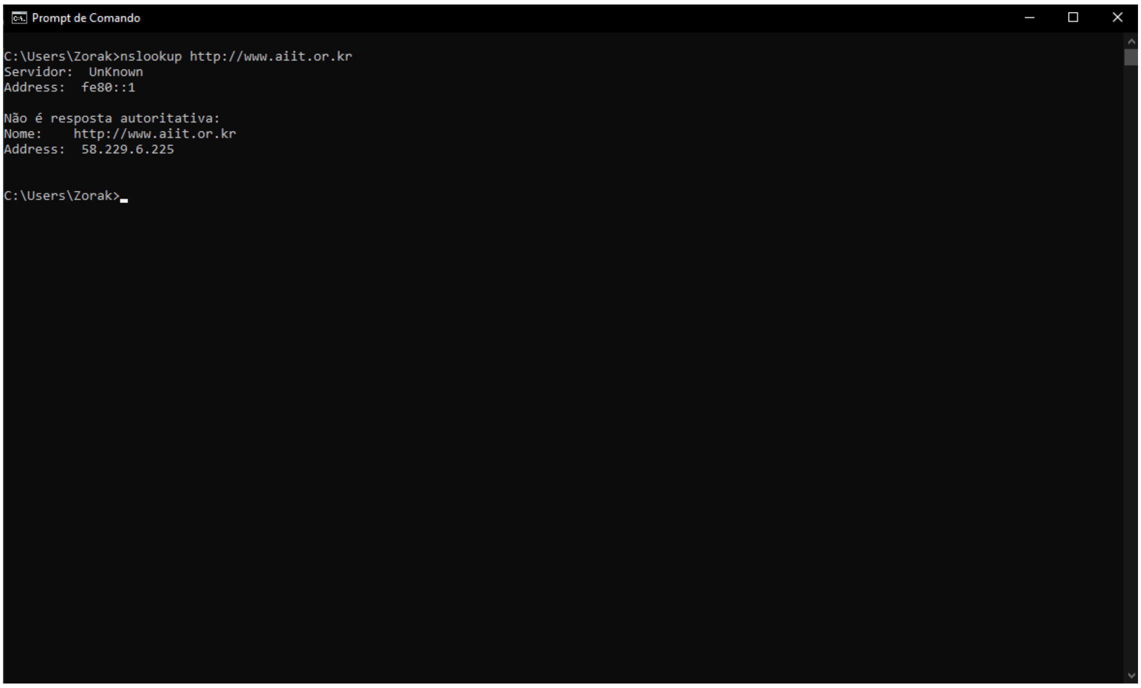
GSI023 – REDE DE COMPUTADORES

Computer Networking – J. F. Kurose and K. W. Ross – 7th Edition Chapter 2 – Camadas de Aplicação

Pedro Henrique Silva Santana – 12011BSI218 – pedro.santana@ufu.br
Victor Hugo Martins Alves – 12011BSI217 – victor.alves1@ufu.br

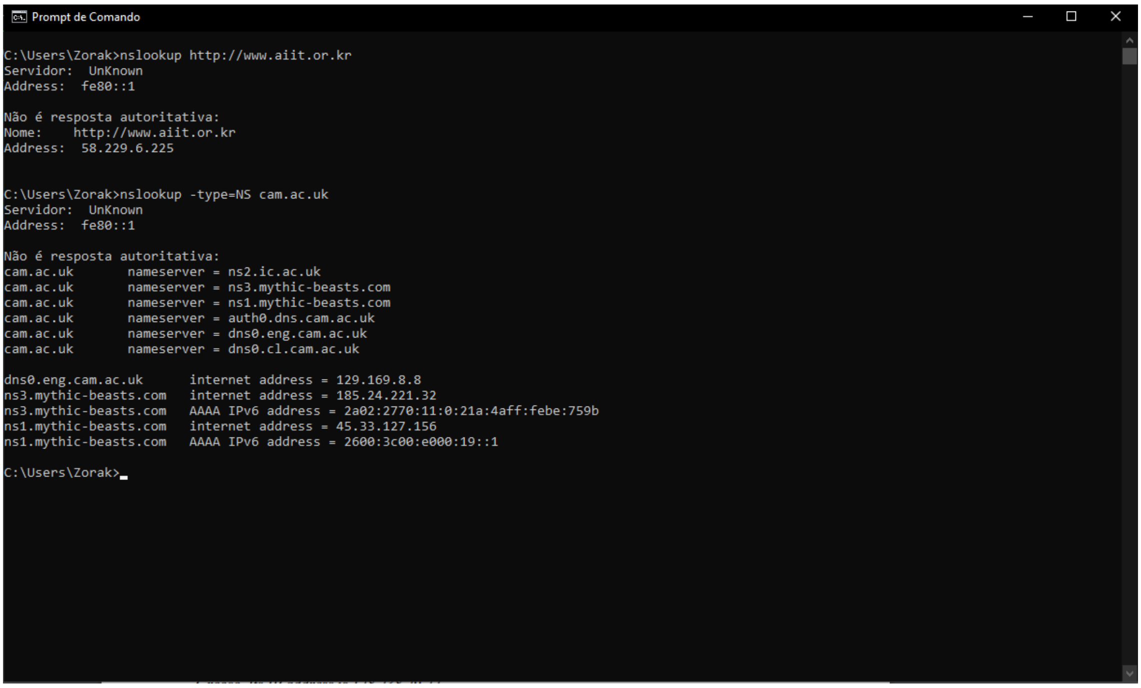
1.Run nslookup to obtain the IP address of a Web server in Asia. What is its IP address?



```
C:\Users\Zorak>nslookup http://www.aiit.or.kr
Servidor:  UnKnown
Address:  fe80::1

Não é resposta autoritativa:
Nome:    http://www.aiit.or.kr
Address:  58.229.6.225


C:\Users\Zorak>
```

