Gökhan Özeloğlu - 21627557
Burak Yılmaz - 21627868

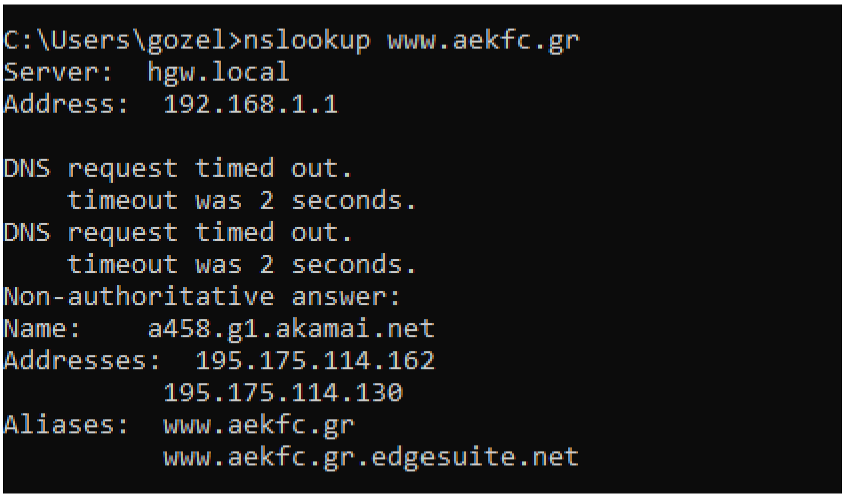
BBM 453 Computer Networks Lab - DNS Lab Assignment

Group ID: 1

Source IP: 192.168.1.1

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

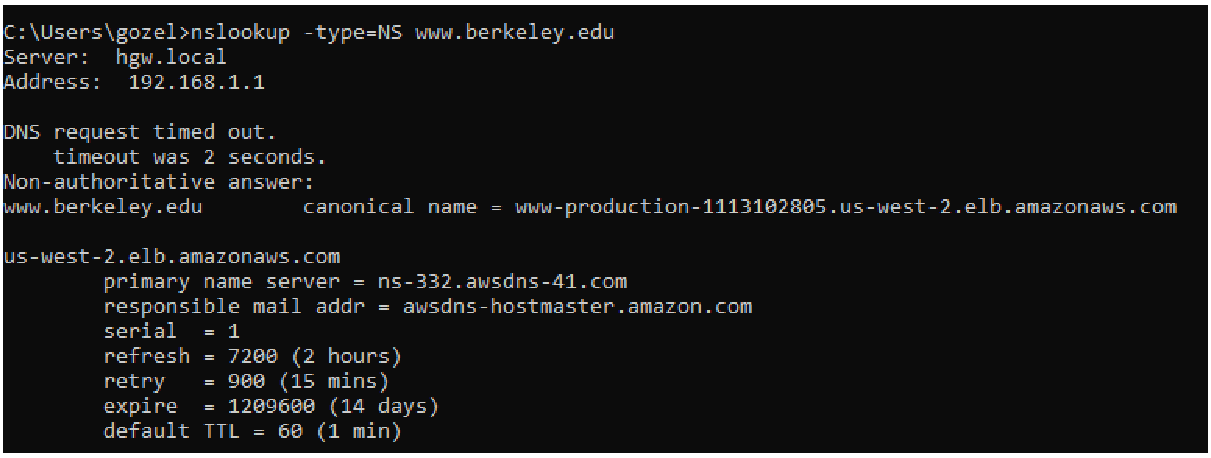
   Ans: We obtained the IP addresses as in the screenshot. The IP addresses are: *195.175.114.130 - 195.175.114.162*



```
C:\Users\gozel>nslookup www.aekfc.gr
Server:  hgw.local
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    a458.g1.akamai.net
Addresses:  195.175.114.162
          195.175.114.130
Aliases:  www.aekfc.gr
          www.aekfc.gr.edgesuite.net
```

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

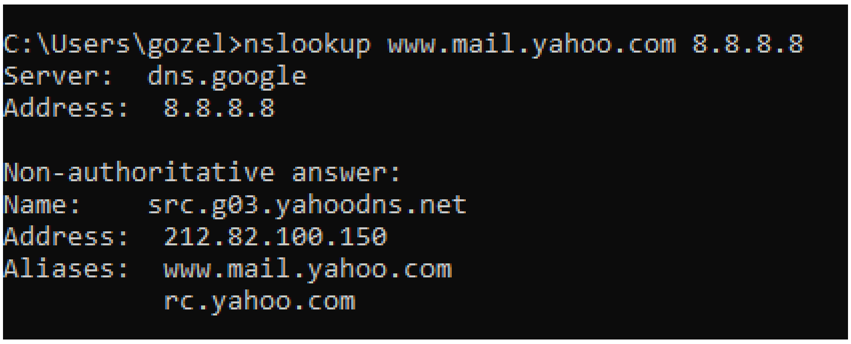
   ANS:



```
C:\Users\gozel>nslookup -type=NS www.berkeley.edu
Server:  hgw.local
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
www.berkeley.edu        canonical name = www-production-1113102805.us-west-2.elb.amazonaws.com

us-west-2.elb.amazonaws.com
        primary name server = ns-332.awsdns-41.com
        responsible mail addr = awsdns-hostmaster.amazon.com
        serial  = 1
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 60 (1 min)
```

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

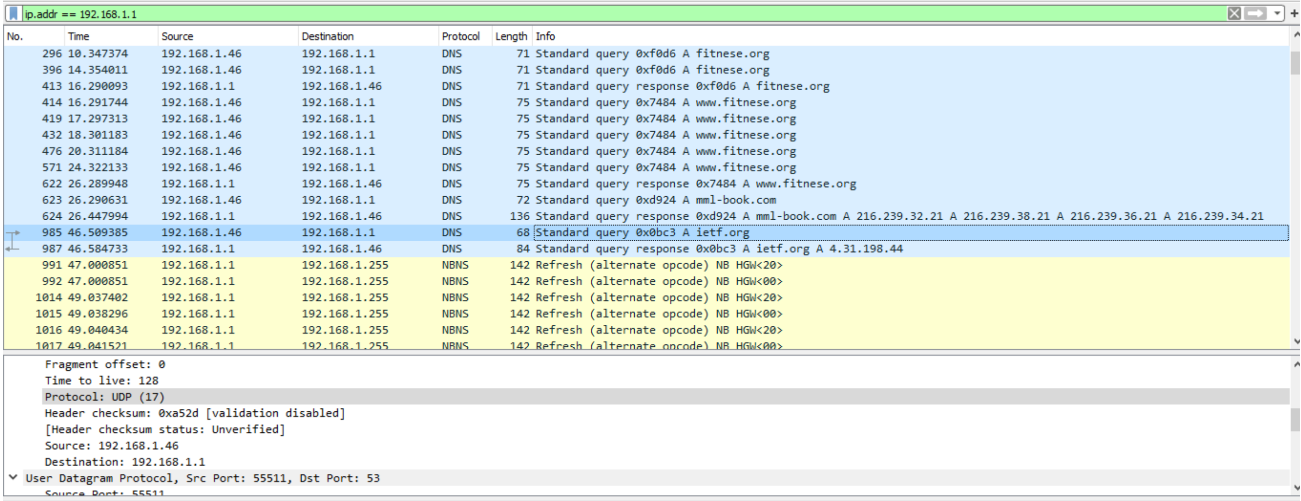
   ANS: IP Address: 212.82.100.150



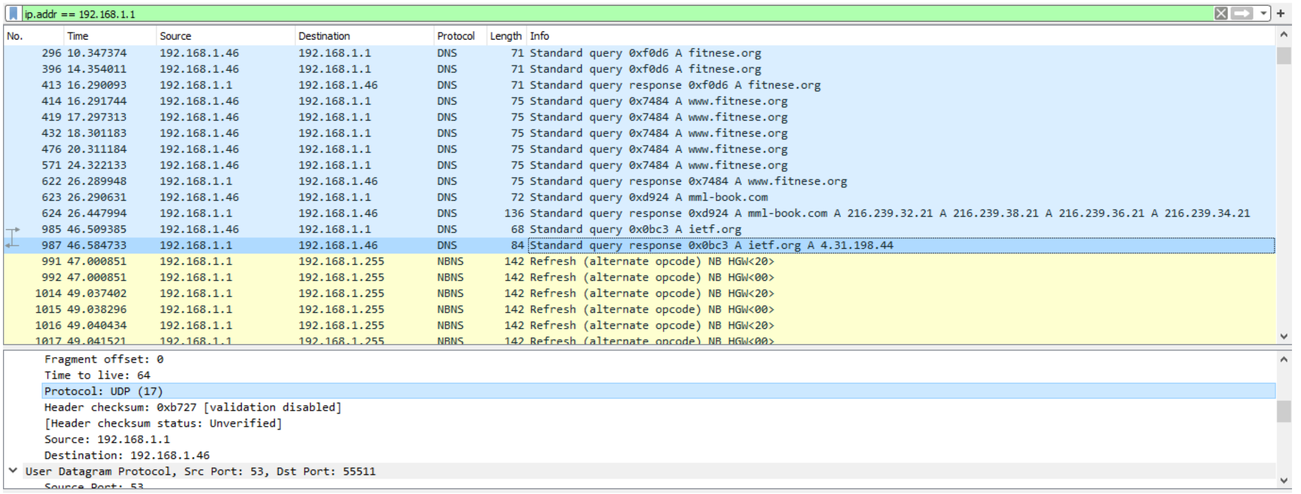
```
C:\Users\gozel>nslookup www.mail.yahoo.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    src.g03.yahoodns.net
Address:  212.82.100.150
Aliases:  www.mail.yahoo.com
          rc.yahoo.com
```

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

   ANS: It is sent over UDP as seen in the screenshot.



