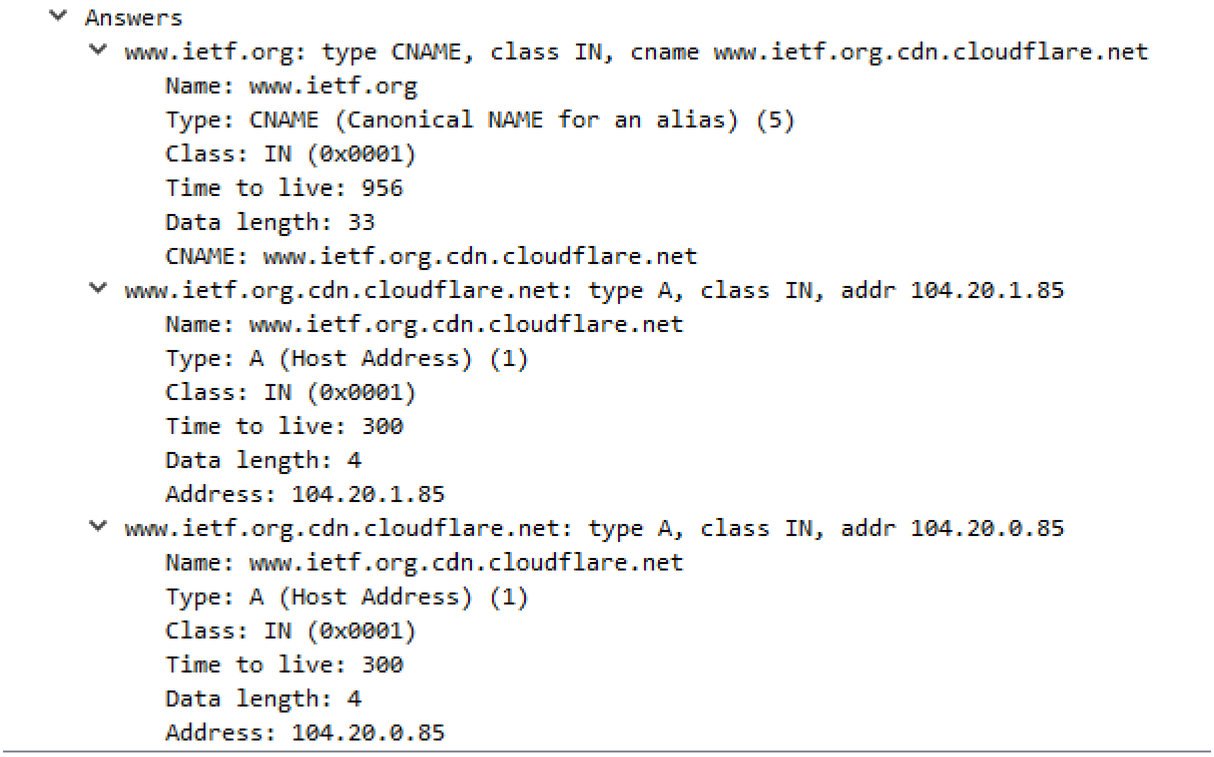


```
1569 80.192445   192.168.1.39   192.168.1.1    DNS    72 Standard query 0x40a6 A www.ietf.org
1570 80.209943   192.168.1.39   192.168.1.1    DNS    72 Standard query 0x40a6 A www.ietf.org
1602 80.296127   192.168.1.1    192.168.1.39   DNS   149 Standard query response 0x40a6 A www.ietf.org CNAM
```

*Figure 10. Answer of the seventh question*

**8.** Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

There were 3 answers as figure below;



```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
     Name: www.ietf.org
     Type: CNAME (Canonical NAME for an alias) (5)
     Class: IN (0x0001)
     Time to live: 956
     Data length: 33
     CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
     Name: www.ietf.org.cdn.cloudflare.net
     Type: A (Host Address) (1)
     Class: IN (0x0001)
     Time to live: 300
     Data length: 4
     Address: 104.20.1.85
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
     Name: www.ietf.org.cdn.cloudflare.net
     Type: A (Host Address) (1)
     Class: IN (0x0001)
     Time to live: 300
     Data length: 4
     Address: 104.20.0.85
```

*Figure 11. Answer of the eighth question*

**9.** Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

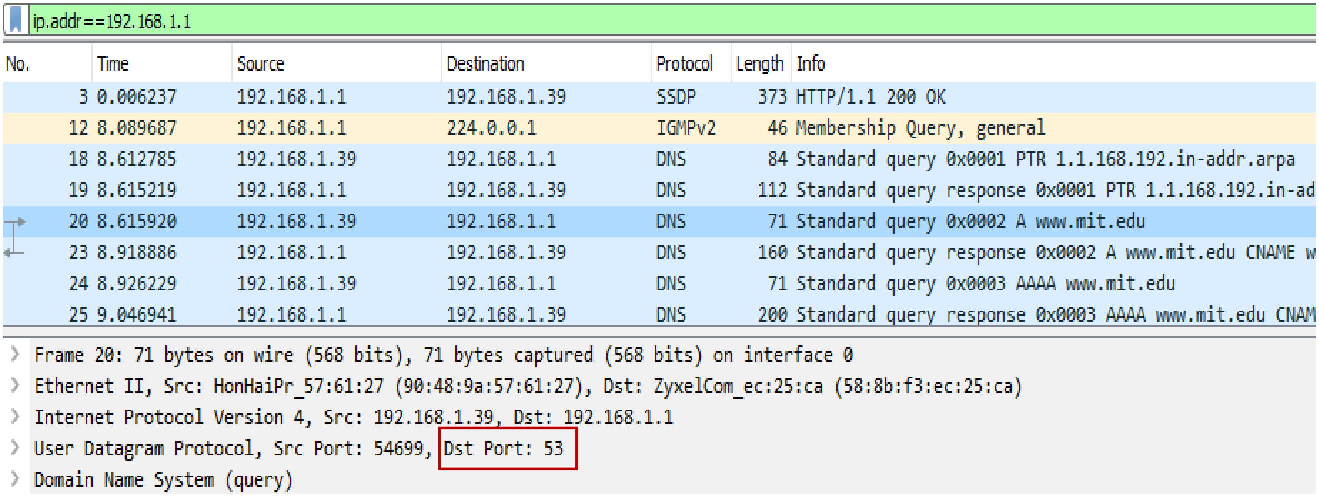
The first SYN packet is sent to 104.20.1.85 that is the first IP address provided in the DNS response message.