O endereço é 58.229.6.225

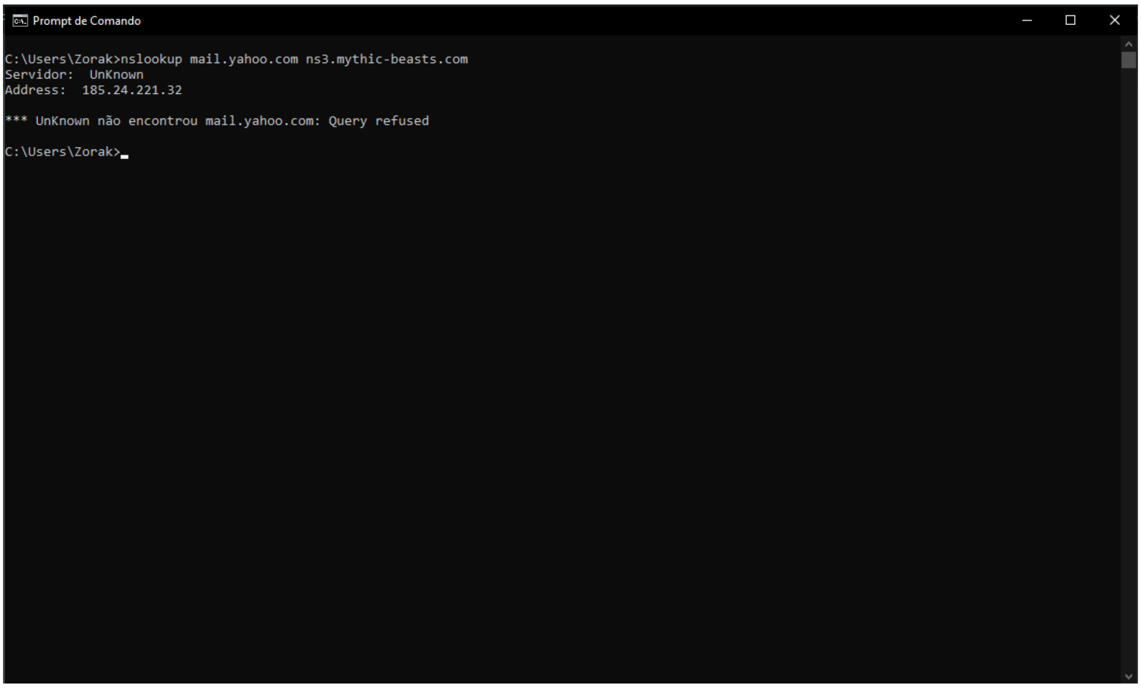
2. Run nslookup to determine the authoritative DNS servers for a university in Europe. What is its IP address.



```
C:\Users\Zorak>nslookup http://www.aiit.or.kr
Servidor:  UnKnown
Address:  fe80::1

Não é resposta autoritativa:
Nome:    http://www.aiit.or.kr
Address:  58.229.6.225


C:\Users\Zorak>nslookup -type=NS cam.ac.uk
Servidor:  UnKnown
Address:  fe80::1

Não é resposta autoritativa:
cam.ac.uk       nameserver = ns2.ic.ac.uk
cam.ac.uk       nameserver = ns3.mythic-beasts.com
cam.ac.uk       nameserver = ns1.mythic-beasts.com
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk

dns0.eng.cam.ac.uk      internet address = 129.169.8.8
ns3.mythic-beasts.com   internet address = 185.24.221.32
ns3.mythic-beasts.com   AAAA IPv6 address = 2a02:2770:11:0:21a:4aff:febe:759b
ns1.mythic-beasts.com   internet address = 45.33.127.156
ns1.mythic-beasts.com   AAAA IPv6 address = 2600:3c00:e000:19::1

C:\Users\Zorak>
```

O endereço IP da Universidade de Cambridge é : 129.169.8.8

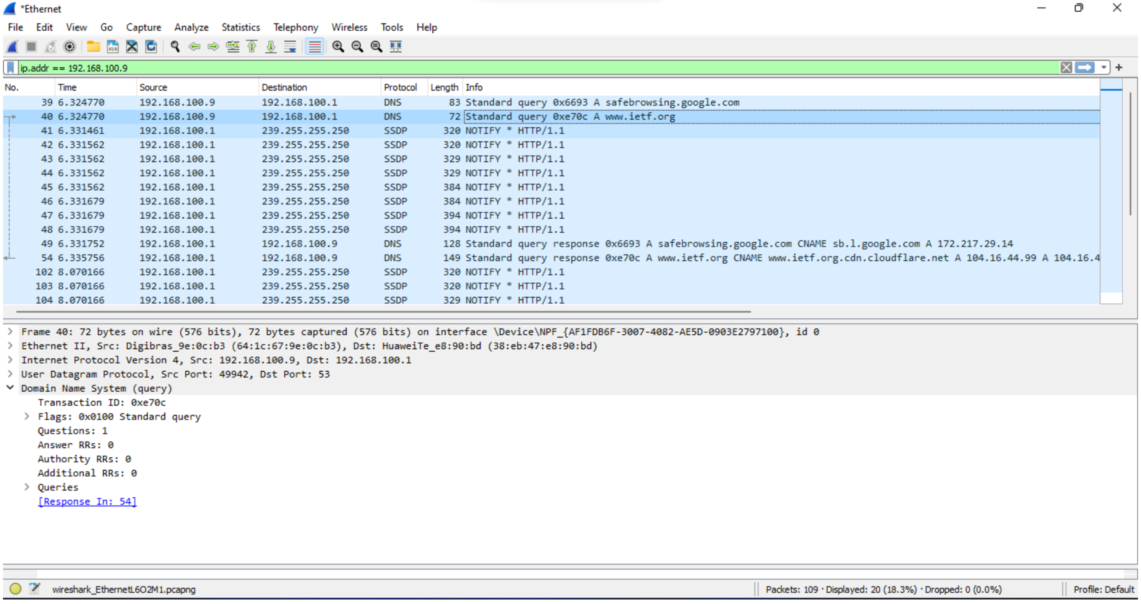
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?



```
C:\Users\Zorak>nslookup mail.yahoo.com ns3.mythic-beasts.com
Servidor:  UnKnown
Address:  185.24.221.32

*** UnKnown não encontrou mail.yahoo.com: Query refused

C:\Users\Zorak>
```