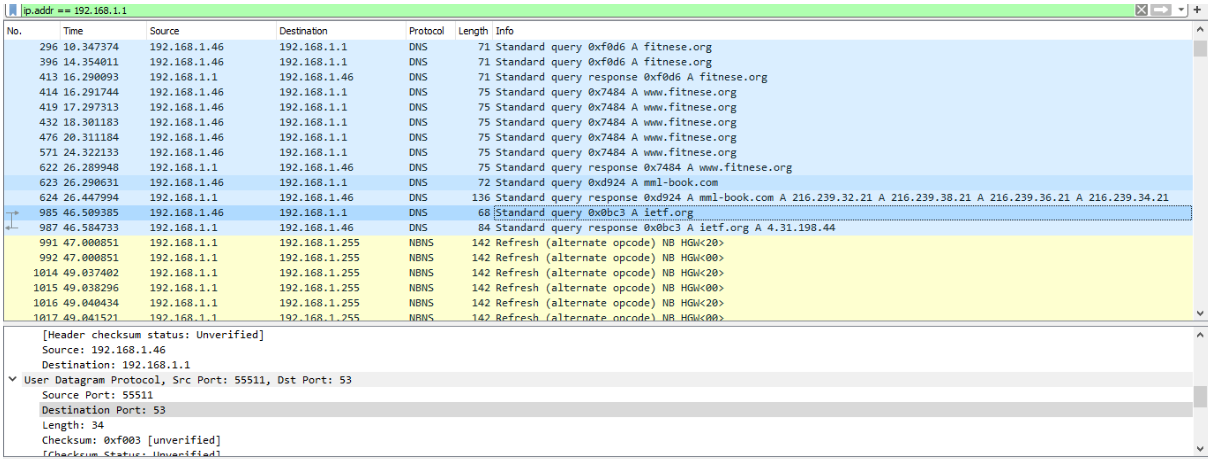
```
ip.addr == 192.168.1.1
No.    Time       Source         Destination    Protocol Length Info
  296 10.347374  192.168.1.46   192.168.1.1    DNS      71 Standard query 0xf0d6 A fitnese.org
  396 14.354011  192.168.1.46   192.168.1.1    DNS      71 Standard query 0xf0d6 A fitnese.org
  413 16.290093  192.168.1.1    192.168.1.46   DNS      71 Standard query response 0xf0d6 A fitnese.org
  414 16.291744  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  419 17.297313  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  432 18.301183  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  476 20.311184  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  571 24.322133  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  622 26.289948  192.168.1.1    192.168.1.46   DNS      75 Standard query response 0x7484 A www.fitnese.org
  623 26.290631  192.168.1.46   192.168.1.1    DNS      72 Standard query 0xd924 A mml-book.com
  624 26.447994  192.168.1.1    192.168.1.46   DNS     136 Standard query response 0xd924 A mml-book.com A 216.239.32.21 A 216.239.38.21 A 216.239.36.21 A 216.239.34.21
  985 46.509385  192.168.1.46   192.168.1.1    DNS      68 Standard query 0x0bc3 A ietf.org
  987 46.584733  192.168.1.1    192.168.1.46   DNS      84 Standard query response 0x0bc3 A ietf.org A 4.31.198.44
  991 47.000851  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<20>
  992 47.000851  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<00>
 1014 49.037402  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<20>
 1015 49.038296  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<00>
 1016 49.040434  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<20>
 1017 49.041521  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<00>

      Fragment offset: 0
      Time to live: 128
      Protocol: UDP (17)
      Header checksum: 0xa52d [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.1.46
      Destination: 192.168.1.1
  User Datagram Protocol, Src Port: 55511, Dst Port: 53
      Source Port: 55511
```



```
ip.addr == 192.168.1.1
No.    Time       Source         Destination    Protocol Length Info
  296 10.347374  192.168.1.46   192.168.1.1    DNS      71 Standard query 0xf0d6 A fitnese.org
  396 14.354011  192.168.1.46   192.168.1.1    DNS      71 Standard query 0xf0d6 A fitnese.org
  413 16.290093  192.168.1.1    192.168.1.46   DNS      71 Standard query response 0xf0d6 A fitnese.org
  414 16.291744  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  419 17.297313  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  432 18.301183  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  476 20.311184  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  571 24.322133  192.168.1.46   192.168.1.1    DNS      75 Standard query 0x7484 A www.fitnese.org
  622 26.289948  192.168.1.1    192.168.1.46   DNS      75 Standard query response 0x7484 A www.fitnese.org
  623 26.290631  192.168.1.46   192.168.1.1    DNS      72 Standard query 0xd924 A mml-book.com
  624 26.447994  192.168.1.1    192.168.1.46   DNS     136 Standard query response 0xd924 A mml-book.com A 216.239.32.21 A 216.239.38.21 A 216.239.36.21 A 216.239.34.21
  985 46.509385  192.168.1.46   192.168.1.1    DNS      68 Standard query 0x0bc3 A ietf.org
  987 46.584733  192.168.1.1    192.168.1.46   DNS      84 Standard query response 0x0bc3 A ietf.org A 4.31.198.44
  991 47.000851  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<20>
  992 47.000851  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<00>
 1014 49.037402  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<20>
 1015 49.038296  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<00>
 1016 49.040434  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<20>
 1017 49.041521  192.168.1.1    192.168.1.255  NBNS    142 Refresh (alternate opcode) NB HGW<00>

      Fragment offset: 0
      Time to live: 64
      Protocol: UDP (17)
      Header checksum: 0xb727 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.1.1
      Destination: 192.168.1.46
  User Datagram Protocol, Src Port: 53, Dst Port: 55511
      Source Port: 53
```

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

ANS: Source port: 55511 Destination port: 53 (Query Message)
Source port:53 Destination port: 55511 (Response Message)



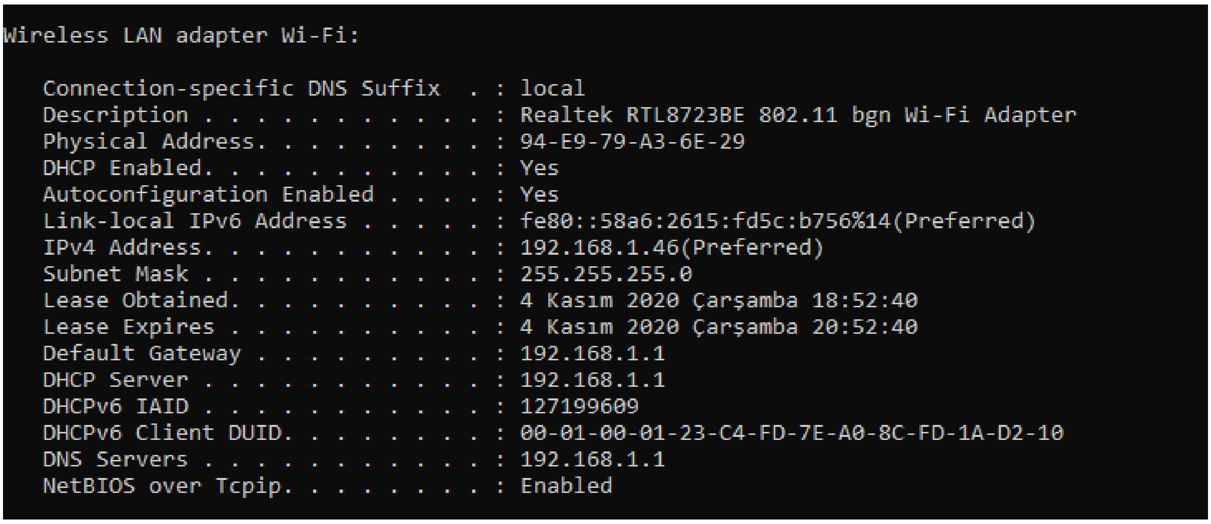
ip.addr == 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
296	10.347374	192.168.1.46	192.168.1.1	DNS	71	Standard query 0xf0d6 A fitnese.org
396	14.354011	192.168.1.46	192.168.1.1	DNS	71	Standard query 0xf0d6 A fitnese.org
413	16.290093	192.168.1.1	192.168.1.46	DNS	71	Standard query response 0xf0d6 A fitnese.org
414	16.291744	192.168.1.46	192.168.1.1	DNS	75	Standard query 0x7484 A www.fitnese.org
419	17.297313	192.168.1.46	192.168.1.1	DNS	75	Standard query 0x7484 A www.fitnese.org
432	18.301183	192.168.1.46	192.168.1.1	DNS	75	Standard query 0x7484 A www.fitnese.org
476	20.311184	192.168.1.46	192.168.1.1	DNS	75	Standard query 0x7484 A www.fitnese.org
571	24.322133	192.168.1.46	192.168.1.1	DNS	75	Standard query 0x7484 A www.fitnese.org
622	26.289948	192.168.1.1	192.168.1.46	DNS	75	Standard query response 0x7484 A www.fitnese.org
623	26.290631	192.168.1.46	192.168.1.1	DNS	72	Standard query 0xd924 A mml-book.com
624	26.447994	192.168.1.1	192.168.1.46	DNS	136	Standard query response 0xd924 A mml-book.com A 216.239.32.21 A 216.239.38.21 A 216.239.36.21 A 216.239.34.21
985	46.509385	192.168.1.46	192.168.1.1	DNS	68	Standard query 0x0bc3 A ietf.org
987	46.584733	192.168.1.1	192.168.1.46	DNS	84	Standard query response 0x0bc3 A ietf.org A 4.31.198.44
991	47.000851	192.168.1.1	192.168.1.255	NBNS	142	Refresh (alternate opcode) NB HGW<20>
992	47.000851	192.168.1.1	192.168.1.255	NBNS	142	Refresh (alternate opcode) NB HGW<00>
1014	49.037402	192.168.1.1	192.168.1.255	NBNS	142	Refresh (alternate opcode) NB HGW<20>
1015	49.038296	192.168.1.1	192.168.1.255	NBNS	142	Refresh (alternate opcode) NB HGW<00>
1016	49.040434	192.168.1.1	192.168.1.255	NBNS	142	Refresh (alternate opcode) NB HGW<20>
1017	49.041521	192.168.1.1	192.168.1.255	NBNS	142	Refresh (alternate opcode) NB HGW<00>

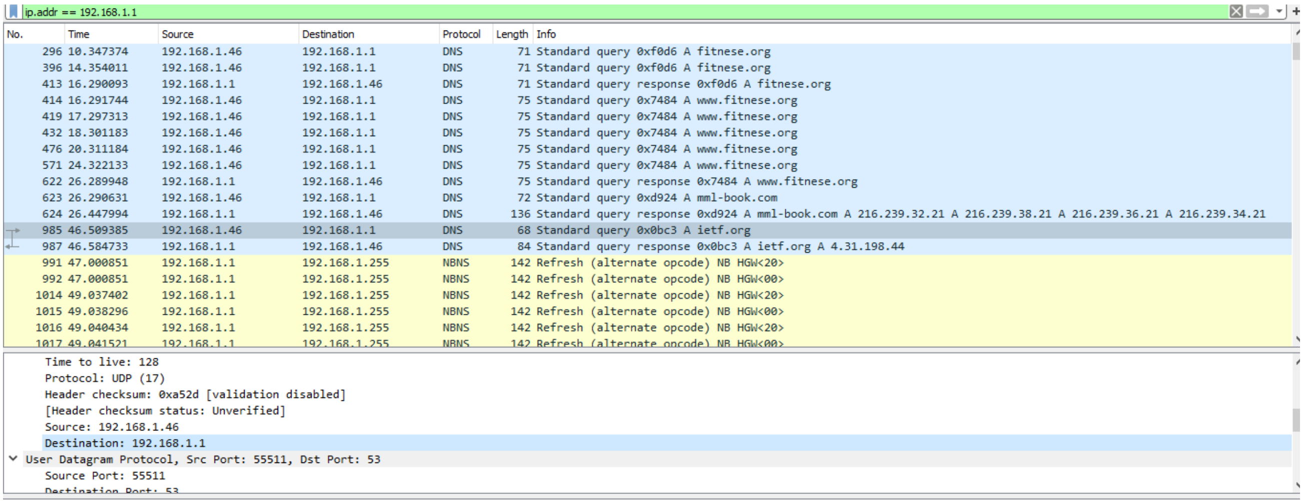
```
    [Header checksum status: Unverified]
    Source: 192.168.1.46
    Destination: 192.168.1.1
User Datagram Protocol, Src Port: 55511, Dst Port: 53
    Source Port: 55511
    Destination Port: 53
    Length: 34
    Checksum: 0xf003 [unverified]
    [Checksum Status: Unverified]
```

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?

