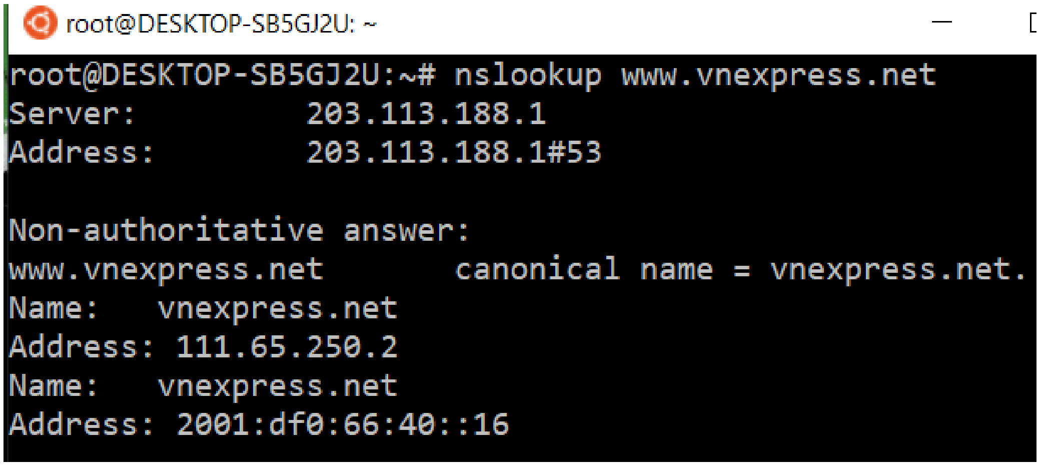
COMPUTER NETWORK
Lab 2b

Student name: Nguyễn Minh Tâm
ID: 1952968

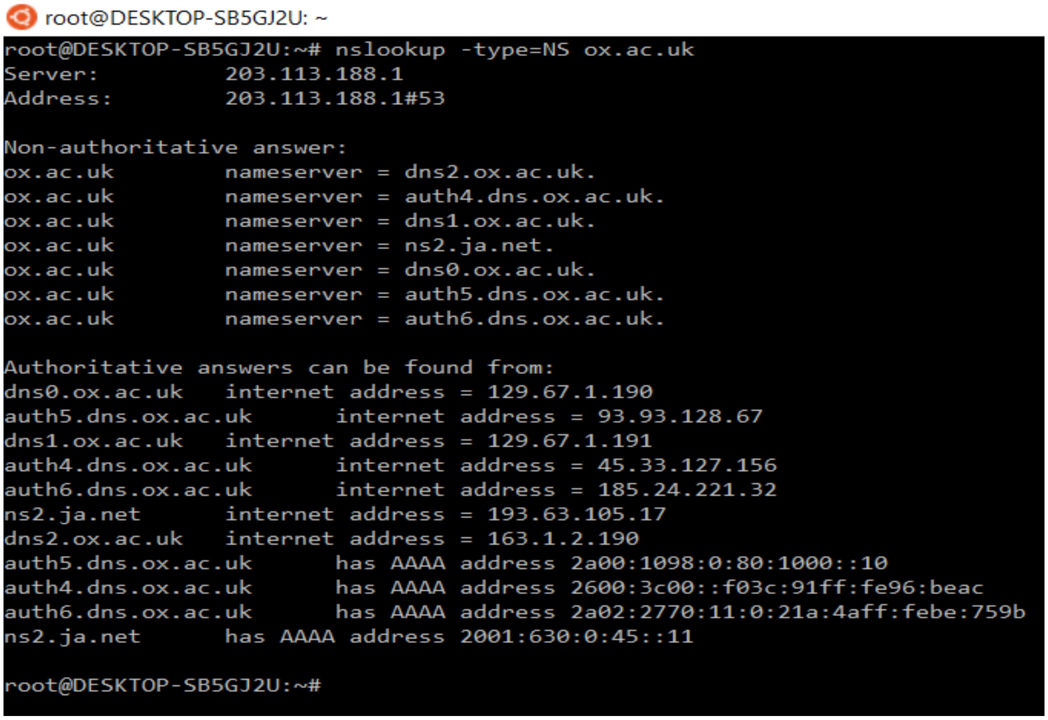
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?



```
root@DESKTOP-SB5GJ2U:~# nslookup www.vnexpress.net
Server:         203.113.188.1
Address:        203.113.188.1#53

Non-authoritative answer:
www.vnexpress.net       canonical name = vnexpress.net.
Name:   vnexpress.net
Address: 111.65.250.2
Name:   vnexpress.net
Address: 2001:df0:66:40::16
```

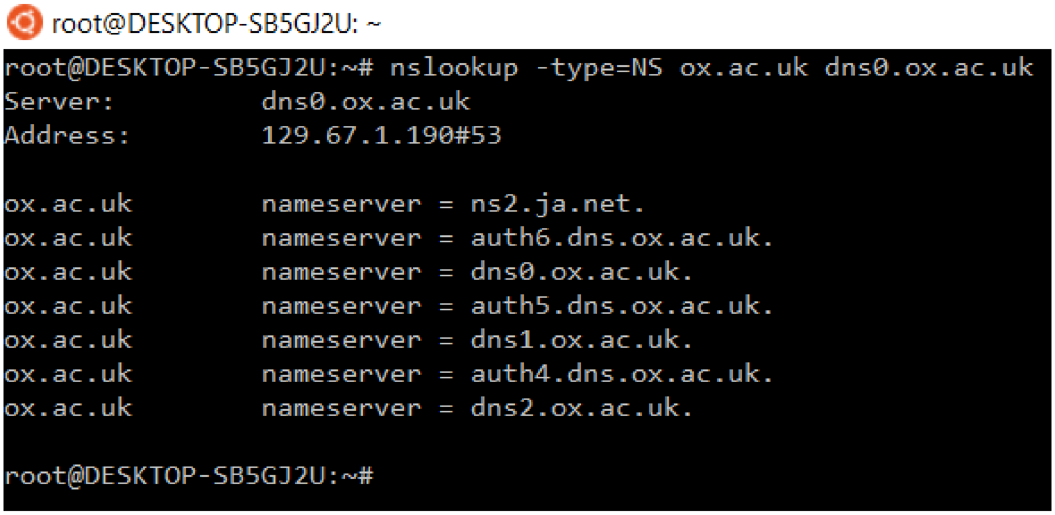
The IP address of that server: 111.65.250.2

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



```
root@DESKTOP-SB5GJ2U:~# nslookup -type=NS ox.ac.uk
Server:         203.113.188.1
Address:        203.113.188.1#53

Non-authoritative answer:
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.

Authoritative answers can be found from:
dns0.ox.ac.uk   internet address = 129.67.1.190
auth5.dns.ox.ac.uk      internet address = 93.93.128.67
dns1.ox.ac.uk   internet address = 129.67.1.191
auth4.dns.ox.ac.uk      internet address = 45.33.127.156
auth6.dns.ox.ac.uk      internet address = 185.24.221.32
ns2.ja.net      internet address = 193.63.105.17
dns2.ox.ac.uk   internet address = 163.1.2.190
auth5.dns.ox.ac.uk      has AAAA address 2a00:1098:0:80:1000::10
auth4.dns.ox.ac.uk      has AAAA address 2600:3c00::f03c:91ff:fe96:beac
auth6.dns.ox.ac.uk      has AAAA address 2a02:2770:11:0:21a:4aff:febe:759b
ns2.ja.net      has AAAA address 2001:630:0:45::11

root@DESKTOP-SB5GJ2U:~#
```

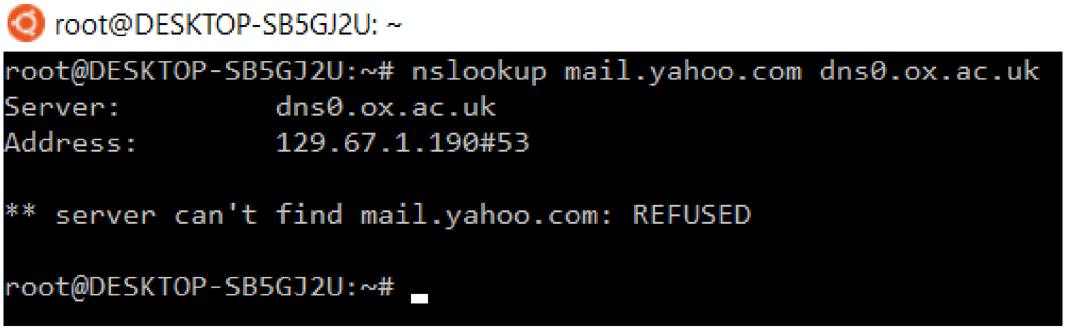
There are multiple authoritative servers. To confirm the authoritative DNS servers, we perform the same DNS query of one of the servers that can provide authoritative answers.



root@DESKTOP-SB5GJ2U: ~

```
root@DESKTOP-SB5GJ2U:~# nslookup -type=NS ox.ac.uk dns0.ox.ac.uk
Server:         dns0.ox.ac.uk
Address:        129.67.1.190#53

ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.

root@DESKTOP-SB5GJ2U:~#
```

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?