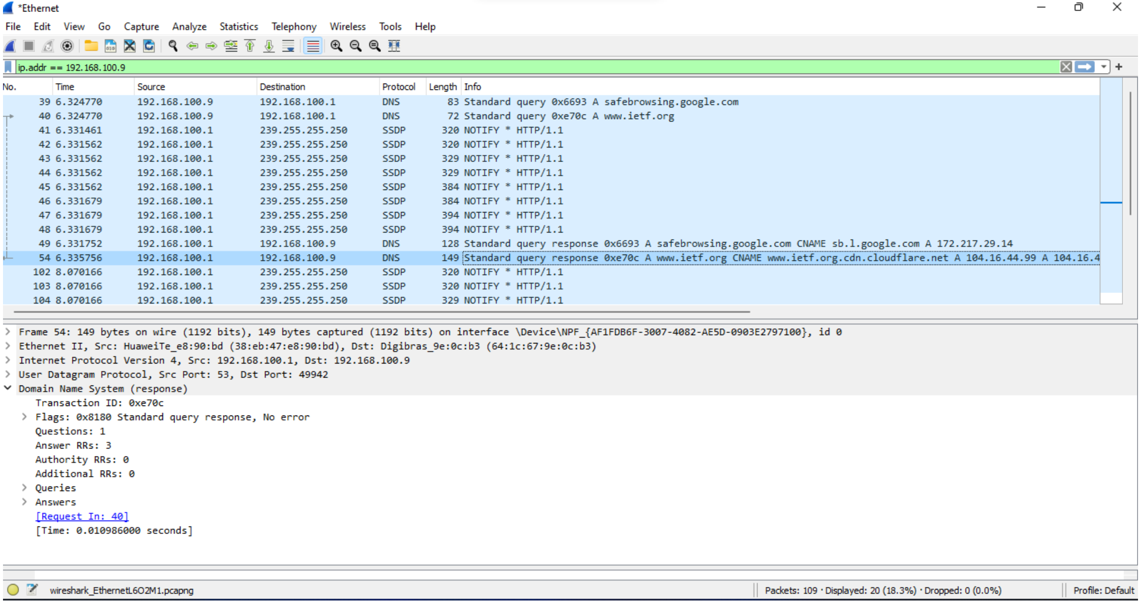
O endereço IP é: 185.24.221.32

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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.100.9

No.   Time      Source          Destination      Protocol Length Info
 39 6.324770   192.168.100.9   192.168.100.1    DNS        83 Standard query 0x6693 A safebrowsing.google.com
 40 6.324770   192.168.100.9   192.168.100.1    DNS        72 Standard query 0xe70c A www.ietf.org
 41 6.331461   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
 42 6.331562   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
 43 6.331562   192.168.100.1   239.255.255.250  SSDP      329 NOTIFY * HTTP/1.1
 44 6.331562   192.168.100.1   239.255.255.250  SSDP      329 NOTIFY * HTTP/1.1
 45 6.331562   192.168.100.1   239.255.255.250  SSDP      384 NOTIFY * HTTP/1.1
 46 6.331679   192.168.100.1   239.255.255.250  SSDP      384 NOTIFY * HTTP/1.1
 47 6.331679   192.168.100.1   239.255.255.250  SSDP      394 NOTIFY * HTTP/1.1
 48 6.331679   192.168.100.1   239.255.255.250  SSDP      394 NOTIFY * HTTP/1.1
 49 6.331752   192.168.100.1   192.168.100.9    DNS       128 Standard query response 0x6693 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.29.14
 54 6.335756   192.168.100.1   192.168.100.9    DNS       149 Standard query response 0xe70c A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.4
102 8.070166   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
103 8.070166   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
104 8.070166   192.168.100.1   239.255.255.250  SSDP      329 NOTIFY * HTTP/1.1

> Frame 40: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3), Dst: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd)
> Internet Protocol Version 4, Src: 192.168.100.9, Dst: 192.168.100.1
> User Datagram Protocol, Src Port: 49942, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xe70c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 54]

wireshark_EthernetL6O2M1.pcapng    Packets: 109 · Displayed: 20 (18.3%) · Dropped: 0 (0.0%)    Profile: Default
```

Requisição.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.100.9

No.   Time      Source          Destination      Protocol Length Info
 39 6.324770   192.168.100.9   192.168.100.1    DNS        83 Standard query 0x6693 A safebrowsing.google.com
 40 6.324770   192.168.100.9   192.168.100.1    DNS        72 Standard query 0xe70c A www.ietf.org
 41 6.331461   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
 42 6.331562   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
 43 6.331562   192.168.100.1   239.255.255.250  SSDP      329 NOTIFY * HTTP/1.1
 44 6.331562   192.168.100.1   239.255.255.250  SSDP      329 NOTIFY * HTTP/1.1
 45 6.331562   192.168.100.1   239.255.255.250  SSDP      384 NOTIFY * HTTP/1.1
 46 6.331679   192.168.100.1   239.255.255.250  SSDP      384 NOTIFY * HTTP/1.1
 47 6.331679   192.168.100.1   239.255.255.250  SSDP      394 NOTIFY * HTTP/1.1
 48 6.331679   192.168.100.1   239.255.255.250  SSDP      394 NOTIFY * HTTP/1.1
 49 6.331752   192.168.100.1   192.168.100.9    DNS       128 Standard query response 0x6693 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.29.14
 54 6.335756   192.168.100.1   192.168.100.9    DNS       149 Standard query response 0xe70c A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.4
102 8.070166   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
103 8.070166   192.168.100.1   239.255.255.250  SSDP      320 NOTIFY * HTTP/1.1
104 8.070166   192.168.100.1   239.255.255.250  SSDP      329 NOTIFY * HTTP/1.1

> Frame 54: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd), Dst: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.9
> User Datagram Protocol, Src Port: 53, Dst Port: 49942
v Domain Name System (response)
    Transaction ID: 0xe70c
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 40]
    [Time: 0.010986000 seconds]

wireshark_EthernetL6O2M1.pcapng    Packets: 109 · Displayed: 20 (18.3%) · Dropped: 0 (0.0%)    Profile: Default
```

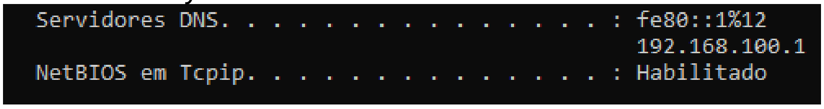
Resposta.

Foram enviados via UDP.

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

Porta 53 para ambas.

