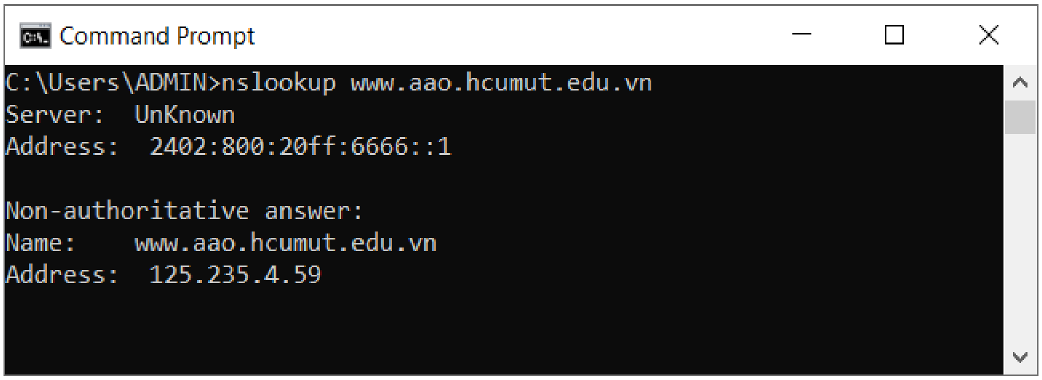
LAB 2B
Wireshark DNS v8.0

Name: Hồ Đức Trí
Student No: 1912288

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

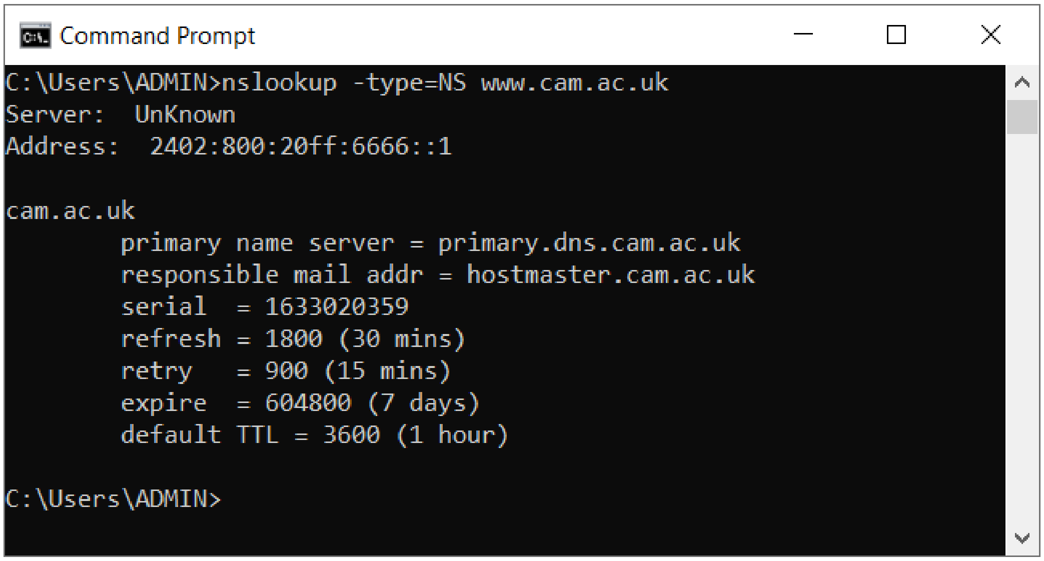


```
C:\Users\ADMIN>nslookup www.aao.hcumut.edu.vn
Server:  UnKnown
Address:  2402:800:20ff:6666::1

Non-authoritative answer:
Name:    www.aao.hcumut.edu.vn
Address:  125.235.4.59
```

Web server: www.aao.hcmut.edu.vn

IP address: 125.235.4.59

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

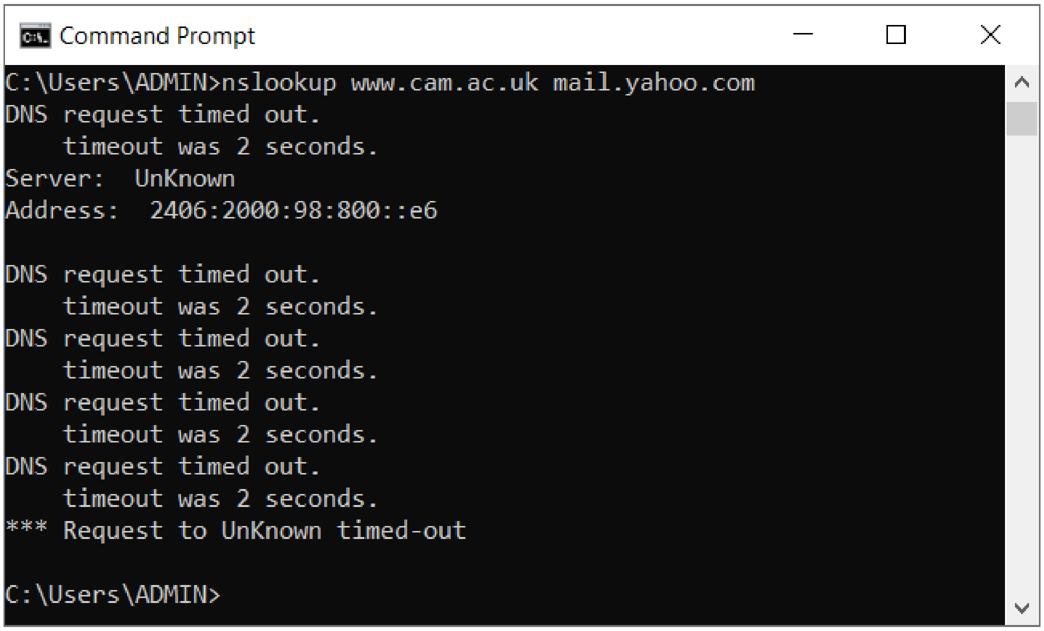


```
C:\Users\ADMIN>nslookup -type=NS www.cam.ac.uk
Server:  UnKnown
Address:  2402:800:20ff:6666::1

cam.ac.uk
        primary name server = primary.dns.cam.ac.uk
        responsible mail addr = hostmaster.cam.ac.uk
        serial  = 1633020359
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)

C:\Users\ADMIN>
```