**10.** This wep page contains images. Before retrieving each image, does your host issue new DNS queries?

No, the images are all loaded from www.ietf.org, that means no additional DNS queries needed.

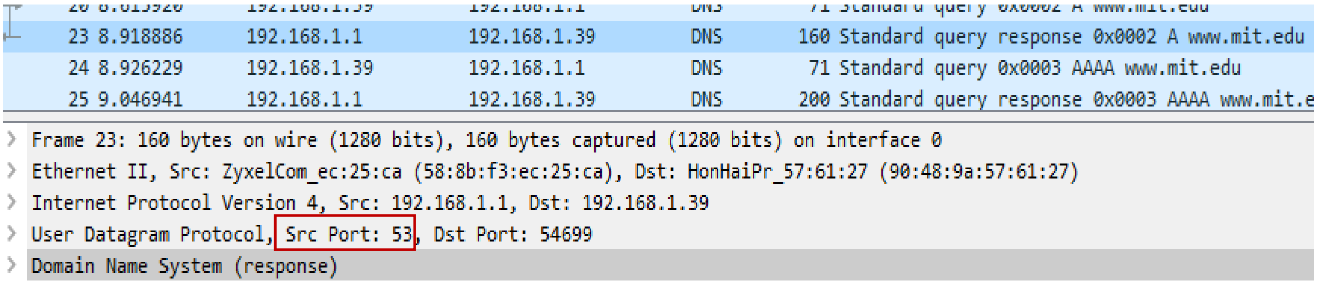
**11.** What is the destination port of DNS query message? What is the source port of DNS response message?

They are both same 53.



```
ip.addr==192.168.1.1

No.   Time       Source         Destination    Protocol  Length Info
    3 0.006237   192.168.1.1    192.168.1.39   SSDP         373 HTTP/1.1 200 OK
   12 8.089687   192.168.1.1    224.0.0.1      IGMPv2        46 Membership Query, general
   18 8.612785   192.168.1.39   192.168.1.1    DNS           84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
   19 8.615219   192.168.1.1    192.168.1.39   DNS          112 Standard query response 0x0001 PTR 1.1.168.192.in-ad
   20 8.615920   192.168.1.39   192.168.1.1    DNS           71 Standard query 0x0002 A www.mit.edu
   23 8.918886   192.168.1.1    192.168.1.39   DNS          160 Standard query response 0x0002 A www.mit.edu CNAME w
   24 8.926229   192.168.1.39   192.168.1.1    DNS           71 Standard query 0x0003 AAAA www.mit.edu
   25 9.046941   192.168.1.1    192.168.1.39   DNS          200 Standard query response 0x0003 AAAA www.mit.edu CNAM

> Frame 20: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: HonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
> Internet Protocol Version 4, Src: 192.168.1.39, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 54699, Dst Port: 53
> Domain Name System (query)
```

*Figure 12. DNS query message*

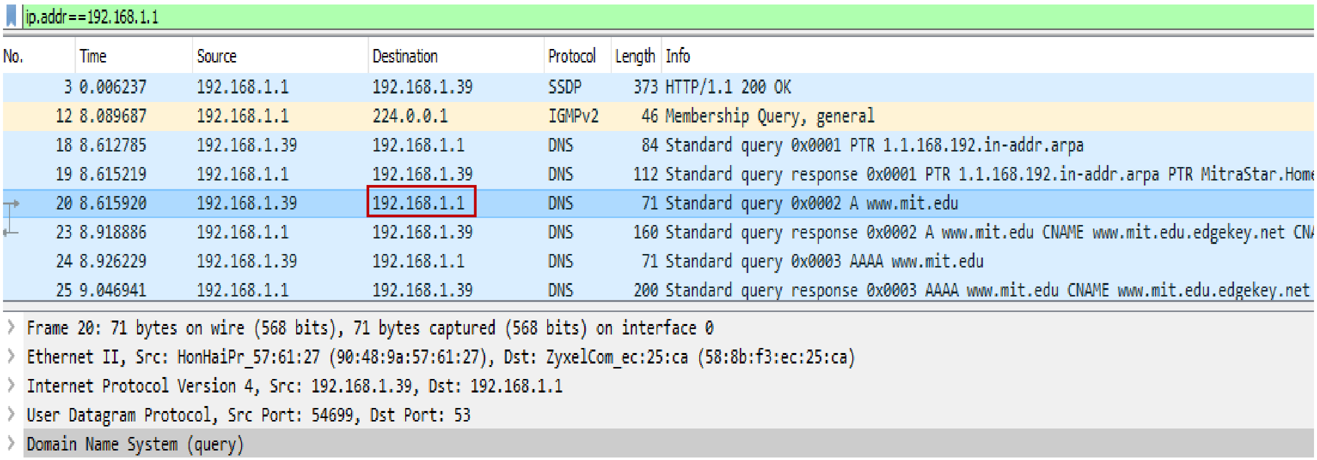


```
   20 8.615920   192.168.1.39   192.168.1.1    DNS           71 Standard query 0x0002 A www.mit.edu
   23 8.918886   192.168.1.1    192.168.1.39   DNS          160 Standard query response 0x0002 A www.mit.edu
   24 8.926229   192.168.1.39   192.168.1.1    DNS           71 Standard query 0x0003 AAAA www.mit.edu
   25 9.046941   192.168.1.1    192.168.1.39   DNS          200 Standard query response 0x0003 AAAA www.mit.e

> Frame 23: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
> Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.39
> User Datagram Protocol, Src Port: 53, Dst Port: 54699
> Domain Name System (response)
```

