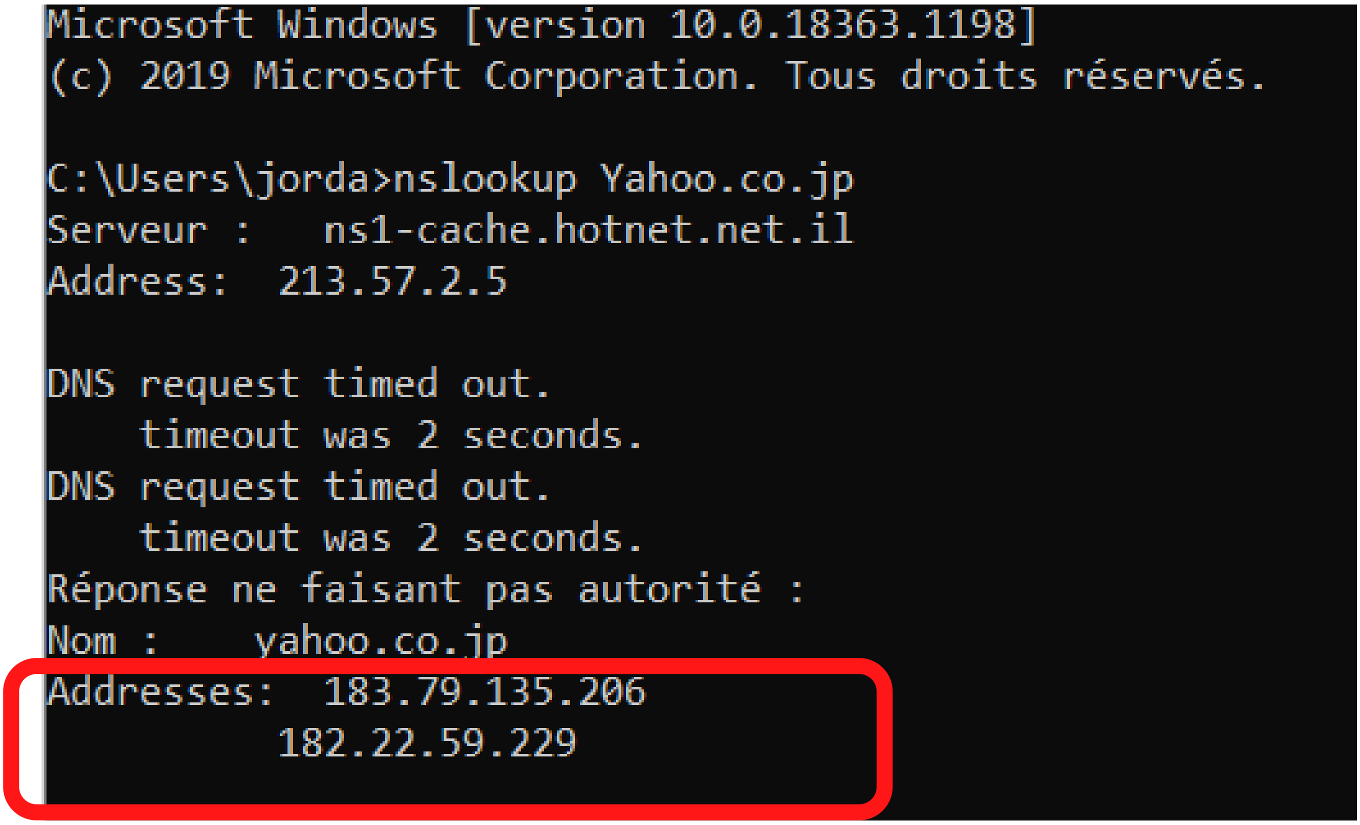
Jordan Perez
336165733

DNS HW2

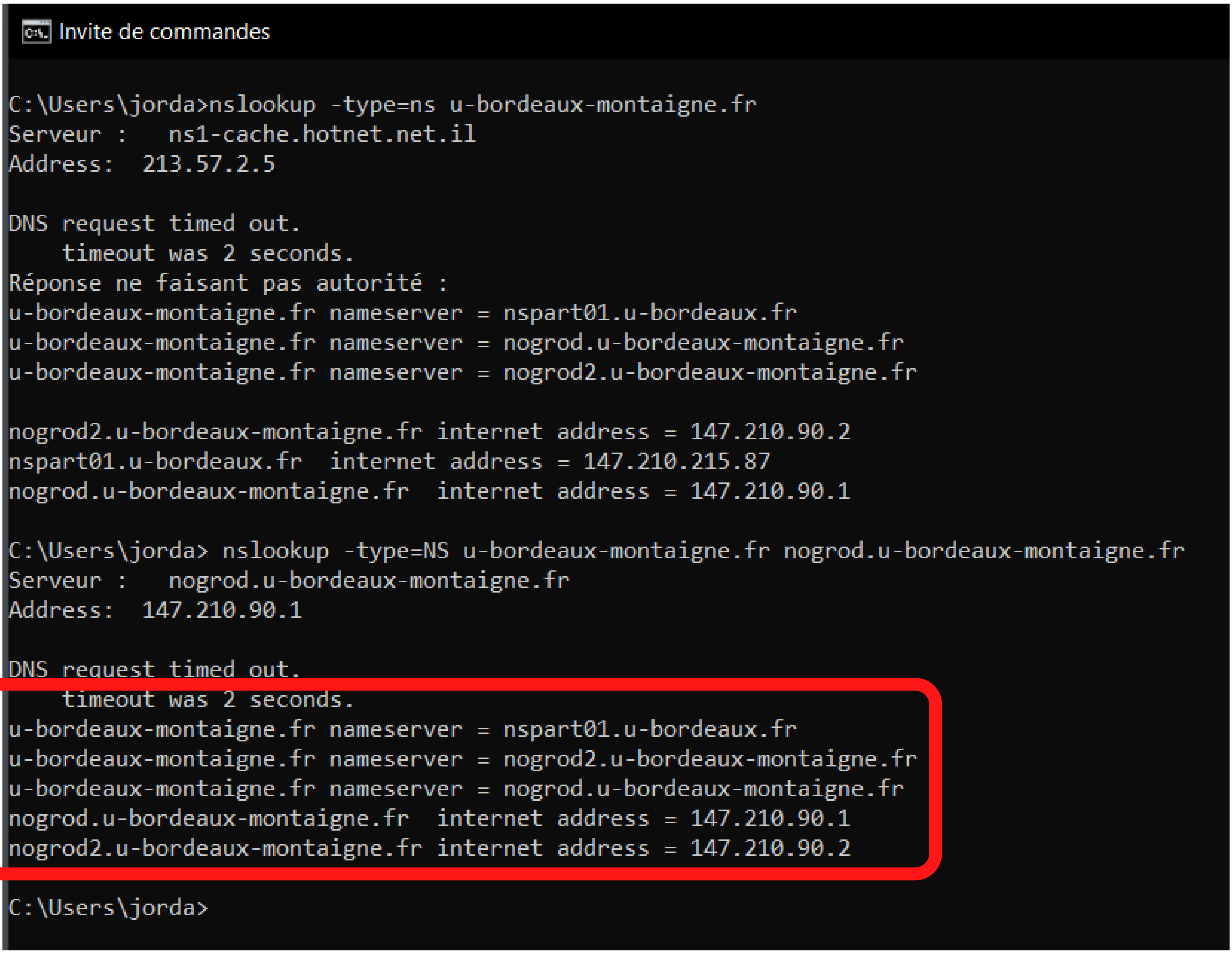
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?



```
Microsoft Windows [version 10.0.18363.1198]
(c) 2019 Microsoft Corporation. Tous droits réservés.

C:\Users\jorda>nslookup Yahoo.co.jp
Serveur :   ns1-cache.hotnet.net.il
Address:  213.57.2.5

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Réponse ne faisant pas autorité :
Nom :    yahoo.co.jp
Addresses:  183.79.135.206
          182.22.59.229
```

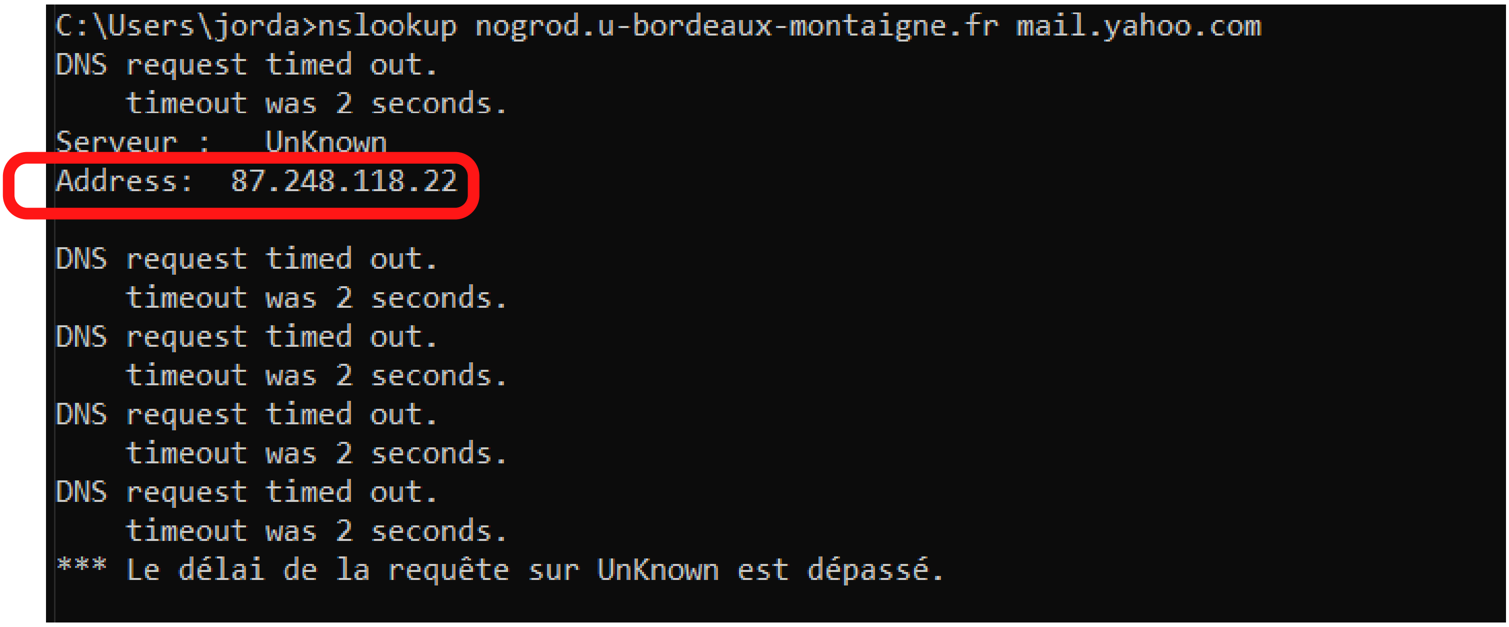
Answers: **183.79.135.206 and 182.22.59.229**

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



```
C:\Users\jorda>nslookup -type=ns u-bordeaux-montaigne.fr
Serveur :   ns1-cache.hotnet.net.il
Address:  213.57.2.5

DNS request timed out.
    timeout was 2 seconds.
Réponse ne faisant pas autorité :
u-bordeaux-montaigne.fr nameserver = nspart01.u-bordeaux.fr
u-bordeaux-montaigne.fr nameserver = nogrod.u-bordeaux-montaigne.fr
u-bordeaux-montaigne.fr nameserver = nogrod2.u-bordeaux-montaigne.fr

nogrod2.u-bordeaux-montaigne.fr internet address = 147.210.90.2
nspart01.u-bordeaux.fr  internet address = 147.210.215.87
nogrod.u-bordeaux-montaigne.fr  internet address = 147.210.90.1

C:\Users\jorda> nslookup -type=NS u-bordeaux-montaigne.fr nogrod.u-bordeaux-montaigne.fr
Serveur :   nogrod.u-bordeaux-montaigne.fr
Address:  147.210.90.1

DNS request timed out.
    timeout was 2 seconds.
u-bordeaux-montaigne.fr nameserver = nspart01.u-bordeaux.fr
u-bordeaux-montaigne.fr nameserver = nogrod2.u-bordeaux-montaigne.fr
u-bordeaux-montaigne.fr nameserver = nogrod.u-bordeaux-montaigne.fr
nogrod.u-bordeaux-montaigne.fr  internet address = 147.210.90.1
nogrod2.u-bordeaux-montaigne.fr internet address = 147.210.90.2

C:\Users\jorda>
```