Web server: www.cam.ac.uk (University of Cambridge)

The authoritative DNS server: primary.dns.cam.ac.uk

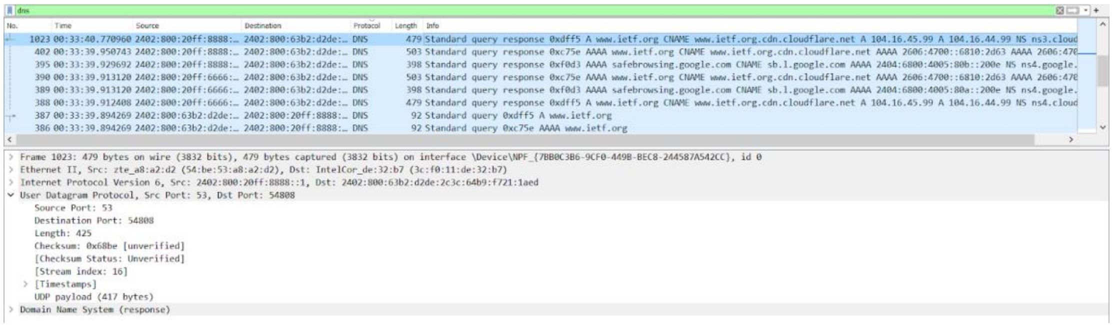
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?



```
C:\Users\ADMIN>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  2406:2000:98:800::e6

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\ADMIN>
```

Its IP address: 2406:2000:98:800::e6

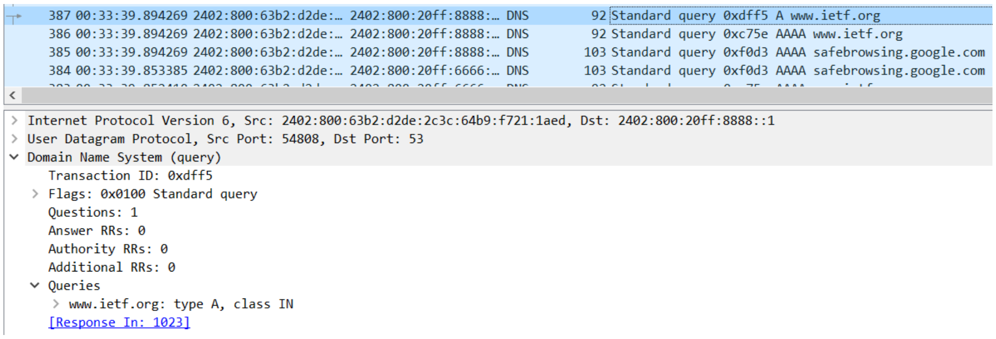
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?



```
No.   Time            Source                Destination           Protocol  Length Info
 1023 00:33:40.770960 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS          479 Standard query response 0xdff5 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99 NS ns3.cloud
  402 00:33:39.950743 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS          503 Standard query response 0xc75e AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 AAAA 2606:470
  395 00:33:39.929692 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS          398 Standard query response 0xf0d3 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2404:6800:4005:80b::200e NS ns4.google.
  390 00:33:39.913120 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS          503 Standard query response 0xc75e AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 AAAA 2606:470
  389 00:33:39.913120 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS          398 Standard query response 0xf0d3 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2404:6800:4005:80a::200e NS ns4.google.
  388 00:33:39.912408 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS          479 Standard query response 0xdff5 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99 NS ns4.cloud
  387 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS           92 Standard query 0xdff5 A www.ietf.org
  386 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS           92 Standard query 0xc75e AAAA www.ietf.org

> Frame 1023: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: zte_a8:a2:d2 (54:be:53:a8:a2:d2), Dst: IntelCor_de:32:b7 (3c:f0:11:de:32:b7)
> Internet Protocol Version 6, Src: 2402:800:20ff:8888::1, Dst: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed
v User Datagram Protocol, Src Port: 53, Dst Port: 54808
    Source Port: 53
    Destination Port: 54808
    Length: 425
    Checksum: 0x68be [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
  > [Timestamps]
    UDP payload (417 bytes)
> Domain Name System (response)
```