*Figure 13. DNS response message*

**12.** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

It is sent to 192.168.1.1, and I can see from ipconfig all that is the exact same ip address wiith my local DNS server.

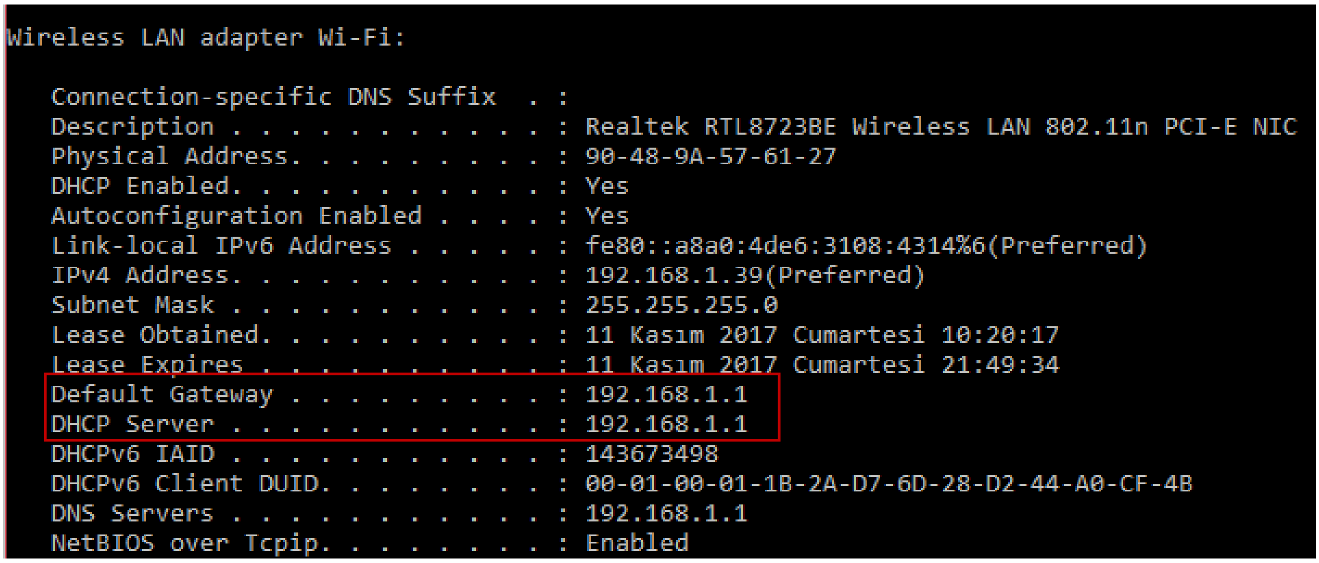


ip.addr==192.168.1.1

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 0.006237 | 192.168.1.1 | 192.168.1.39 | SSDP | 373 | HTTP/1.1 200 OK |
| 12 | 8.089687 | 192.168.1.1 | 224.0.0.1 | IGMPv2 | 46 | Membership Query, general |
| 18 | 8.612785 | 192.168.1.39 | 192.168.1.1 | DNS | 84 | Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa |
| 19 | 8.615219 | 192.168.1.1 | 192.168.1.39 | DNS | 112 | Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR MitraStar.Home |
| 20 | 8.615920 | 192.168.1.39 | 192.168.1.1 | DNS | 71 | Standard query 0x0002 A www.mit.edu |
| 23 | 8.918886 | 192.168.1.1 | 192.168.1.39 | DNS | 160 | Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CN |
| 24 | 8.926229 | 192.168.1.39 | 192.168.1.1 | DNS | 71 | Standard query 0x0003 AAAA www.mit.edu |
| 25 | 9.046941 | 192.168.1.1 | 192.168.1.39 | DNS | 200 | Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net |

```
> Frame 20: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: HonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
> Internet Protocol Version 4, Src: 192.168.1.39, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 54699, Dst Port: 53
> Domain Name System (query)
```