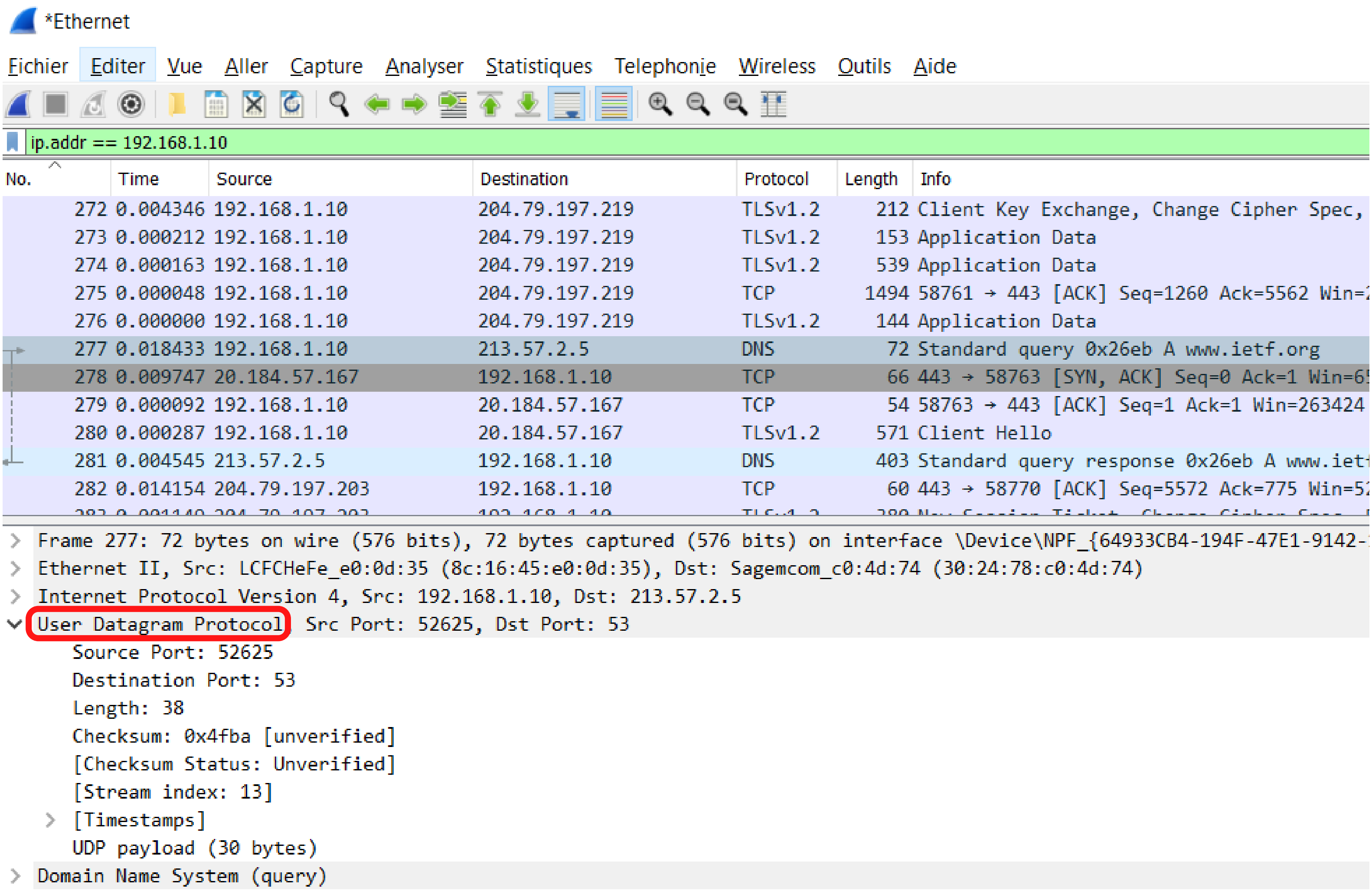
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?



```
C:\Users\jorda>nslookup nogrod.u-bordeaux-montaigne.fr mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Serveur :   UnKnown
Address:  87.248.118.22

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.
*** Le délai de la requête sur UnKnown est dépassé.
```

Answer: 87.248.118.22

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



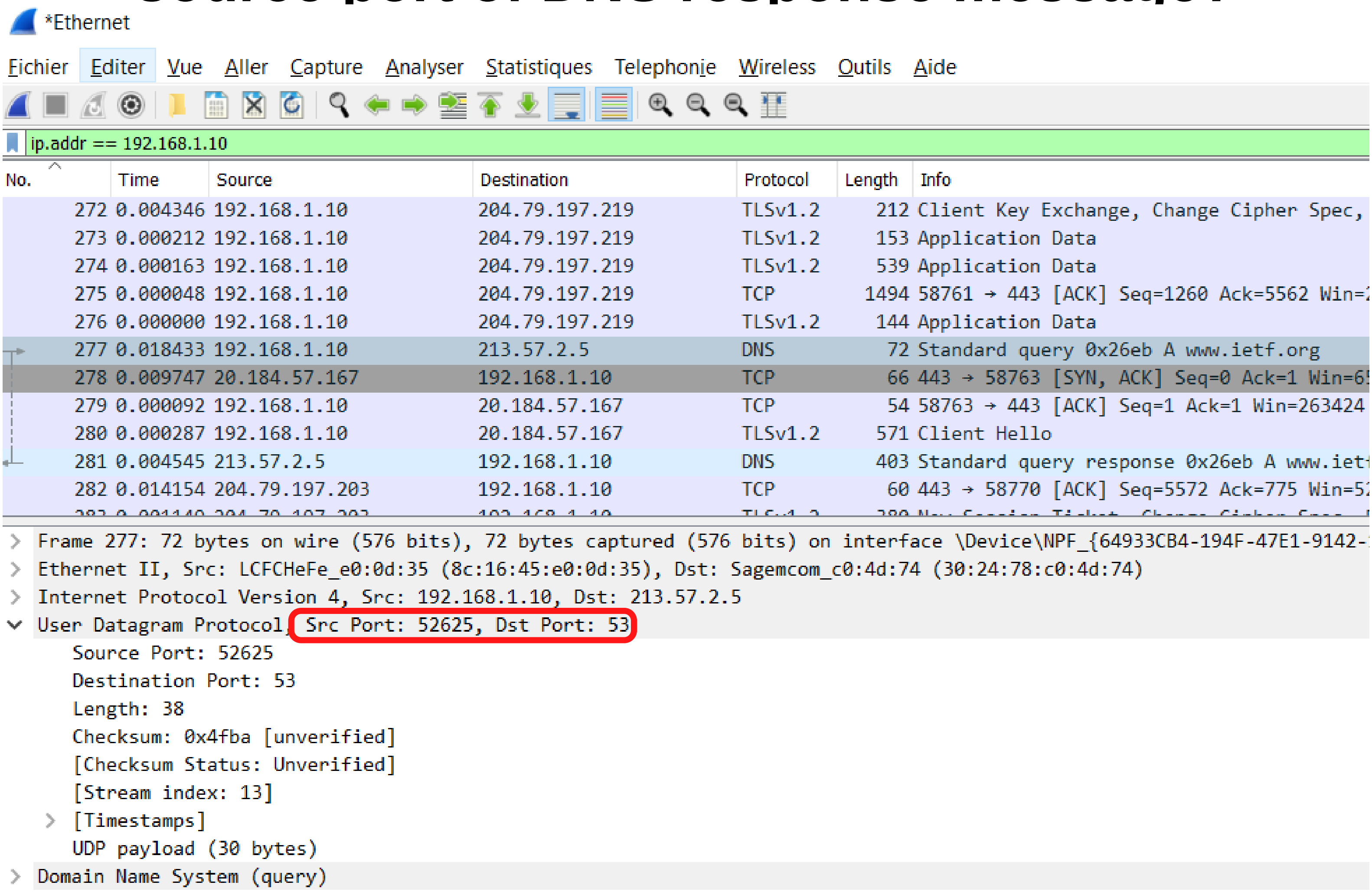
```
ip.addr == 192.168.1.10
```

```
No.   Time     Source           Destination      Protocol  Length Info
  272 0.004346 192.168.1.10     204.79.197.219   TLSv1.2     212 Client Key Exchange, Change Cipher Spec,
  273 0.000212 192.168.1.10     204.79.197.219   TLSv1.2     153 Application Data
  274 0.000163 192.168.1.10     204.79.197.219   TLSv1.2     539 Application Data
  275 0.000048 192.168.1.10     204.79.197.219   TCP        1494 58761 → 443 [ACK] Seq=1260 Ack=5562 Win=
  276 0.000000 192.168.1.10     204.79.197.219   TLSv1.2     144 Application Data
  277 0.018433 192.168.1.10     213.57.2.5       DNS          72 Standard query 0x26eb A www.ietf.org
  278 0.009747 20.184.57.167    192.168.1.10     TCP          66 443 → 58763 [SYN, ACK] Seq=0 Ack=1 Win=6
  279 0.000092 192.168.1.10     20.184.57.167    TCP          54 58763 → 443 [ACK] Seq=1 Ack=1 Win=263424
  280 0.000287 192.168.1.10     20.184.57.167    TLSv1.2     571 Client Hello
  281 0.004545 213.57.2.5       192.168.1.10     DNS         403 Standard query response 0x26eb A www.iet
  282 0.014154 204.79.197.203   192.168.1.10     TCP          60 443 → 58770 [ACK] Seq=5572 Ack=775 Win=5
  283 0.001140 204.79.197.203   192.168.1.10     TLSv1.2     290 New Session Ticket, Change Cipher Spec,
```

```
> Frame 277: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
v User Datagram Protocol, Src Port: 52625, Dst Port: 53
     Source Port: 52625
     Destination Port: 53
     Length: 38
     Checksum: 0x4fba [unverified]
     [Checksum Status: Unverified]
     [Stream index: 13]
   > [Timestamps]
     UDP payload (30 bytes)
> Domain Name System (query)
```

<u>Answer:</u> **UDP**

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



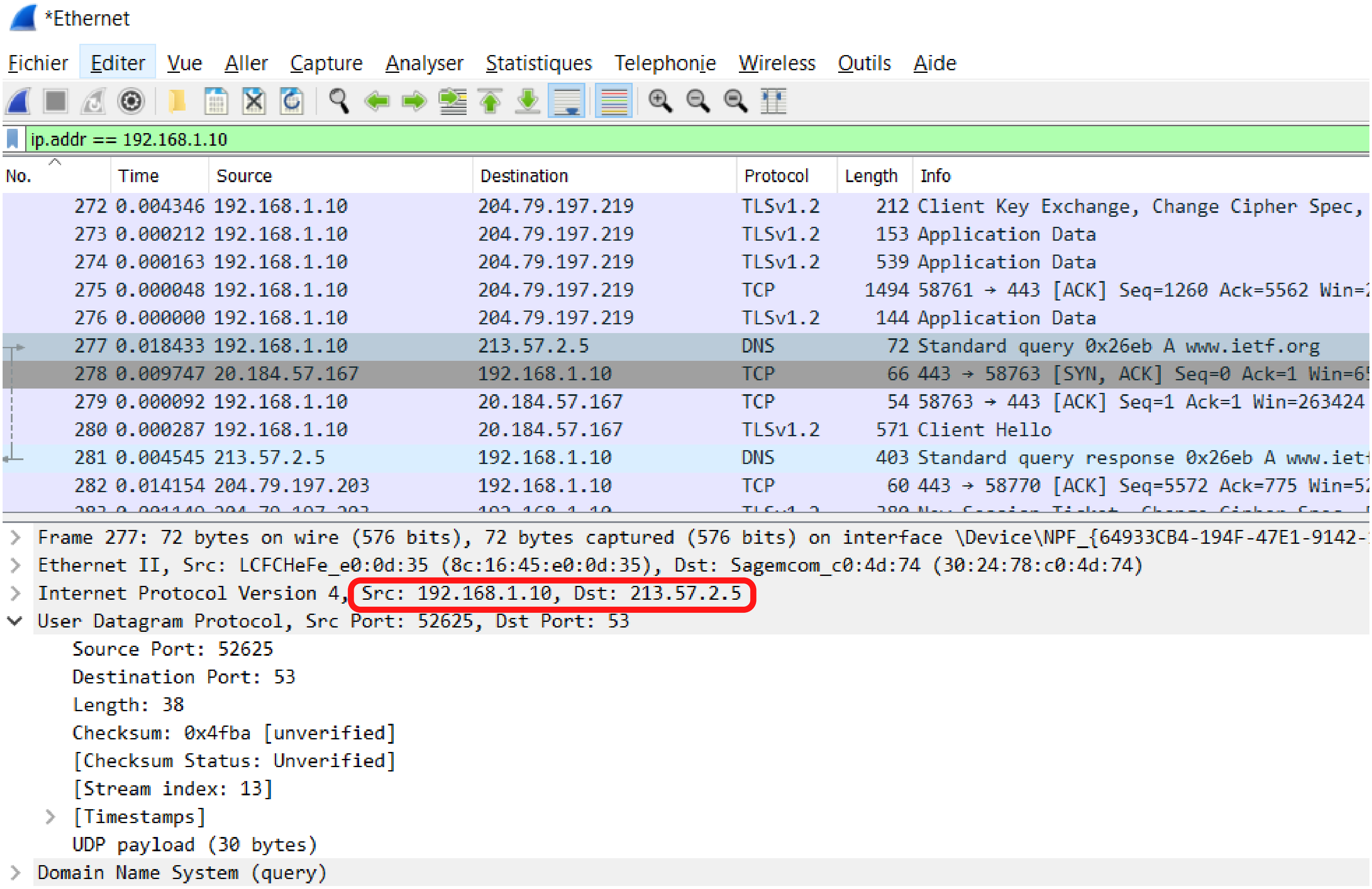
ip.addr == 192.168.1.10

```
No.   Time     Source          Destination      Protocol  Length Info
  272 0.004346 192.168.1.10    204.79.197.219   TLSv1.2      212 Client Key Exchange, Change Cipher Spec,
  273 0.000212 192.168.1.10    204.79.197.219   TLSv1.2      153 Application Data
  274 0.000163 192.168.1.10    204.79.197.219   TLSv1.2      539 Application Data
  275 0.000048 192.168.1.10    204.79.197.219   TCP         1494 58761 → 443 [ACK] Seq=1260 Ack=5562 Win=2
  276 0.000000 192.168.1.10    204.79.197.219   TLSv1.2      144 Application Data
  277 0.018433 192.168.1.10    213.57.2.5       DNS           72 Standard query 0x26eb A www.ietf.org
  278 0.009747 20.184.57.167   192.168.1.10     TCP           66 443 → 58763 [SYN, ACK] Seq=0 Ack=1 Win=65
  279 0.000092 192.168.1.10    20.184.57.167    TCP           54 58763 → 443 [ACK] Seq=1 Ack=1 Win=263424
  280 0.000287 192.168.1.10    20.184.57.167    TLSv1.2      571 Client Hello
  281 0.004545 213.57.2.5      192.168.1.10     DNS          403 Standard query response 0x26eb A www.iet
  282 0.014154 204.79.197.203  192.168.1.10     TCP           60 443 → 58770 [ACK] Seq=5572 Ack=775 Win=52
```

```
> Frame 277: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
v User Datagram Protocol, Src Port: 52625, Dst Port: 53
     Source Port: 52625
     Destination Port: 53
     Length: 38
     Checksum: 0x4fba [unverified]
     [Checksum Status: Unverified]
     [Stream index: 13]
   > [Timestamps]
     UDP payload (30 bytes)
> Domain Name System (query)
```

<u>Answer:</u> **Source port: 52625 & Dest port: 53**

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?