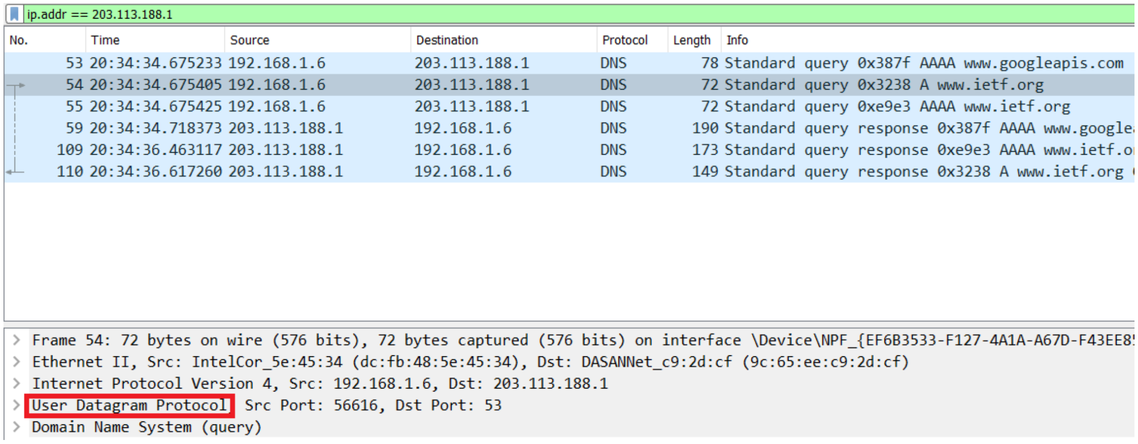


root@DESKTOP-SB5GJ2U: ~

```
root@DESKTOP-SB5GJ2U:~# nslookup mail.yahoo.com dns0.ox.ac.uk
Server:         dns0.ox.ac.uk
Address:        129.67.1.190#53

** server can't find mail.yahoo.com: REFUSED

root@DESKTOP-SB5GJ2U:~# _
```

As you can see, I cannot get the DNS servers to answer a query for a Yahoo mail server.

4. Locate the DNS query and response messages. Are they sent over UDP or TCP?



ip.addr == 203.113.188.1

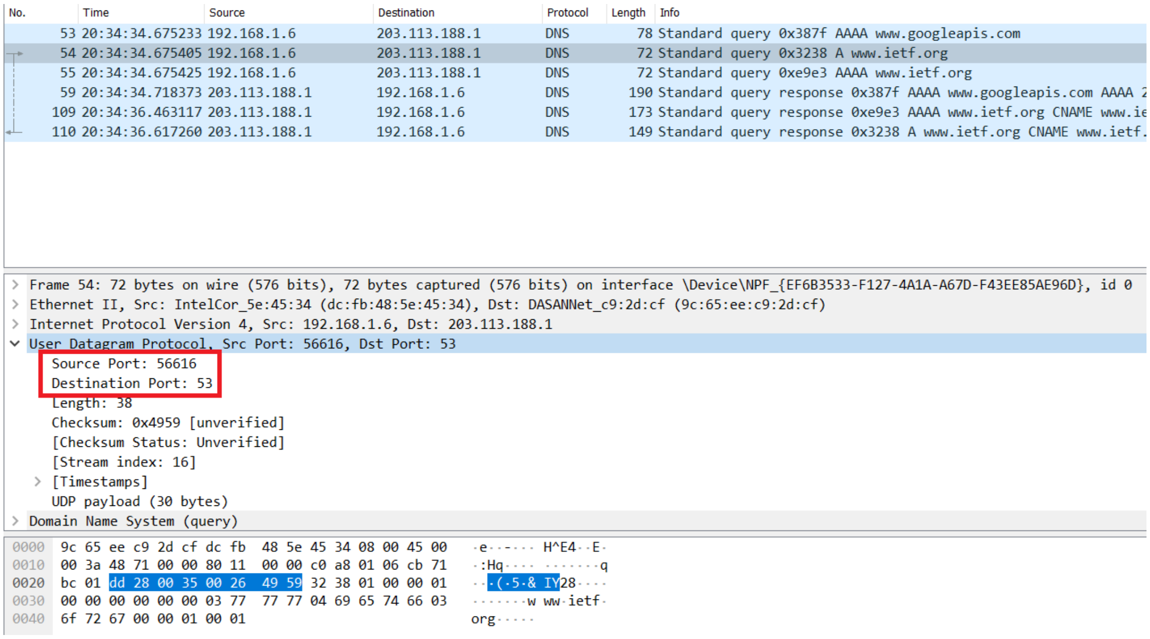
No.	Time	Source	Destination	Protocol	Length	Info
53	20:34:34.675233	192.168.1.6	203.113.188.1	DNS	78	Standard query 0x387f AAAA www.googleapis.com
54	20:34:34.675405	192.168.1.6	203.113.188.1	DNS	72	Standard query 0x3238 A www.ietf.org
55	20:34:34.675425	192.168.1.6	203.113.188.1	DNS	72	Standard query 0xe9e3 AAAA www.ietf.org
59	20:34:34.718373	203.113.188.1	192.168.1.6	DNS	190	Standard query response 0x387f AAAA www.google
109	20:34:36.463117	203.113.188.1	192.168.1.6	DNS	173	Standard query response 0xe9e3 AAAA www.ietf.o
110	20:34:36.617260	203.113.188.1	192.168.1.6	DNS	149	Standard query response 0x3238 A www.ietf.org

```
> Frame 54: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE8
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.113.188.1
> User Datagram Protocol, Src Port: 56616, Dst Port: 53
> Domain Name System (query)
```

They are sent over UDP.

5. What is the destination port for the DNS query message? What is the source port of DNS response message?
Destination port: 53

Source port: 56616



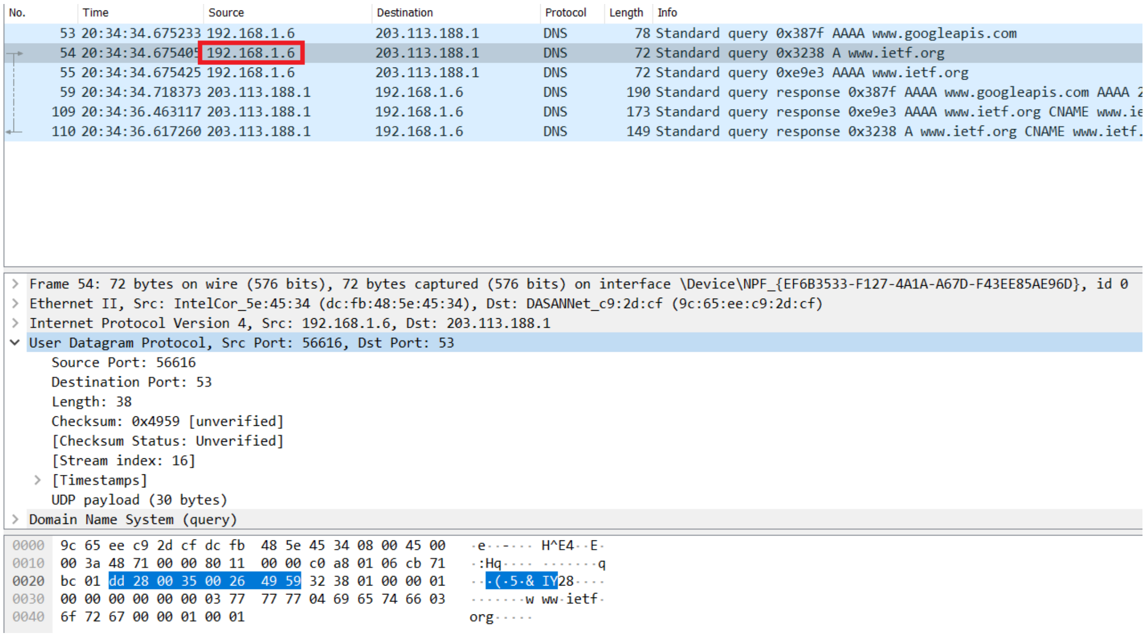
```
No.    Time               Source          Destination     Protocol  Length  Info
    53 20:34:34.675233 192.168.1.6     203.113.188.1   DNS          78 Standard query 0x387f AAAA www.googleapis.com
    54 20:34:34.675405 192.168.1.6     203.113.188.1   DNS          72 Standard query 0x3238 A www.ietf.org
    55 20:34:34.675425 192.168.1.6     203.113.188.1   DNS          72 Standard query 0xe9e3 AAAA www.ietf.org
    59 20:34:34.718373 203.113.188.1   192.168.1.6     DNS         190 Standard query response 0x387f AAAA www.googleapis.com AAAA 2
   109 20:34:36.463117 203.113.188.1   192.168.1.6     DNS         173 Standard query response 0xe9e3 AAAA www.ietf.org CNAME www.ie
   110 20:34:36.617260 203.113.188.1   192.168.1.6     DNS         149 Standard query response 0x3238 A www.ietf.org CNAME www.ietf.
```

```
> Frame 54: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.113.188.1
v User Datagram Protocol, Src Port: 56616, Dst Port: 53
    Source Port: 56616
    Destination Port: 53
    Length: 38
    Checksum: 0x4959 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