*Figure 14. DNS query message*

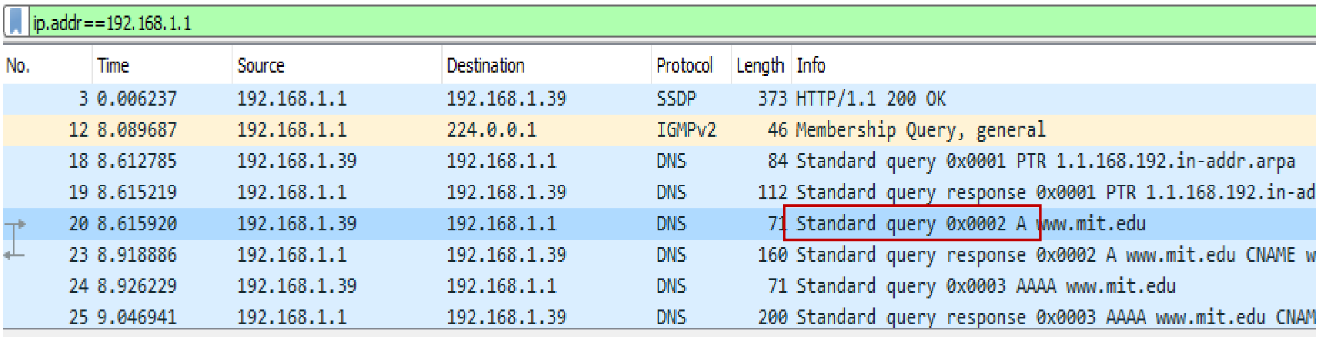


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8723BE Wireless LAN 802.11n PCI-E NIC
   Physical Address. . . . . . . . . : 90-48-9A-57-61-27
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a8a0:4de6:3108:4314%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.39(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 11 Kasım 2017 Cumartesi 10:20:17
   Lease Expires . . . . . . . . . . : 11 Kasım 2017 Cumartesi 21:49:34
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 143673498
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-2A-D7-6D-28-D2-44-A0-CF-4B
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

*Figure 15. Some part of result of ipconfig –all*

**13.** Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

It is a Type A standard query. And it does not contain any answers.



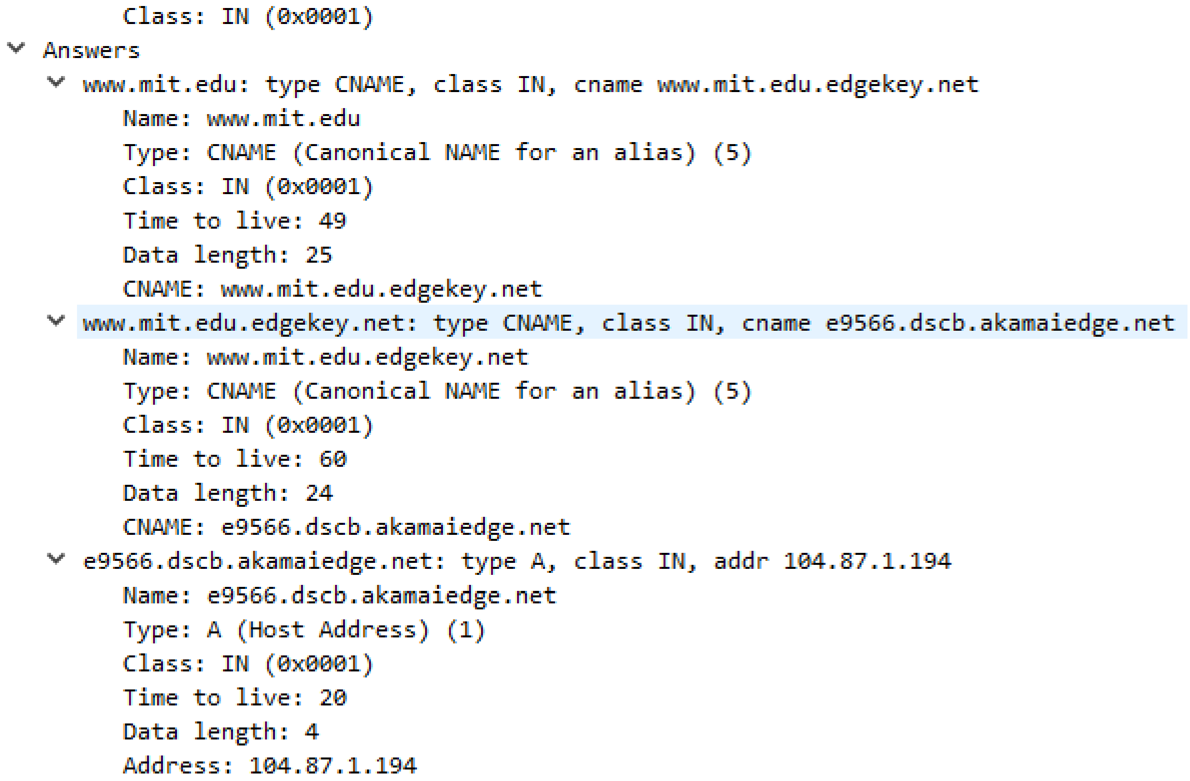
ip.addr==192.168.1.1

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 0.006237 | 192.168.1.1 | 192.168.1.39 | SSDP | 373 | HTTP/1.1 200 OK |
| 12 | 8.089687 | 192.168.1.1 | 224.0.0.1 | IGMPv2 | 46 | Membership Query, general |
| 18 | 8.612785 | 192.168.1.39 | 192.168.1.1 | DNS | 84 | Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa |
| 19 | 8.615219 | 192.168.1.1 | 192.168.1.39 | DNS | 112 | Standard query response 0x0001 PTR 1.1.168.192.in-ad |
| 20 | 8.615920 | 192.168.1.39 | 192.168.1.1 | DNS | 71 | Standard query 0x0002 A www.mit.edu |
| 23 | 8.918886 | 192.168.1.1 | 192.168.1.39 | DNS | 160 | Standard query response 0x0002 A www.mit.edu CNAME w |
| 24 | 8.926229 | 192.168.1.39 | 192.168.1.1 | DNS | 71 | Standard query 0x0003 AAAA www.mit.edu |
| 25 | 9.046941 | 192.168.1.1 | 192.168.1.39 | DNS | 200 | Standard query response 0x0003 AAAA www.mit.edu CNAM |