   ANS: Yes, they are the same. As we can see in the second screenshot, the destination IP address is the same as ipconfig result.



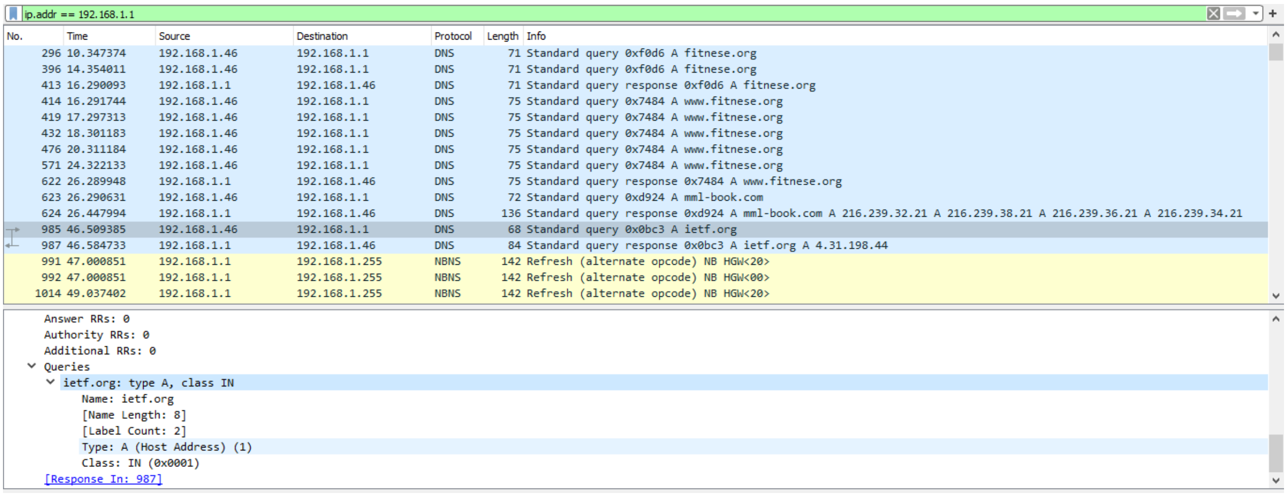
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : local
   Description . . . . . . . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 94-E9-79-A3-6E-29
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::58a6:2615:fd5c:b756%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.46(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 4 Kasım 2020 Çarşamba 18:52:40
   Lease Expires . . . . . . . . . . : 4 Kasım 2020 Çarşamba 20:52:40
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 127199609
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-C4-FD-7E-A0-8C-FD-1A-D2-10
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```



```
ip.addr == 192.168.1.1

No.   Time        Source          Destination     Protocol Length Info
  296 10.347374   192.168.1.46    192.168.1.1     DNS        71 Standard query 0xf0d6 A fitnese.org
  396 14.354011   192.168.1.46    192.168.1.1     DNS        71 Standard query 0xf0d6 A fitnese.org
  413 16.290093   192.168.1.1     192.168.1.46    DNS        71 Standard query response 0xf0d6 A fitnese.org
  414 16.291744   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  419 17.297313   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  432 18.301183   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  476 20.311184   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  571 24.322133   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  622 26.289948   192.168.1.1     192.168.1.46    DNS        75 Standard query response 0x7484 A www.fitnese.org
  623 26.290631   192.168.1.46    192.168.1.1     DNS        72 Standard query 0xd924 A mml-book.com
  624 26.447994   192.168.1.1     192.168.1.46    DNS       136 Standard query response 0xd924 A mml-book.com A 216.239.32.21 A 216.239.38.21 A 216.239.36.21 A 216.239.34.21
  985 46.509385   192.168.1.46    192.168.1.1     DNS        68 Standard query 0x0bc3 A ietf.org
  987 46.584733   192.168.1.1     192.168.1.46    DNS        84 Standard query response 0x0bc3 A ietf.org A 4.31.198.44
  991 47.000851   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<20>
  992 47.000851   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<00>
 1014 49.037402   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<20>
 1015 49.038296   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<00>
 1016 49.040434   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<20>
 1017 49.041521   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<00>

    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xa52d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.46
    Destination: 192.168.1.1
v User Datagram Protocol, Src Port: 55511, Dst Port: 53
    Source Port: 55511
    Destination Port: 53
```

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

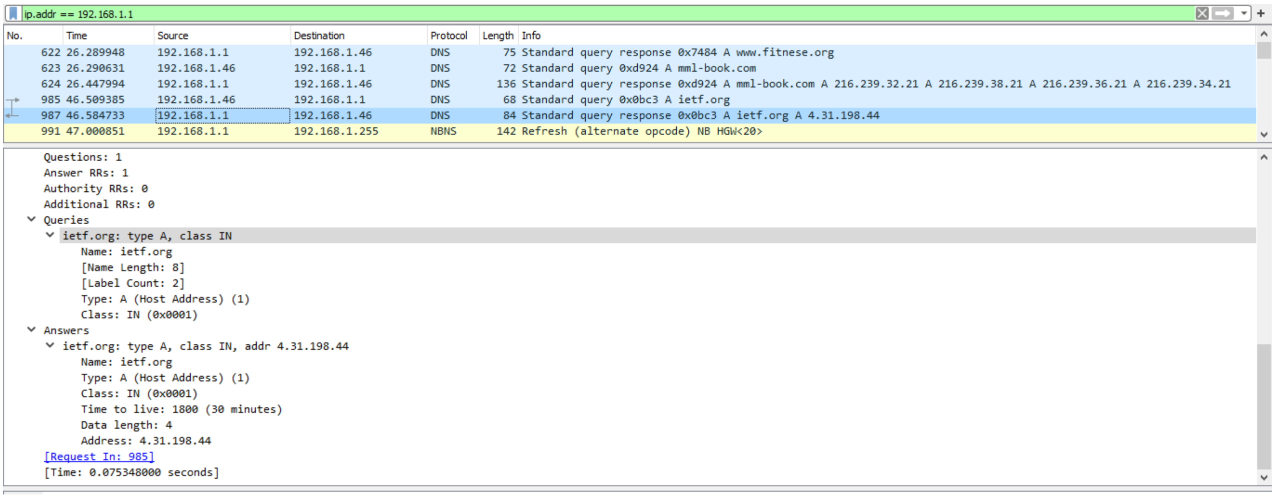
   ANS: The type of DNS query is A and it does not contain any answers.



```
ip.addr == 192.168.1.1

No.   Time        Source          Destination     Protocol Length Info
  296 10.347374   192.168.1.46    192.168.1.1     DNS        71 Standard query 0xf0d6 A fitnese.org
  396 14.354011   192.168.1.46    192.168.1.1     DNS        71 Standard query 0xf0d6 A fitnese.org
  413 16.290093   192.168.1.1     192.168.1.46    DNS        71 Standard query response 0xf0d6 A fitnese.org
  414 16.291744   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  419 17.297313   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  432 18.301183   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  476 20.311184   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  571 24.322133   192.168.1.46    192.168.1.1     DNS        75 Standard query 0x7484 A www.fitnese.org
  622 26.289948   192.168.1.1     192.168.1.46    DNS        75 Standard query response 0x7484 A www.fitnese.org
  623 26.290631   192.168.1.46    192.168.1.1     DNS        72 Standard query 0xd924 A mml-book.com
  624 26.447994   192.168.1.1     192.168.1.46    DNS       136 Standard query response 0xd924 A mml-book.com A 216.239.32.21 A 216.239.38.21 A 216.239.36.21 A 216.239.34.21
  985 46.509385   192.168.1.46    192.168.1.1     DNS        68 Standard query 0x0bc3 A ietf.org
  987 46.584733   192.168.1.1     192.168.1.46    DNS        84 Standard query response 0x0bc3 A ietf.org A 4.31.198.44
  991 47.000851   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<20>
  992 47.000851   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<00>
 1014 49.037402   192.168.1.1     192.168.1.255   NBNS      142 Refresh (alternate opcode) NB HGW<20>

    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v ietf.org: type A, class IN
        Name: ietf.org
        [Name Length: 8]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 987]
```

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

   ANS: There is 1 answer. The answer contains the name, type, address, class, time to live, data length.

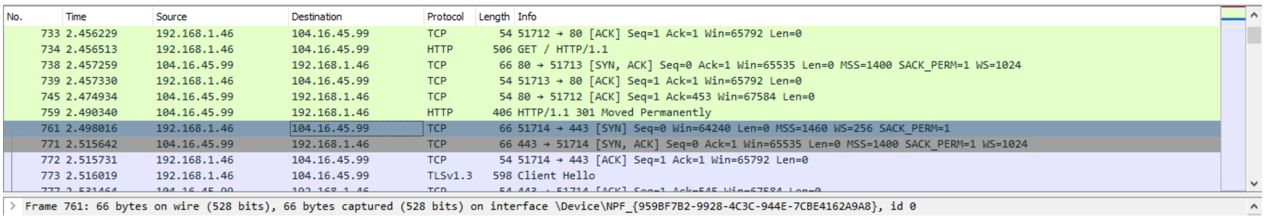


```
ip.addr == 192.168.1.1
No.     Time         Source          Destination     Protocol  Length Info
    622 26.289948    192.168.1.1     192.168.1.46    DNS         75 Standard query response 0x7484 A www.fitnese.org
    623 26.290631    192.168.1.46    192.168.1.1     DNS         72 Standard query 0xd924 A mml-book.com
    624 26.447994    192.168.1.1     192.168.1.46    DNS        136 Standard query response 0xd924 A mml-book.com A 216.239.32.21 A 216.239.38.21 A 216.239.36.21 A 216.239.34.21
    985 46.509385    192.168.1.46    192.168.1.1     DNS         68 Standard query 0x0bc3 A ietf.org
    987 46.584733    192.168.1.1     192.168.1.46    DNS         84 Standard query response 0x0bc3 A ietf.org A 4.31.198.44
    991 47.000851    192.168.1.1     192.168.1.255   NBNS       142 Refresh (alternate opcode) NB HGW<20>
```

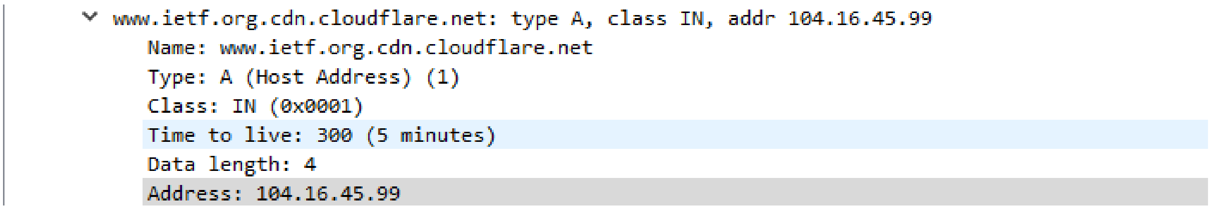
```
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ ietf.org: type A, class IN
        Name: ietf.org
        [Name Length: 8]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ⌄ Answers
    ⌄ ietf.org: type A, class IN, addr 4.31.198.44
        Name: ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 4
        Address: 4.31.198.44
    [Request In: 985]
    [Time: 0.075348000 seconds]
```

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?