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?



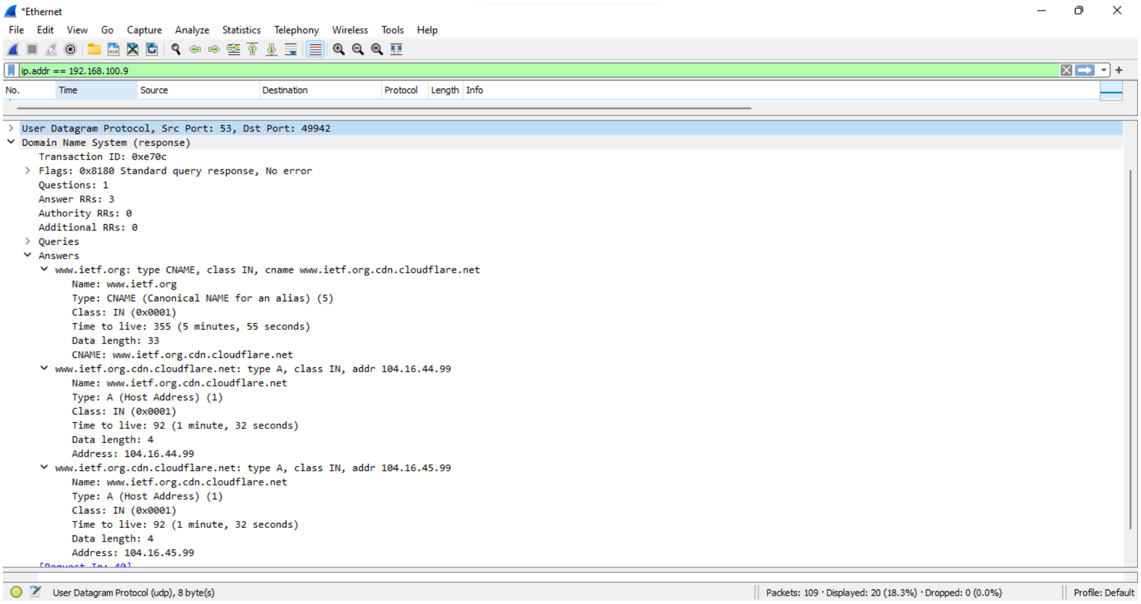
```
   Servidores DNS. . . . . . . . . . . . . . : fe80::1%12
                                               192.168.100.1
   NetBIOS em Tcpip. . . . . . . . . . . . . : Habilitado
```

192.168.100.1. Sim, este é um dos endereços DNS local.

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

Standard Query. Não possui nenhuma resposta.

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



```
ip.addr == 192.168.100.9
```

```
> User Datagram Protocol, Src Port: 53, Dst Port: 49942
v Domain Name System (response)
    Transaction ID: 0xe70c
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v 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: 355 (5 minutes, 55 seconds)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    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: 92 (1 minute, 32 seconds)
        Data length: 4
        Address: 104.16.44.99
    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: 92 (1 minute, 32 seconds)
        Data length: 4
        Address: 104.16.45.99
    [Request In: 40]
```

User Datagram Protocol (udp), 8 byte(s) | Packets: 109 · Displayed: 20 (18.3%) · Dropped: 0 (0.0%) | Profile: Default

Foram providas 3 respostas. Elas contem: nome, tipo, classe, tempo de vida, tamanho de dados e endereço OU cname.

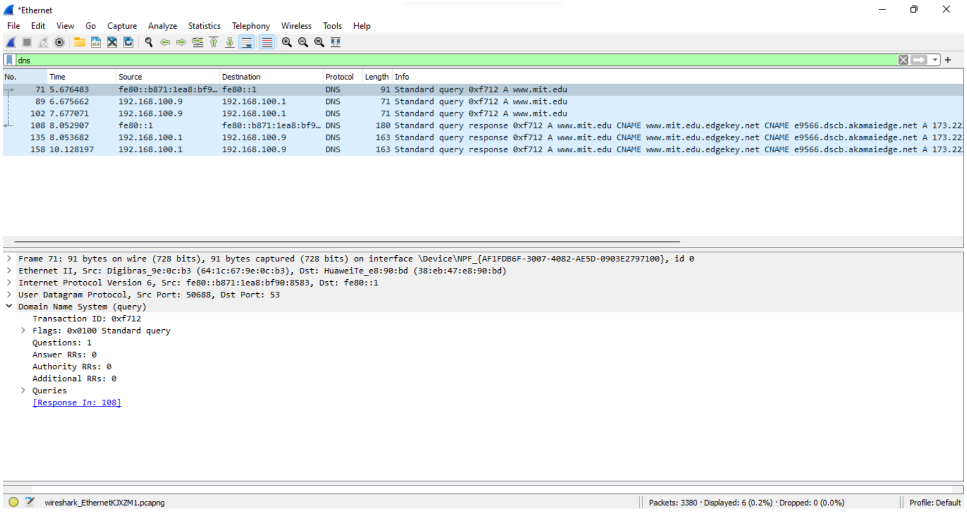
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Sim.

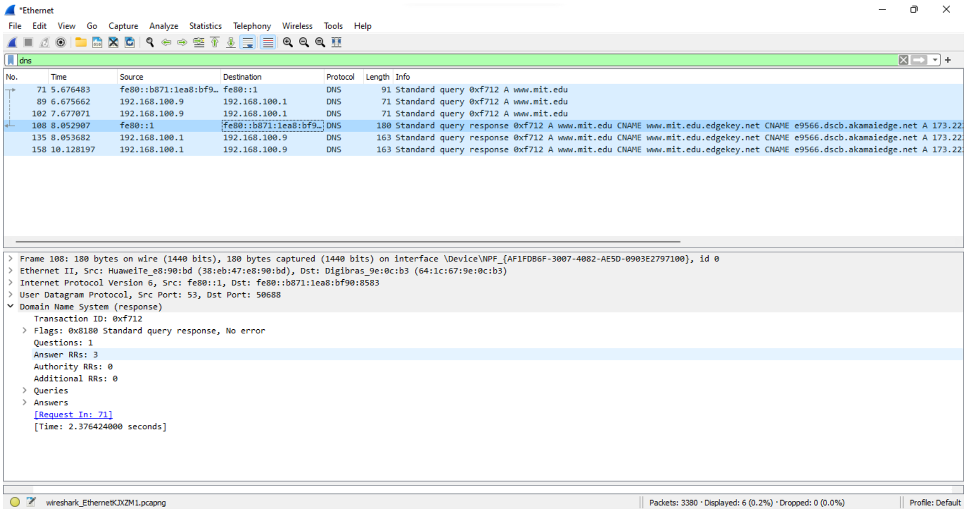
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Não.