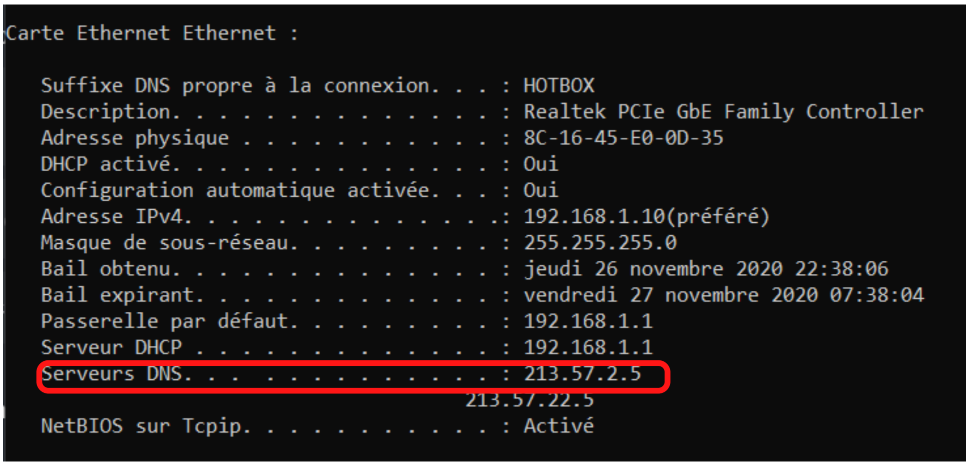


```
ip.addr == 192.168.1.10
```

```
No.     Time     Source          Destination     Protocol  Length  Info
    272 0.004346 192.168.1.10    204.79.197.219  TLSv1.2      212 Client Key Exchange, Change Cipher Spec,
    273 0.000212 192.168.1.10    204.79.197.219  TLSv1.2      153 Application Data
    274 0.000163 192.168.1.10    204.79.197.219  TLSv1.2      539 Application Data
    275 0.000048 192.168.1.10    204.79.197.219  TCP         1494 58761 → 443 [ACK] Seq=1260 Ack=5562 Win=
    276 0.000000 192.168.1.10    204.79.197.219  TLSv1.2      144 Application Data
    277 0.018433 192.168.1.10    213.57.2.5      DNS           72 Standard query 0x26eb A www.ietf.org
    278 0.009747 20.184.57.167   192.168.1.10    TCP           66 443 → 58763 [SYN, ACK] Seq=0 Ack=1 Win=6
    279 0.000092 192.168.1.10    20.184.57.167   TCP           54 58763 → 443 [ACK] Seq=1 Ack=1 Win=263424
    280 0.000287 192.168.1.10    20.184.57.167   TLSv1.2      571 Client Hello
    281 0.004545 213.57.2.5      192.168.1.10    DNS          403 Standard query response 0x26eb A www.iet
    282 0.014154 204.79.197.203  192.168.1.10    TCP           60 443 → 58770 [ACK] Seq=5572 Ack=775 Win=5
```

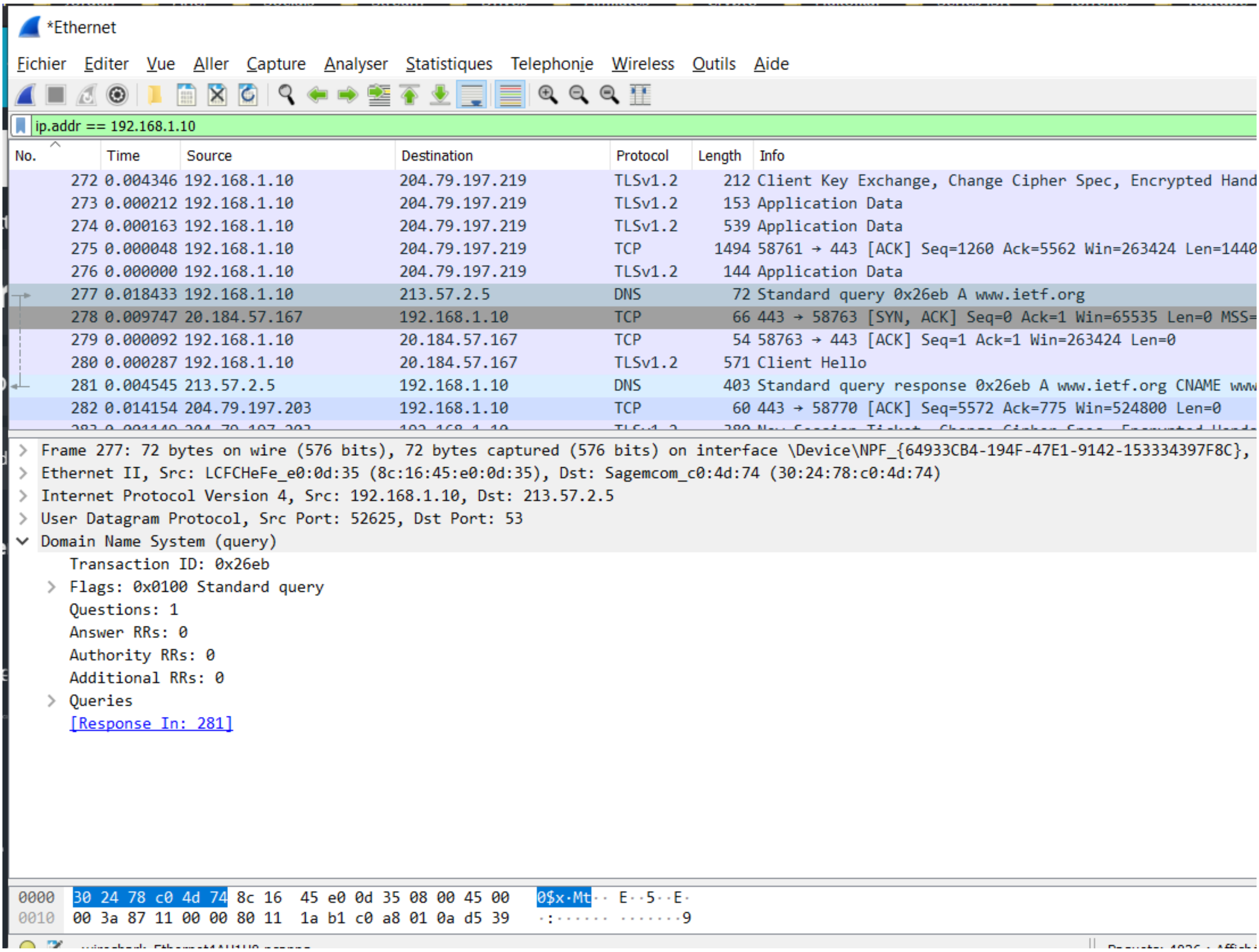
```
> Frame 277: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
v User Datagram Protocol, Src Port: 52625, Dst Port: 53
    Source Port: 52625
    Destination Port: 53
    Length: 38
    Checksum: 0x4fba [unverified]
    [Checksum Status: Unverified]
    [Stream index: 13]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

<u>Answer:</u> The screenshot shows that the DNS message was sent to 213.57.2.5. This matches the DNS server listed by the command ipconfig /all



```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : HOTBOX
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : 8C-16-45-E0-0D-35
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.10(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : jeudi 26 novembre 2020 22:38:06
   Bail expirant. . . . . . . . . . . . . : vendredi 27 novembre 2020 07:38:04
   Passerelle par défaut. . . . . . . . . : 192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
   Serveurs DNS. . .  . . . . . . . . . . : 213.57.2.5
                                       213.57.22.5
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

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



*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.1.10
```

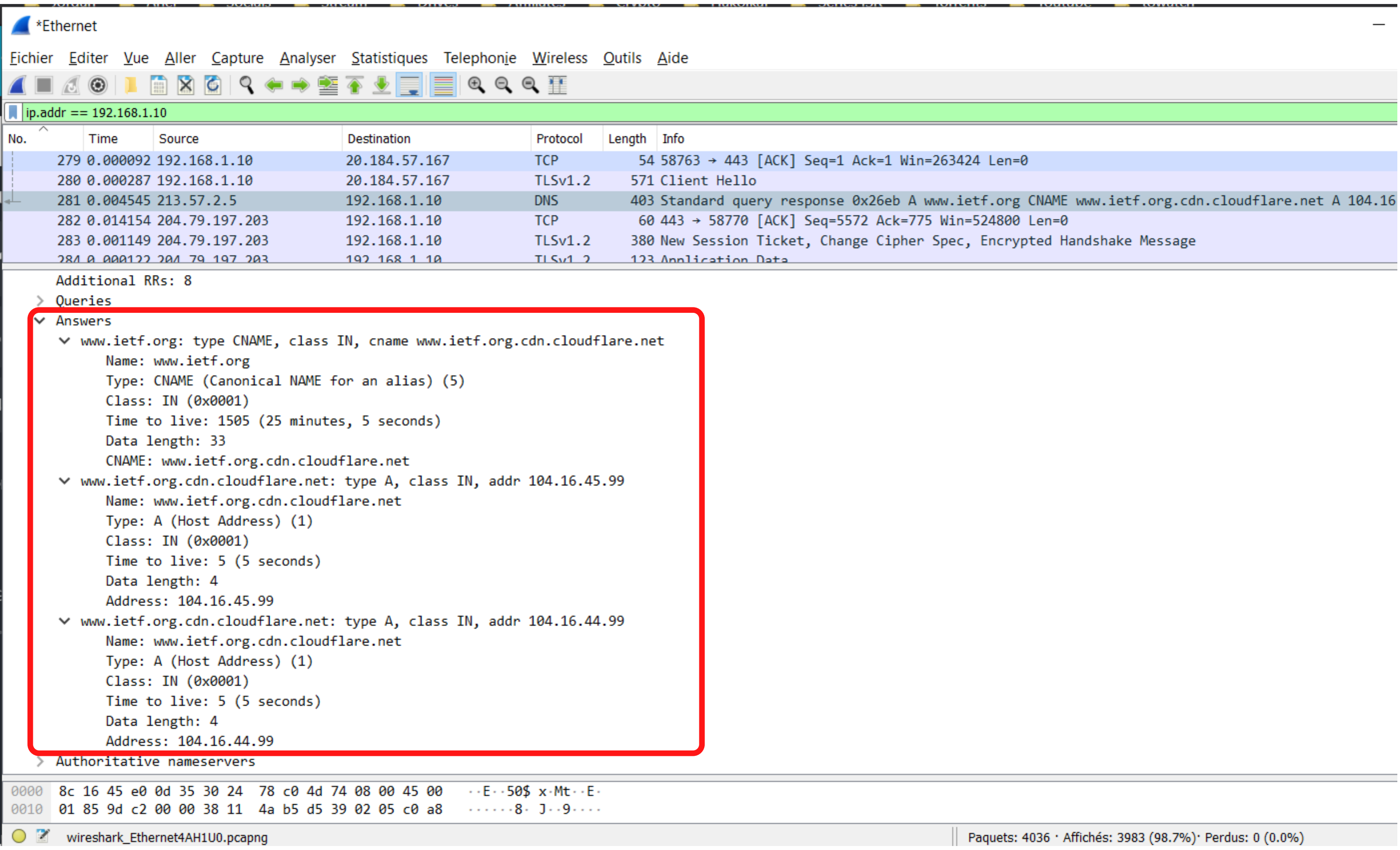
```
No.   Time     Source          Destination     Protocol  Length Info
  272 0.004346 192.168.1.10    204.79.197.219  TLSv1.2     212 Client Key Exchange, Change Cipher Spec, Encrypted Hand
  273 0.000212 192.168.1.10    204.79.197.219  TLSv1.2     153 Application Data
  274 0.000163 192.168.1.10    204.79.197.219  TLSv1.2     539 Application Data
  275 0.000048 192.168.1.10    204.79.197.219  TCP        1494 58761 → 443 [ACK] Seq=1260 Ack=5562 Win=263424 Len=1440
  276 0.000000 192.168.1.10    204.79.197.219  TLSv1.2     144 Application Data
  277 0.018433 192.168.1.10    213.57.2.5      DNS          72 Standard query 0x26eb A www.ietf.org
  278 0.009747 20.184.57.167   192.168.1.10    TCP          66 443 → 58763 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
  279 0.000092 192.168.1.10    20.184.57.167   TCP          54 58763 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
  280 0.000287 192.168.1.10    20.184.57.167   TLSv1.2     571 Client Hello
  281 0.004545 213.57.2.5      192.168.1.10    DNS         403 Standard query response 0x26eb A www.ietf.org CNAME www
  282 0.014154 204.79.197.203  192.168.1.10    TCP          60 443 → 58770 [ACK] Seq=5572 Ack=775 Win=524800 Len=0
```

```
> Frame 277: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-153334397F8C},
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
> User Datagram Protocol, Src Port: 52625, Dst Port: 53
v Domain Name System (query)
     Transaction ID: 0x26eb
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   > Queries
     [Response In: 281]
```

```
0000  30 24 78 c0 4d 74 8c 16  45 e0 0d 35 08 00 45 00   0$x·Mt·· E··5··E·
0010  00 3a 87 11 00 00 80 11  1a b1 c0 a8 01 0a d5 39   ·:······ ·······9
```

Answer: Standard query, type A, no answer

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