*Figure 16. Type of DNS query message*

**14.** Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

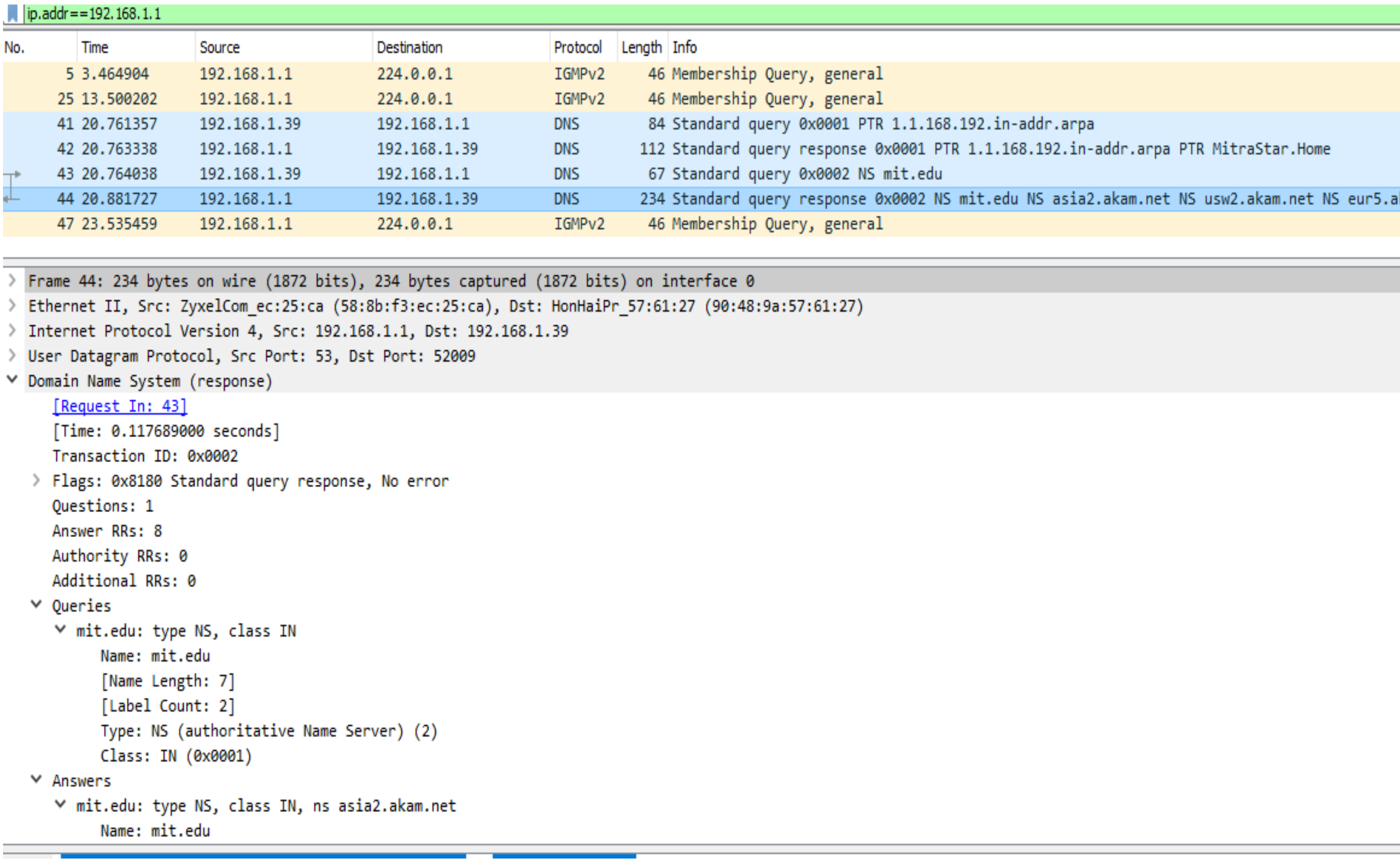
It contains three answers as below figure;



```
        Class: IN (0x0001)
⌄ Answers
  ⌄ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 49
        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 (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
  ⌄ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.87.1.194
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20
        Data length: 4
        Address: 104.87.1.194
```