   ANS: Yes, The IP address is 104.16.45.99



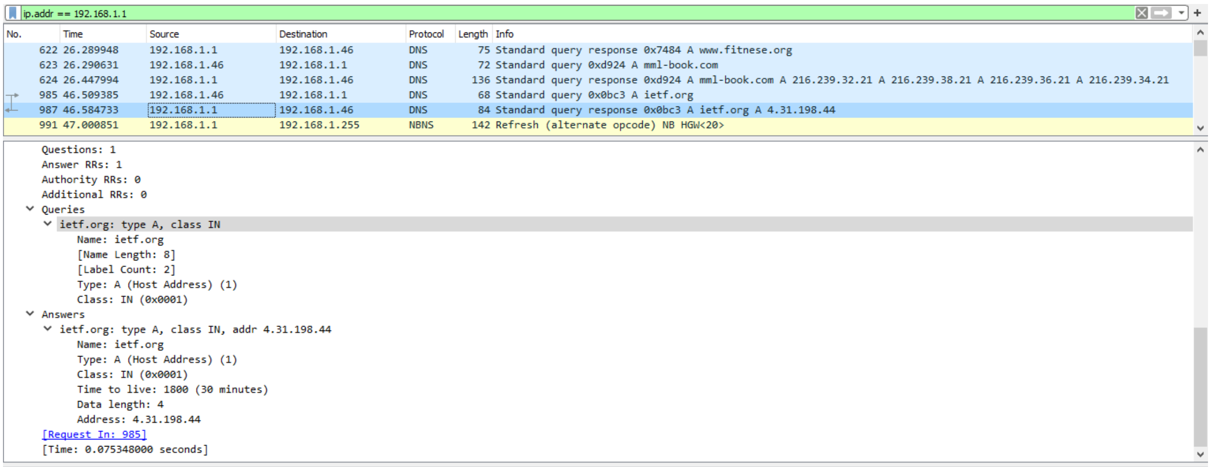
```
No.     Time         Source          Destination     Protocol  Length Info
    733 2.456229     192.168.1.46    104.16.45.99    TCP         54 51712 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    734 2.456513     192.168.1.46    104.16.45.99    HTTP       506 GET / HTTP/1.1
    738 2.457259     104.16.45.99    192.168.1.46    TCP         66 80 → 51713 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
    739 2.457330     192.168.1.46    104.16.45.99    TCP         54 51713 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    745 2.474934     104.16.45.99    192.168.1.46    TCP         54 80 → 51712 [ACK] Seq=1 Ack=453 Win=67584 Len=0
    759 2.490340     104.16.45.99    192.168.1.46    HTTP       406 HTTP/1.1 301 Moved Permanently
    761 2.498016     192.168.1.46    104.16.45.99    TCP         66 51714 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    771 2.515642     104.16.45.99    192.168.1.46    TCP         66 443 → 51714 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
    772 2.515731     192.168.1.46    104.16.45.99    TCP         54 51714 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    773 2.516019     192.168.1.46    104.16.45.99    TLSv1.3    598 Client Hello
    777 2.531464     104.16.45.99    192.168.1.46    TCP         54 443 → 51714 [ACK] Seq=1 Ack=545 Win=67584 Len=0
> Frame 761: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{959BF7B2-9928-4C3C-944E-7CBE4162A9A8}, id 0
```



```
⌄ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.16.45.99
```

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

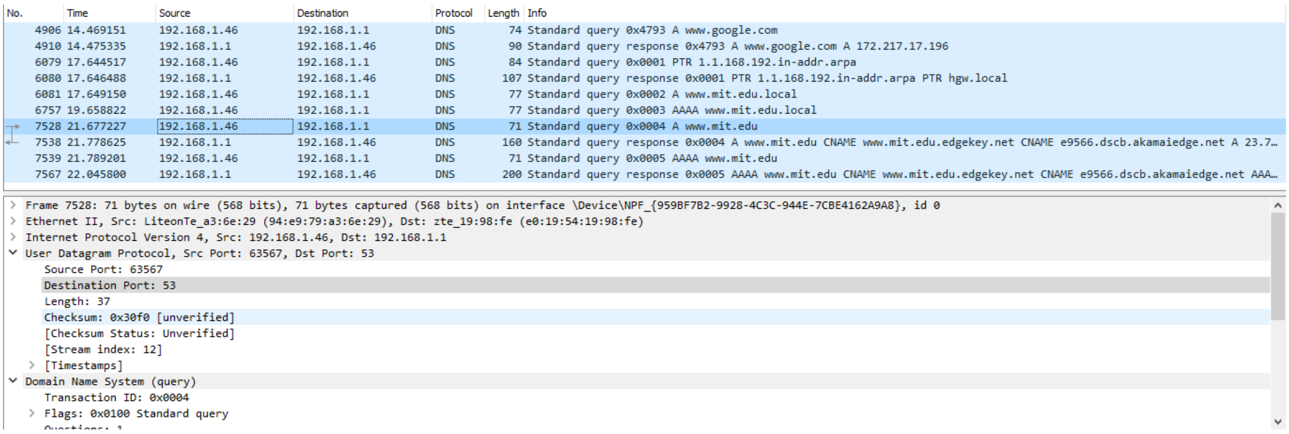
    ANS: No, all images are loaded from the web page. There is one DNS query.



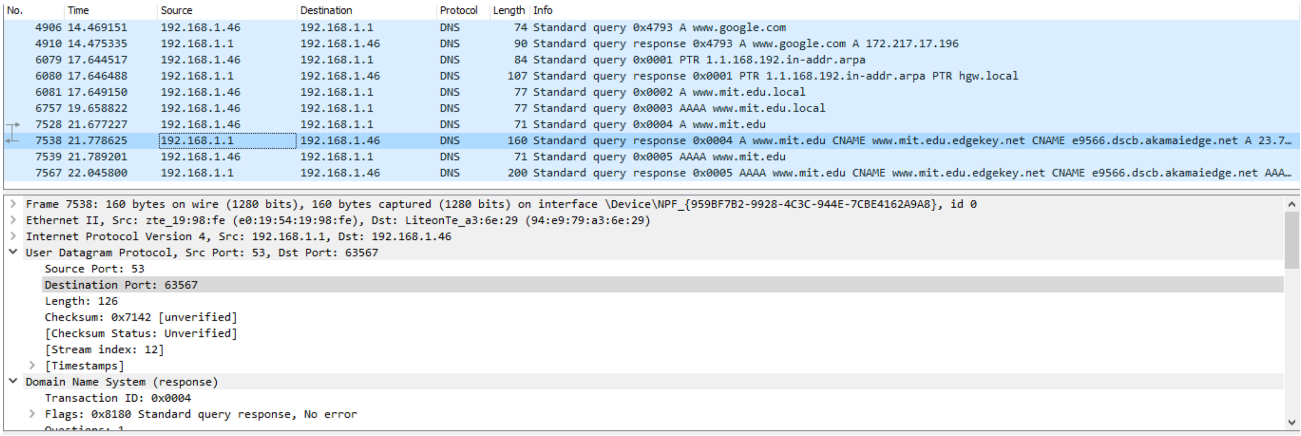
```
ip.addr == 192.168.1.1

No.   Time       Source        Destination    Protocol Length Info
  622 26.289948  192.168.1.1   192.168.1.46   DNS        75 Standard query response 0x7484 A www.fitnese.org
  623 26.290631  192.168.1.46  192.168.1.1    DNS        72 Standard query 0xd924 A mml-book.com
  624 26.447994  192.168.1.1   192.168.1.46   DNS       136 Standard query response 0xd924 A mml-book.com A 216.239.32.21 A 216.239.38.21 A 216.239.36.21 A 216.239.34.21
  985 46.509385  192.168.1.46  192.168.1.1    DNS        68 Standard query 0x0bc3 A ietf.org
  987 46.584733  192.168.1.1   192.168.1.46   DNS        84 Standard query response 0x0bc3 A ietf.org A 4.31.198.44
  991 47.000851  192.168.1.1   192.168.1.255  NBNS      142 Refresh (alternate opcode) NB HGW<20>

    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    ietf.org: type A, class IN
        Name: ietf.org
        [Name Length: 8]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    ietf.org: type A, class IN, addr 4.31.198.44
        Name: ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 4
        Address: 4.31.198.44
    [Request In: 985]
    [Time: 0.075348000 seconds]
```

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

ANS: Destination port for the DNS query message and source port of DNS response message are the same. The port is ***53.***



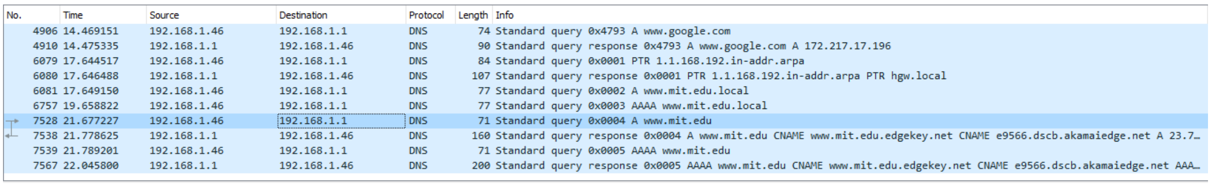
```
No.   Time       Source        Destination    Protocol Length Info
 4906 14.469151  192.168.1.46  192.168.1.1    DNS        74 Standard query 0x4793 A www.google.com
 4910 14.475335  192.168.1.1   192.168.1.46   DNS        90 Standard query response 0x4793 A www.google.com A 172.217.17.196
 6079 17.644517  192.168.1.46  192.168.1.1    DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
 6080 17.646488  192.168.1.1   192.168.1.46   DNS       107 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
 6081 17.649150  192.168.1.46  192.168.1.1    DNS        77 Standard query 0x0002 A www.mit.edu.local
 6757 19.658822  192.168.1.46  192.168.1.1    DNS        77 Standard query 0x0003 AAAA www.mit.edu.local
 7528 21.677227  192.168.1.46  192.168.1.1    DNS        71 Standard query 0x0004 A www.mit.edu
 7538 21.778625  192.168.1.1   192.168.1.46   DNS       160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7…
 7539 21.789201  192.168.1.46  192.168.1.1    DNS        71 Standard query 0x0005 AAAA www.mit.edu
 7567 22.045800  192.168.1.1   192.168.1.46   DNS       200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAA…

> Frame 7528: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{959BF7B2-9928-4C3C-944E-7CBE4162A9A8}, id 0
> Ethernet II, Src: LiteonTe_a3:6e:29 (94:e9:79:a3:6e:29), Dst: zte_19:98:fe (e0:19:54:19:98:fe)
> Internet Protocol Version 4, Src: 192.168.1.46, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 63567, Dst Port: 53
    Source Port: 63567
    Destination Port: 53
    Length: 37
    Checksum: 0x30f0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 12]
  > [Timestamps]
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
```