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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

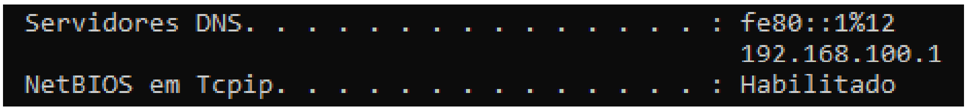
```
No.   Time       Source               Destination          Protocol Length Info
   71 5.676483   fe80::b871:1ea8:bf9… fe80::1              DNS      91 Standard query 0xf712 A www.mit.edu
   89 6.675662   192.168.100.9        192.168.100.1        DNS      71 Standard query 0xf712 A www.mit.edu
  102 7.677071   192.168.100.9        192.168.100.1        DNS      71 Standard query 0xf712 A www.mit.edu
  108 8.052907   fe80::1              fe80::b871:1ea8:bf9… DNS     180 Standard query response 0xf712 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 173.22
  135 8.053682   192.168.100.1        192.168.100.9        DNS     163 Standard query response 0xf712 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 173.22
  158 10.128197  192.168.100.1        192.168.100.9        DNS     163 Standard query response 0xf712 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 173.22

> Frame 71: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3), Dst: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd)
> Internet Protocol Version 6, Src: fe80::b871:1ea8:bf90:8583, Dst: fe80::1
> User Datagram Protocol, Src Port: 50688, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xf712
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 108]

wireshark_EthernetKJXZM1.pcapng    Packets: 3380 · Displayed: 6 (0.2%) · Dropped: 0 (0.0%)    Profile: Default
```


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time       Source               Destination          Protocol Length Info
   71 5.676483   fe80::b871:1ea8:bf9… fe80::1              DNS      91 Standard query 0xf712 A www.mit.edu
   89 6.675662   192.168.100.9        192.168.100.1        DNS      71 Standard query 0xf712 A www.mit.edu
  102 7.677071   192.168.100.9        192.168.100.1        DNS      71 Standard query 0xf712 A www.mit.edu
  108 8.052907   fe80::1              fe80::b871:1ea8:bf9… DNS     180 Standard query response 0xf712 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 173.22
  135 8.053682   192.168.100.1        192.168.100.9        DNS     163 Standard query response 0xf712 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 173.22
  158 10.128197  192.168.100.1        192.168.100.9        DNS     163 Standard query response 0xf712 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 173.22

> Frame 108: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd), Dst: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3)
> Internet Protocol Version 6, Src: fe80::1, Dst: fe80::b871:1ea8:bf90:8583
> User Datagram Protocol, Src Port: 53, Dst Port: 50688
v Domain Name System (response)
    Transaction ID: 0xf712
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 71]
    [Time: 2.376424000 seconds]

wireshark_EthernetKJXZM1.pcapng    Packets: 3380 · Displayed: 6 (0.2%) · Dropped: 0 (0.0%)    Profile: Default
```

Destination Port da query 53, Source Port da response 53.

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



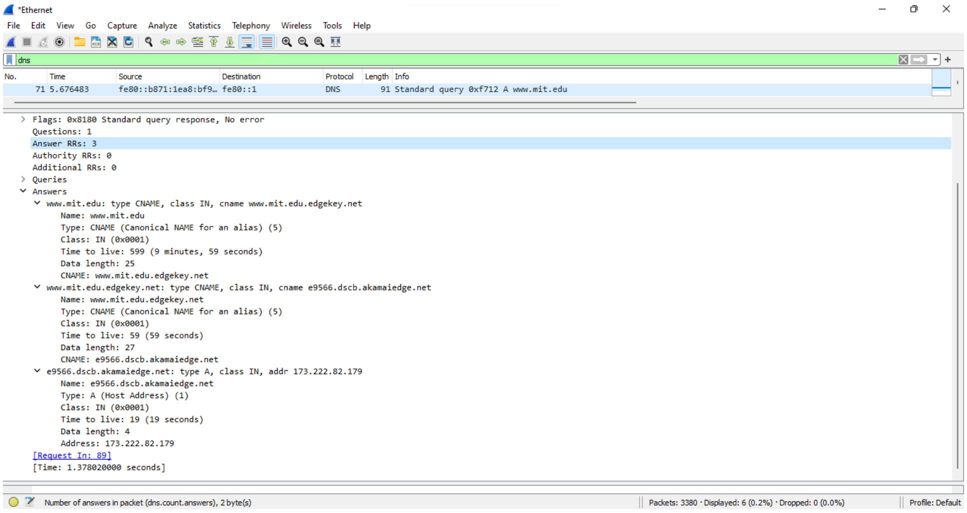
```
Servidores DNS. . . . . . . . . . . . . . : fe80::1%12
                                            192.168.100.1
NetBIOS em Tcpip. . . . . . . . . . . . . : Habilitado
```

192.168.100.1, sim é o endereço do servidor DNS local.

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

Standard query. Não contém nenhuma resposta.

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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time      Source                Destination  Protocol  Length  Info
  71 5.676483   fe80::b871:1ea8:bf9…  fe80::1      DNS          91  Standard query 0xf712 A www.mit.edu
```