*Figure 17. Answers of the DNS responnse*

**15.** Provide a screenshot.



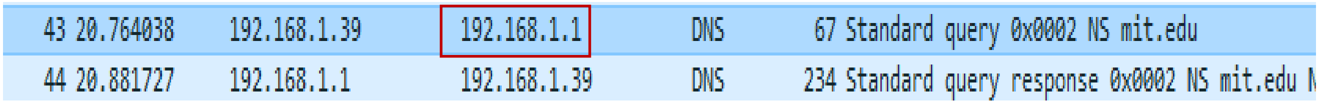
```
ip.addr==192.168.1.1

No.    Time        Source          Destination     Protocol  Length Info
     5 3.464904    192.168.1.1     224.0.0.1       IGMPv2      46 Membership Query, general
    25 13.500202   192.168.1.1     224.0.0.1       IGMPv2      46 Membership Query, general
    41 20.761357   192.168.1.39    192.168.1.1     DNS         84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
    42 20.763338   192.168.1.1     192.168.1.39    DNS        112 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR MitraStar.Home
    43 20.764038   192.168.1.39    192.168.1.1     DNS         67 Standard query 0x0002 NS mit.edu
    44 20.881727   192.168.1.1     192.168.1.39    DNS        234 Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS usw2.akam.net NS eur5.a
    47 23.535459   192.168.1.1     224.0.0.1       IGMPv2      46 Membership Query, general
```

```
> Frame 44: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
> Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.39
> User Datagram Protocol, Src Port: 53, Dst Port: 52009
v Domain Name System (response)
    [Request In: 43]
    [Time: 0.117689000 seconds]
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  v Answers
    v mit.edu: type NS, class IN, ns asia2.akam.net
        Name: mit.edu
```

*Figure 18. DNS response*

**16.** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

It is sent to 192.168.1.1 which is my local DNS server too.

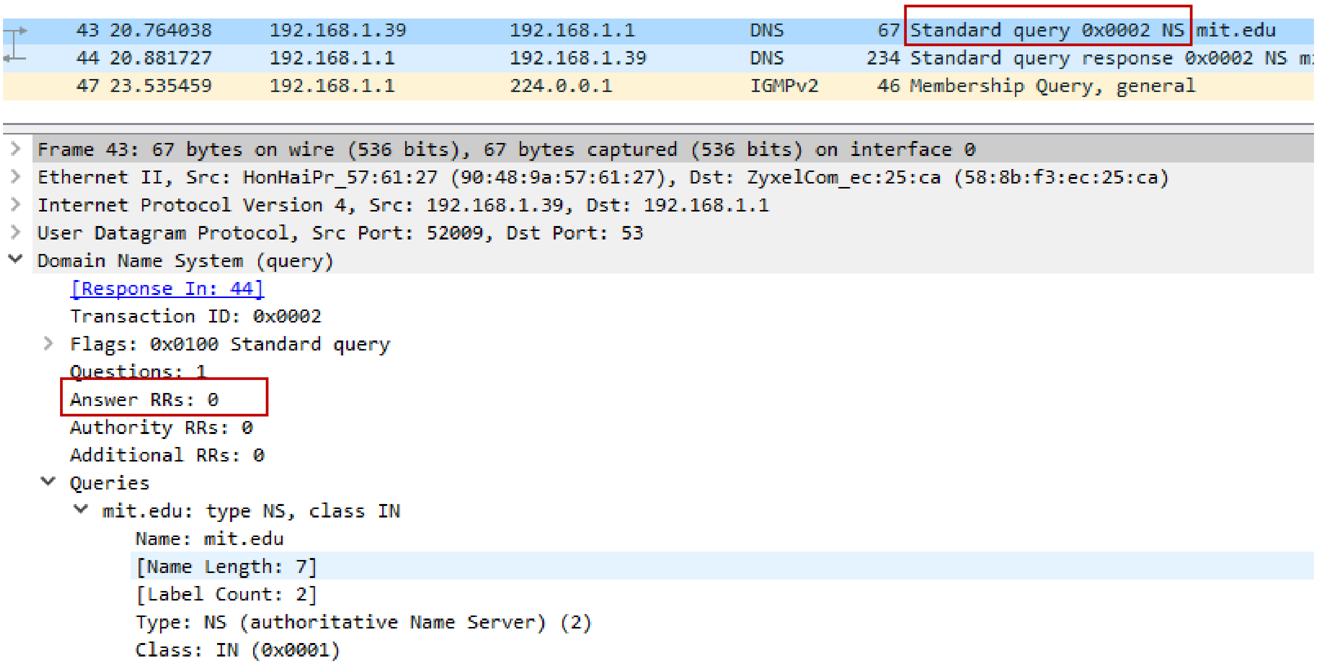


```
43 20.764038   192.168.1.39   192.168.1.1    DNS   67 Standard query 0x0002 NS mit.edu
44 20.881727   192.168.1.1    192.168.1.39   DNS   234 Standard query response 0x0002 NS mit.edu N
```

*Figure 19. DNS query message*

**17.** Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

It is a type of NS DNS query and it does not contain any answers.