```
ip.addr == 192.168.1.10
```

```
No.     Time     Source          Destination     Protocol  Length Info
    279 0.000092 192.168.1.10    20.184.57.167   TCP         54 58763 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
    280 0.000287 192.168.1.10    20.184.57.167   TLSv1.2    571 Client Hello
    281 0.004545 213.57.2.5      192.168.1.10    DNS        403 Standard query response 0x26eb A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16
    282 0.014154 204.79.197.203  192.168.1.10    TCP         60 443 → 58770 [ACK] Seq=5572 Ack=775 Win=524800 Len=0
    283 0.001149 204.79.197.203  192.168.1.10    TLSv1.2    380 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
    284 0.000122 204.79.197.203  192.168.1.10    TLSv1.2    123 Application Data
```

```
    Additional RRs: 8
  > 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: 1505 (25 minutes, 5 seconds)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 5 (5 seconds)
        Data length: 4
        Address: 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: 5 (5 seconds)
        Data length: 4
        Address: 104.16.44.99
  > Authoritative nameservers
```

```
0000  8c 16 45 e0 0d 35 30 24  78 c0 4d 74 08 00 45 00   ··E··50$ x·Mt··E·
0010  01 85 9d c2 00 00 38 11  4a b5 d5 39 02 05 c0 a8   ······8· J··9····
```

```
wireshark_Ethernet4AH1U0.pcapng          Paquets: 4036 · Affichés: 3983 (98.7%)· Perdus: 0 (0.0%)
```

<u>Answer:</u> 3 answers provided. Each of them contains a name, a type, a class, a time to live, a data length and an adress

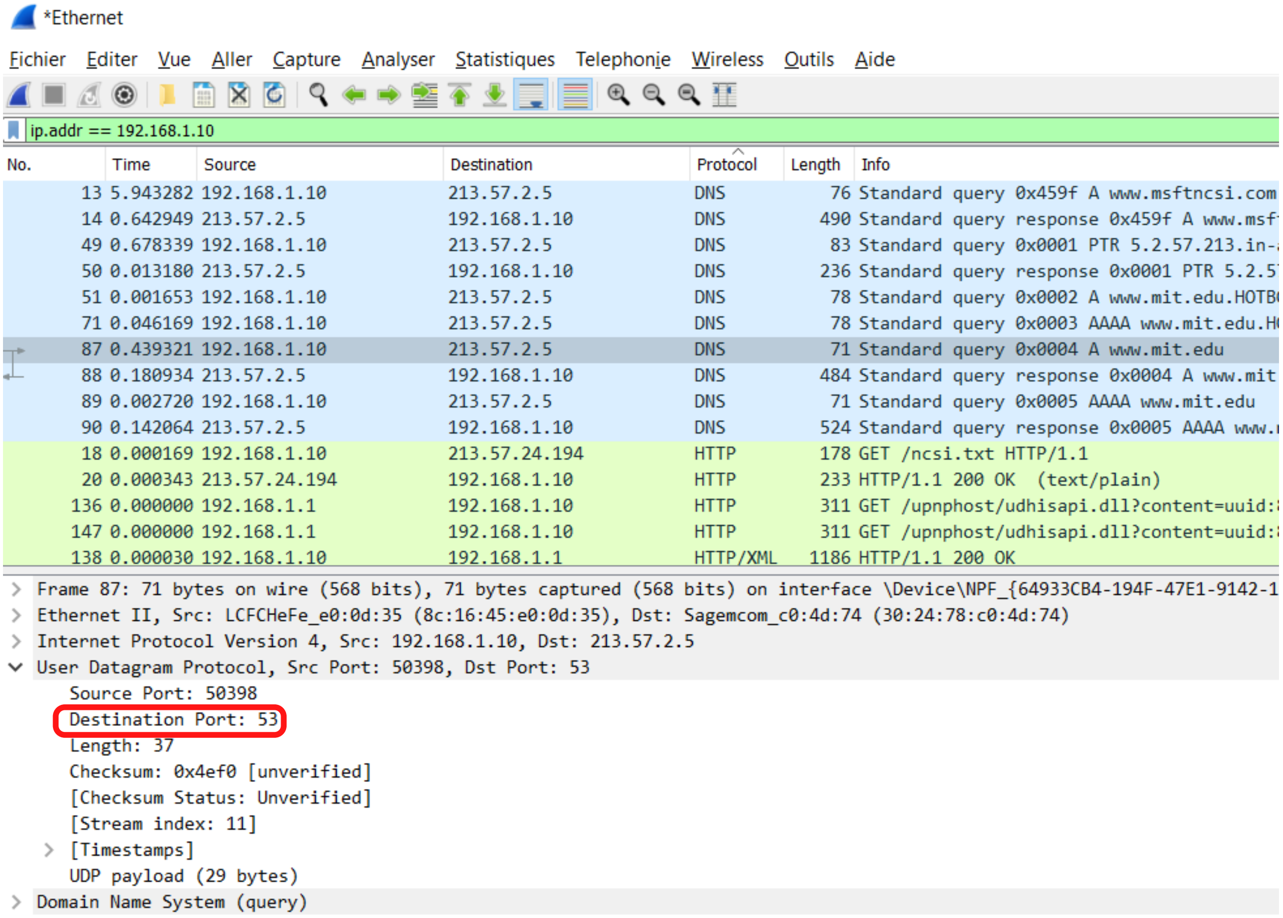
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer: **Yes, as seen in the prior screenshot, the destination address is 104.16.44.99 which is the address provided by the DNS server for www.ietf.org.**

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

Answer: **No, the images are all loaded from www.ietf.org, so no additional DNS queries are necessary**

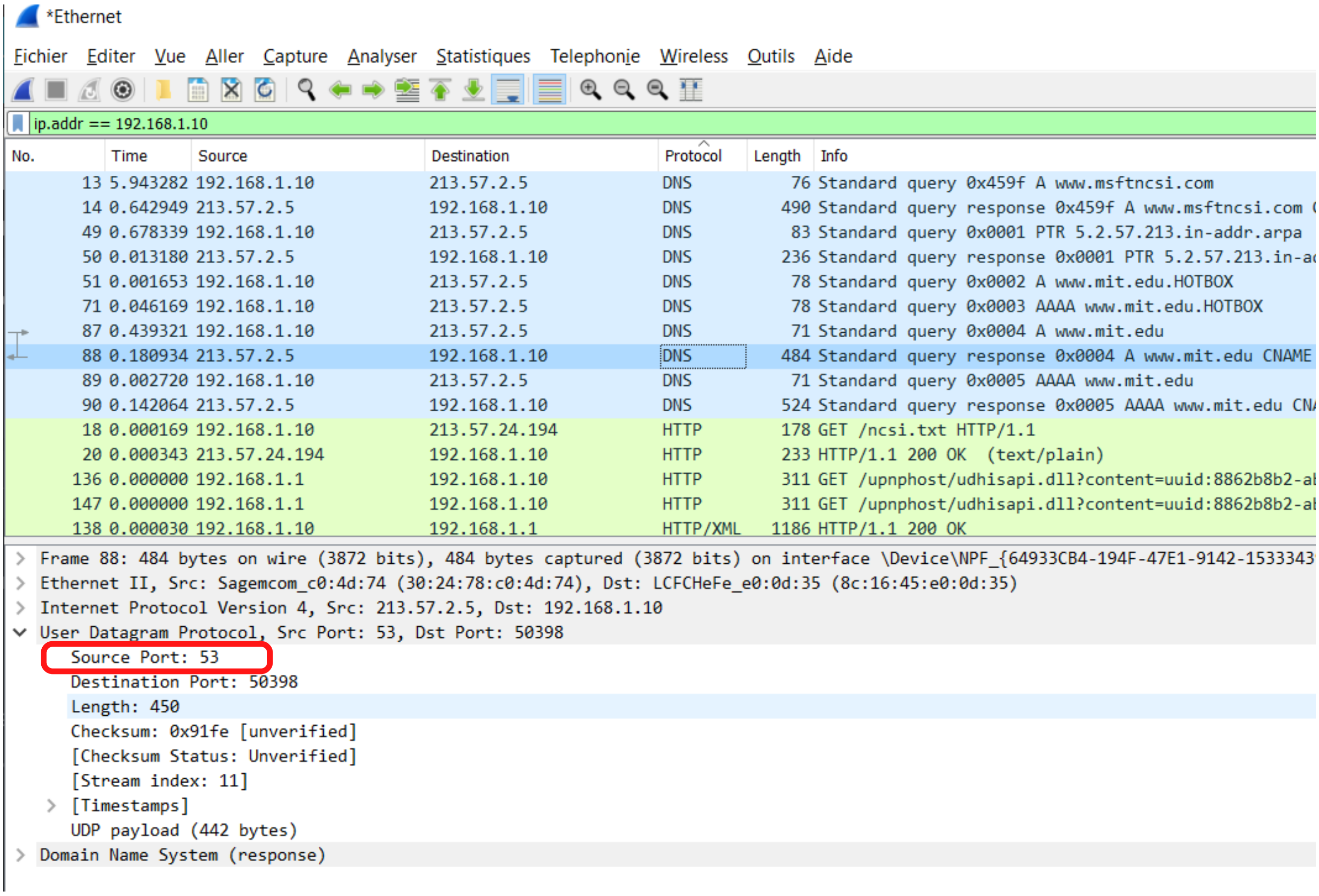
11. What is the destination port for the DNS query message? What is the source port of DNS response message?


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ip.addr == 192.168.1.10

```
No.   Time      Source          Destination     Protocol  Length Info
   13 5.943282 192.168.1.10    213.57.2.5      DNS        76 Standard query 0x459f A www.msftncsi.com
   14 0.642949 213.57.2.5      192.168.1.10    DNS       490 Standard query response 0x459f A www.msf
   49 0.678339 192.168.1.10    213.57.2.5      DNS        83 Standard query 0x0001 PTR 5.2.57.213.in-
   50 0.013180 213.57.2.5      192.168.1.10    DNS       236 Standard query response 0x0001 PTR 5.2.5
   51 0.001653 192.168.1.10    213.57.2.5      DNS        78 Standard query 0x0002 A www.mit.edu.HOTB
   71 0.046169 192.168.1.10    213.57.2.5      DNS        78 Standard query 0x0003 AAAA www.mit.edu.H
   87 0.439321 192.168.1.10    213.57.2.5      DNS        71 Standard query 0x0004 A www.mit.edu
   88 0.180934 213.57.2.5      192.168.1.10    DNS       484 Standard query response 0x0004 A www.mit
   89 0.002720 192.168.1.10    213.57.2.5      DNS        71 Standard query 0x0005 AAAA www.mit.edu
   90 0.142064 213.57.2.5      192.168.1.10    DNS       524 Standard query response 0x0005 AAAA www.
   18 0.000169 192.168.1.10    213.57.24.194   HTTP      178 GET /ncsi.txt HTTP/1.1
   20 0.000343 213.57.24.194   192.168.1.10    HTTP      233 HTTP/1.1 200 OK  (text/plain)
  136 0.000000 192.168.1.1     192.168.1.10    HTTP      311 GET /upnphost/udhisapi.dll?content=uuid:
  147 0.000000 192.168.1.1     192.168.1.10    HTTP      311 GET /upnphost/udhisapi.dll?content=uuid:
  138 0.000030 192.168.1.10    192.168.1.1     HTTP/XML 1186 HTTP/1.1 200 OK
```

```
> Frame 87: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-1
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
v User Datagram Protocol, Src Port: 50398, Dst Port: 53
    Source Port: 50398
    Destination Port: 53
    Length: 37
    Checksum: 0x4ef0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