```
0000  9c 65 ee c9 2d cf dc fb  48 5e 45 34 08 00 45 00   ·e··-··· H^E4··E·
0010  00 3a 48 71 00 00 80 11  00 00 c0 a8 01 06 cb 71   ·:Hq···· ·······q
0020  bc 01 dd 28 00 35 00 26  49 59 32 38 01 00 00 01   ···(·5·& IY28····
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·····
```

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?

The IP address that the DNS query message sent to: 192.168.1.6

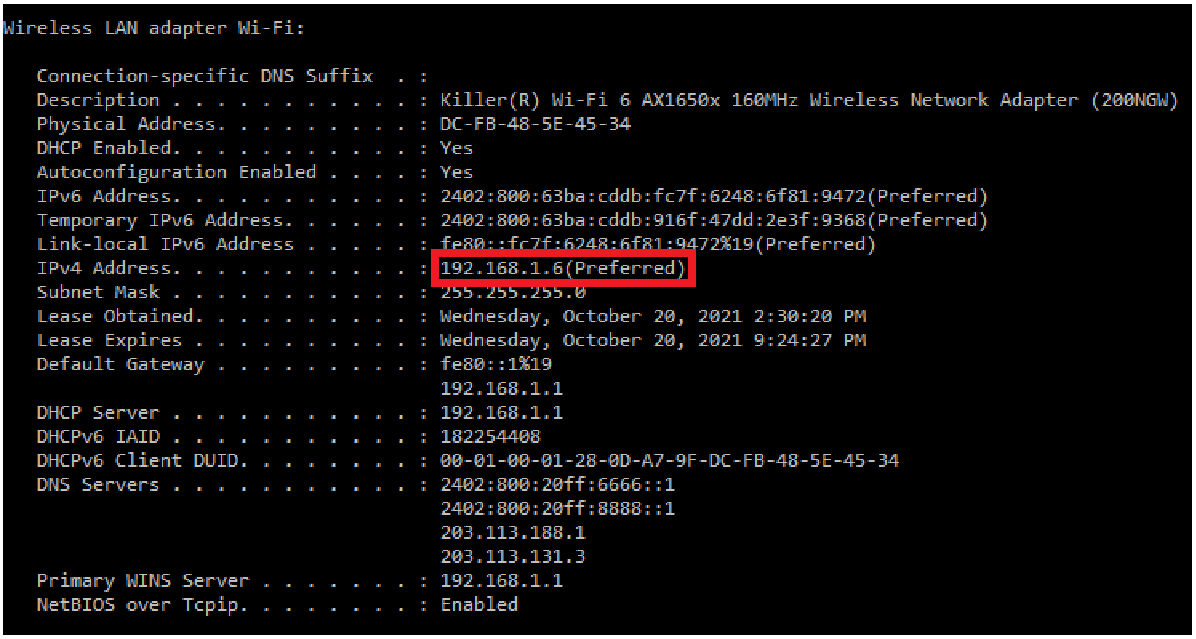


```
No.    Time               Source          Destination     Protocol  Length  Info
    53 20:34:34.675233 192.168.1.6     203.113.188.1   DNS          78 Standard query 0x387f AAAA www.googleapis.com
    54 20:34:34.675405 192.168.1.6     203.113.188.1   DNS          72 Standard query 0x3238 A www.ietf.org
    55 20:34:34.675425 192.168.1.6     203.113.188.1   DNS          72 Standard query 0xe9e3 AAAA www.ietf.org
    59 20:34:34.718373 203.113.188.1   192.168.1.6     DNS         190 Standard query response 0x387f AAAA www.googleapis.com AAAA 2
   109 20:34:36.463117 203.113.188.1   192.168.1.6     DNS         173 Standard query response 0xe9e3 AAAA www.ietf.org CNAME www.ie
   110 20:34:36.617260 203.113.188.1   192.168.1.6     DNS         149 Standard query response 0x3238 A www.ietf.org CNAME www.ietf.
```

```
> Frame 54: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.113.188.1
v User Datagram Protocol, Src Port: 56616, Dst Port: 53
    Source Port: 56616
    Destination Port: 53
    Length: 38
    Checksum: 0x4959 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

```
0000  9c 65 ee c9 2d cf dc fb  48 5e 45 34 08 00 45 00   ·e··-··· H^E4··E·
0010  00 3a 48 71 00 00 80 11  00 00 c0 a8 01 06 cb 71   ·:Hq···· ·······q
0020  bc 01 dd 28 00 35 00 26  49 59 32 38 01 00 00 01   ···(·5·& IY28····
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·····
```

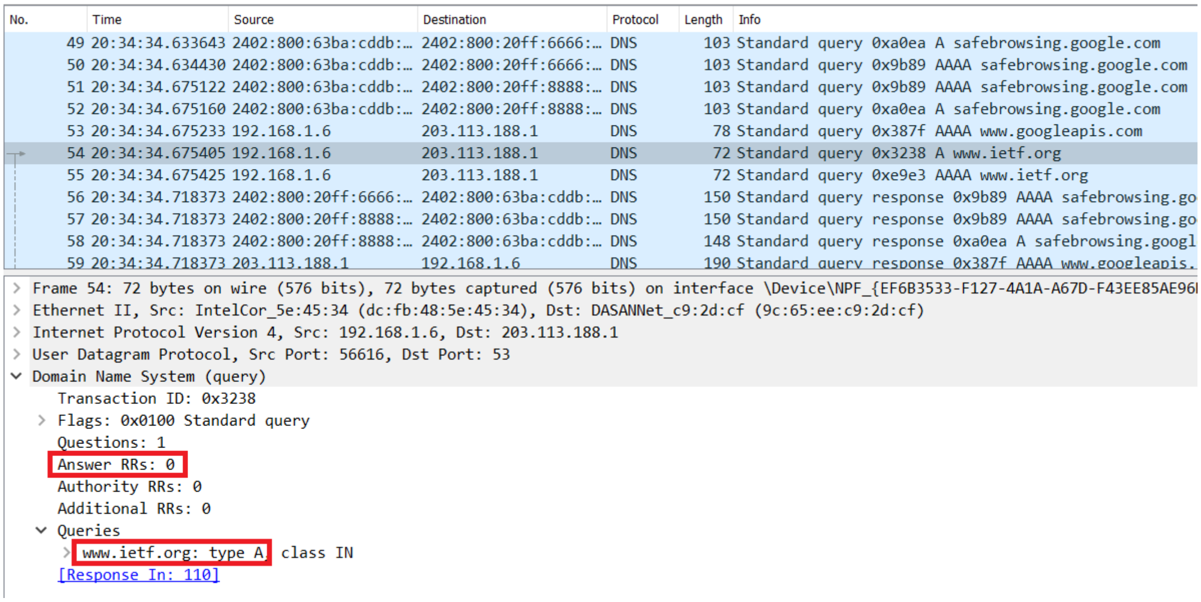
IP address of local DNS server: 192.168.1.6