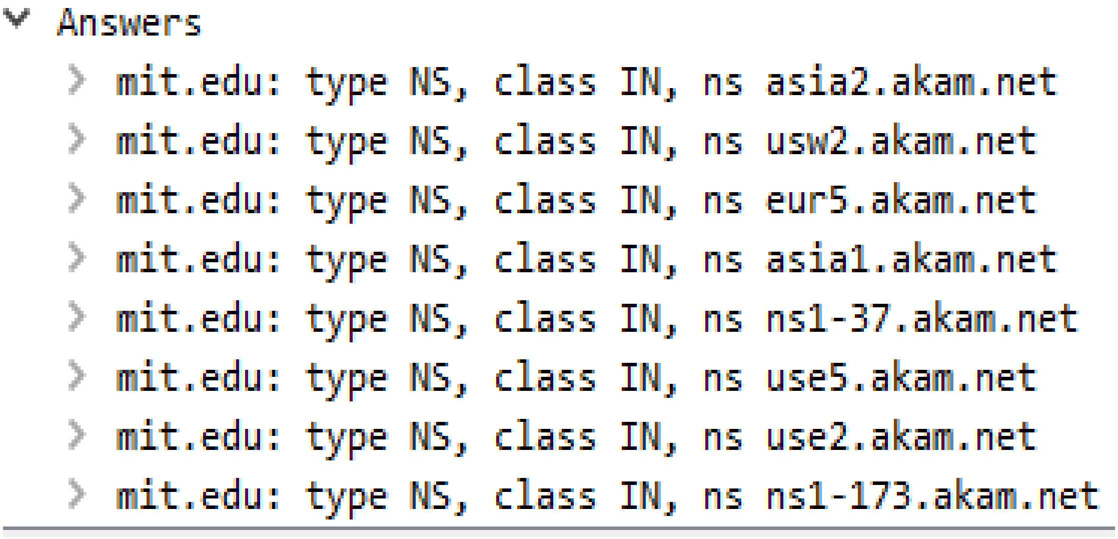


```
43 20.764038    192.168.1.39    192.168.1.1     DNS       67 Standard query 0x0002 NS mit.edu
44 20.881727    192.168.1.1     192.168.1.39    DNS      234 Standard query response 0x0002 NS m
47 23.535459    192.168.1.1     224.0.0.1       IGMPv2    46 Membership Query, general

> Frame 43: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: HonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
> Internet Protocol Version 4, Src: 192.168.1.39, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 52009, Dst Port: 53
v Domain Name System (query)
    [Response In: 44]
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
```

*Figure 20. DNS query message*

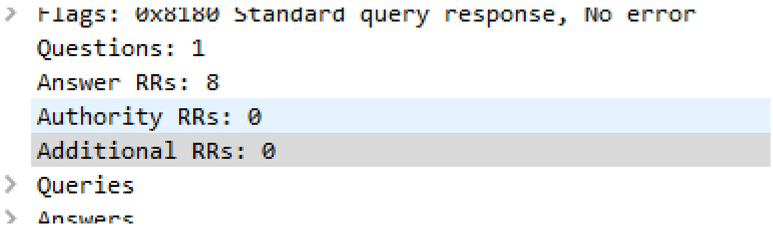
**18.** Examine the DNS response message.What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

The nameservers are asia2, usw2, eur5, asia1, ns1-37, use5, use2, ns1-173.
We cannot find their IP addresses because they dont have any additional records.



```
v Answers
  > mit.edu: type NS, class IN, ns asia2.akam.net
  > mit.edu: type NS, class IN, ns usw2.akam.net
  > mit.edu: type NS, class IN, ns eur5.akam.net
  > mit.edu: type NS, class IN, ns asia1.akam.net
  > mit.edu: type NS, class IN, ns ns1-37.akam.net
  > mit.edu: type NS, class IN, ns use5.akam.net
  > mit.edu: type NS, class IN, ns use2.akam.net
  > mit.edu: type NS, class IN, ns ns1-173.akam.net
```

*Figure 21. Answer with the nameservers of DNS response*

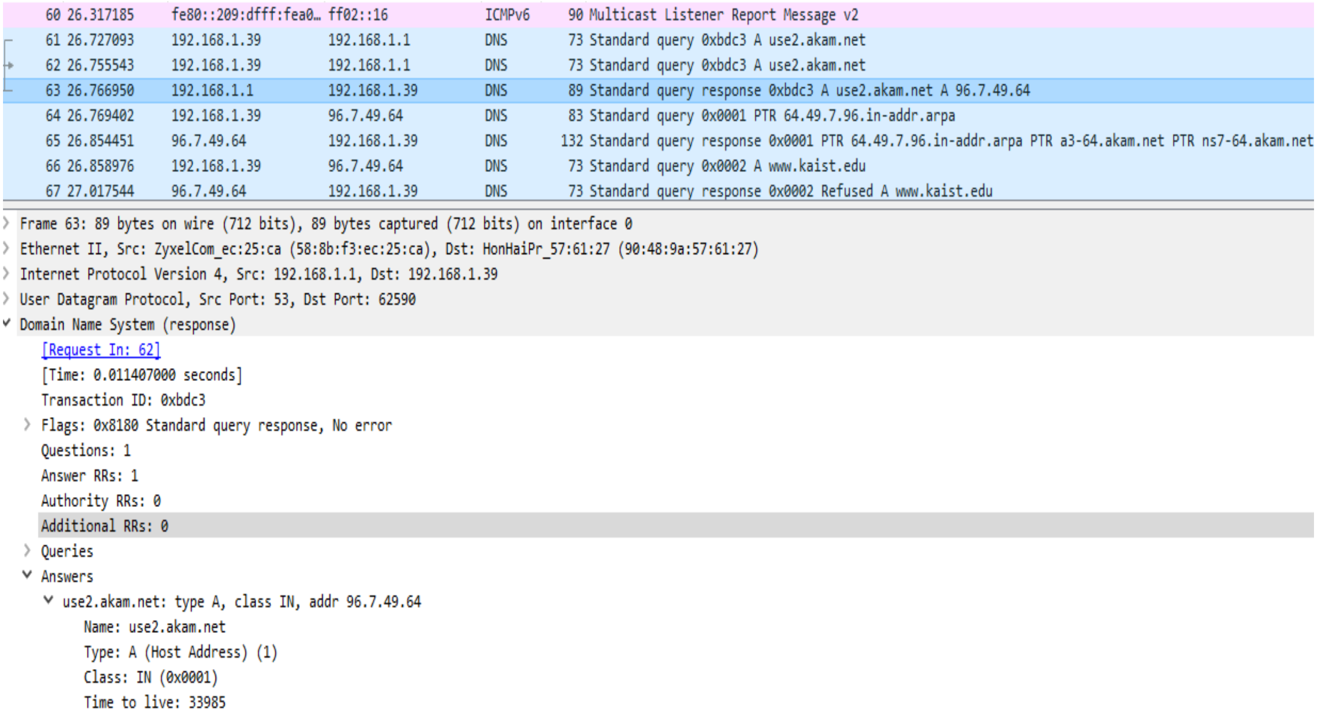


```
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
> Queries
> Answers
```

*Figure 22. DNS response*

Figure 22 says that there is 8 answers but no additional records.