The DNS query and response message are sent over UDP

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



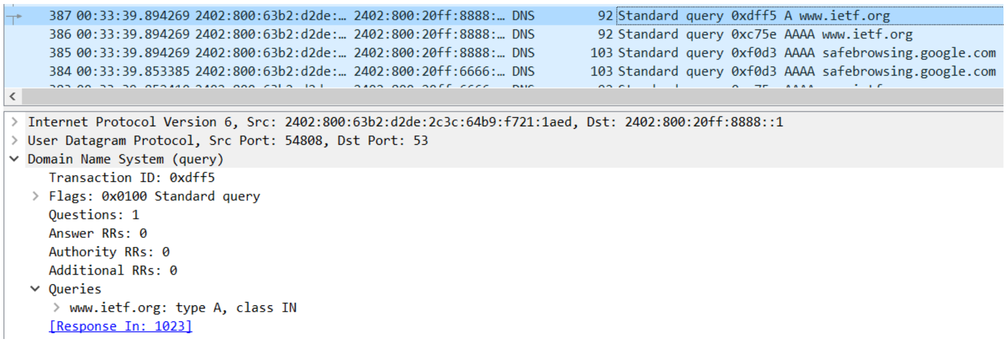
```
387 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS       92 Standard query 0xdff5 A www.ietf.org
386 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS       92 Standard query 0xc75e AAAA www.ietf.org
385 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS      103 Standard query 0xf0d3 AAAA safebrowsing.google.com
384 00:33:39.853385 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS      103 Standard query 0xf0d3 AAAA safebrowsing.google.com
```

```
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:8888::1
> User Datagram Protocol, Src Port: 54808, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xdff5
  > 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: 1023]
```

Destination port: 53

Source port: 54808

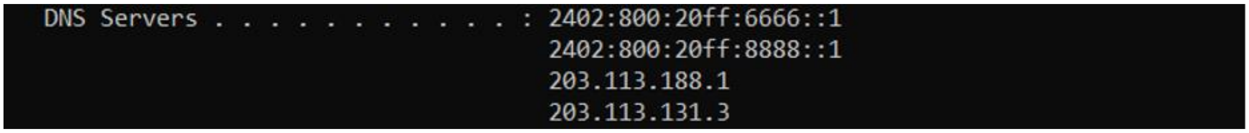
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?



```
387 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS       92 Standard query 0xdff5 A www.ietf.org
386 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS       92 Standard query 0xc75e AAAA www.ietf.org
385 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS      103 Standard query 0xf0d3 AAAA safebrowsing.google.com
384 00:33:39.853385 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS      103 Standard query 0xf0d3 AAAA safebrowsing.google.com
```

```
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:8888::1
> User Datagram Protocol, Src Port: 54808, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xdff5
  > 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: 1023]
```

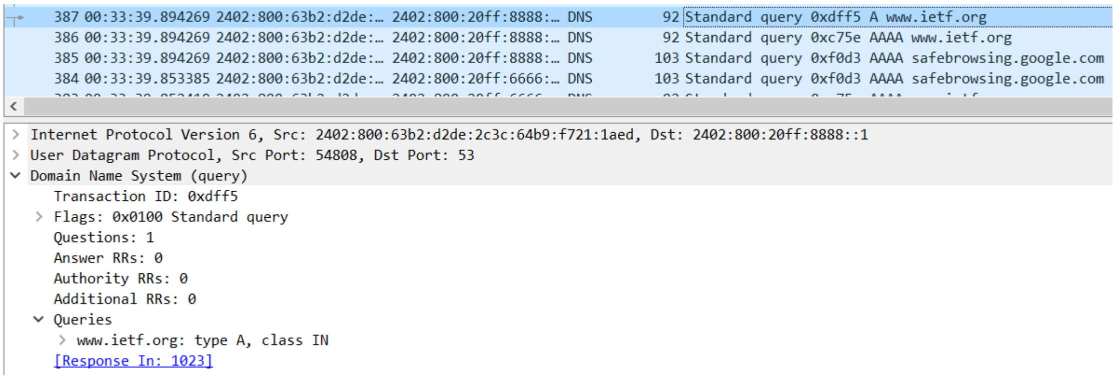
IP address the DNS query message sent to: 2402:800:20ff:8888::1



```
   DNS Servers . . . . . . . . . . . : 2402:800:20ff:6666::1
                                       2402:800:20ff:8888::1
                                       203.113.188.1
                                       203.113.131.3
```

IP address of my local DNS server is: 2402:800:20ff:8888::1. So yes, they are the same.

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

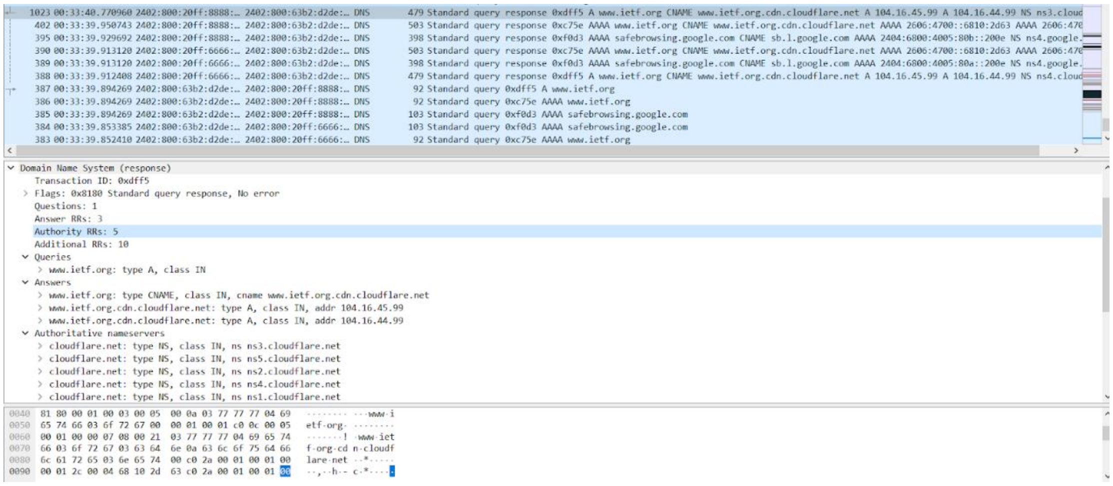


```
387 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS     92 Standard query 0xdff5 A www.ietf.org
386 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS     92 Standard query 0xc75e AAAA www.ietf.org
385 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS    103 Standard query 0xf0d3 AAAA safebrowsing.google.com
384 00:33:39.853385 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    103 Standard query 0xf0d3 AAAA safebrowsing.google.com

> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:8888::1
> User Datagram Protocol, Src Port: 54808, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xdff5
  > 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: 1023]
```