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Killer(R) Wi-Fi 6 AX1650x 160MHz Wireless Network Adapter (200NGW)
   Physical Address. . . . . . . . . : DC-FB-48-5E-45-34
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2402:800:63ba:cddb:fc7f:6248:6f81:9472(Preferred)
   Temporary IPv6 Address. . . . . . : 2402:800:63ba:cddb:916f:47dd:2e3f:9368(Preferred)
   Link-local IPv6 Address . . . . . : fe80::fc7f:6248:6f81:9472%19(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, October 20, 2021 2:30:20 PM
   Lease Expires . . . . . . . . . . : Wednesday, October 20, 2021 9:24:27 PM
   Default Gateway . . . . . . . . . : fe80::1%19
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 182254408
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-0D-A7-9F-DC-FB-48-5E-45-34
   DNS Servers . . . . . . . . . . . : 2402:800:20ff:6666::1
                                       2402:800:20ff:8888::1
                                       203.113.188.1
                                       203.113.131.3
   Primary WINS Server . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

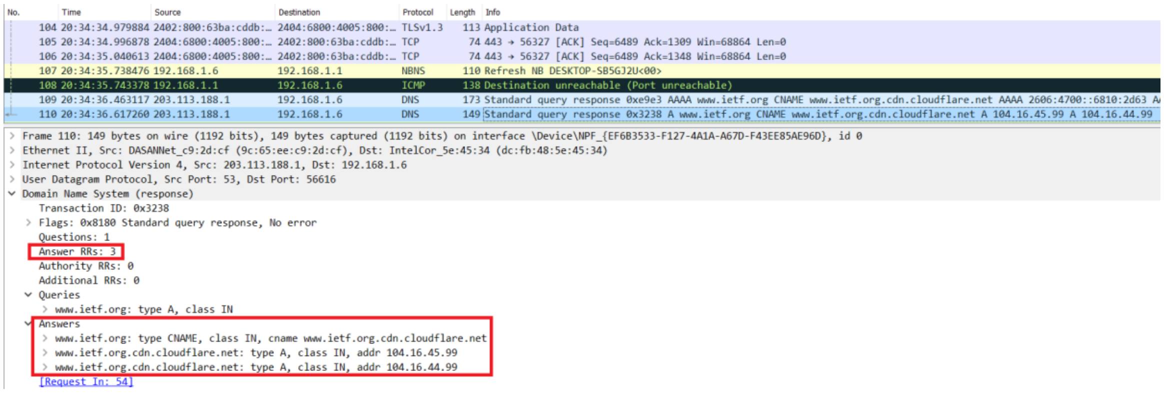
These two IP addresses are the same.

7. Examine the DNS query message. What type of DNS query is it? Does the query message contain any answers?
   Type of DNS query: A
   The query does not contain any answers.

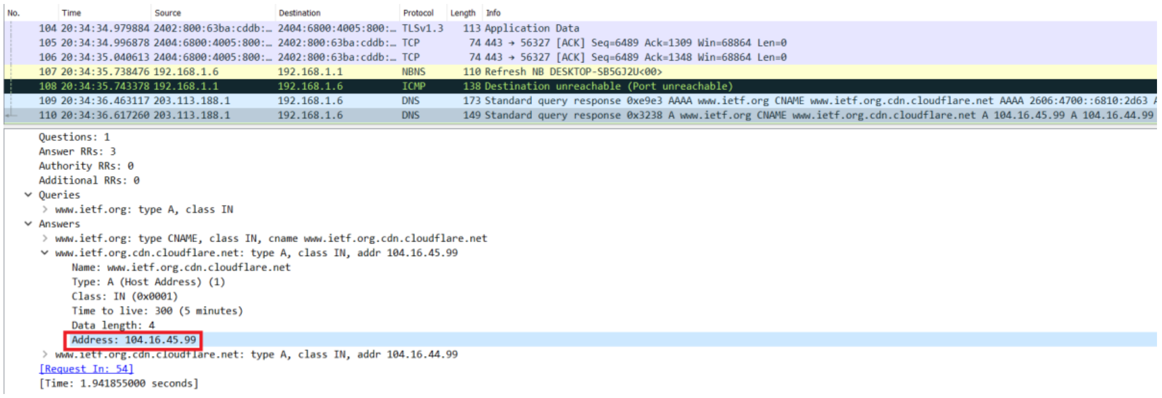


```
No.   Time              Source                  Destination             Protocol  Length  Info
   49 20:34:34.633643 2402:800:63ba:cddb:… 2402:800:20ff:6666:… DNS        103 Standard query 0xa0ea A safebrowsing.google.com
   50 20:34:34.634430 2402:800:63ba:cddb:… 2402:800:20ff:6666:… DNS        103 Standard query 0x9b89 AAAA safebrowsing.google.com
   51 20:34:34.675122 2402:800:63ba:cddb:… 2402:800:20ff:8888:… DNS        103 Standard query 0x9b89 AAAA safebrowsing.google.com
   52 20:34:34.675160 2402:800:63ba:cddb:… 2402:800:20ff:8888:… DNS        103 Standard query 0xa0ea A safebrowsing.google.com
   53 20:34:34.675233 192.168.1.6          203.113.188.1        DNS         78 Standard query 0x387f AAAA www.googleapis.com
   54 20:34:34.675405 192.168.1.6          203.113.188.1        DNS         72 Standard query 0x3238 A www.ietf.org
   55 20:34:34.675425 192.168.1.6          203.113.188.1        DNS         72 Standard query 0xe9e3 AAAA www.ietf.org
   56 20:34:34.718373 2402:800:20ff:6666:… 2402:800:63ba:cddb:… DNS        150 Standard query response 0x9b89 AAAA safebrowsing.go
   57 20:34:34.718373 2402:800:20ff:8888:… 2402:800:63ba:cddb:… DNS        150 Standard query response 0x9b89 AAAA safebrowsing.go
   58 20:34:34.718373 2402:800:20ff:8888:… 2402:800:63ba:cddb:… DNS        148 Standard query response 0xa0ea A safebrowsing.googl
   59 20:34:34.718373 203.113.188.1        192.168.1.6          DNS        190 Standard query response 0x387f AAAA www.googleapis.

> Frame 54: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 203.113.188.1
> User Datagram Protocol, Src Port: 56616, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x3238
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 110]
```

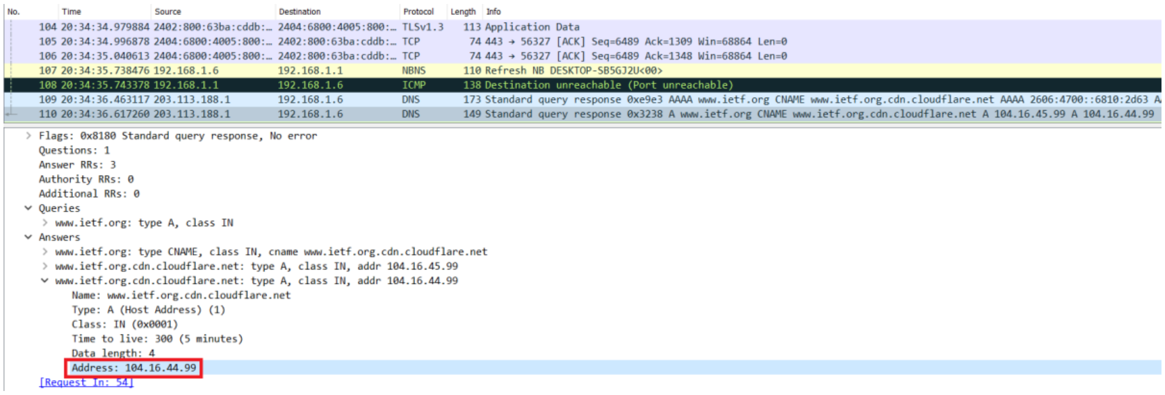
8. Examine the DNS response message. How many answers are provided? What do each of these answers contain?
   There are 3 answers. First answer has type CNAME, the others contain the address of the website it was queried for.



```
No.   Time               Source               Destination          Protocol  Length Info
  104 20:34:34.979884 2402:800:63ba:cddb:… 2404:6800:4005:800:… TLSv1.3   113 Application Data
  105 20:34:34.996878 2404:6800:4005:800:… 2402:800:63ba:cddb:… TCP        74 443 → 56327 [ACK] Seq=6489 Ack=1309 Win=68864 Len=0
  106 20:34:35.040613 2404:6800:4005:800:… 2402:800:63ba:cddb:… TCP        74 443 → 56327 [ACK] Seq=6489 Ack=1348 Win=68864 Len=0
  107 20:34:35.738476 192.168.1.6          192.168.1.1          NBNS      110 Refresh NB DESKTOP-SB5GJ2U<00>
  108 20:34:35.743378 192.168.1.1          192.168.1.6          ICMP      138 Destination unreachable (Port unreachable)
  109 20:34:36.463117 203.113.188.1        192.168.1.6          DNS       173 Standard query response 0xe9e3 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 A
  110 20:34:36.617260 203.113.188.1        192.168.1.6          DNS       149 Standard query response 0x3238 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99

> Frame 110: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_5e:45:34 (dc:fb:48:5e:45:34)
> Internet Protocol Version 4, Src: 203.113.188.1, Dst: 192.168.1.6
> User Datagram Protocol, Src Port: 53, Dst Port: 56616
v Domain Name System (response)
    Transaction ID: 0x3238
  > 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 104.16.45.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    [Request In: 54]
```



```
No.   Time               Source               Destination          Protocol  Length Info
  104 20:34:34.979884 2402:800:63ba:cddb:… 2404:6800:4005:800:… TLSv1.3   113 Application Data
  105 20:34:34.996878 2404:6800:4005:800:… 2402:800:63ba:cddb:… TCP        74 443 → 56327 [ACK] Seq=6489 Ack=1309 Win=68864 Len=0
  106 20:34:35.040613 2404:6800:4005:800:… 2402:800:63ba:cddb:… TCP        74 443 → 56327 [ACK] Seq=6489 Ack=1348 Win=68864 Len=0
  107 20:34:35.738476 192.168.1.6          192.168.1.1          NBNS      110 Refresh NB DESKTOP-SB5GJ2U<00>
  108 20:34:35.743378 192.168.1.1          192.168.1.6          ICMP      138 Destination unreachable (Port unreachable)
  109 20:34:36.463117 203.113.188.1        192.168.1.6          DNS       173 Standard query response 0xe9e3 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 A
  110 20:34:36.617260 203.113.188.1        192.168.1.6          DNS       149 Standard query response 0x3238 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99

    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
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.45.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    [Request In: 54]
    [Time: 1.941855000 seconds]
```