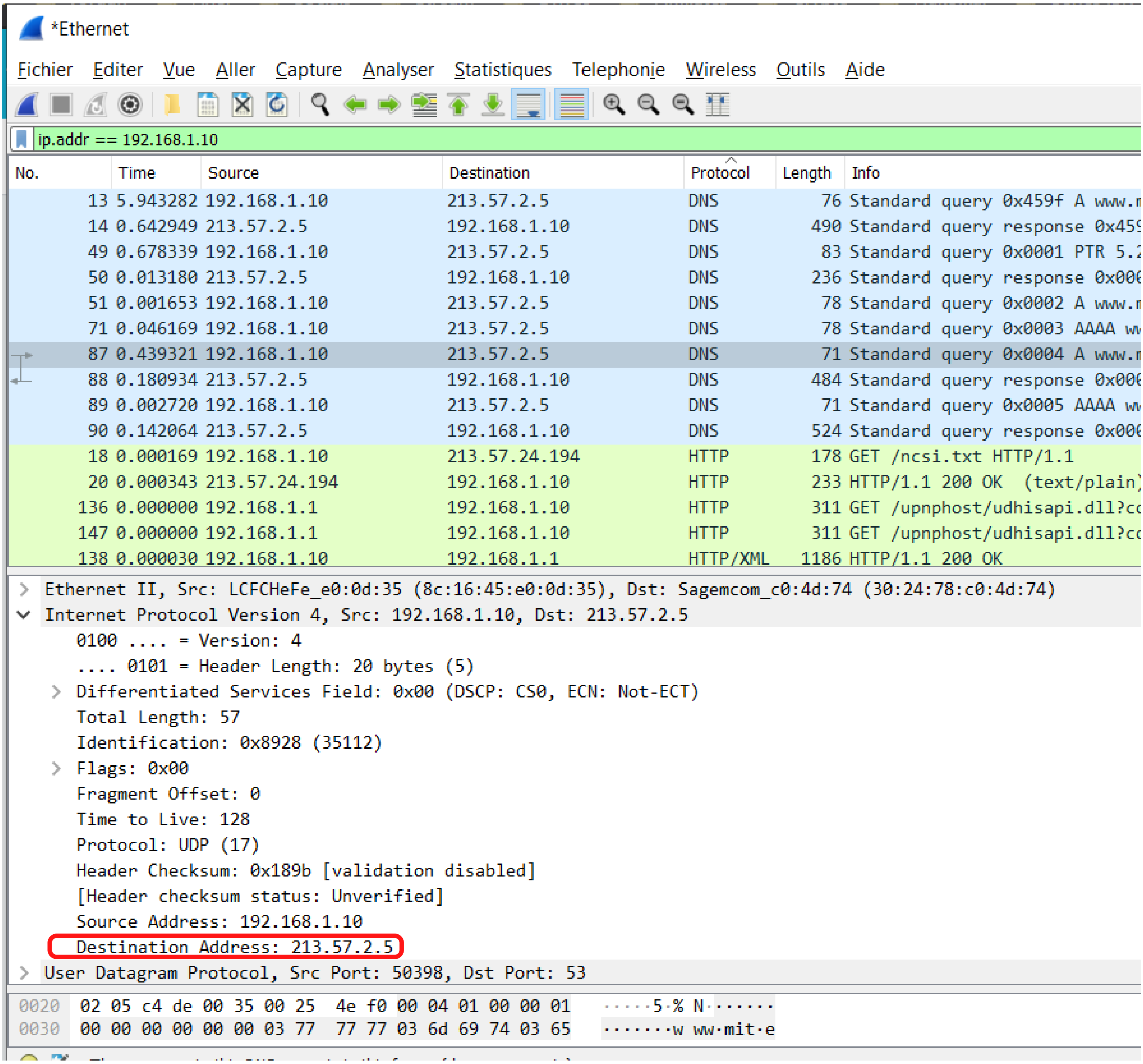

*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ip.addr == 192.168.1.10

```
No.   Time      Source          Destination     Protocol  Length Info
   13 5.943282 192.168.1.10    213.57.2.5      DNS        76 Standard query 0x459f A www.msftncsi.com
   14 0.642949 213.57.2.5      192.168.1.10    DNS       490 Standard query response 0x459f A www.msftncsi.com (
   49 0.678339 192.168.1.10    213.57.2.5      DNS        83 Standard query 0x0001 PTR 5.2.57.213.in-addr.arpa
   50 0.013180 213.57.2.5      192.168.1.10    DNS       236 Standard query response 0x0001 PTR 5.2.57.213.in-ad
   51 0.001653 192.168.1.10    213.57.2.5      DNS        78 Standard query 0x0002 A www.mit.edu.HOTBOX
   71 0.046169 192.168.1.10    213.57.2.5      DNS        78 Standard query 0x0003 AAAA www.mit.edu.HOTBOX
   87 0.439321 192.168.1.10    213.57.2.5      DNS        71 Standard query 0x0004 A www.mit.edu
   88 0.180934 213.57.2.5      192.168.1.10    DNS       484 Standard query response 0x0004 A www.mit.edu CNAME
   89 0.002720 192.168.1.10    213.57.2.5      DNS        71 Standard query 0x0005 AAAA www.mit.edu
   90 0.142064 213.57.2.5      192.168.1.10    DNS       524 Standard query response 0x0005 AAAA www.mit.edu CN/
   18 0.000169 192.168.1.10    213.57.24.194   HTTP      178 GET /ncsi.txt HTTP/1.1
   20 0.000343 213.57.24.194   192.168.1.10    HTTP      233 HTTP/1.1 200 OK  (text/plain)
  136 0.000000 192.168.1.1     192.168.1.10    HTTP      311 GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab
  147 0.000000 192.168.1.1     192.168.1.10    HTTP      311 GET /upnphost/udhisapi.dll?content=uuid:8862b8b2-ab
  138 0.000030 192.168.1.10    192.168.1.1     HTTP/XML 1186 HTTP/1.1 200 OK
```

```
> Frame 88: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-1533343
> Ethernet II, Src: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74), Dst: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35)
> Internet Protocol Version 4, Src: 213.57.2.5, Dst: 192.168.1.10
v User Datagram Protocol, Src Port: 53, Dst Port: 50398
    Source Port: 53
    Destination Port: 50398
    Length: 450
    Checksum: 0x91fe [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
  > [Timestamps]
    UDP payload (442 bytes)
> Domain Name System (response)
```

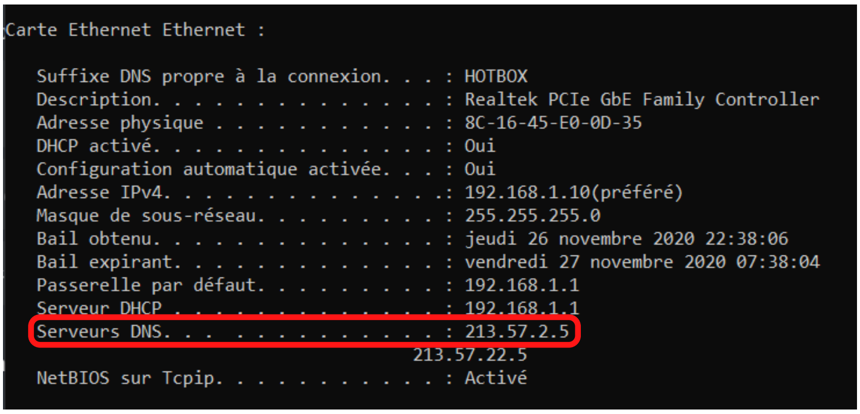
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.1.10
```

```
No.          Time     Source          Destination     Protocol   Length Info
         13 5.943282 192.168.1.10    213.57.2.5      DNS          76 Standard query 0x459f A www.m
         14 0.642949 213.57.2.5      192.168.1.10    DNS         490 Standard query response 0x459
         49 0.678339 192.168.1.10    213.57.2.5      DNS          83 Standard query 0x0001 PTR 5.2
         50 0.013180 213.57.2.5      192.168.1.10    DNS         236 Standard query response 0x000
         51 0.001653 192.168.1.10    213.57.2.5      DNS          78 Standard query 0x0002 A www.m
         71 0.046169 192.168.1.10    213.57.2.5      DNS          78 Standard query 0x0003 AAAA ww
         87 0.439321 192.168.1.10    213.57.2.5      DNS          71 Standard query 0x0004 A www.m
         88 0.180934 213.57.2.5      192.168.1.10    DNS         484 Standard query response 0x000
         89 0.002720 192.168.1.10    213.57.2.5      DNS          71 Standard query 0x0005 AAAA ww
         90 0.142064 213.57.2.5      192.168.1.10    DNS         524 Standard query response 0x000
         18 0.000169 192.168.1.10    213.57.24.194   HTTP        178 GET /ncsi.txt HTTP/1.1
         20 0.000343 213.57.24.194   192.168.1.10    HTTP        233 HTTP/1.1 200 OK  (text/plain)
        136 0.000000 192.168.1.1     192.168.1.10    HTTP        311 GET /upnphost/udhisapi.dll?co
        147 0.000000 192.168.1.1     192.168.1.10    HTTP        311 GET /upnphost/udhisapi.dll?co
        138 0.000030 192.168.1.10    192.168.1.1     HTTP/XML   1186 HTTP/1.1 200 OK
```

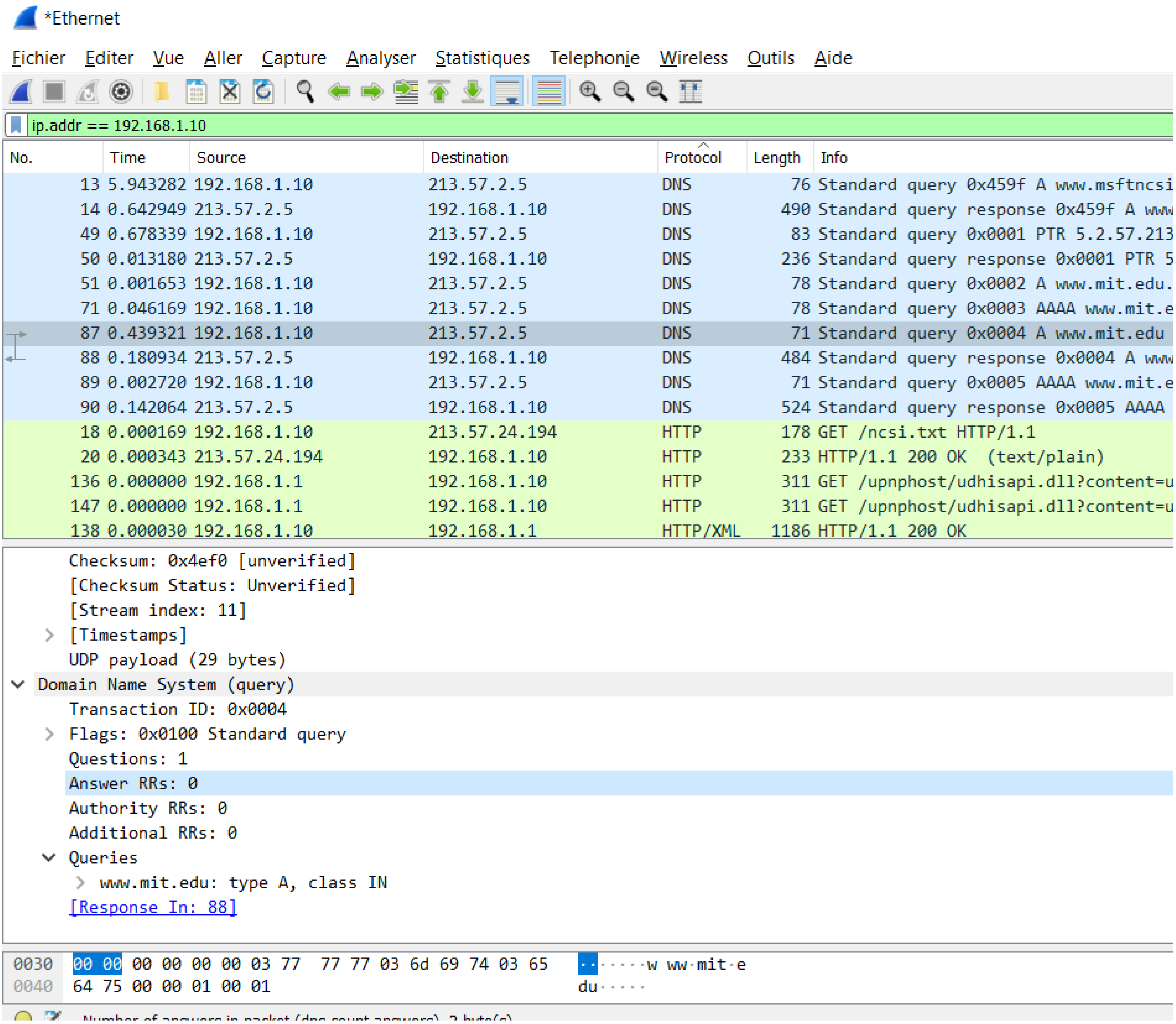
```
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
v Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 57
     Identification: 0x8928 (35112)
   > Flags: 0x00
     Fragment Offset: 0
     Time to Live: 128
     Protocol: UDP (17)
     Header Checksum: 0x189b [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.10
     Destination Address: 213.57.2.5
> User Datagram Protocol, Src Port: 50398, Dst Port: 53

0020  02 05 c4 de 00 35 00 25  4e f0 00 04 01 00 00 01   ·····5·% N·······
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
```



```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : HOTBOX
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : 8C-16-45-E0-0D-35
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.10(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : jeudi 26 novembre 2020 22:38:06
   Bail expirant. . . . . . . . . . . . . : vendredi 27 novembre 2020 07:38:04
   Passerelle par défaut. . . . . . . . . : 192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
   Serveurs DNS. . .  . . . . . . . . . . : 213.57.2.5
                                       213.57.22.5
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

<u>Answer:</u> to 213.57.2.5, and yes it's my IP adress for 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”?



ip.addr == 192.168.1.10

No.	Time	Source	Destination	Protocol	Length	Info
13	5.943282	192.168.1.10	213.57.2.5	DNS	76	Standard query 0x459f A www.msftncsi
14	0.642949	213.57.2.5	192.168.1.10	DNS	490	Standard query response 0x459f A www
49	0.678339	192.168.1.10	213.57.2.5	DNS	83	Standard query 0x0001 PTR 5.2.57.213
50	0.013180	213.57.2.5	192.168.1.10	DNS	236	Standard query response 0x0001 PTR 5
51	0.001653	192.168.1.10	213.57.2.5	DNS	78	Standard query 0x0002 A www.mit.edu.
71	0.046169	192.168.1.10	213.57.2.5	DNS	78	Standard query 0x0003 AAAA www.mit.e
87	0.439321	192.168.1.10	213.57.2.5	DNS	71	Standard query 0x0004 A www.mit.edu
88	0.180934	213.57.2.5	192.168.1.10	DNS	484	Standard query response 0x0004 A www
89	0.002720	192.168.1.10	213.57.2.5	DNS	71	Standard query 0x0005 AAAA www.mit.e
90	0.142064	213.57.2.5	192.168.1.10	DNS	524	Standard query response 0x0005 AAAA
18	0.000169	192.168.1.10	213.57.24.194	HTTP	178	GET /ncsi.txt HTTP/1.1
20	0.000343	213.57.24.194	192.168.1.10	HTTP	233	HTTP/1.1 200 OK (text/plain)
136	0.000000	192.168.1.1	192.168.1.10	HTTP	311	GET /upnphost/udhisapi.dll?content=u
147	0.000000	192.168.1.1	192.168.1.10	HTTP	311	GET /upnphost/udhisapi.dll?content=u
138	0.000030	192.168.1.10	192.168.1.1	HTTP/XML	1186	HTTP/1.1 200 OK