Type of DNS query: A

No, the query message does not contain any answer

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



```
1023 00:33:40.770960 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS    479 Standard query response 0xdff5 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99 NS ns3.cloud
 402 00:33:39.950743 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS    503 Standard query response 0xc75e AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 AAAA 2606:470
 395 00:33:39.929692 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS    398 Standard query response 0xf0d3 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2404:6800:4005:80b::200e NS ns4.google.
 390 00:33:39.913120 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS    503 Standard query response 0xc75e AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 AAAA 2606:470
 389 00:33:39.913120 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS    398 Standard query response 0xf0d3 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2404:6800:4005:80a::200e NS ns4.google.
 388 00:33:39.912408 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS    479 Standard query response 0xdff5 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99 NS ns4.cloud
 387 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS     92 Standard query 0xdff5 A www.ietf.org
 386 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS     92 Standard query 0xc75e AAAA www.ietf.org
 385 00:33:39.894269 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS    103 Standard query 0xf0d3 AAAA safebrowsing.google.com
 384 00:33:39.853385 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    103 Standard query 0xf0d3 AAAA safebrowsing.google.com
 383 00:33:39.852410 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS     92 Standard query 0xc75e AAAA www.ietf.org

v Domain Name System (response)
    Transaction ID: 0xdff5
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 5
    Additional RRs: 10
  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
  v Authoritative nameservers
    > cloudflare.net: type NS, class IN, ns ns3.cloudflare.net
    > cloudflare.net: type NS, class IN, ns ns5.cloudflare.net
    > cloudflare.net: type NS, class IN, ns ns2.cloudflare.net
    > cloudflare.net: type NS, class IN, ns ns4.cloudflare.net
    > cloudflare.net: type NS, class IN, ns ns1.cloudflare.net

0040  81 80 00 01 00 03 00 05  00 0a 03 77 77 77 04 69   ········ ···www·i
0050  65 74 66 03 6f 72 67 00  00 01 00 01 c0 0c 00 05   etf·org· ········
0060  00 01 00 00 07 08 00 21  03 77 77 77 04 69 65 74   ·······! ·www·iet
0070  66 03 6f 72 67 03 63 64  6e 0a 63 6c 6f 75 64 66   f·org·cd n·cloudf
0080  6c 61 72 65 03 6e 65 74  00 c0 2a 00 01 00 01 00   lare·net ··*·····
0090  00 01 2c 00 04 68 10 2d  63 c0 2a 00 01 00 01 00   ··,··h·- c·*·····
```

3 answers are provided

They contain answers to the query: nameservers, address

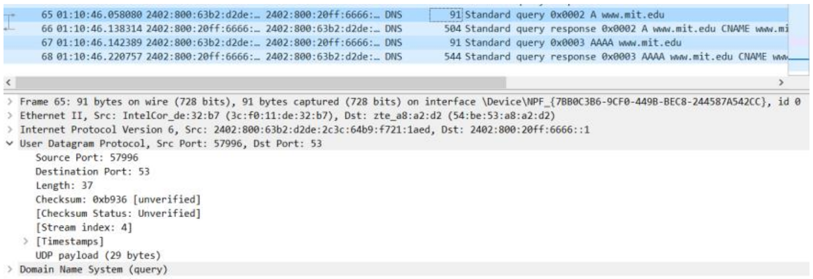
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

No, it does not

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

No, it does not

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

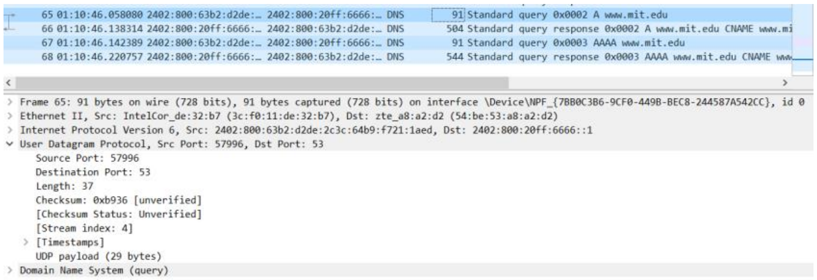


```
65 01:10:46.058080 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    91 Standard query 0x0002 A www.mit.edu
66 01:10:46.138314 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS   504 Standard query response 0x0002 A www.mit.edu CNAME www.mi
67 01:10:46.142389 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    91 Standard query 0x0003 AAAA www.mit.edu
68 01:10:46.220757 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS   544 Standard query response 0x0003 AAAA www.mit.edu CNAME www

> Frame 65: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: IntelCor_de:32:b7 (3c:f0:11:de:32:b7), Dst: zte_a8:a2:d2 (54:be:53:a8:a2:d2)
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:6666::1
v User Datagram Protocol, Src Port: 57996, Dst Port: 53
    Source Port: 57996
    Destination Port: 53
    Length: 37
    Checksum: 0xb936 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

Destination port: 53

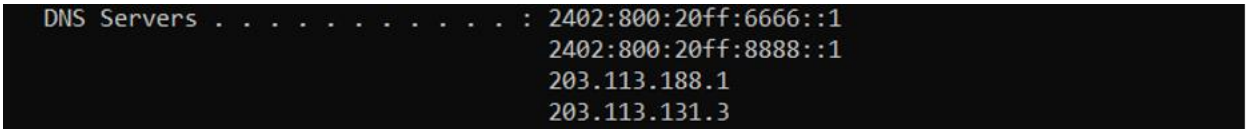
Source port: 57996

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