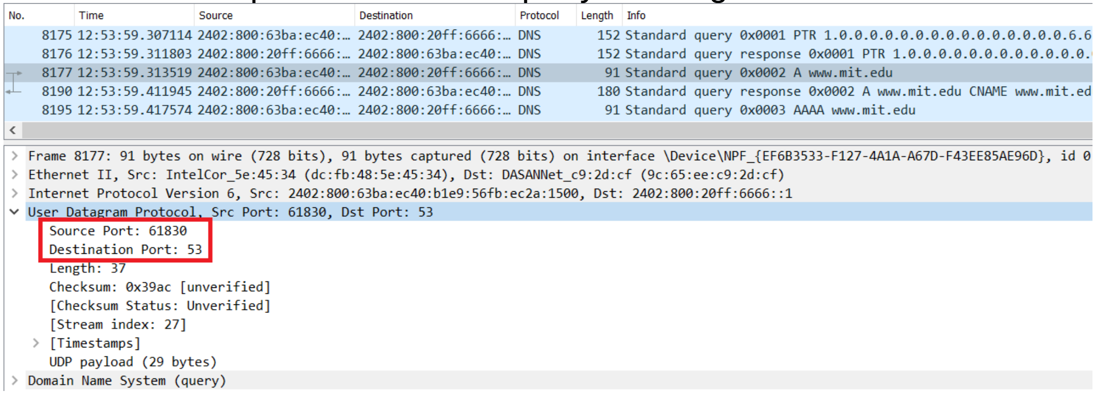
```
No.   Time               Source               Destination          Protocol  Length Info
  104 20:34:34.979884 2402:800:63ba:cddb:… 2404:6800:4005:800:… TLSv1.3   113 Application Data
  105 20:34:34.996878 2404:6800:4005:800:… 2402:800:63ba:cddb:… TCP        74 443 → 56327 [ACK] Seq=6489 Ack=1309 Win=68864 Len=0
  106 20:34:35.040613 2404:6800:4005:800:… 2402:800:63ba:cddb:… TCP        74 443 → 56327 [ACK] Seq=6489 Ack=1348 Win=68864 Len=0
  107 20:34:35.738476 192.168.1.6          192.168.1.1          NBNS      110 Refresh NB DESKTOP-SB5GJ2U<00>
  108 20:34:35.743378 192.168.1.1          192.168.1.6          ICMP      138 Destination unreachable (Port unreachable)
  109 20:34:36.463117 203.113.188.1        192.168.1.6          DNS       173 Standard query response 0xe9e3 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 A
  110 20:34:36.617260 203.113.188.1        192.168.1.6          DNS       149 Standard query response 0x3238 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99

  > 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 104.16.45.99
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.44.99
    [Request In: 54]
```

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 destination of the SYN packet is 104.16.45.99, the same address that was provided in the DNS response message as the type “A” address of the webpage.

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    No because all the images are loaded from www.ietf.org so there is no need for additional DNS queries.

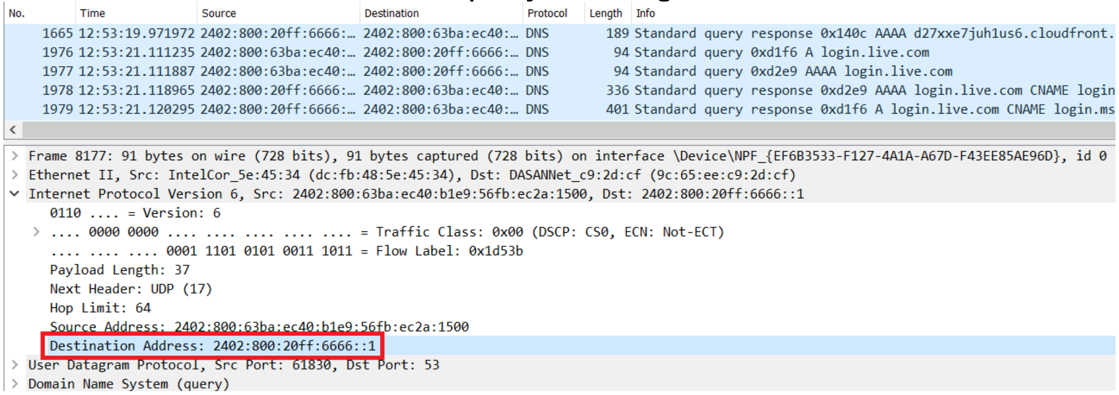
11. What is the destination port for the DNS query message? What is the source port of DNS response message?

The source port of DNS response message: 61830
The destination port for the DNS query message: 53



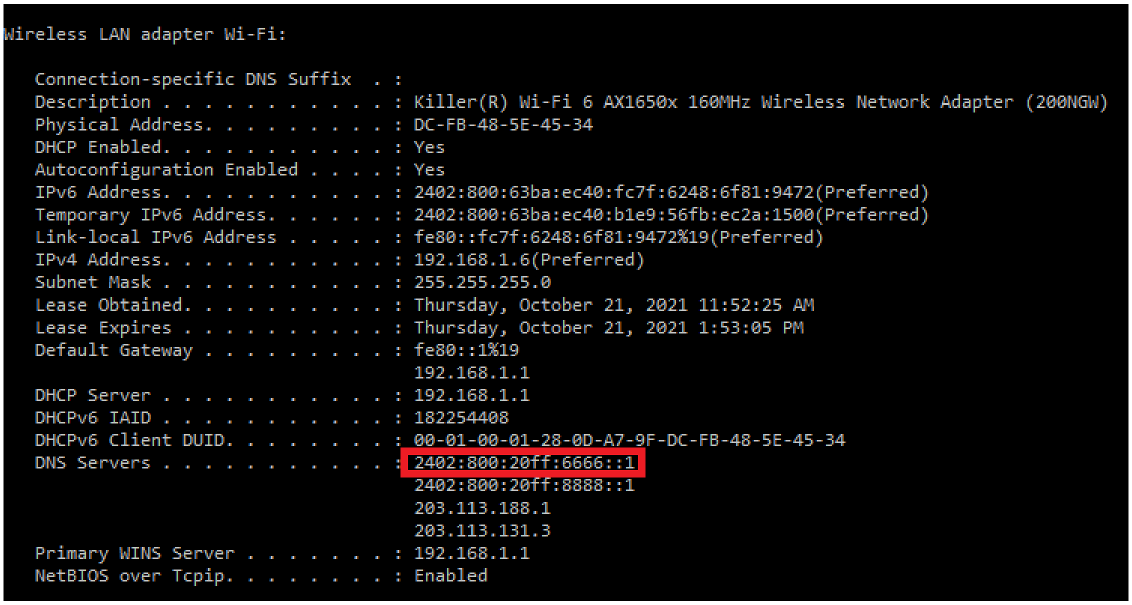
```
No.   Time            Source                Destination           Protocol Length Info
 8175 12:53:59.307114 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS       152 Standard query 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.6
 8176 12:53:59.311803 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS       152 Standard query response 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
 8177 12:53:59.313519 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS        91 Standard query 0x0002 A www.mit.edu
 8190 12:53:59.411945 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS       180 Standard query response 0x0002 A www.mit.edu CNAME www.mit.ed
 8195 12:53:59.417574 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS        91 Standard query 0x0003 AAAA www.mit.edu

> Frame 8177: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 6, Src: 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500, Dst: 2402:800:20ff:6666::1
v User Datagram Protocol, Src Port: 61830, Dst Port: 53
    Source Port: 61830
    Destination Port: 53
    Length: 37
    Checksum: 0x39ac [unverified]
    [Checksum Status: Unverified]
    [Stream index: 27]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
The IP address that the DNS query message sent to: 2402:800:20ff:6666::1