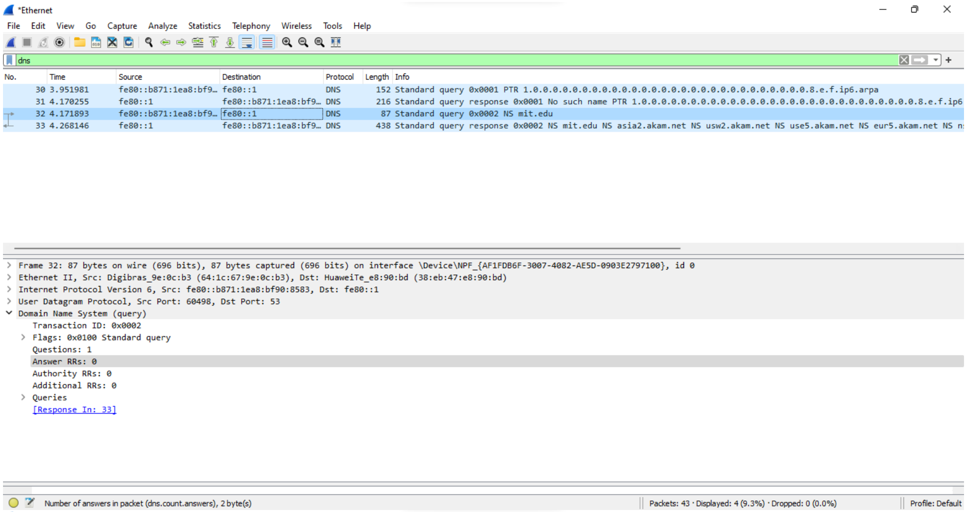
```
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
> Queries
v Answers
  v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 599 (9 minutes, 59 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
  v 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: 59 (59 seconds)
        Data length: 27
        CNAME: e9566.dscb.akamaiedge.net
  v e9566.dscb.akamaiedge.net: type A, class IN, addr 173.222.82.179
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 19 (19 seconds)
        Data length: 4
        Address: 173.222.82.179
  [Request In: 89]
  [Time: 1.378020000 seconds]
```

```
Number of answers in packet (dns.count.answers), 2 byte(s)    Packets: 3380 · Displayed: 6 (0.2%) · Dropped: 0 (0.0%)    Profile: Default
```

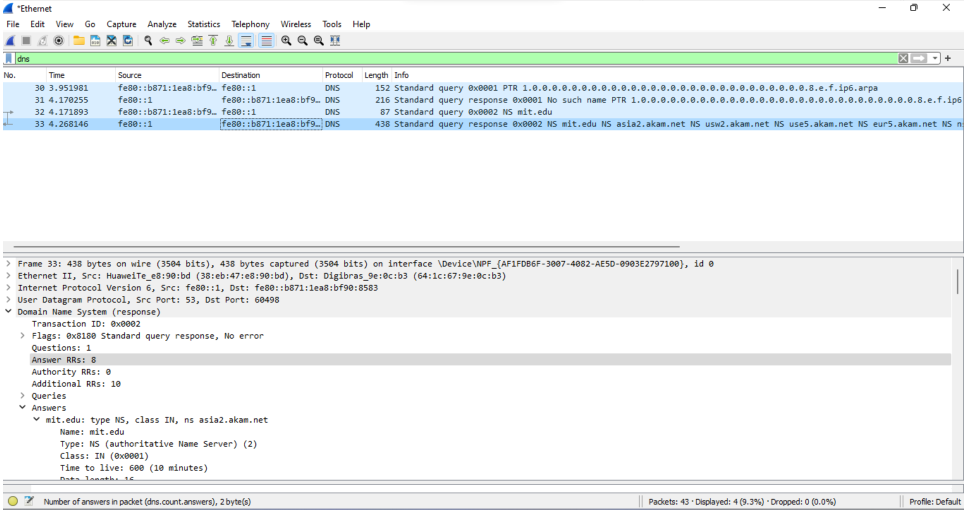
3 respostas que possuem o nome do host, tipo, classe, tempo de vida, tamanho e o endereço IP.

15. Provide a screenshot.

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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time      Source                 Destination            Protocol Length Info
  30 3.951981  fe80::b871:1ea8:bf9…   fe80::1                DNS       152 Standard query 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa
  31 4.170255  fe80::1                fe80::b871:1ea8:bf9…   DNS       216 Standard query response 0x0001 No such name PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6
  32 4.171893  fe80::b871:1ea8:bf9…   fe80::1                DNS        87 Standard query 0x0002 NS mit.edu
  33 4.268146  fe80::1                fe80::b871:1ea8:bf9…   DNS       438 Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS usw2.akam.net NS use5.akam.net NS eur5.akam.net NS n

> Frame 32: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3), Dst: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd)
> Internet Protocol Version 6, Src: fe80::b871:1ea8:bf90:8583, Dst: fe80::1
> User Datagram Protocol, Src Port: 60498, 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
  > Queries
    [Response In: 33]

Number of answers in packet (dns.count.answers), 2 byte(s)    Packets: 43 · Displayed: 4 (9.3%) · Dropped: 0 (0.0%)    Profile: Default
```


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

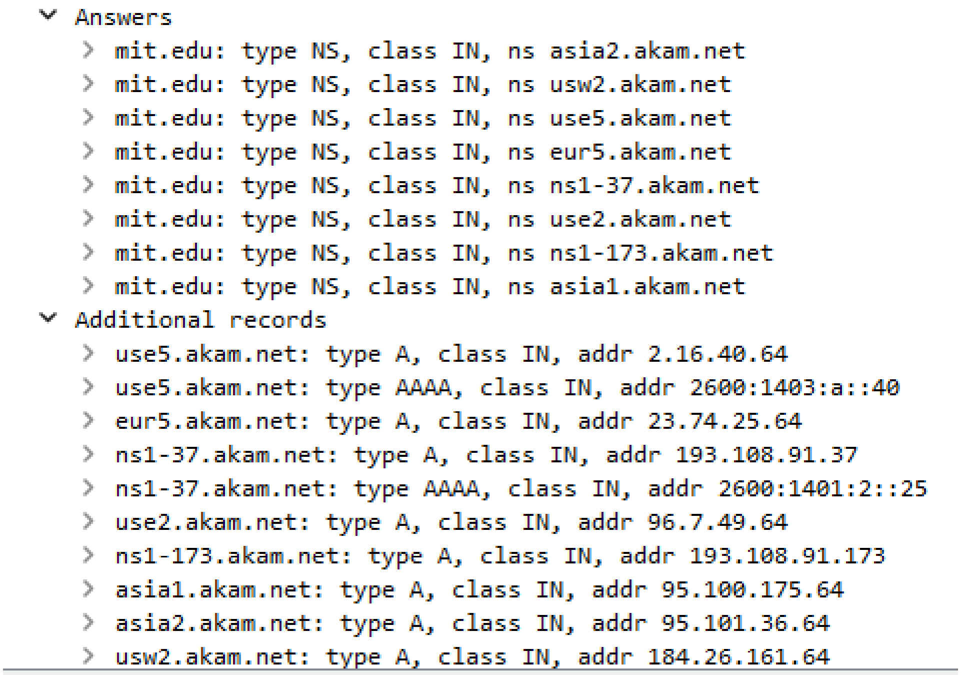
```
No.  Time      Source                 Destination            Protocol Length Info
  30 3.951981  fe80::b871:1ea8:bf9…   fe80::1                DNS       152 Standard query 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa
  31 4.170255  fe80::1                fe80::b871:1ea8:bf9…   DNS       216 Standard query response 0x0001 No such name PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6
  32 4.171893  fe80::b871:1ea8:bf9…   fe80::1                DNS        87 Standard query 0x0002 NS mit.edu
  33 4.268146  fe80::1                fe80::b871:1ea8:bf9…   DNS       438 Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS usw2.akam.net NS use5.akam.net NS eur5.akam.net NS n