**19.** Provide a screenshot.



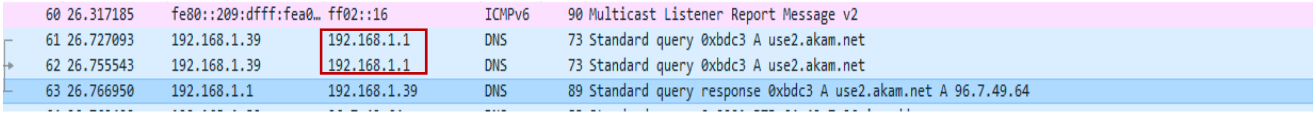
```
60 26.317185  fe80::209:dfff:fea0… ff02::16      ICMPv6   90 Multicast Listener Report Message v2
61 26.727093  192.168.1.39         192.168.1.1   DNS      73 Standard query 0xbdc3 A use2.akam.net
62 26.755543  192.168.1.39         192.168.1.1   DNS      73 Standard query 0xbdc3 A use2.akam.net
63 26.766950  192.168.1.1          192.168.1.39  DNS      89 Standard query response 0xbdc3 A use2.akam.net A 96.7.49.64
64 26.769402  192.168.1.39         96.7.49.64    DNS      83 Standard query 0x0001 PTR 64.49.7.96.in-addr.arpa
65 26.854451  96.7.49.64           192.168.1.39  DNS     132 Standard query response 0x0001 PTR 64.49.7.96.in-addr.arpa PTR a3-64.akam.net PTR ns7-64.akam.net
66 26.858976  192.168.1.39         96.7.49.64    DNS      73 Standard query 0x0002 A www.kaist.edu
67 27.017544  96.7.49.64           192.168.1.39  DNS      73 Standard query response 0x0002 Refused A www.kaist.edu
```

```
> Frame 63: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
> Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.39
> User Datagram Protocol, Src Port: 53, Dst Port: 62590
v Domain Name System (response)
    [Request In: 62]
    [Time: 0.011407000 seconds]
    Transaction ID: 0xbdc3
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v use2.akam.net: type A, class IN, addr 96.7.49.64
          Name: use2.akam.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 33985
```

*Figure 23. DNS response*

**20.** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The query is sent to 192.168.1.1 which is same with my local DNS server.

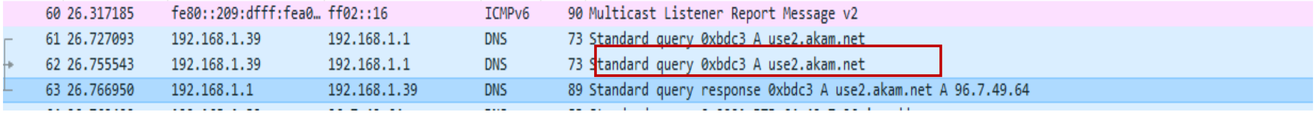


```
60 26.317185  fe80::209:dfff:fea0… ff02::16      ICMPv6   90 Multicast Listener Report Message v2
61 26.727093  192.168.1.39         192.168.1.1   DNS      73 Standard query 0xbdc3 A use2.akam.net
62 26.755543  192.168.1.39         192.168.1.1   DNS      73 Standard query 0xbdc3 A use2.akam.net
63 26.766950  192.168.1.1          192.168.1.39  DNS      89 Standard query response 0xbdc3 A use2.akam.net A 96.7.49.64
```

*Figure 24. DNS query message*

**21.** Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

It is a type A standard query and does not contain any answers.

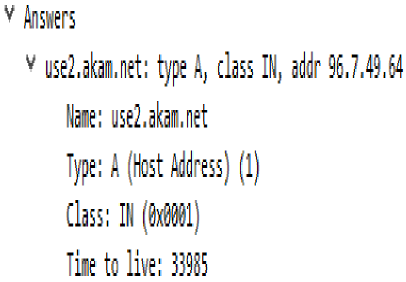


```
60 26.317185   fe80::209:dfff:fea0… ff02::16      ICMPv6   90 Multicast Listener Report Message v2
61 26.727093   192.168.1.39         192.168.1.1   DNS      73 Standard query 0xbdc3 A use2.akam.net
62 26.755543   192.168.1.39         192.168.1.1   DNS      73 Standard query 0xbdc3 A use2.akam.net
63 26.766950   192.168.1.1          192.168.1.39  DNS      89 Standard query response 0xbdc3 A use2.akam.net A 96.7.49.64
```

*Figure 25. DNS query message*

**22.** Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

One answer contained as following figure;



```
∨ Answers
  ∨ use2.akam.net: type A, class IN, addr 96.7.49.64
      Name: use2.akam.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 33985
```

*Figure 26. Answer of the DNS response*