```
65 01:10:46.058080 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    91 Standard query 0x0002 A www.mit.edu
66 01:10:46.138314 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS   504 Standard query response 0x0002 A www.mit.edu CNAME www.mi
67 01:10:46.142389 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    91 Standard query 0x0003 AAAA www.mit.edu
68 01:10:46.220757 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS   544 Standard query response 0x0003 AAAA www.mit.edu CNAME www

> Frame 65: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: IntelCor_de:32:b7 (3c:f0:11:de:32:b7), Dst: zte_a8:a2:d2 (54:be:53:a8:a2:d2)
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:6666::1
v User Datagram Protocol, Src Port: 57996, Dst Port: 53
    Source Port: 57996
    Destination Port: 53
    Length: 37
    Checksum: 0xb936 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

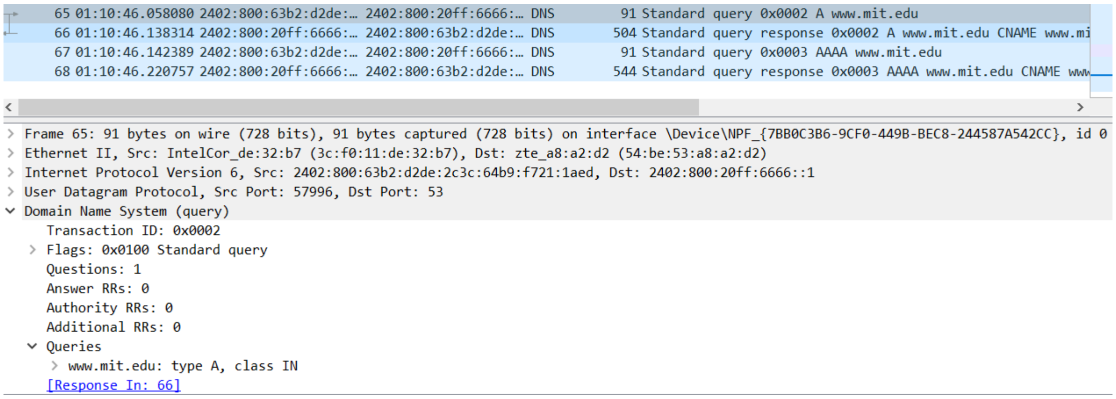
IP address the DNS query message sent to: 2402:800:20ff:6666::1



```
  DNS Servers . . . . . . . . . . . : 2402:800:20ff:6666::1
                                      2402:800:20ff:8888::1
                                      203.113.188.1
                                      203.113.131.3
```

Yes, it is the IP address of my default local DNS server

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

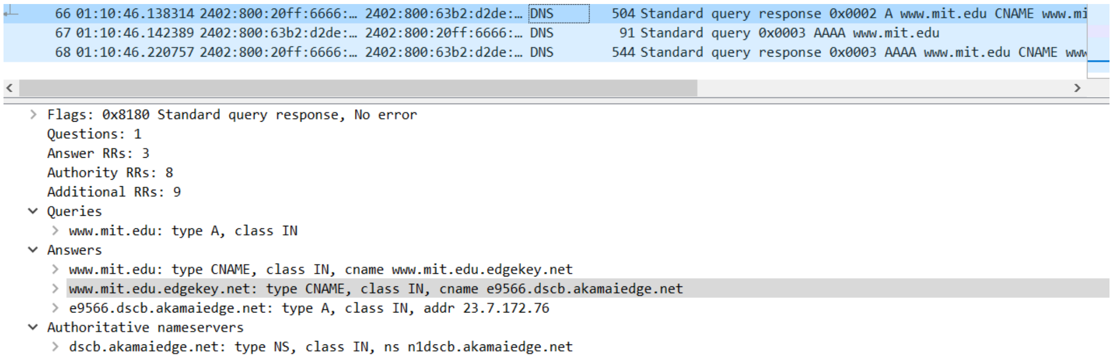


```
65 01:10:46.058080 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    91 Standard query 0x0002 A www.mit.edu
66 01:10:46.138314 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS   504 Standard query response 0x0002 A www.mit.edu CNAME www.mi
67 01:10:46.142389 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS    91 Standard query 0x0003 AAAA www.mit.edu
68 01:10:46.220757 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS   544 Standard query response 0x0003 AAAA www.mit.edu CNAME www

> Frame 65: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: IntelCor_de:32:b7 (3c:f0:11:de:32:b7), Dst: zte_a8:a2:d2 (54:be:53:a8:a2:d2)
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 57996, 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: 66]
```