> Frame 33: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd), Dst: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3)
> Internet Protocol Version 6, Src: fe80::1, Dst: fe80::b871:1ea8:bf90:8583
> User Datagram Protocol, Src Port: 53, Dst Port: 60498
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 10
  > Queries
  v Answers
    v mit.edu: type NS, class IN, ns asia2.akam.net
          Name: mit.edu
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
          Time to live: 600 (10 minutes)
          Data length: 16

Number of answers in packet (dns.count.answers), 2 byte(s)    Packets: 43 · Displayed: 4 (9.3%) · Dropped: 0 (0.0%)    Profile: Default
```

Fe80::1, sim é o endereço do servidor DNS local.

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

Standard query, não possui respostas.

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 namesers?

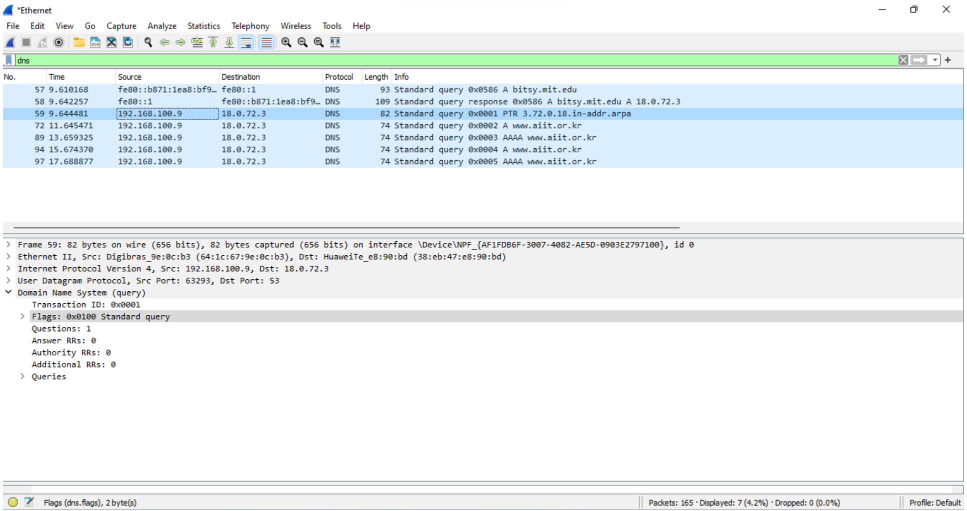


```
Answers
    mit.edu: type NS, class IN, ns asia2.akam.net
    mit.edu: type NS, class IN, ns usw2.akam.net
    mit.edu: type NS, class IN, ns use5.akam.net
    mit.edu: type NS, class IN, ns eur5.akam.net
    mit.edu: type NS, class IN, ns ns1-37.akam.net
    mit.edu: type NS, class IN, ns use2.akam.net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

Os nomes dos servidores estão listados abaixo, assim como o IP no Additional records.

19. Provide a screenshot.

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?

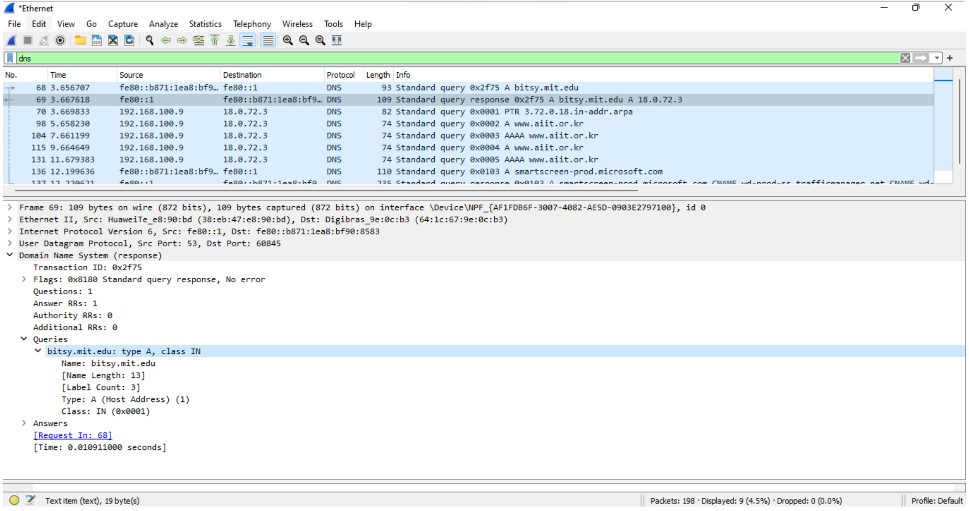

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.  Time       Source                 Destination            Protocol Length Info
  57 9.610168   fe80::b871:1ea8:bf9…   fe80::1                DNS       93 Standard query 0x0586 A bitsy.mit.edu
  58 9.642257   fe80::1                fe80::b871:1ea8:bf9…   DNS      109 Standard query response 0x0586 A bitsy.mit.edu A 18.0.72.3
  59 9.644481   192.168.100.9          18.0.72.3              DNS       82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  72 11.645471  192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0002 A www.aiit.or.kr
  89 13.659325  192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0003 AAAA www.aiit.or.kr
  94 15.674370  192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0004 A www.aiit.or.kr
  97 17.688877  192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
> Frame 59: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3), Dst: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd)
> Internet Protocol Version 4, Src: 192.168.100.9, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 63293, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