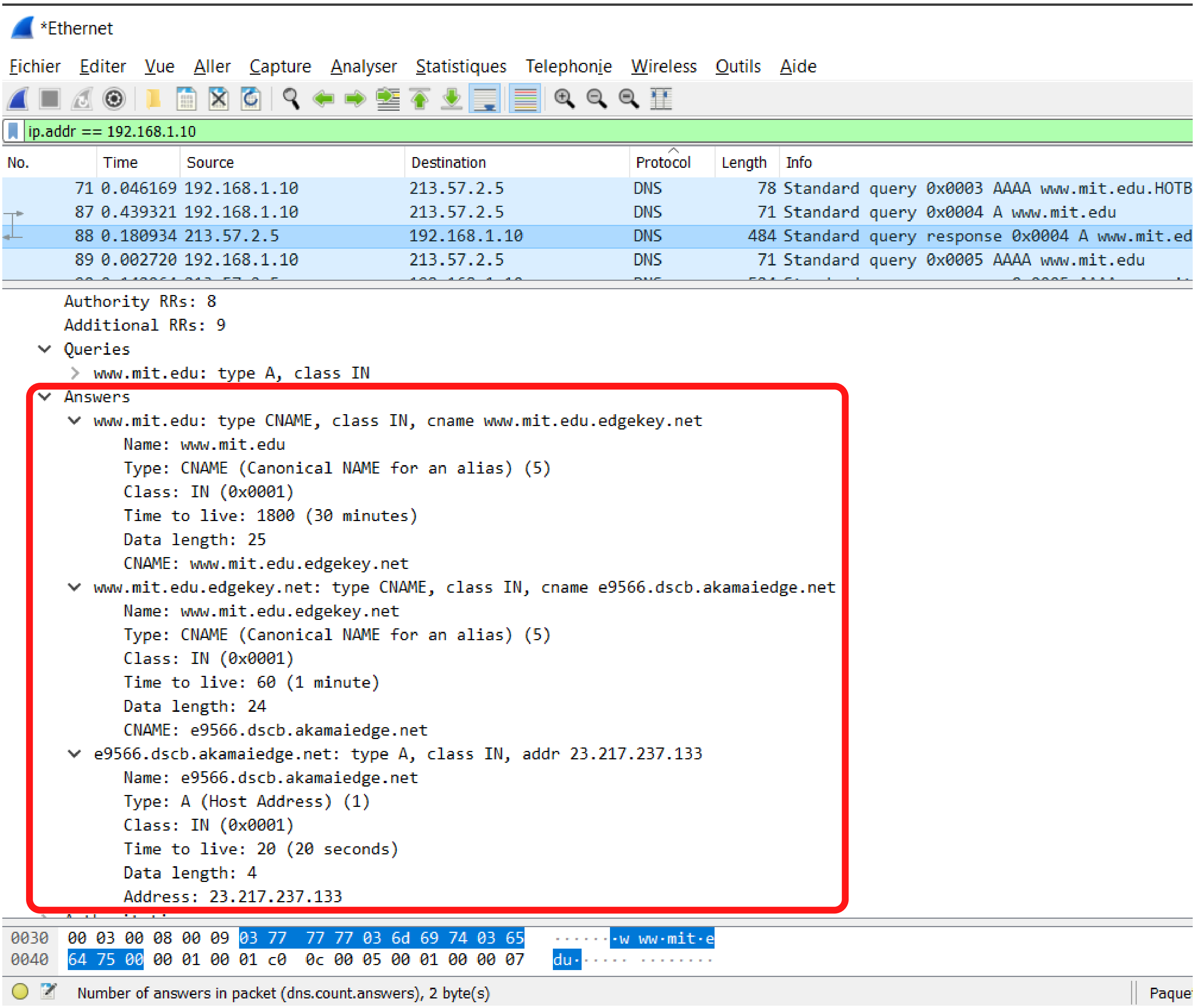
```
    Checksum: 0x4ef0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
  > [Timestamps]
    UDP payload (29 bytes)
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
    [Response In: 88]
```

```
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ······w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

Number of answers in packet (dns.count.answers), 2 byte(s)

<u>Answer:</u> Type A query, and no answer

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



Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ip.addr == 192.168.1.10

```
No.     Time     Source         Destination    Protocol  Length Info
     71 0.046169 192.168.1.10   213.57.2.5     DNS           78 Standard query 0x0003 AAAA www.mit.edu.HOTB
     87 0.439321 192.168.1.10   213.57.2.5     DNS           71 Standard query 0x0004 A www.mit.edu
     88 0.180934 213.57.2.5     192.168.1.10   DNS          484 Standard query response 0x0004 A www.mit.ed
     89 0.002720 192.168.1.10   213.57.2.5     DNS           71 Standard query 0x0005 AAAA www.mit.edu
```

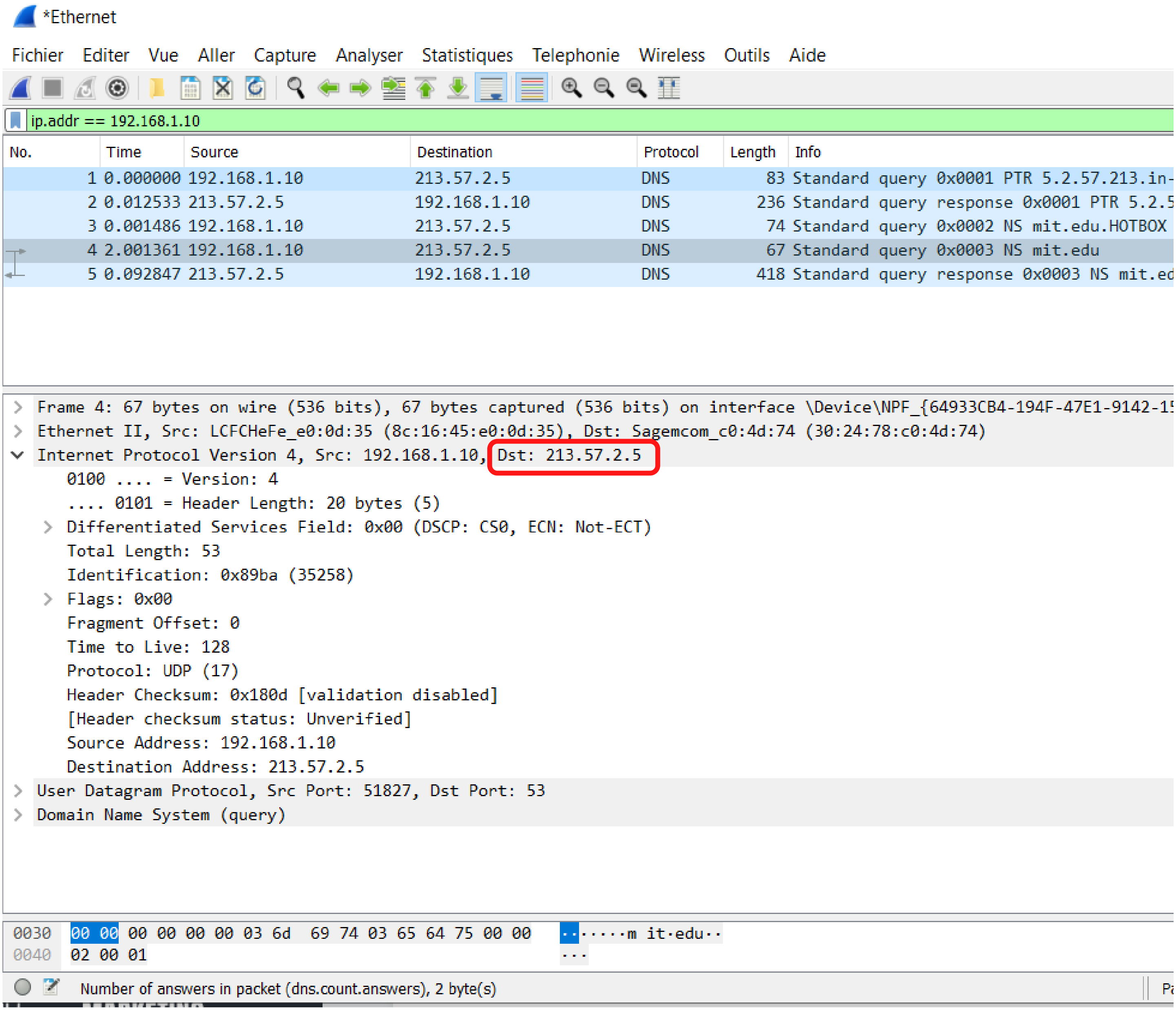
```
    Authority RRs: 8
    Additional RRs: 9
  ∨ Queries
    > www.mit.edu: type A, class IN
  ∨ Answers
    ∨ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    ∨ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    ∨ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.217.237.133
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 23.217.237.133
```

```
0030  00 03 00 08 00 09 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 07   du······ ········
```

Number of answers in packet (dns.count.answers), 2 byte(s)

<u>Answer:</u> 3 answers provided. Each of them contains a name, a type, a class, a time to live, a data length and an adress

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

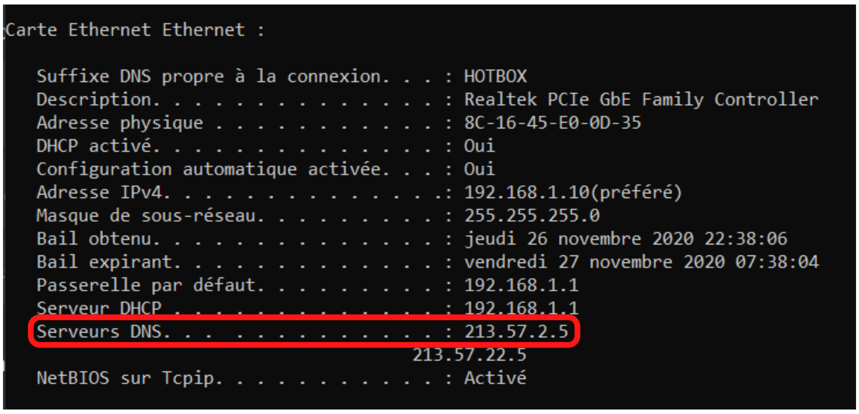

*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
ip.addr == 192.168.1.10

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.10	213.57.2.5	DNS	83	Standard query 0x0001 PTR 5.2.57.213.in-
2	0.012533	213.57.2.5	192.168.1.10	DNS	236	Standard query response 0x0001 PTR 5.2.5
3	0.001486	192.168.1.10	213.57.2.5	DNS	74	Standard query 0x0002 NS mit.edu.HOTBOX
4	2.001361	192.168.1.10	213.57.2.5	DNS	67	Standard query 0x0003 NS mit.edu
5	0.092847	213.57.2.5	192.168.1.10	DNS	418	Standard query response 0x0003 NS mit.ed

```
> Frame 4: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-15
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
v Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 53
     Identification: 0x89ba (35258)
   > Flags: 0x00
     Fragment Offset: 0
     Time to Live: 128
     Protocol: UDP (17)
     Header Checksum: 0x180d [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.10
     Destination Address: 213.57.2.5
> User Datagram Protocol, Src Port: 51827, Dst Port: 53
> Domain Name System (query)
```

```
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ······m it·edu··
0040  02 00 01                                           ···
```

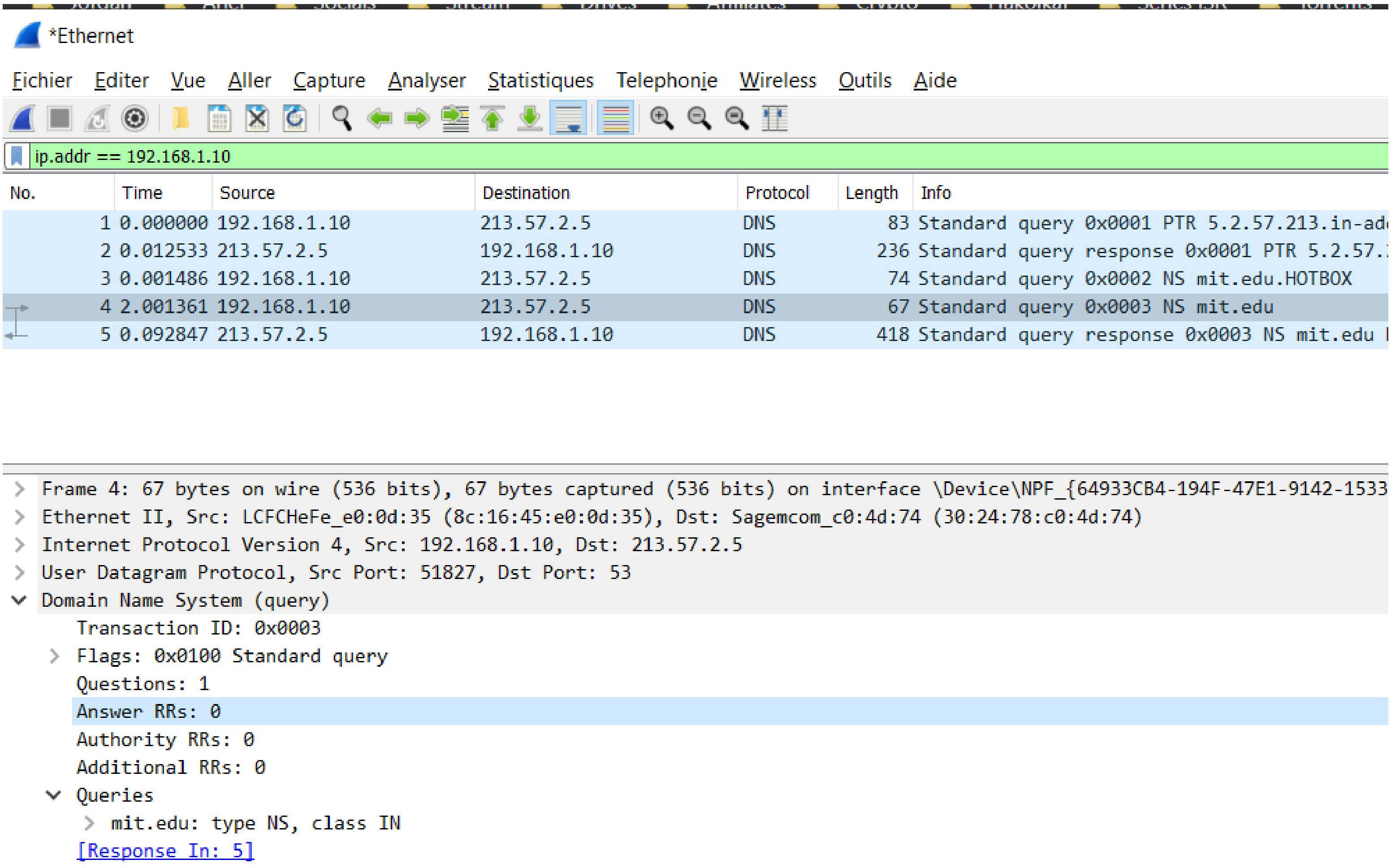
Number of answers in packet (dns.count.answers), 2 byte(s)



```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : HOTBOX
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : 8C-16-45-E0-0D-35
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.10(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : jeudi 26 novembre 2020 22:38:06
   Bail expirant. . . . . . . . . . . . . : vendredi 27 novembre 2020 07:38:04
   Passerelle par défaut. . . . . . . . . : 192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
   Serveurs DNS. . .  . . . . . . . . . . : 213.57.2.5
                                       213.57.22.5
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

<u>Answer:</u> to 213.57.2.5, and yes it's my IP adress for 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”?