Type of DNS query: A

No, the query message does not contain any answer

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



```
66 01:10:46.138314 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS    504 Standard query response 0x0002 A www.mit.edu CNAME www.mi
67 01:10:46.142389 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS     91 Standard query 0x0003 AAAA www.mit.edu
68 01:10:46.220757 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS    544 Standard query response 0x0003 AAAA www.mit.edu CNAME www

  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 8
    Additional RRs: 9
  ∨ Queries
    > www.mit.edu: type A, class IN
  ∨ 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 23.7.172.76
  ∨ Authoritative nameservers
    > dscb.akamaiedge.net: type NS, class IN, ns n1dscb.akamaiedge.net
```

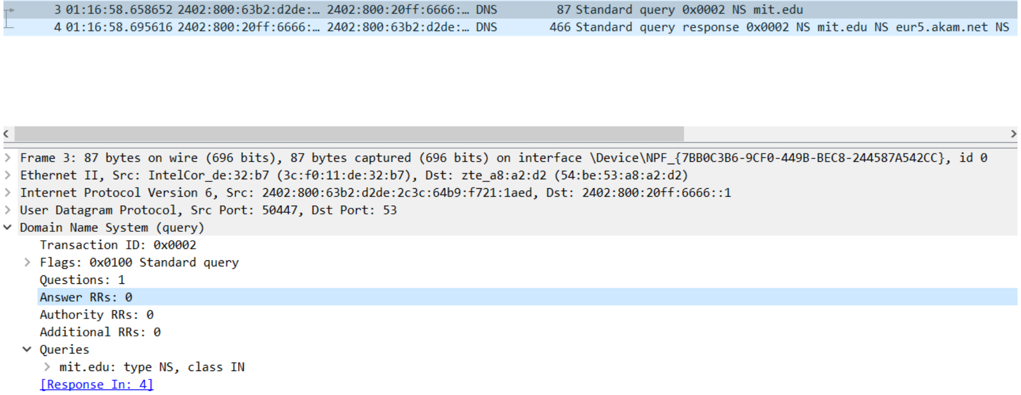
3 answers are provided

They contain the answers for the query: nameservers, address

15. Provide a screenshot.

They are provided in each question

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

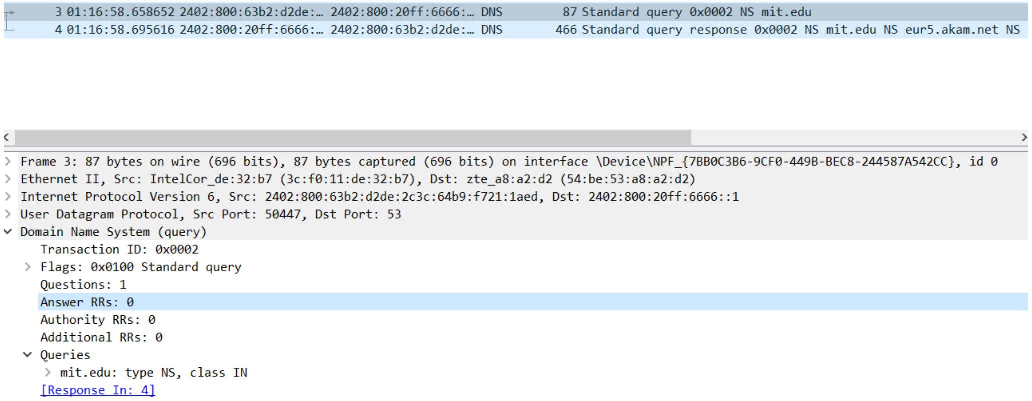


```
3 01:16:58.658652 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS      87 Standard query 0x0002 NS mit.edu
4 01:16:58.695616 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS     466 Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS

> Frame 3: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: IntelCor_de:32:b7 (3c:f0:11:de:32:b7), Dst: zte_a8:a2:d2 (54:be:53:a8:a2:d2)
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 50447, 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
    > mit.edu: type NS, class IN
    [Response In: 4]
```

IP address the DNS query sent to: 2402:800:20ff:6666::1

Yes, it is the IP address of my default local DNS server

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



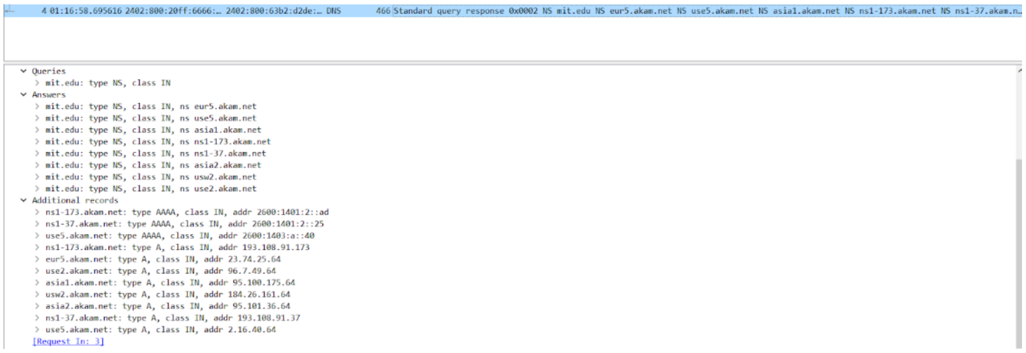
```
3 01:16:58.658652 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS        87 Standard query 0x0002 NS mit.edu
4 01:16:58.695616 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS       466 Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS
```

```
> Frame 3: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: IntelCor_de:32:b7 (3c:f0:11:de:32:b7), Dst: zte_a8:a2:d2 (54:be:53:a8:a2:d2)
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 50447, 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: 4]
```