```
No.   Time            Source                Destination           Protocol Length Info
 1665 12:53:19.971972 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS       189 Standard query response 0x140c AAAA d27xxe7juh1us6.cloudfront.
 1976 12:53:21.111235 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS        94 Standard query 0xd1f6 A login.live.com
 1977 12:53:21.111887 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS        94 Standard query 0xd2e9 AAAA login.live.com
 1978 12:53:21.118965 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS       336 Standard query response 0xd2e9 AAAA login.live.com CNAME login
 1979 12:53:21.120295 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS       401 Standard query response 0xd1f6 A login.live.com CNAME login.ms

> Frame 8177: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
v Internet Protocol Version 6, Src: 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500, Dst: 2402:800:20ff:6666::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0001 1101 0101 0011 1011 = Flow Label: 0x1d53b
    Payload Length: 37
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500
    Destination Address: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 61830, Dst Port: 53
> Domain Name System (query)
```

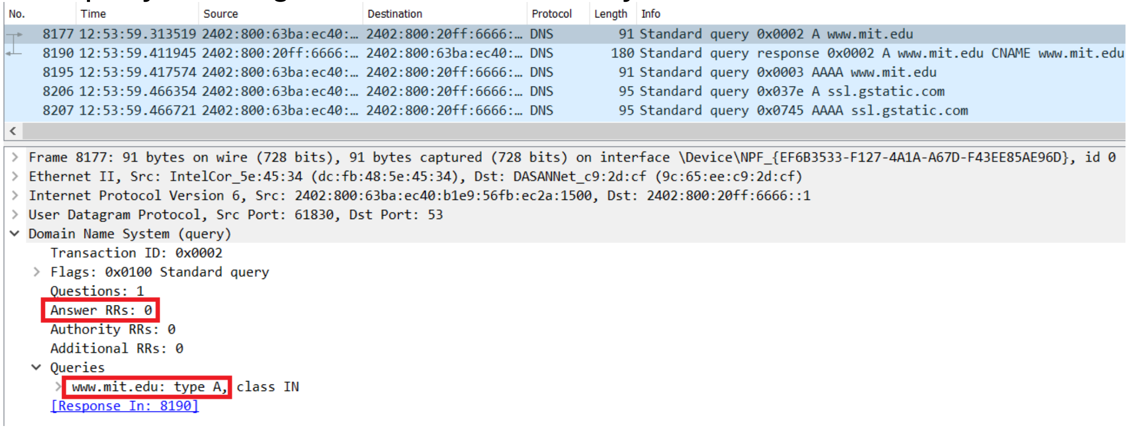
This IP address is the same as my default local DNS server.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Killer(R) Wi-Fi 6 AX1650x 160MHz Wireless Network Adapter (200NGW)
   Physical Address. . . . . . . . . : DC-FB-48-5E-45-34
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2402:800:63ba:ec40:fc7f:6248:6f81:9472(Preferred)
   Temporary IPv6 Address. . . . . . : 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500(Preferred)
   Link-local IPv6 Address . . . . . : fe80::fc7f:6248:6f81:9472%19(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, October 21, 2021 11:52:25 AM
   Lease Expires . . . . . . . . . . : Thursday, October 21, 2021 1:53:05 PM
   Default Gateway . . . . . . . . . : fe80::1%19
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 182254408
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-0D-A7-9F-DC-FB-48-5E-45-34
   DNS Servers . . . . . . . . . . . : 2402:800:20ff:6666::1
                                       2402:800:20ff:8888::1
                                       203.113.188.1
                                       203.113.131.3
   Primary WINS Server . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

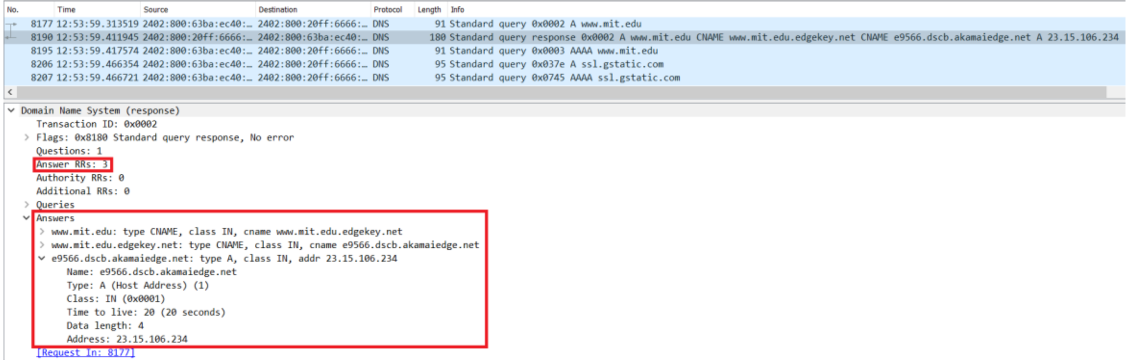
13. Examine the DNS query message. What type of DNS query is it? Does the query message contain any answers?
Type of DNS query: A.

The query message does not contain any answers.



```
No.    Time            Source                 Destination            Protocol  Length  Info
  8177 12:53:59.313519 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          91 Standard query 0x0002 A www.mit.edu
  8190 12:53:59.411945 2402:800:20ff:6666:…  2402:800:63ba:ec40:…  DNS         180 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
  8195 12:53:59.417574 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          91 Standard query 0x0003 AAAA www.mit.edu
  8206 12:53:59.466354 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          95 Standard query 0x037e A ssl.gstatic.com
  8207 12:53:59.466721 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          95 Standard query 0x0745 AAAA ssl.gstatic.com

> Frame 8177: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 6, Src: 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500, Dst: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 61830, 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
    > www.mit.edu: type A, class IN
    [Response In: 8190]
```

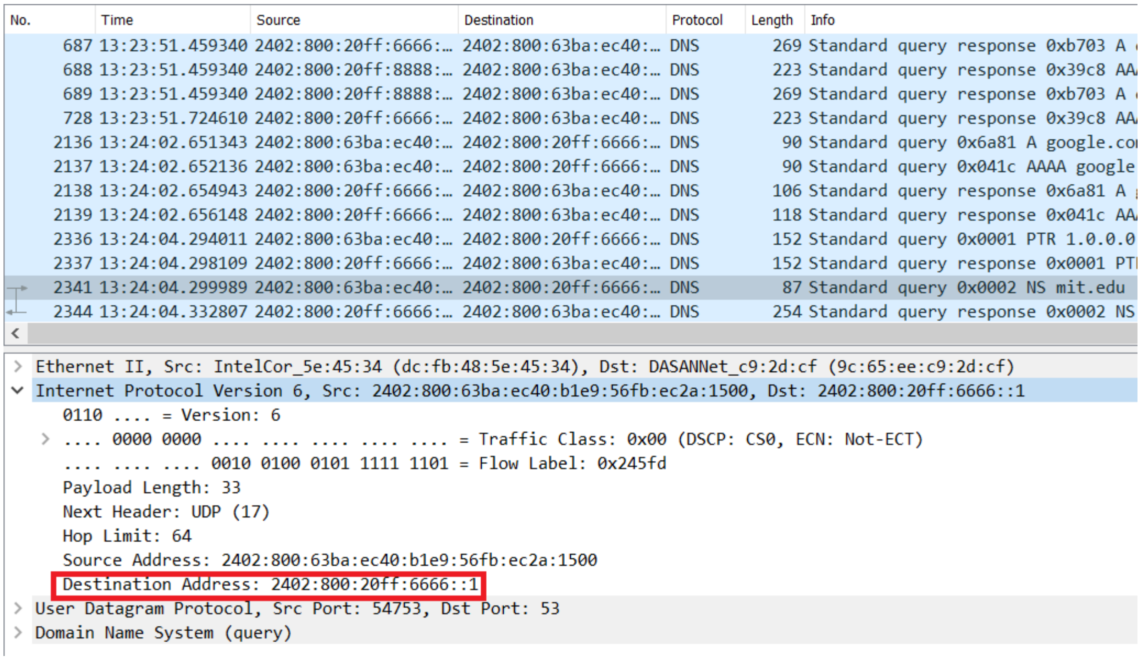
14. Examine the DNS response message. How many answers are provided? What do each of these answers contain?
There are 3 answers provided. First two answers have type CNAME, the last answer contains the address of the website it was queried for.