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

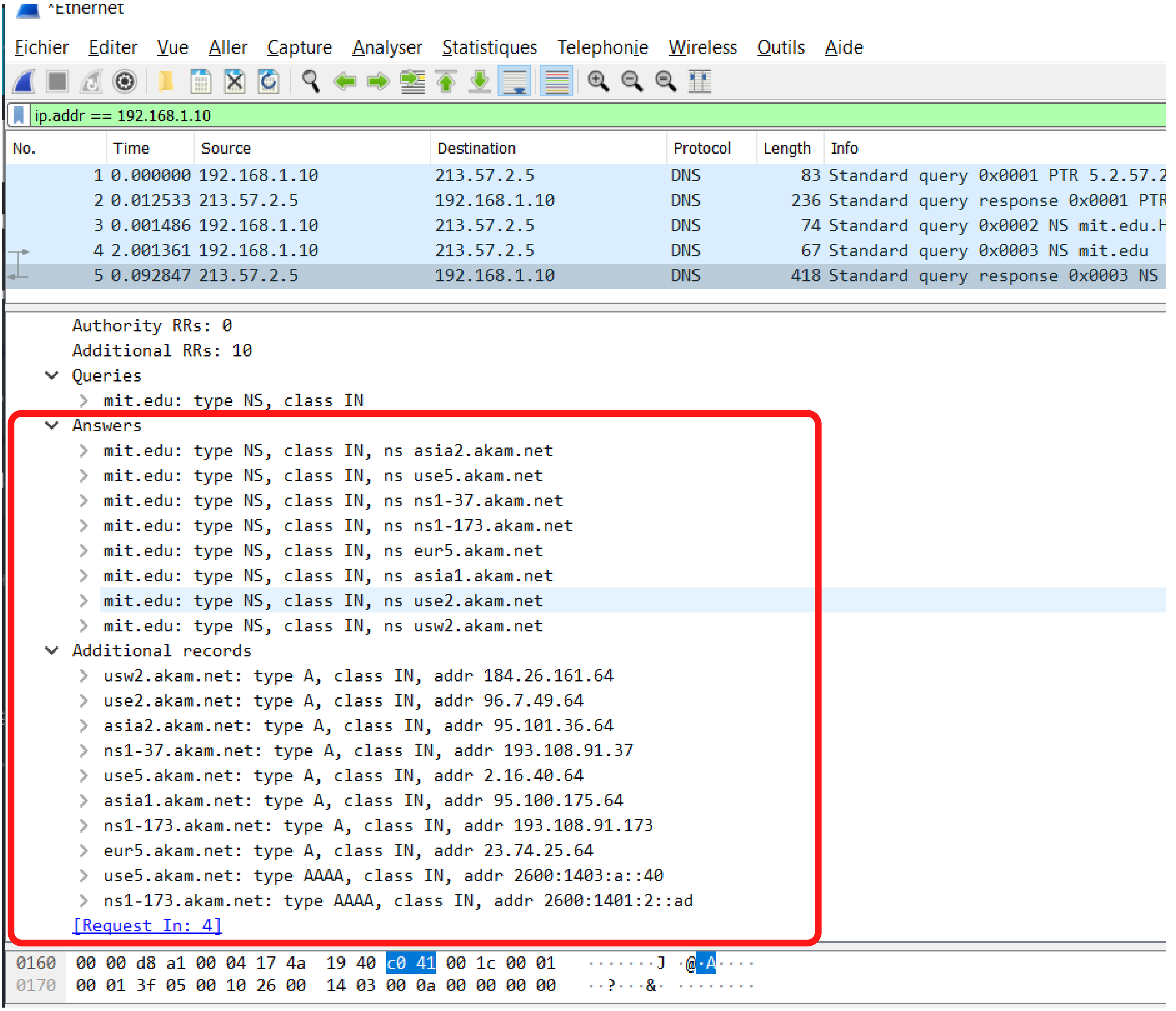
```
ip.addr == 192.168.1.10
```

```
No.   Time     Source        Destination   Protocol Length Info
    1 0.000000 192.168.1.10  213.57.2.5    DNS        83 Standard query 0x0001 PTR 5.2.57.213.in-ad
    2 0.012533 213.57.2.5    192.168.1.10  DNS       236 Standard query response 0x0001 PTR 5.2.57.
    3 0.001486 192.168.1.10  213.57.2.5    DNS        74 Standard query 0x0002 NS mit.edu.HOTBOX
    4 2.001361 192.168.1.10  213.57.2.5    DNS        67 Standard query 0x0003 NS mit.edu
    5 0.092847 213.57.2.5    192.168.1.10  DNS       418 Standard query response 0x0003 NS mit.edu
```

```
> Frame 4: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{64933CB4-194F-47E1-9142-1533
> Ethernet II, Src: LCFCHeFe_e0:0d:35 (8c:16:45:e0:0d:35), Dst: Sagemcom_c0:4d:74 (30:24:78:c0:4d:74)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 213.57.2.5
> User Datagram Protocol, Src Port: 51827, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > 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: 5]
```

Answer: Type NS query, and no 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 namesers?



```
ip.addr == 192.168.1.10
```

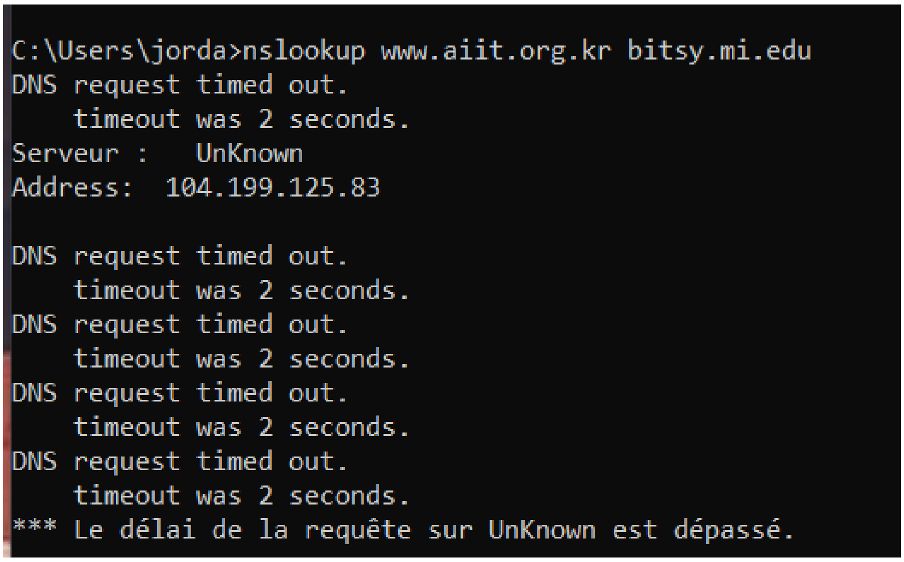
```
No.      Time     Source         Destination    Protocol  Length Info
       1 0.000000 192.168.1.10   213.57.2.5     DNS           83 Standard query 0x0001 PTR 5.2.57.2
       2 0.012533 213.57.2.5     192.168.1.10   DNS          236 Standard query response 0x0001 PTR
       3 0.001486 192.168.1.10   213.57.2.5     DNS           74 Standard query 0x0002 NS mit.edu.H
       4 2.001361 192.168.1.10   213.57.2.5     DNS           67 Standard query 0x0003 NS mit.edu
       5 0.092847 213.57.2.5     192.168.1.10   DNS          418 Standard query response 0x0003 NS
```

```
    Authority RRs: 0
    Additional RRs: 10
  ⌄ Queries
    > mit.edu: type NS, class IN
  ⌄ Answers
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
  ⌄ Additional records
    > usw2.akam.net: type A, class IN, addr 184.26.161.64
    > use2.akam.net: type A, class IN, addr 96.7.49.64
    > 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
    > asia1.akam.net: type A, class IN, addr 95.100.175.64
    > 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
    > use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    > ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    [Request In: 4]
```

```
0160  00 00 d8 a1 00 04 17 4a  19 40 c0 41 00 1c 00 01   .......J .@.A....
0170  00 01 3f 05 00 10 26 00  14 03 00 0a 00 00 00 00   ..?...&. ........
```

<u>Answer:</u> 8 nameservers, IP's included in the Additional records part

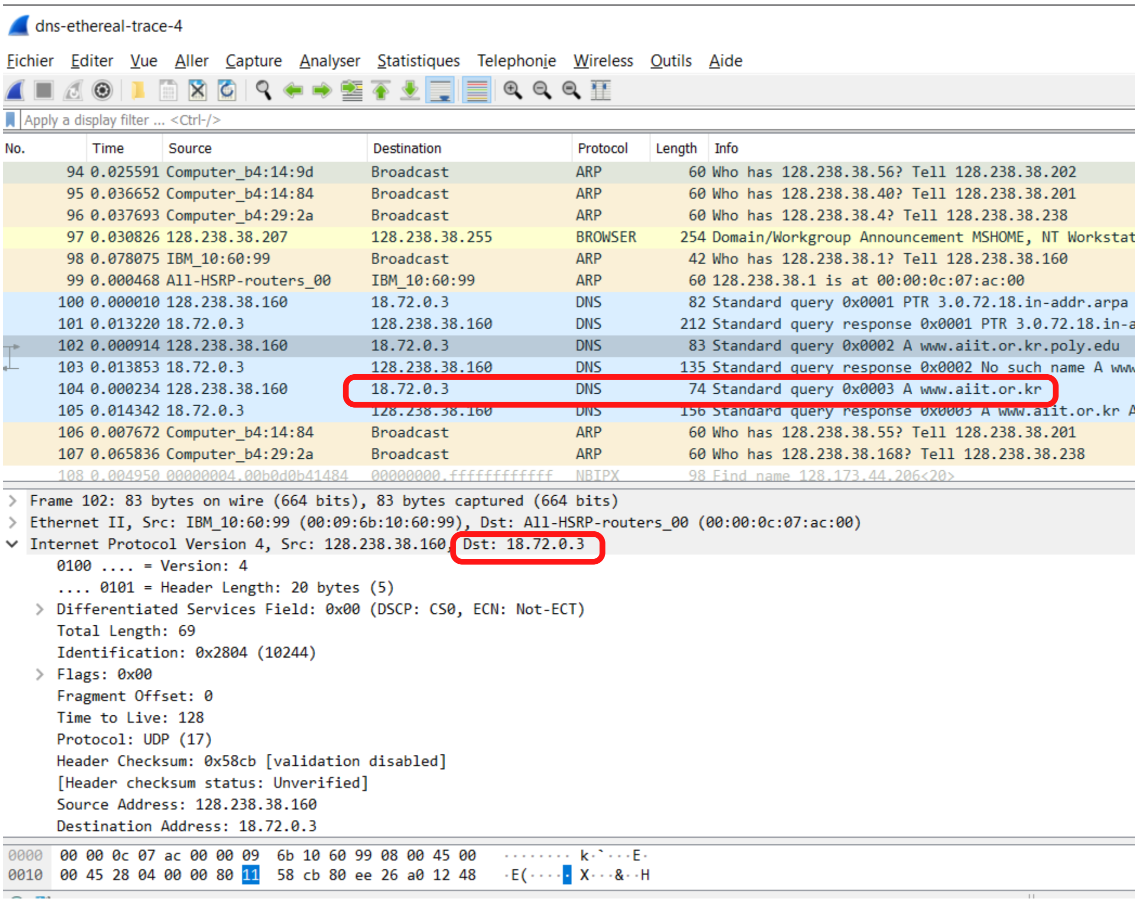
For the last questions I didn't succeed in running the command:



```
C:\Users\jorda>nslookup www.aiit.org.kr bitsy.mi.edu
DNS request timed out.
    timeout was 2 seconds.
Serveur :   UnKnown
Address:  104.199.125.83

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.
*** Le délai de la requête sur UnKnown est dépassé.
```