Flags (dns.flags), 2 byte(s) | Packets: 165 · Displayed: 7 (4.2%) · Dropped: 0 (0.0%) | Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.  Time       Source                 Destination            Protocol Length Info
  68 3.656707   fe80::b871:1ea8:bf9…   fe80::1                DNS       93 Standard query 0x2f75 A bitsy.mit.edu
  69 3.667618   fe80::1                fe80::b871:1ea8:bf9…   DNS      109 Standard query response 0x2f75 A bitsy.mit.edu A 18.0.72.3
  70 3.669833   192.168.100.9          18.0.72.3              DNS       82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  98 5.658230   192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0002 A www.aiit.or.kr
 104 7.661199   192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0003 AAAA www.aiit.or.kr
 115 9.664649   192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0004 A www.aiit.or.kr
 131 11.679383  192.168.100.9          18.0.72.3              DNS       74 Standard query 0x0005 AAAA www.aiit.or.kr
 136 12.199636  fe80::b871:1ea8:bf9…   fe80::1                DNS      110 Standard query 0x0103 A smartscreen-prod.microsoft.com
 137 12.220621  fe80::1                fe80::b871:1ea8:bf9    DNS      235 Standard query response 0x0103 A smartscreen-prod.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-
```

```
> Frame 69: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd), Dst: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3)
> Internet Protocol Version 6, Src: fe80::1, Dst: fe80::b871:1ea8:bf90:8583
> User Datagram Protocol, Src Port: 53, Dst Port: 60845
v Domain Name System (response)
    Transaction ID: 0x2f75
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  > Answers
    [Request In: 68]
    [Time: 0.010911000 seconds]
```

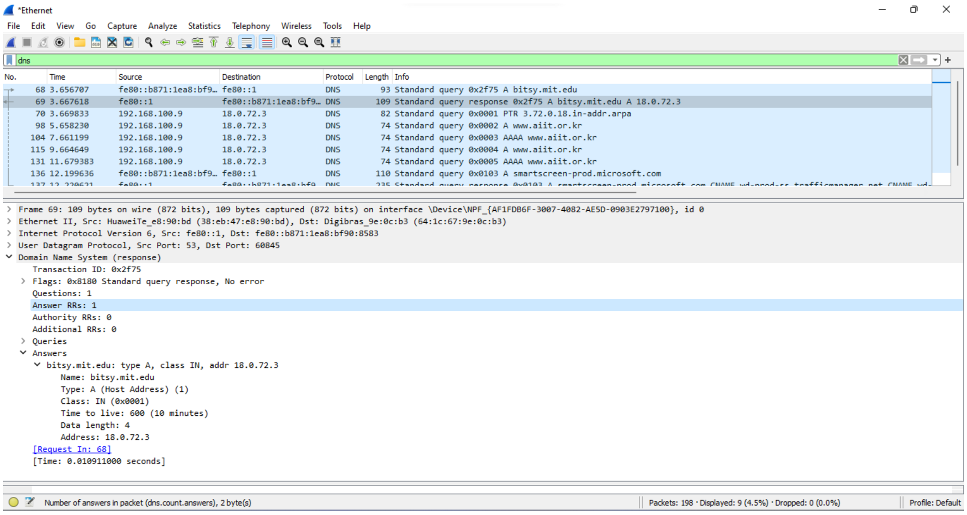
Text item (text), 19 byte(s) | Packets: 198 · Displayed: 9 (4.5%) · Dropped: 0 (0.0%) | Profile: Default

18.0.72.3, que corresponde ao bitsy.mit.edu

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

Standand query, não contém nenhuma resposta.

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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time        Source                Destination           Protocol Length Info
   68 3.656707    fe80::b871:1ea8:bf9… fe80::1               DNS        93 Standard query 0x2f75 A bitsy.mit.edu
   69 3.667618    fe80::1               fe80::b871:1ea8:bf9… DNS       109 Standard query response 0x2f75 A bitsy.mit.edu A 18.0.72.3
   70 3.669833    192.168.100.9         18.0.72.3             DNS        82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
   98 5.658230    192.168.100.9         18.0.72.3             DNS        74 Standard query 0x0002 A www.aiit.or.kr
  104 7.661199    192.168.100.9         18.0.72.3             DNS        74 Standard query 0x0003 AAAA www.aiit.or.kr
  115 9.664649    192.168.100.9         18.0.72.3             DNS        74 Standard query 0x0004 A www.aiit.or.kr
  131 11.679383   192.168.100.9         18.0.72.3             DNS        74 Standard query 0x0005 AAAA www.aiit.or.kr
  136 12.199636   fe80::b871:1ea8:bf9… fe80::1               DNS       110 Standard query 0x0103 A smartscreen-prod.microsoft.com
  137 12.220621   fe80::1               fe80::b871:1ea8:bf9   DNS       235 Standard query response 0x0103 A smartscreen-prod.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-
```

```
> Frame 69: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF_{AF1FDB6F-3007-4082-AE5D-0903E2797100}, id 0
> Ethernet II, Src: HuaweiTe_e8:90:bd (38:eb:47:e8:90:bd), Dst: Digibras_9e:0c:b3 (64:1c:67:9e:0c:b3)
> Internet Protocol Version 6, Src: fe80::1, Dst: fe80::b871:1ea8:bf90:8583
> User Datagram Protocol, Src Port: 53, Dst Port: 60845
v Domain Name System (response)
    Transaction ID: 0x2f75
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v bitsy.mit.edu: type A, class IN, addr 18.0.72.3
          Name: bitsy.mit.edu
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 600 (10 minutes)
          Data length: 4
          Address: 18.0.72.3
    [Request In: 68]
    [Time: 0.010911000 seconds]
```

Number of answers in packet (dns.count.answers), 2 byte(s) | Packets: 198 · Displayed: 9 (4.5%) · Dropped: 0 (0.0%) | Profile: Default

Possui uma resposta, com o nome do host, tipo, classe, tempo de vida, tamanho e o endereço IP.

23. Provide a screenshot.