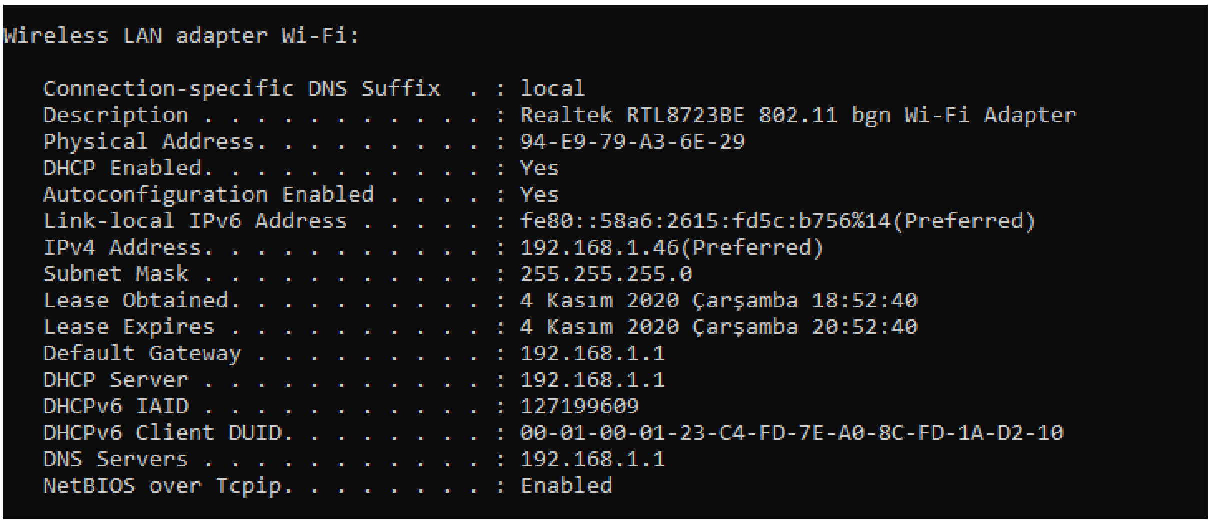
```
No.   Time       Source        Destination    Protocol Length Info
 4906 14.469151  192.168.1.46  192.168.1.1    DNS        74 Standard query 0x4793 A www.google.com
 4910 14.475335  192.168.1.1   192.168.1.46   DNS        90 Standard query response 0x4793 A www.google.com A 172.217.17.196
 6079 17.644517  192.168.1.46  192.168.1.1    DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
 6080 17.646488  192.168.1.1   192.168.1.46   DNS       107 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
 6081 17.649150  192.168.1.46  192.168.1.1    DNS        77 Standard query 0x0002 A www.mit.edu.local
 6757 19.658822  192.168.1.46  192.168.1.1    DNS        77 Standard query 0x0003 AAAA www.mit.edu.local
 7528 21.677227  192.168.1.46  192.168.1.1    DNS        71 Standard query 0x0004 A www.mit.edu
 7538 21.778625  192.168.1.1   192.168.1.46   DNS       160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7…
 7539 21.789201  192.168.1.46  192.168.1.1    DNS        71 Standard query 0x0005 AAAA www.mit.edu
 7567 22.045800  192.168.1.1   192.168.1.46   DNS       200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAA…

> Frame 7538: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{959BF7B2-9928-4C3C-944E-7CBE4162A9A8}, id 0
> Ethernet II, Src: zte_19:98:fe (e0:19:54:19:98:fe), Dst: LiteonTe_a3:6e:29 (94:e9:79:a3:6e:29)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.46
v User Datagram Protocol, Src Port: 53, Dst Port: 63567
    Source Port: 53
    Destination Port: 63567
    Length: 126
    Checksum: 0x7142 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 12]
  > [Timestamps]
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
```

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

ANS: Yes. 192.168.1.1



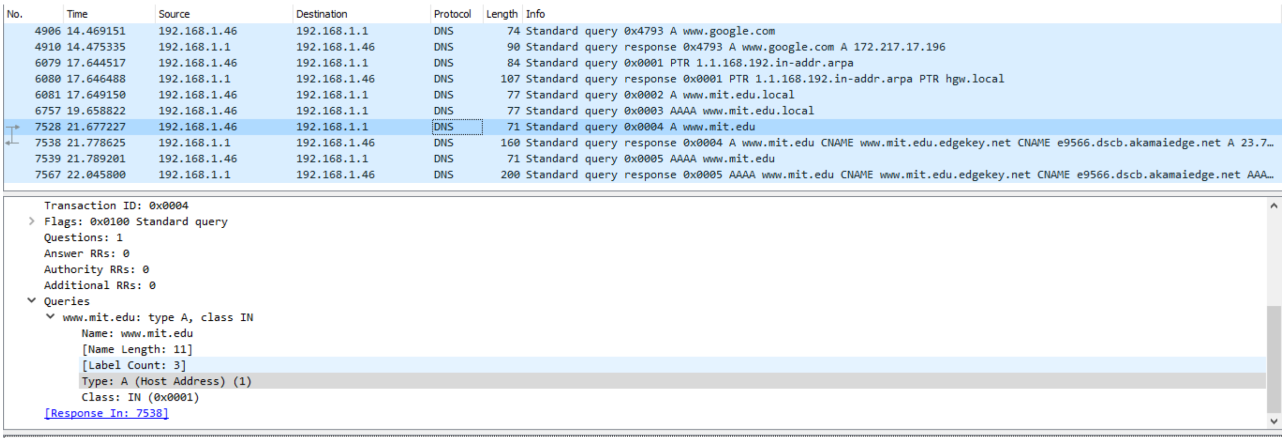
```
No.   Time      Source        Destination   Protocol Length Info
 4906 14.469151 192.168.1.46  192.168.1.1   DNS       74 Standard query 0x4793 A www.google.com
 4910 14.475335 192.168.1.1   192.168.1.46  DNS       90 Standard query response 0x4793 A www.google.com A 172.217.17.196
 6079 17.644517 192.168.1.46  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
 6080 17.646488 192.168.1.1   192.168.1.46  DNS      107 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
 6081 17.649150 192.168.1.46  192.168.1.1   DNS       77 Standard query 0x0002 A www.mit.edu.local
 6757 19.658822 192.168.1.46  192.168.1.1   DNS       77 Standard query 0x0003 AAAA www.mit.edu.local
 7528 21.677227 192.168.1.46  192.168.1.1   DNS       71 Standard query 0x0004 A www.mit.edu
 7538 21.778625 192.168.1.1   192.168.1.46  DNS      160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7…
 7539 21.789201 192.168.1.46  192.168.1.1   DNS       71 Standard query 0x0005 AAAA www.mit.edu
 7567 22.045800 192.168.1.1   192.168.1.46  DNS      200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAA…
```



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : local
   Description . . . . . . . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 94-E9-79-A3-6E-29
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::58a6:2615:fd5c:b756%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.46(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 4 Kasım 2020 Çarşamba 18:52:40
   Lease Expires . . . . . . . . . . : 4 Kasım 2020 Çarşamba 20:52:40
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 127199609
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-C4-FD-7E-A0-8C-FD-1A-D2-10
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

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

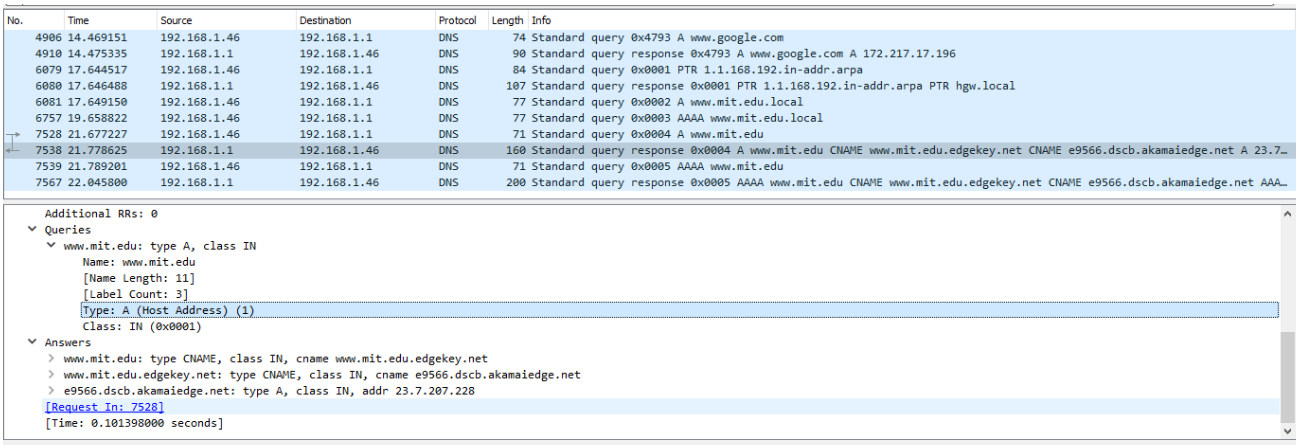
ANS: Type of DNS query is A. It does not contain any answer.



```
No.   Time      Source        Destination   Protocol Length Info
 4906 14.469151 192.168.1.46  192.168.1.1   DNS       74 Standard query 0x4793 A www.google.com
 4910 14.475335 192.168.1.1   192.168.1.46  DNS       90 Standard query response 0x4793 A www.google.com A 172.217.17.196
 6079 17.644517 192.168.1.46  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
 6080 17.646488 192.168.1.1   192.168.1.46  DNS      107 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
 6081 17.649150 192.168.1.46  192.168.1.1   DNS       77 Standard query 0x0002 A www.mit.edu.local
 6757 19.658822 192.168.1.46  192.168.1.1   DNS       77 Standard query 0x0003 AAAA www.mit.edu.local
 7528 21.677227 192.168.1.46  192.168.1.1   DNS       71 Standard query 0x0004 A www.mit.edu
 7538 21.778625 192.168.1.1   192.168.1.46  DNS      160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7…
 7539 21.789201 192.168.1.46  192.168.1.1   DNS       71 Standard query 0x0005 AAAA www.mit.edu
 7567 22.045800 192.168.1.1   192.168.1.46  DNS      200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAA…

    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 7538]
```