So I used the script file given at the end of the PDF

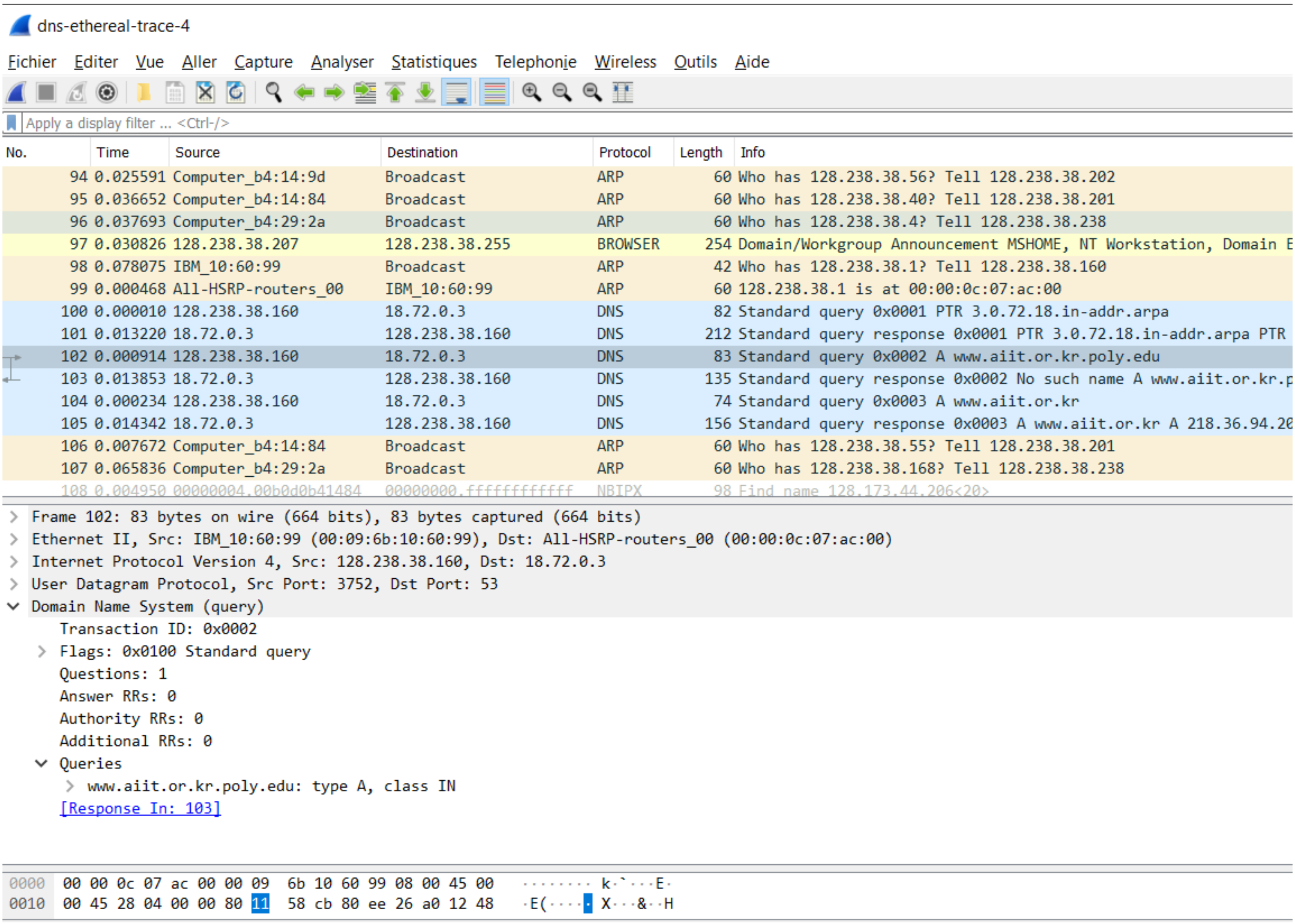
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?



```
No.    Time     Source                 Destination          Protocol Length Info
    94 0.025591 Computer_b4:14:9d      Broadcast            ARP         60 Who has 128.238.38.56? Tell 128.238.38.202
    95 0.036652 Computer_b4:14:84      Broadcast            ARP         60 Who has 128.238.38.40? Tell 128.238.38.201
    96 0.037693 Computer_b4:29:2a      Broadcast            ARP         60 Who has 128.238.38.4? Tell 128.238.38.238
    97 0.030826 128.238.38.207         128.238.38.255       BROWSER    254 Domain/Workgroup Announcement MSHOME, NT Workstat
    98 0.078075 IBM_10:60:99           Broadcast            ARP         42 Who has 128.238.38.1? Tell 128.238.38.160
    99 0.000468 All-HSRP-routers_00    IBM_10:60:99         ARP         60 128.238.38.1 is at 00:00:0c:07:ac:00
   100 0.000010 128.238.38.160         18.72.0.3            DNS         82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
   101 0.013220 18.72.0.3              128.238.38.160       DNS        212 Standard query response 0x0001 PTR 3.0.72.18.in-a
   102 0.000914 128.238.38.160         18.72.0.3            DNS         83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
   103 0.013853 18.72.0.3              128.238.38.160       DNS        135 Standard query response 0x0002 No such name A www
   104 0.000234 128.238.38.160         18.72.0.3            DNS         74 Standard query 0x0003 A www.aiit.or.kr
   105 0.014342 18.72.0.3              128.238.38.160       DNS        156 Standard query response 0x0003 A www.aiit.or.kr A
   106 0.007672 Computer_b4:14:84      Broadcast            ARP         60 Who has 128.238.38.55? Tell 128.238.38.201
   107 0.065836 Computer_b4:29:2a      Broadcast            ARP         60 Who has 128.238.38.168? Tell 128.238.38.238
   108 0.004950 00000004.00b0d0b41484  00000000.ffffffffffff NBIPX       98 Find name 128.173.44.206<20>

> Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
v Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 69
    Identification: 0x2804 (10244)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x58cb [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.238.38.160
    Destination Address: 18.72.0.3

0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········k·`···E·
0010  00 45 28 04 00 00 80 11  58 cb 80 ee 26 a0 12 48   ·E(·····X···&··H
```

<u>Answer:</u> This DNS query message is sent to 18.72.0.3 which is the IP address of the aiit response sender.

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


dns-ethereal-trace-4
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Apply a display filter ... <Ctrl-/>

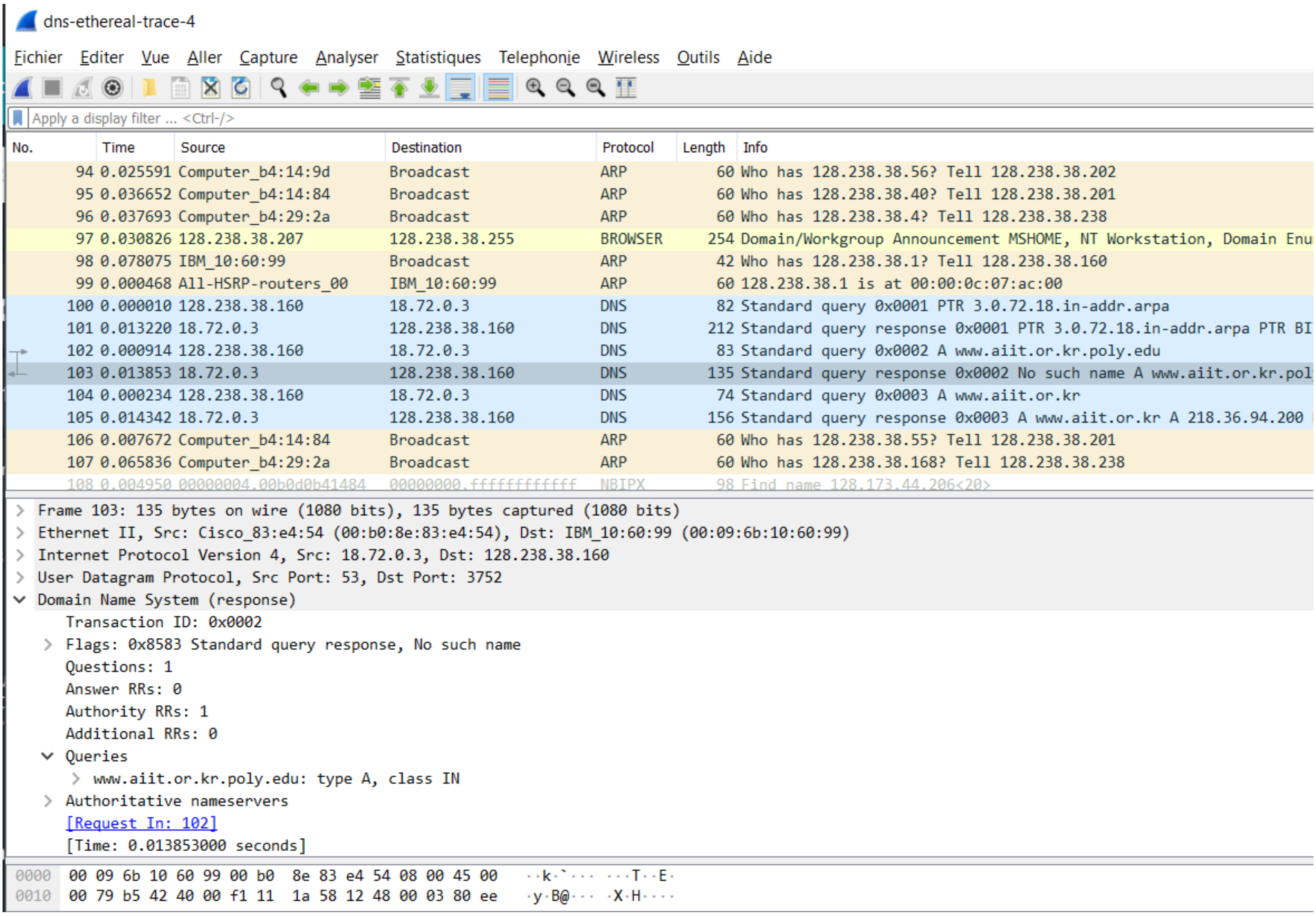
```
No.    Time     Source                Destination        Protocol  Length Info
    94 0.025591 Computer_b4:14:9d     Broadcast          ARP        60 Who has 128.238.38.56? Tell 128.238.38.202
    95 0.036652 Computer_b4:14:84     Broadcast          ARP        60 Who has 128.238.38.40? Tell 128.238.38.201
    96 0.037693 Computer_b4:29:2a     Broadcast          ARP        60 Who has 128.238.38.4? Tell 128.238.38.238
    97 0.030826 128.238.38.207        128.238.38.255     BROWSER   254 Domain/Workgroup Announcement MSHOME, NT Workstation, Domain E
    98 0.078075 IBM_10:60:99          Broadcast          ARP        42 Who has 128.238.38.1? Tell 128.238.38.160
    99 0.000468 All-HSRP-routers_00   IBM_10:60:99       ARP        60 128.238.38.1 is at 00:00:0c:07:ac:00
   100 0.000010 128.238.38.160        18.72.0.3          DNS        82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
   101 0.013220 18.72.0.3             128.238.38.160     DNS       212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR
   102 0.000914 128.238.38.160        18.72.0.3          DNS        83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
   103 0.013853 18.72.0.3             128.238.38.160     DNS       135 Standard query response 0x0002 No such name A www.aiit.or.kr.p
   104 0.000234 128.238.38.160        18.72.0.3          DNS        74 Standard query 0x0003 A www.aiit.or.kr
   105 0.014342 18.72.0.3             128.238.38.160     DNS       156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.20
   106 0.007672 Computer_b4:14:84     Broadcast          ARP        60 Who has 128.238.38.55? Tell 128.238.38.201
   107 0.065836 Computer_b4:29:2a     Broadcast          ARP        60 Who has 128.238.38.168? Tell 128.238.38.238
   108 0.004950 00000004.00b0d0b41484 00000000.ffffffffffff NBIPX   98 Find name 128.173.44.206<20>
```

```
> Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3752, 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.aiit.or.kr.poly.edu: type A, class IN
    [Response In: 103]
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ........ k·`···E·
0010  00 45 28 04 00 00 80 11  58 cb 80 ee 26 a0 12 48   ·E(····· X···&··H
```

Answer: Type A query, and no answer

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



dns-ethereal-trace-4
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Apply a display filter ... <Ctrl-/>

```
No.     Time     Source                 Destination      Protocol  Length Info
     94 0.025591 Computer_b4:14:9d      Broadcast        ARP           60 Who has 128.238.38.56? Tell 128.238.38.202
     95 0.036652 Computer_b4:14:84      Broadcast        ARP           60 Who has 128.238.38.40? Tell 128.238.38.201
     96 0.037693 Computer_b4:29:2a      Broadcast        ARP           60 Who has 128.238.38.4? Tell 128.238.38.238
     97 0.030826 128.238.38.207         128.238.38.255   BROWSER      254 Domain/Workgroup Announcement MSHOME, NT Workstation, Domain Enu
     98 0.078075 IBM_10:60:99           Broadcast        ARP           42 Who has 128.238.38.1? Tell 128.238.38.160
     99 0.000468 All-HSRP-routers_00    IBM_10:60:99     ARP           60 128.238.38.1 is at 00:00:0c:07:ac:00
    100 0.000010 128.238.38.160         18.72.0.3        DNS           82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
    101 0.013220 18.72.0.3              128.238.38.160   DNS          212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BI
    102 0.000914 128.238.38.160         18.72.0.3        DNS           83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
    103 0.013853 18.72.0.3              128.238.38.160   DNS          135 Standard query response 0x0002 No such name A www.aiit.or.kr.pol
    104 0.000234 128.238.38.160         18.72.0.3        DNS           74 Standard query 0x0003 A www.aiit.or.kr
    105 0.014342 18.72.0.3              128.238.38.160   DNS          156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200
    106 0.007672 Computer_b4:14:84      Broadcast        ARP           60 Who has 128.238.38.55? Tell 128.238.38.201
    107 0.065836 Computer_b4:29:2a      Broadcast        ARP           60 Who has 128.238.38.168? Tell 128.238.38.238
    108 0.004950 00000004.00b0d0b41484  00000000.ffffffffffff NBIPX    98 Find name 128.173.44.206<20>
```

```
> Frame 103: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3752
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8583 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    > www.aiit.or.kr.poly.edu: type A, class IN
  > Authoritative nameservers
    [Request In: 102]
    [Time: 0.013853000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 79 b5 42 40 00 f1 11  1a 58 12 48 00 03 80 ee   ·y·B@··· ·X·H····
```

<u>Answer:</u> Type A query, and no answer