Type of DNS query: NS

No, the query message does not contain any answer

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?



```
4 01:16:58.695616 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS       466 Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS use5.akam.net NS asia1.akam.net NS ns1-173.akam.net NS ns1-37.akam.n…
```

```
v Queries
  > mit.edu: type NS, class IN
v Answers
  > mit.edu: type NS, class IN, ns eur5.akam.net
  > mit.edu: type NS, class IN, ns use5.akam.net
  > mit.edu: type NS, class IN, ns asia1.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 asia2.akam.net
  > mit.edu: type NS, class IN, ns usw2.akam.net
  > mit.edu: type NS, class IN, ns use2.akam.net
v Additional records
  > ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
  > ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
  > use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
  > ns1-173.akam.net: type A, class IN, addr 193.108.91.173
  > eur5.akam.net: type A, class IN, addr 23.74.25.64
  > use2.akam.net: type A, class IN, addr 96.7.49.64
  > asia1.akam.net: type A, class IN, addr 95.100.175.64
  > usw2.akam.net: type A, class IN, addr 184.26.161.64
  > asia2.akam.net: type A, class IN, addr 95.101.36.64
  > ns1-37.akam.net: type A, class IN, addr 193.108.91.37
  > use5.akam.net: type A, class IN, addr 2.16.40.64
  [Request In: 3]
```

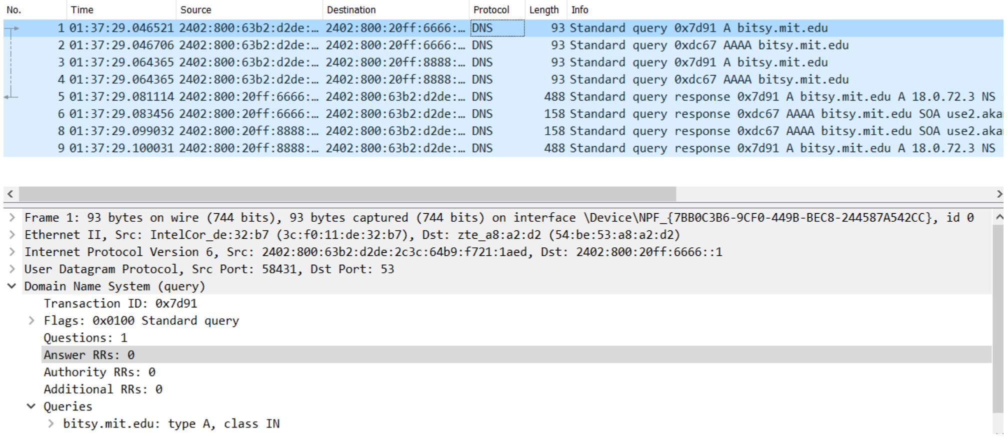
MIT nameservers the response message provides: eur5.akam.net, use5.akam.net, asia1.akam.net, ns1-173.akam.net, ns1-37.akam.net, asia2.akam.net, usw2.akam.net, use2.akam.net

Yes, this response message also provide the IP addresses of the MIT nameservers

19. Provide a screenshot.

They are provided in 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?

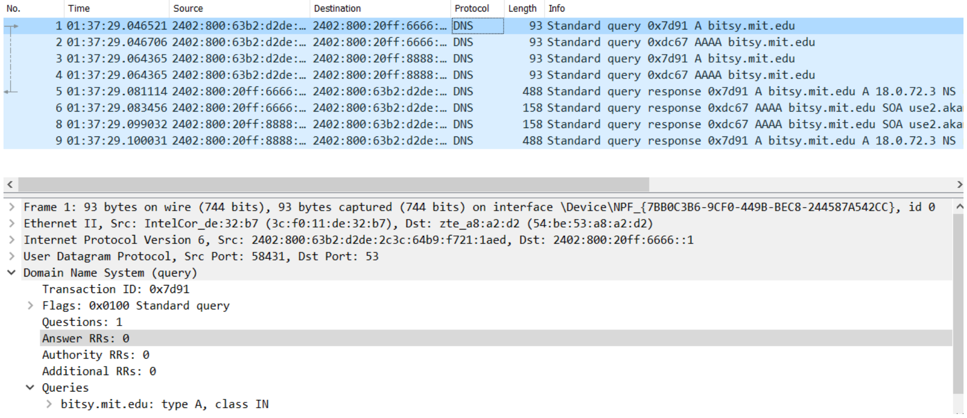


```
No.   Time             Source                   Destination              Protocol  Length  Info
    1 01:37:29.046521 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS         93 Standard query 0x7d91 A bitsy.mit.edu
    2 01:37:29.046706 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS         93 Standard query 0xdc67 AAAA bitsy.mit.edu
    3 01:37:29.064365 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS         93 Standard query 0x7d91 A bitsy.mit.edu
    4 01:37:29.064365 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS         93 Standard query 0xdc67 AAAA bitsy.mit.edu
    5 01:37:29.081114 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS        488 Standard query response 0x7d91 A bitsy.mit.edu A 18.0.72.3 NS
    6 01:37:29.083456 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS        158 Standard query response 0xdc67 AAAA bitsy.mit.edu SOA use2.aka
    8 01:37:29.099032 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS        158 Standard query response 0xdc67 AAAA bitsy.mit.edu SOA use2.aka
    9 01:37:29.100031 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS        488 Standard query response 0x7d91 A bitsy.mit.edu A 18.0.72.3 NS

> Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: IntelCor_de:32:b7 (3c:f0:11:de:32:b7), Dst: zte_a8:a2:d2 (54:be:53:a8:a2:d2)
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 58431, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x7d91
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > bitsy.mit.edu: type A, class IN
```