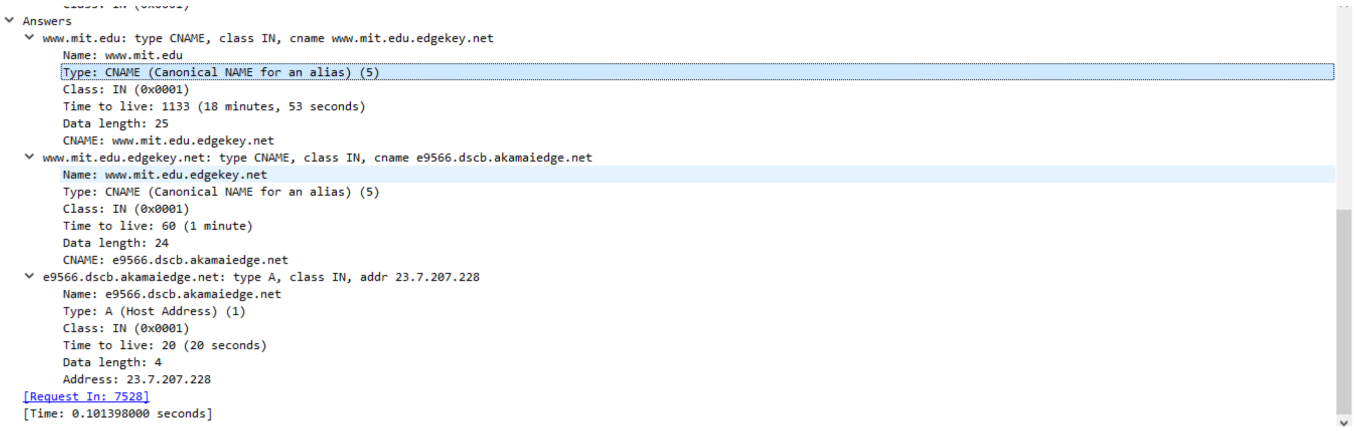
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

ANS: There are 3 answers. Each of them contains name, type, class, time to live, data length, address.



```
No.   Time       Source        Destination   Protocol Length Info
 4906 14.469151  192.168.1.46  192.168.1.1   DNS       74 Standard query 0x4793 A www.google.com
 4910 14.475335  192.168.1.1   192.168.1.46  DNS       90 Standard query response 0x4793 A www.google.com A 172.217.17.196
 6079 17.644517  192.168.1.46  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
 6080 17.646488  192.168.1.1   192.168.1.46  DNS      107 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
 6081 17.649150  192.168.1.46  192.168.1.1   DNS       77 Standard query 0x0002 A www.mit.edu.local
 6757 19.658822  192.168.1.46  192.168.1.1   DNS       77 Standard query 0x0003 AAAA www.mit.edu.local
 7528 21.677227  192.168.1.46  192.168.1.1   DNS       71 Standard query 0x0004 A www.mit.edu
 7538 21.778625  192.168.1.1   192.168.1.46  DNS      160 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7…
 7539 21.789201  192.168.1.46  192.168.1.1   DNS       71 Standard query 0x0005 AAAA www.mit.edu
 7567 22.045800  192.168.1.1   192.168.1.46  DNS      200 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAA…
```

```
    Additional RRs: 0
  Queries
    www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  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 23.7.207.228
    [Request In: 7528]
    [Time: 0.101398000 seconds]
```



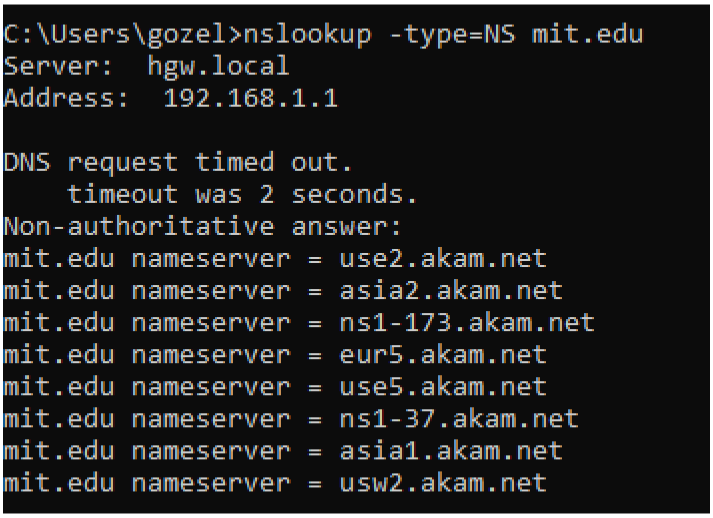
```
        Class: IN (0x0001)
  Answers
    www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1133 (18 minutes, 53 seconds)
        Data length: 25
        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 23.7.207.228
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 23.7.207.228
  [Request In: 7528]
  [Time: 0.101398000 seconds]
```

15. Provide a screenshot.

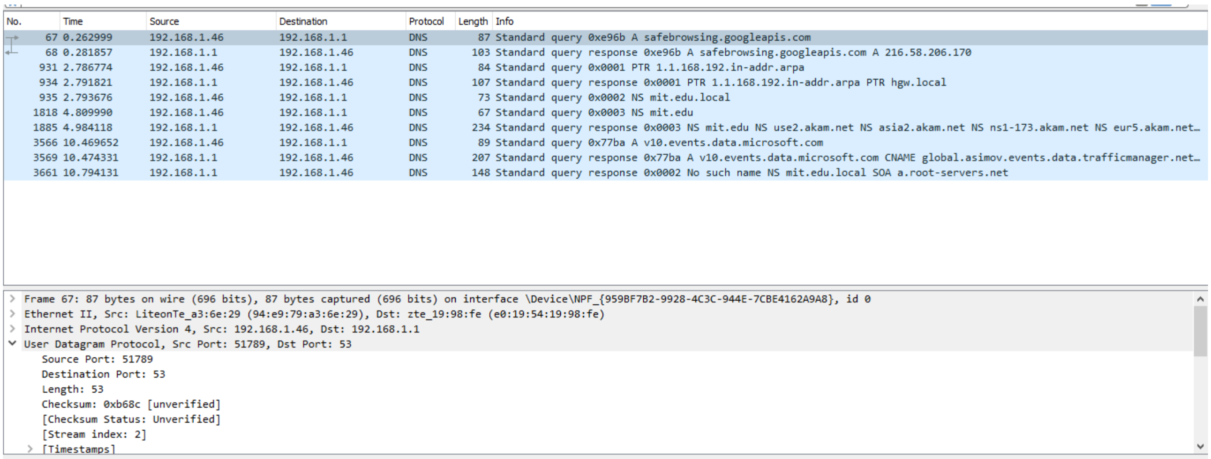
We already did above.

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

ANS: Yes, it is the same. 192.168.1.1

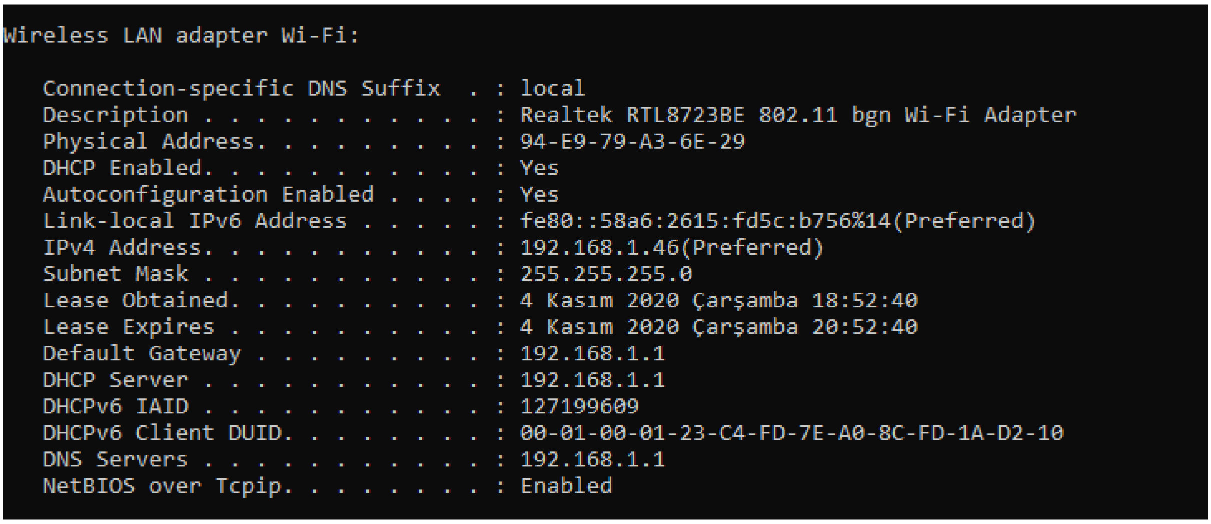


```
C:\Users\gozel>nslookup -type=NS mit.edu
Server:  hgw.local
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = usw2.akam.net
```



```
No.   Time       Source        Destination   Protocol Length Info
   67 0.262999   192.168.1.46  192.168.1.1   DNS       87 Standard query 0xe96b A safebrowsing.googleapis.com
   68 0.281857   192.168.1.1   192.168.1.46  DNS      103 Standard query response 0xe96b A safebrowsing.googleapis.com A 216.58.206.170
  931 2.786774   192.168.1.46  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  934 2.791821   192.168.1.1   192.168.1.46  DNS      107 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
  935 2.793676   192.168.1.46  192.168.1.1   DNS       73 Standard query 0x0002 NS mit.edu.local
 1818 4.809990   192.168.1.46  192.168.1.1   DNS       67 Standard query 0x0003 NS mit.edu
 1885 4.984118   192.168.1.1   192.168.1.46  DNS      234 Standard query response 0x0003 NS mit.edu NS use2.akam.net NS asia2.akam.net NS ns1-173.akam.net NS eur5.akam.net…
 3566 10.469652  192.168.1.46  192.168.1.1   DNS       89 Standard query 0x77ba A v10.events.data.microsoft.com
 3569 10.474331  192.168.1.1   192.168.1.46  DNS      207 Standard query response 0x77ba A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net…
 3661 10.794131  192.168.1.1   192.168.1.46  DNS      148 Standard query response 0x0002 No such name NS mit.edu.local SOA a.root-servers.net
```