```
No.    Time            Source                 Destination            Protocol  Length  Info
  8177 12:53:59.313519 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          91 Standard query 0x0002 A www.mit.edu
  8190 12:53:59.411945 2402:800:20ff:6666:…  2402:800:63ba:ec40:…  DNS         180 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.15.106.234
  8195 12:53:59.417574 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          91 Standard query 0x0003 AAAA www.mit.edu
  8206 12:53:59.466354 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          95 Standard query 0x037e A ssl.gstatic.com
  8207 12:53:59.466721 2402:800:63ba:ec40:…  2402:800:20ff:6666:…  DNS          95 Standard query 0x0745 AAAA ssl.gstatic.com

v 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
  v 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
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.15.106.234
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 23.15.106.234
    [Request In: 8177]
```

15. Provide a screenshot
Each question I have already provided a screenshot.

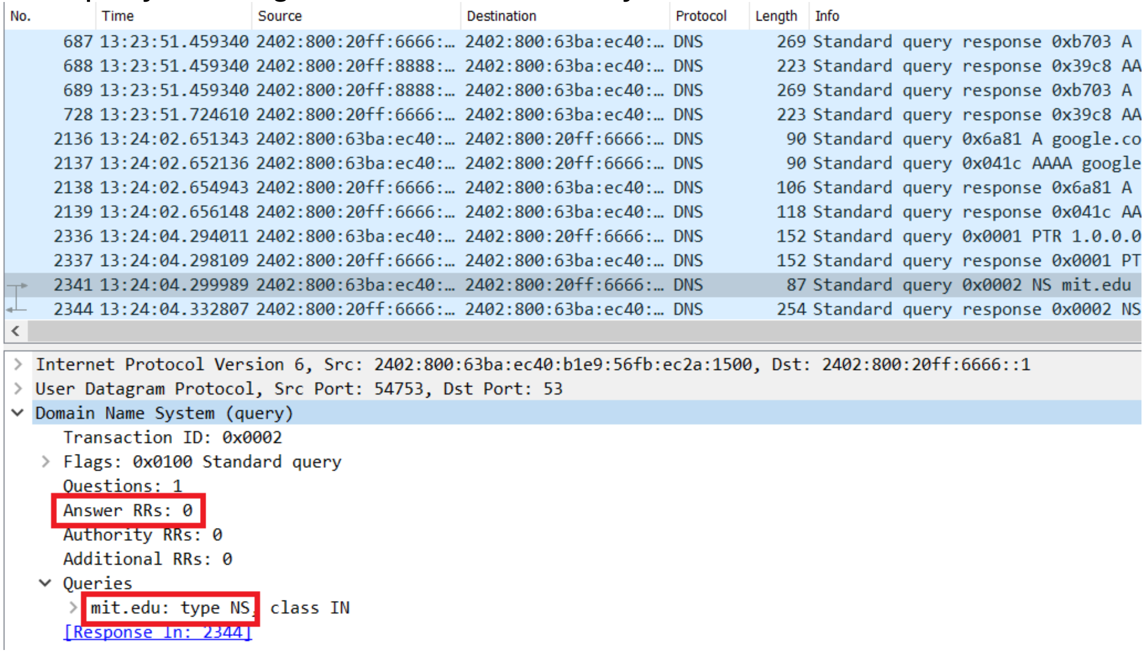
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
The IP address that the DNS query message sent to: 2402:800:20ff:6666::1.
It is the same to my default local DNS server which I have provided above.



```
No.   Time            Source                Destination           Protocol  Length  Info
  687 13:23:51.459340 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          269 Standard query response 0xb703 A
  688 13:23:51.459340 2402:800:20ff:8888:… 2402:800:63ba:ec40:… DNS          223 Standard query response 0x39c8 AA
  689 13:23:51.459340 2402:800:20ff:8888:… 2402:800:63ba:ec40:… DNS          269 Standard query response 0xb703 A
  728 13:23:51.724610 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          223 Standard query response 0x39c8 AA
 2136 13:24:02.651343 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS           90 Standard query 0x6a81 A google.co
 2137 13:24:02.652136 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS           90 Standard query 0x041c AAAA google
 2138 13:24:02.654943 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          106 Standard query response 0x6a81 A
 2139 13:24:02.656148 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          118 Standard query response 0x041c AA
 2336 13:24:04.294011 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS          152 Standard query 0x0001 PTR 1.0.0.0
 2337 13:24:04.298109 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          152 Standard query response 0x0001 PT
 2341 13:24:04.299989 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS           87 Standard query 0x0002 NS mit.edu
 2344 13:24:04.332807 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          254 Standard query response 0x0002 NS

> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
v Internet Protocol Version 6, Src: 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500, Dst: 2402:800:20ff:6666::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0010 0100 0101 1111 1101 = Flow Label: 0x245fd
    Payload Length: 33
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500
    Destination Address: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 54753, Dst Port: 53
> Domain Name System (query)
```

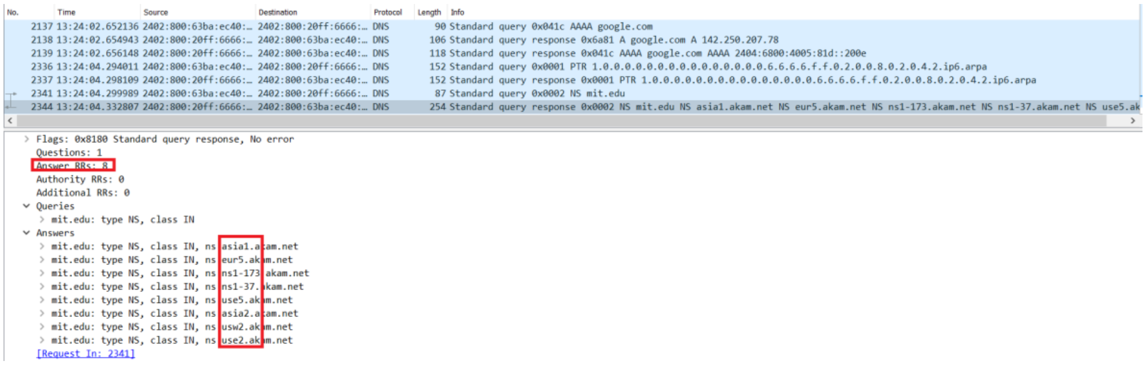
17. Examine the DNS query message. What type of DNS query is it? Does the query message contain any answers?
Type of DNS query: NS.

The query message does not contain any answers.