IP address the DNS query message sent to: 2402:800:20ff:6666::1

Yes, it is the IP address of my default local DNS server

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

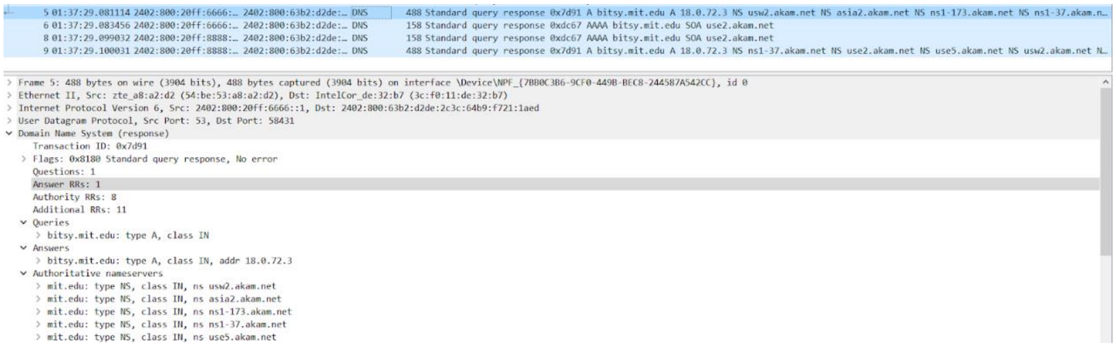


```
No.   Time             Source                   Destination              Protocol  Length  Info
    1 01:37:29.046521 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS         93 Standard query 0x7d91 A bitsy.mit.edu
    2 01:37:29.046706 2402:800:63b2:d2de:… 2402:800:20ff:6666:… DNS         93 Standard query 0xdc67 AAAA bitsy.mit.edu
    3 01:37:29.064365 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS         93 Standard query 0x7d91 A bitsy.mit.edu
    4 01:37:29.064365 2402:800:63b2:d2de:… 2402:800:20ff:8888:… DNS         93 Standard query 0xdc67 AAAA bitsy.mit.edu
    5 01:37:29.081114 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS        488 Standard query response 0x7d91 A bitsy.mit.edu A 18.0.72.3 NS
    6 01:37:29.083456 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS        158 Standard query response 0xdc67 AAAA bitsy.mit.edu SOA use2.aka
    8 01:37:29.099032 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS        158 Standard query response 0xdc67 AAAA bitsy.mit.edu SOA use2.aka
    9 01:37:29.100031 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS        488 Standard query response 0x7d91 A bitsy.mit.edu A 18.0.72.3 NS

> Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: IntelCor_de:32:b7 (3c:f0:11:de:32:b7), Dst: zte_a8:a2:d2 (54:be:53:a8:a2:d2)
> Internet Protocol Version 6, Src: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed, Dst: 2402:800:20ff:6666::1
> User Datagram Protocol, Src Port: 58431, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x7d91
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > bitsy.mit.edu: type A, class IN
```

Type of DNS query: A

No, the query message does not contain any answer

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



```
    5 01:37:29.081114 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS        488 Standard query response 0x7d91 A bitsy.mit.edu A 18.0.72.3 NS usw2.akam.net NS asia2.akam.net NS ns1-173.akam.net NS ns1-37.akam.n…
    6 01:37:29.083456 2402:800:20ff:6666:… 2402:800:63b2:d2de:… DNS        158 Standard query response 0xdc67 AAAA bitsy.mit.edu SOA use2.akam.net
    8 01:37:29.099032 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS        158 Standard query response 0xdc67 AAAA bitsy.mit.edu SOA use2.akam.net
    9 01:37:29.100031 2402:800:20ff:8888:… 2402:800:63b2:d2de:… DNS        488 Standard query response 0x7d91 A bitsy.mit.edu A 18.0.72.3 NS ns1-37.akam.net NS use2.akam.net NS use5.akam.net NS usw2.akam.net N…

> Frame 5: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface \Device\NPF_{7BB0C3B6-9CF0-449B-BEC8-244587A542CC}, id 0
> Ethernet II, Src: zte_a8:a2:d2 (54:be:53:a8:a2:d2), Dst: IntelCor_de:32:b7 (3c:f0:11:de:32:b7)
> Internet Protocol Version 6, Src: 2402:800:20ff:6666::1, Dst: 2402:800:63b2:d2de:2c3c:64b9:f721:1aed
> User Datagram Protocol, Src Port: 53, Dst Port: 58431
v Domain Name System (response)
    Transaction ID: 0x7d91
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 8
    Additional RRs: 11
  v Queries
    > bitsy.mit.edu: type A, class IN
  v Answers
    > bitsy.mit.edu: type A, class IN, addr 18.0.72.3
  v Authoritative nameservers
    > mit.edu: type NS, class IN, ns usw2.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 ns1-37.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
```

1 answer is provided

It contains the answer for the query: address

23. Provide a screenshot.

They are provided in each question