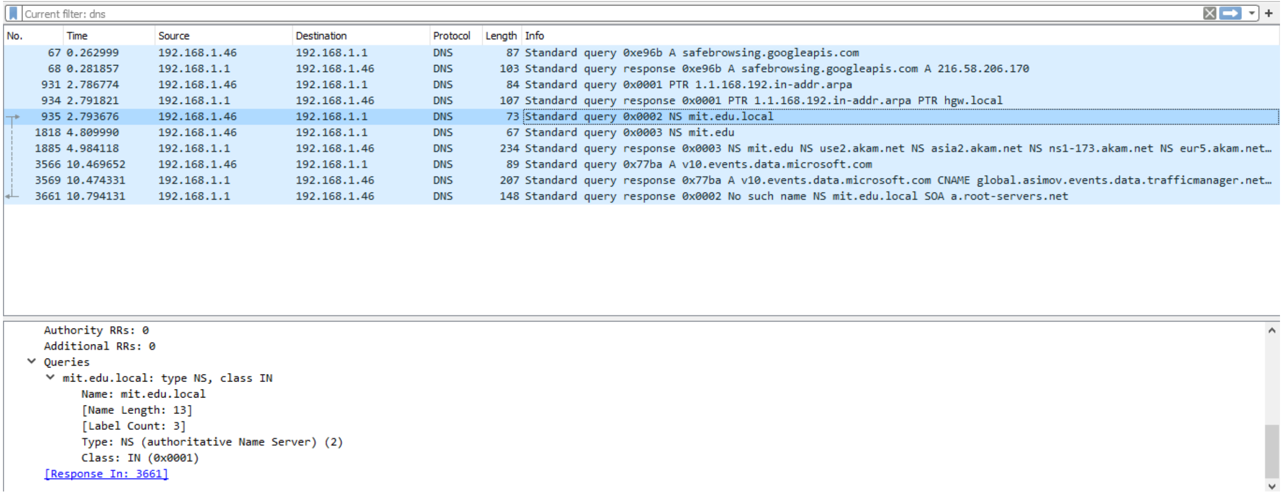
```
> Frame 67: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{959BF7B2-9928-4C3C-944E-7CBE4162A9A8}, id 0
> Ethernet II, Src: LiteonTe_a3:6e:29 (94:e9:79:a3:6e:29), Dst: zte_19:98:fe (e0:19:54:19:98:fe)
> Internet Protocol Version 4, Src: 192.168.1.46, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 51789, Dst Port: 53
    Source Port: 51789
    Destination Port: 53
    Length: 53
    Checksum: 0xb68c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
```



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : local
   Description . . . . . . . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 94-E9-79-A3-6E-29
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::58a6:2615:fd5c:b756%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.46(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 4 Kasım 2020 Çarşamba 18:52:40
   Lease Expires . . . . . . . . . . : 4 Kasım 2020 Çarşamba 20:52:40
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 127199609
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-C4-FD-7E-A0-8C-FD-1A-D2-10
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

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

ANS: The DNS query type is **NS.** It does not contain answers.



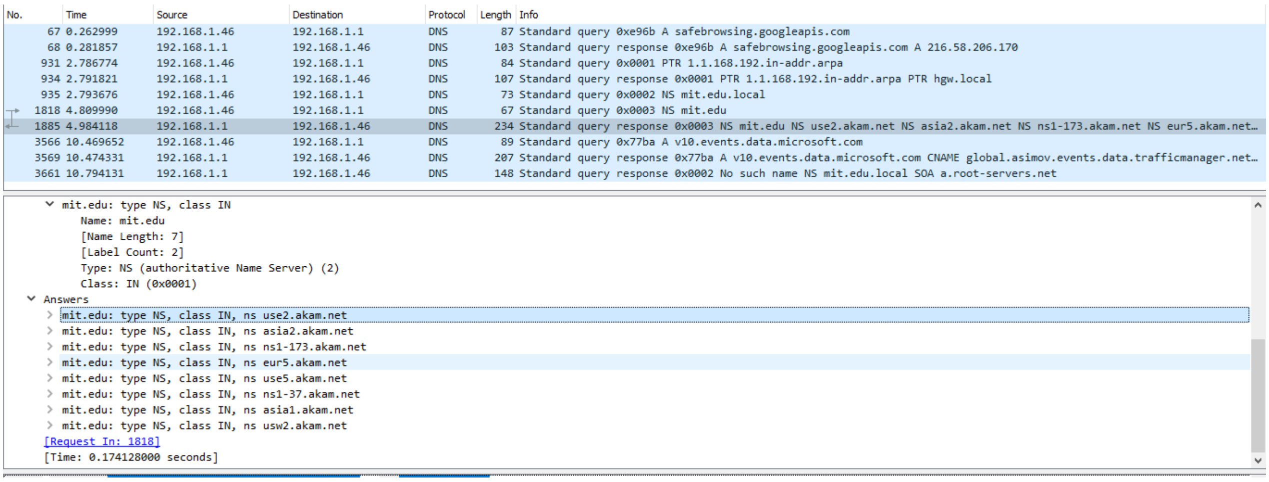
Current filter: dns

```
No.   Time       Source        Destination   Protocol Length Info
   67 0.262999   192.168.1.46  192.168.1.1   DNS       87 Standard query 0xe96b A safebrowsing.googleapis.com
   68 0.281857   192.168.1.1   192.168.1.46  DNS      103 Standard query response 0xe96b A safebrowsing.googleapis.com A 216.58.206.170
  931 2.786774   192.168.1.46  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  934 2.791821   192.168.1.1   192.168.1.46  DNS      107 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
  935 2.793676   192.168.1.46  192.168.1.1   DNS       73 Standard query 0x0002 NS mit.edu.local
 1818 4.809990   192.168.1.46  192.168.1.1   DNS       67 Standard query 0x0003 NS mit.edu
 1885 4.984118   192.168.1.1   192.168.1.46  DNS      234 Standard query response 0x0003 NS mit.edu NS use2.akam.net NS asia2.akam.net NS ns1-173.akam.net NS eur5.akam.net…
 3566 10.469652  192.168.1.46  192.168.1.1   DNS       89 Standard query 0x77ba A v10.events.data.microsoft.com
 3569 10.474331  192.168.1.1   192.168.1.46  DNS      207 Standard query response 0x77ba A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net…
 3661 10.794131  192.168.1.1   192.168.1.46  DNS      148 Standard query response 0x0002 No such name NS mit.edu.local SOA a.root-servers.net
```

```
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu.local: type NS, class IN
        Name: mit.edu.local
        [Name Length: 13]
        [Label Count: 3]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 3661]
```

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

ANS: MIT name servers are **use2.akam.net, asia2.akam.net, ns1-173.akam.net, eur5.akam.net, use5.akam.net, ns1-37.akam.net, asia1.akam.net, usw2.akam.net.** It does not provide IP addresses of the MIT name servers.



No.	Time	Source	Destination	Protocol	Length	Info
67	0.262999	192.168.1.46	192.168.1.1	DNS	87	Standard query 0xe96b A safebrowsing.googleapis.com
68	0.281857	192.168.1.1	192.168.1.46	DNS	103	Standard query response 0xe96b A safebrowsing.googleapis.com A 216.58.206.170
931	2.786774	192.168.1.46	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
934	2.791821	192.168.1.1	192.168.1.46	DNS	107	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR hgw.local
935	2.793676	192.168.1.46	192.168.1.1	DNS	73	Standard query 0x0002 NS mit.edu.local
1818	4.809990	192.168.1.46	192.168.1.1	DNS	67	Standard query 0x0003 NS mit.edu
1885	4.984118	192.168.1.1	192.168.1.46	DNS	234	Standard query response 0x0003 NS mit.edu NS use2.akam.net NS asia2.akam.net NS ns1-173.akam.net NS eur5.akam.net…
3566	10.469652	192.168.1.46	192.168.1.1	DNS	89	Standard query 0x77ba A v10.events.data.microsoft.com
3569	10.474331	192.168.1.1	192.168.1.46	DNS	207	Standard query response 0x77ba A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net…
3661	10.794131	192.168.1.1	192.168.1.46	DNS	148	Standard query response 0x0002 No such name NS mit.edu.local SOA a.root-servers.net

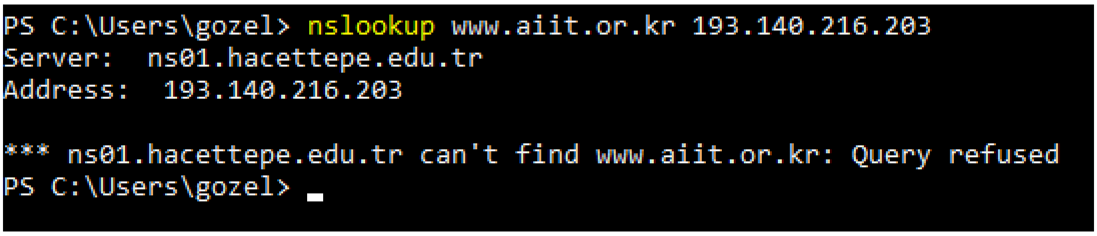
```
    ˅ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ˅ Answers
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns eur5.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 asia1.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
  [Request In: 1818]
  [Time: 0.174128000 seconds]
```

19. Provide a screenshot.

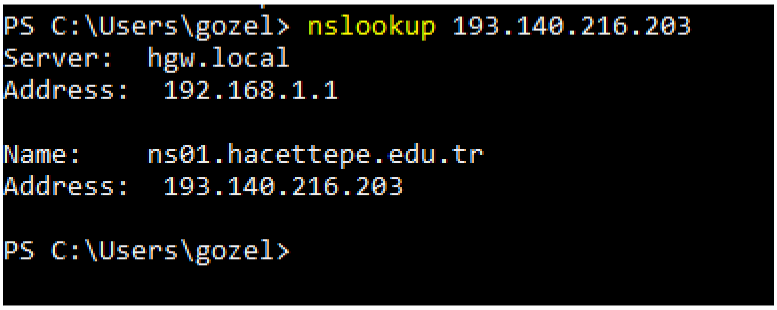
We already did above.

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?

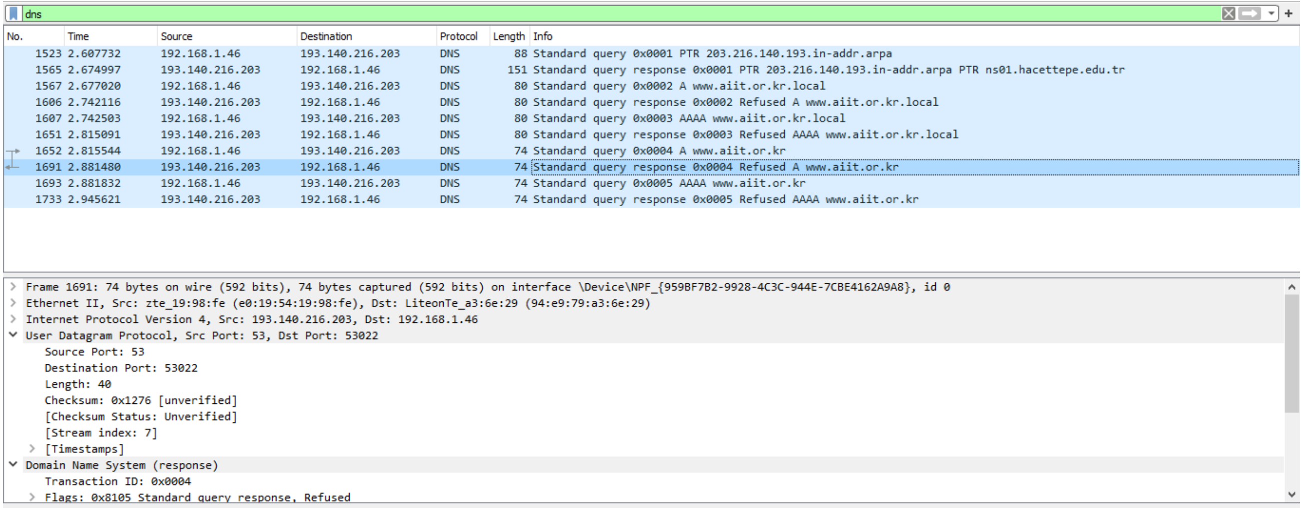
ANS: We got the **Query refused** result because we are not in the Hacettepe network.



```
PS C:\Users\gozel> nslookup www.aiit.or.kr 193.140.216.203
Server:  ns01.hacettepe.edu.tr
Address:  193.140.216.203

*** ns01.hacettepe.edu.tr can't find www.aiit.or.kr: Query refused
PS C:\Users\gozel> _
```



```
PS C:\Users\gozel> nslookup 193.140.216.203
Server:  hgw.local
Address:  192.168.1.1

Name:    ns01.hacettepe.edu.tr
Address:  193.140.216.203

PS C:\Users\gozel>
```