```
No.   Time            Source                Destination           Protocol  Length  Info
  687 13:23:51.459340 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          269 Standard query response 0xb703 A
  688 13:23:51.459340 2402:800:20ff:8888:… 2402:800:63ba:ec40:… DNS          223 Standard query response 0x39c8 AA
  689 13:23:51.459340 2402:800:20ff:8888:… 2402:800:63ba:ec40:… DNS          269 Standard query response 0xb703 A
  728 13:23:51.724610 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          223 Standard query response 0x39c8 AA
 2136 13:24:02.651343 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS           90 Standard query 0x6a81 A google.co
 2137 13:24:02.652136 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS           90 Standard query 0x041c AAAA google
 2138 13:24:02.654943 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          106 Standard query response 0x6a81 A
 2139 13:24:02.656148 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          118 Standard query response 0x041c AA
 2336 13:24:04.294011 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS          152 Standard query 0x0001 PTR 1.0.0.0
 2337 13:24:04.298109 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          152 Standard query response 0x0001 PT
 2341 13:24:04.299989 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS           87 Standard query 0x0002 NS mit.edu
 2344 13:24:04.332807 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS          254 Standard query response 0x0002 NS

> Internet Protocol Version 6, Src: 2402:800:63ba:ec40:b1e9:56fb:ec2a:1500, Dst: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 54753, 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
    > mit.edu: type NS, class IN
    [Response In: 2344]
```

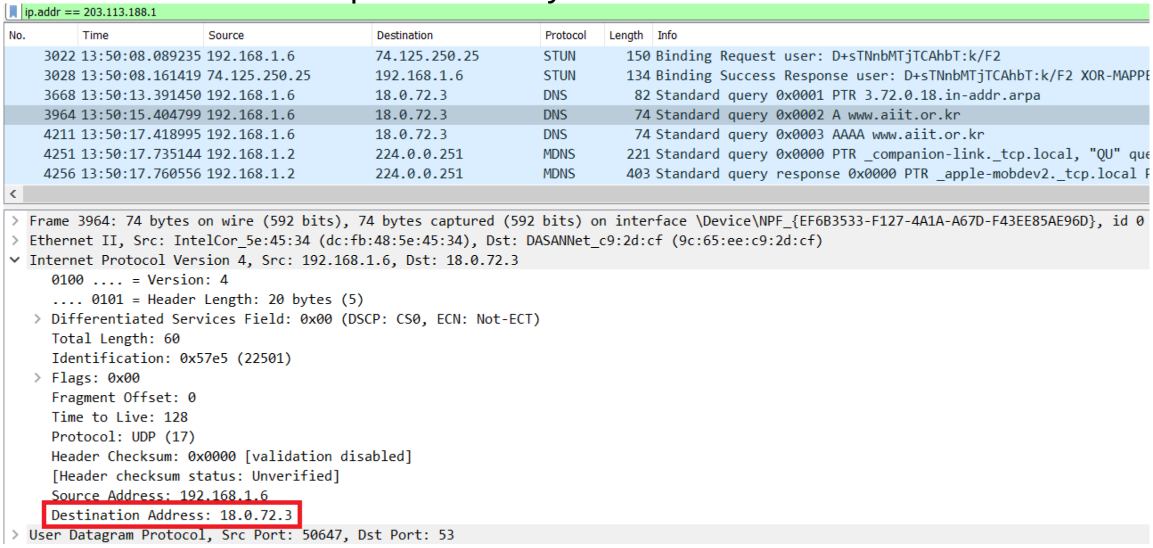
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?
There are 8 MIT nameservers that response message provides: asia1, eur5, ns1-173, ns1-37, use5, asia2, usw2, use2. It does not provide the IP addresses of the MIT nameservers.



```
No.   Time            Source                 Destination            Protocol  Length  Info
 2137 13:24:02.652136 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS          90 Standard query 0x041c AAAA google.com
 2138 13:24:02.654943 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS         106 Standard query response 0x6a81 A google.com A 142.250.207.78
 2139 13:24:02.656148 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS         118 Standard query response 0x041c AAAA google.com AAAA 2404:6800:4005:81d::200e
 2336 13:24:04.294011 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS         152 Standard query 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.6.6.6.f.f.0.2.0.0.8.0.2.0.4.2.ip6.arpa
 2337 13:24:04.298109 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS         152 Standard query response 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.6.6.6.f.f.0.2.0.0.8.0.2.0.4.2.ip6.arpa
 2341 13:24:04.299989 2402:800:63ba:ec40:… 2402:800:20ff:6666:… DNS          87 Standard query 0x0002 NS mit.edu
 2344 13:24:04.332807 2402:800:20ff:6666:… 2402:800:63ba:ec40:… DNS         254 Standard query response 0x0002 NS mit.edu NS asia1.akam.net NS eur5.akam.net NS ns1-173.akam.net NS ns1-37.akam.net NS use5.ak

  > 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 asia1.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.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 asia2.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    [Request In: 2341]
```

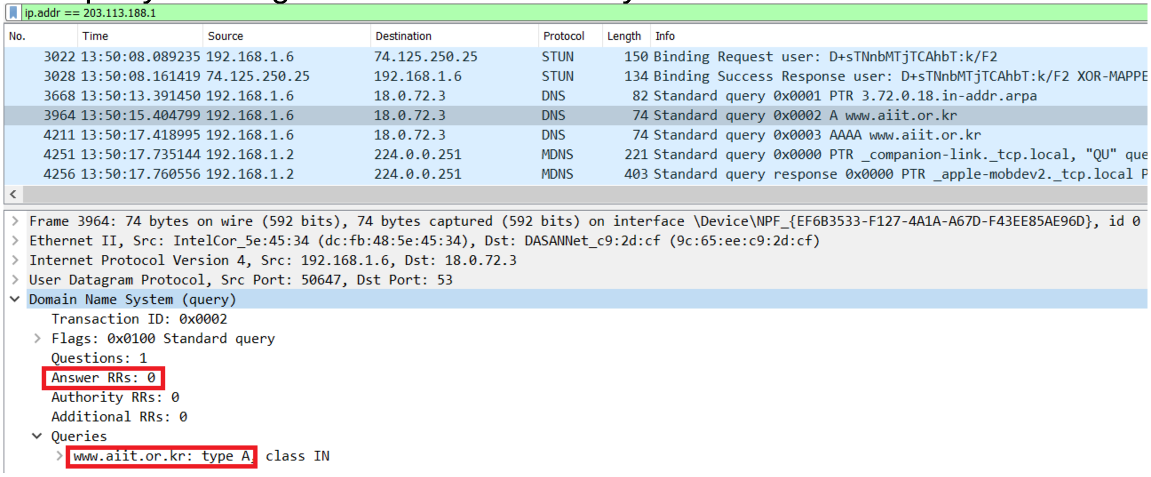
19. Provide a screenshot
I have already provided screenshot for each question.

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 IP address that the DNS query message sent to: 18.0.72.3.
This IP address corresponds to bitsy.mit.edu.



```
ip.addr == 203.113.188.1

No.   Time            Source         Destination    Protocol  Length  Info
 3022 13:50:08.089235 192.168.1.6    74.125.250.25  STUN       150 Binding Request user: D+sTNnbMTjTCAhbT:k/F2
 3028 13:50:08.161419 74.125.250.25  192.168.1.6    STUN       134 Binding Success Response user: D+sTNnbMTjTCAhbT:k/F2 XOR-MAPPE
 3668 13:50:13.391450 192.168.1.6    18.0.72.3      DNS         82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
 3964 13:50:15.404799 192.168.1.6    18.0.72.3      DNS         74 Standard query 0x0002 A www.aiit.or.kr
 4211 13:50:17.418995 192.168.1.6    18.0.72.3      DNS         74 Standard query 0x0003 AAAA www.aiit.or.kr
 4251 13:50:17.735144 192.168.1.2    224.0.0.251    MDNS       221 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" que
 4256 13:50:17.760556 192.168.1.2    224.0.0.251    MDNS       403 Standard query response 0x0000 PTR _apple-mobdev2._tcp.local P

> Frame 3964: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
˅ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 18.0.72.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x57e5 (22501)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.6
    Destination Address: 18.0.72.3
> User Datagram Protocol, Src Port: 50647, Dst Port: 53
```

21. Examine the DNS query message. What type of DNS query is it? Does the query message contain any answers?
Type of DNS query: A.
The query message does not contain any answers.



```
ip.addr == 203.113.188.1

No.   Time            Source         Destination    Protocol  Length  Info
 3022 13:50:08.089235 192.168.1.6    74.125.250.25  STUN       150 Binding Request user: D+sTNnbMTjTCAhbT:k/F2
 3028 13:50:08.161419 74.125.250.25  192.168.1.6    STUN       134 Binding Success Response user: D+sTNnbMTjTCAhbT:k/F2 XOR-MAPPE
 3668 13:50:13.391450 192.168.1.6    18.0.72.3      DNS         82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
 3964 13:50:15.404799 192.168.1.6    18.0.72.3      DNS         74 Standard query 0x0002 A www.aiit.or.kr
 4211 13:50:17.418995 192.168.1.6    18.0.72.3      DNS         74 Standard query 0x0003 AAAA www.aiit.or.kr
 4251 13:50:17.735144 192.168.1.2    224.0.0.251    MDNS       221 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" que
 4256 13:50:17.760556 192.168.1.2    224.0.0.251    MDNS       403 Standard query response 0x0000 PTR _apple-mobdev2._tcp.local P

> Frame 3964: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
> Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 50647, 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.aiit.or.kr: type A, class IN
```

22. Examine the DNS response message. How many answers are provided?

What does each of these answers contain?
There is no response message.

23. Provide a screenshot

I have provided screenshot for each question.