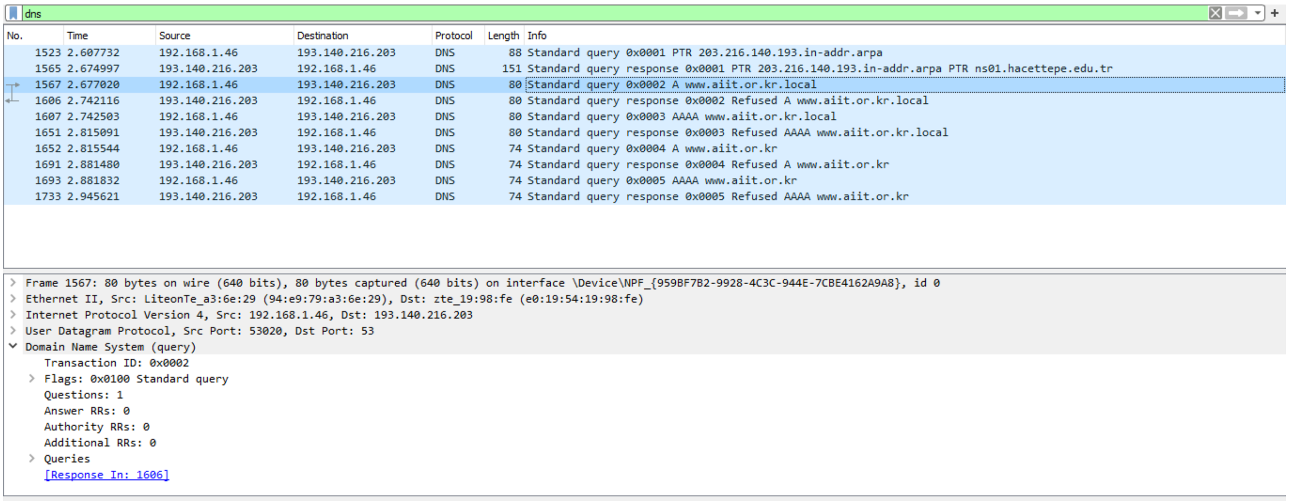


```
No.       Time        Source            Destination       Protocol  Length Info
     1523 2.607732    192.168.1.46      193.140.216.203   DNS         88 Standard query 0x0001 PTR 203.216.140.193.in-addr.arpa
     1565 2.674997    193.140.216.203   192.168.1.46      DNS        151 Standard query response 0x0001 PTR 203.216.140.193.in-addr.arpa PTR ns01.hacettepe.edu.tr
     1567 2.677020    192.168.1.46      193.140.216.203   DNS         80 Standard query 0x0002 A www.aiit.or.kr.local
     1606 2.742116    193.140.216.203   192.168.1.46      DNS         80 Standard query response 0x0002 Refused A www.aiit.or.kr.local
     1607 2.742503    192.168.1.46      193.140.216.203   DNS         80 Standard query 0x0003 AAAA www.aiit.or.kr.local
     1651 2.815091    193.140.216.203   192.168.1.46      DNS         80 Standard query response 0x0003 Refused AAAA www.aiit.or.kr.local
     1652 2.815544    192.168.1.46      193.140.216.203   DNS         74 Standard query 0x0004 A www.aiit.or.kr
     1691 2.881480    193.140.216.203   192.168.1.46      DNS         74 Standard query response 0x0004 Refused A www.aiit.or.kr
     1693 2.881832    192.168.1.46      193.140.216.203   DNS         74 Standard query 0x0005 AAAA www.aiit.or.kr
     1733 2.945621    193.140.216.203   192.168.1.46      DNS         74 Standard query response 0x0005 Refused AAAA www.aiit.or.kr
```

```
> Frame 1691: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{959BF7B2-9928-4C3C-944E-7CBE4162A9A8}, id 0
> Ethernet II, Src: zte_19:98:fe (e0:19:54:19:98:fe), Dst: LiteonTe_a3:6e:29 (94:e9:79:a3:6e:29)
> Internet Protocol Version 4, Src: 193.140.216.203, Dst: 192.168.1.46
v User Datagram Protocol, Src Port: 53, Dst Port: 53022
    Source Port: 53
    Destination Port: 53022
    Length: 40
    Checksum: 0x1276 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8105 Standard query response, Refused
```

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

ANS: The type of the DNS query is A. It does not contain any answers.

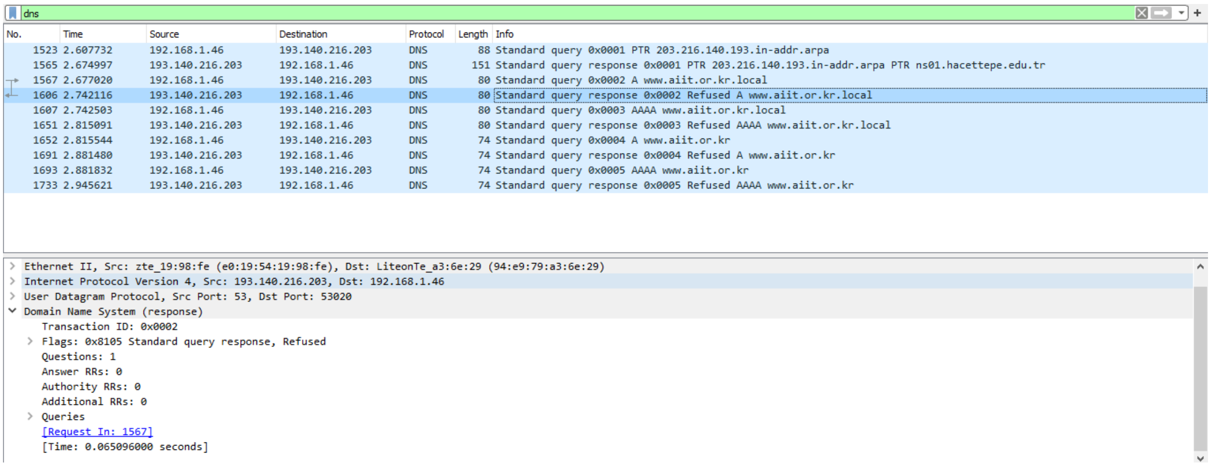


```
No.       Time        Source            Destination       Protocol  Length Info
     1523 2.607732    192.168.1.46      193.140.216.203   DNS         88 Standard query 0x0001 PTR 203.216.140.193.in-addr.arpa
     1565 2.674997    193.140.216.203   192.168.1.46      DNS        151 Standard query response 0x0001 PTR 203.216.140.193.in-addr.arpa PTR ns01.hacettepe.edu.tr
     1567 2.677020    192.168.1.46      193.140.216.203   DNS         80 Standard query 0x0002 A www.aiit.or.kr.local
     1606 2.742116    193.140.216.203   192.168.1.46      DNS         80 Standard query response 0x0002 Refused A www.aiit.or.kr.local
     1607 2.742503    192.168.1.46      193.140.216.203   DNS         80 Standard query 0x0003 AAAA www.aiit.or.kr.local
     1651 2.815091    193.140.216.203   192.168.1.46      DNS         80 Standard query response 0x0003 Refused AAAA www.aiit.or.kr.local
     1652 2.815544    192.168.1.46      193.140.216.203   DNS         74 Standard query 0x0004 A www.aiit.or.kr
     1691 2.881480    193.140.216.203   192.168.1.46      DNS         74 Standard query response 0x0004 Refused A www.aiit.or.kr
     1693 2.881832    192.168.1.46      193.140.216.203   DNS         74 Standard query 0x0005 AAAA www.aiit.or.kr
     1733 2.945621    193.140.216.203   192.168.1.46      DNS         74 Standard query response 0x0005 Refused AAAA www.aiit.or.kr
```

```
> Frame 1567: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{959BF7B2-9928-4C3C-944E-7CBE4162A9A8}, id 0
> Ethernet II, Src: LiteonTe_a3:6e:29 (94:e9:79:a3:6e:29), Dst: zte_19:98:fe (e0:19:54:19:98:fe)
> Internet Protocol Version 4, Src: 192.168.1.46, Dst: 193.140.216.203
> User Datagram Protocol, Src Port: 53020, 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: 1606]
```

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

ANS: There are no answers. That’s why it does not contain anything.



```
No.  Time      Source          Destination     Protocol Length Info
1523 2.607732  192.168.1.46    193.140.216.203 DNS       88 Standard query 0x0001 PTR 203.216.140.193.in-addr.arpa
1565 2.674997  193.140.216.203 192.168.1.46    DNS      151 Standard query response 0x0001 PTR 203.216.140.193.in-addr.arpa PTR ns01.hacettepe.edu.tr
1567 2.677020  192.168.1.46    193.140.216.203 DNS       80 Standard query 0x0002 A www.aiit.or.kr.local
1606 2.742116  193.140.216.203 192.168.1.46    DNS       80 Standard query response 0x0002 Refused A www.aiit.or.kr.local
1607 2.742503  192.168.1.46    193.140.216.203 DNS       80 Standard query 0x0003 AAAA www.aiit.or.kr.local
1651 2.815091  193.140.216.203 192.168.1.46    DNS       80 Standard query response 0x0003 Refused AAAA www.aiit.or.kr.local
1652 2.815544  192.168.1.46    193.140.216.203 DNS       74 Standard query 0x0004 A www.aiit.or.kr
1691 2.881480  193.140.216.203 192.168.1.46    DNS       74 Standard query response 0x0004 Refused A www.aiit.or.kr
1693 2.881832  192.168.1.46    193.140.216.203 DNS       74 Standard query 0x0005 AAAA www.aiit.or.kr
1733 2.945621  193.140.216.203 192.168.1.46    DNS       74 Standard query response 0x0005 Refused AAAA www.aiit.or.kr
```

```
> Ethernet II, Src: zte_19:98:fe (e0:19:54:19:98:fe), Dst: LiteonTe_a3:6e:29 (94:e9:79:a3:6e:29)
> Internet Protocol Version 4, Src: 193.140.216.203, Dst: 192.168.1.46
> User Datagram Protocol, Src Port: 53, Dst Port: 53020
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8105 Standard query response, Refused
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Request In: 1567]
    [Time: 0.065096000 seconds]
```

23. Provide a screenshot.

ANS: We already did the above.