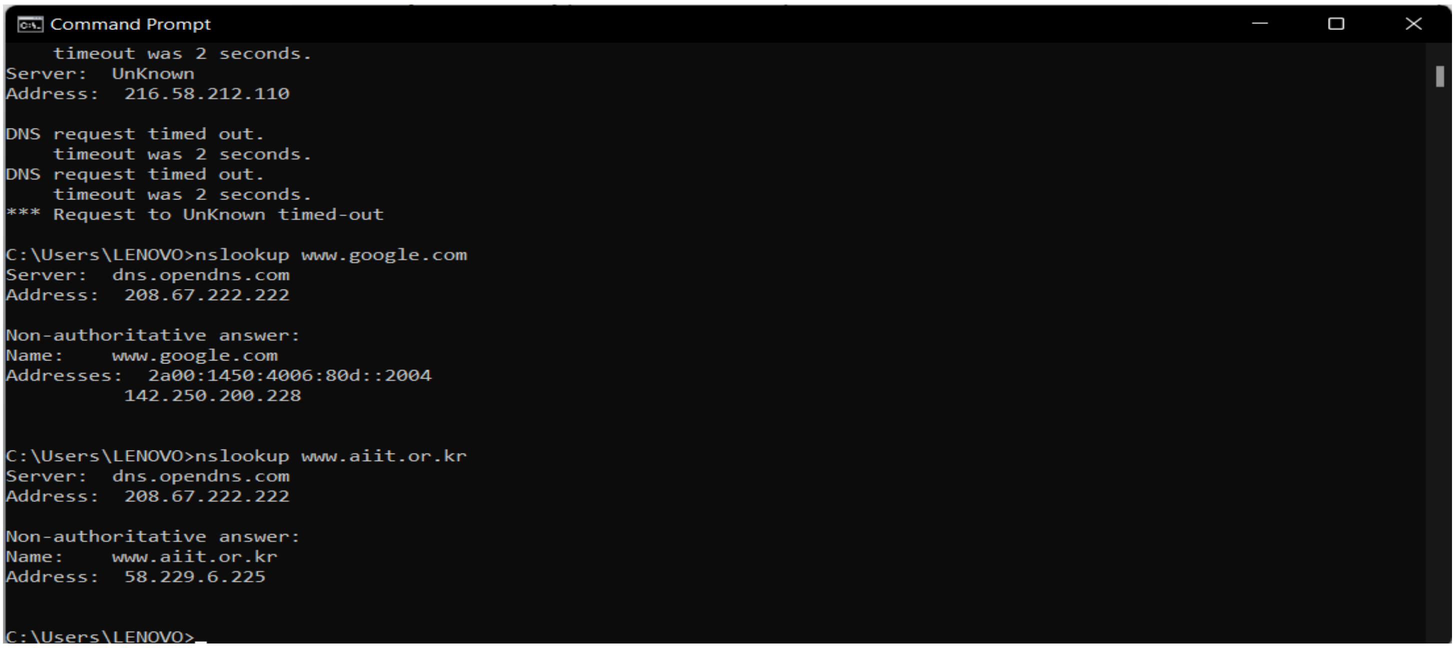
Ex1- DNS

Q1-

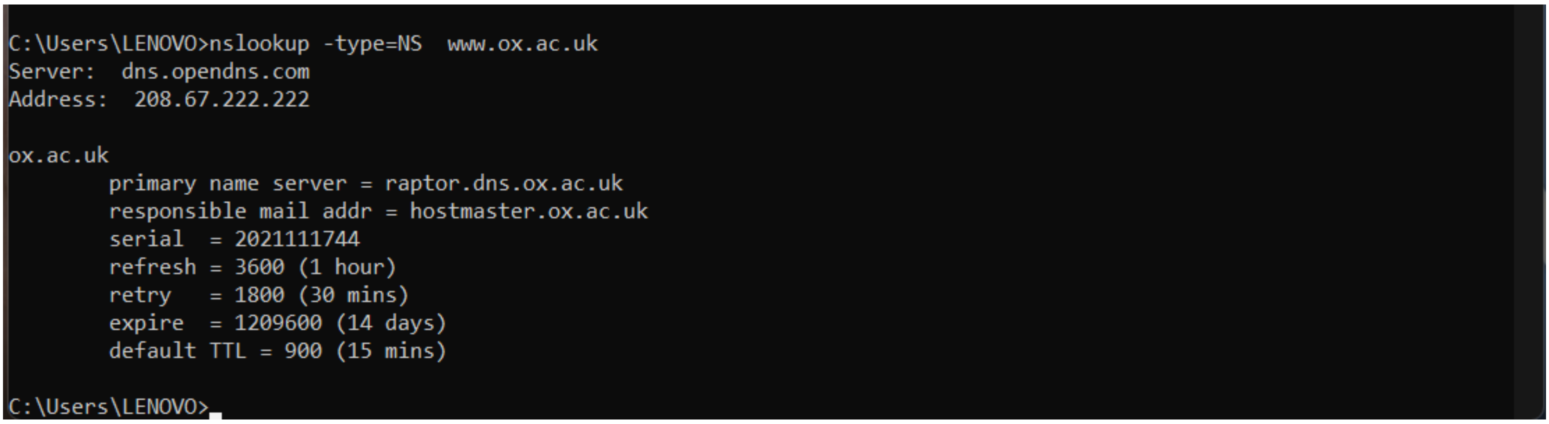
The IP of the web server in ASIA is 58.229.6.225



```
    timeout was 2 seconds.
Server:  UnKnown
Address:  216.58.212.110

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

C:\Users\LENOVO>nslookup www.google.com
Server:  dns.opendns.com
Address:  208.67.222.222

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4006:80d::2004
          142.250.200.228


C:\Users\LENOVO>nslookup www.aiit.or.kr
Server:  dns.opendns.com
Address:  208.67.222.222

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  58.229.6.225


C:\Users\LENOVO>
```

Q2-

The authoritative DNS server for Oxford University is

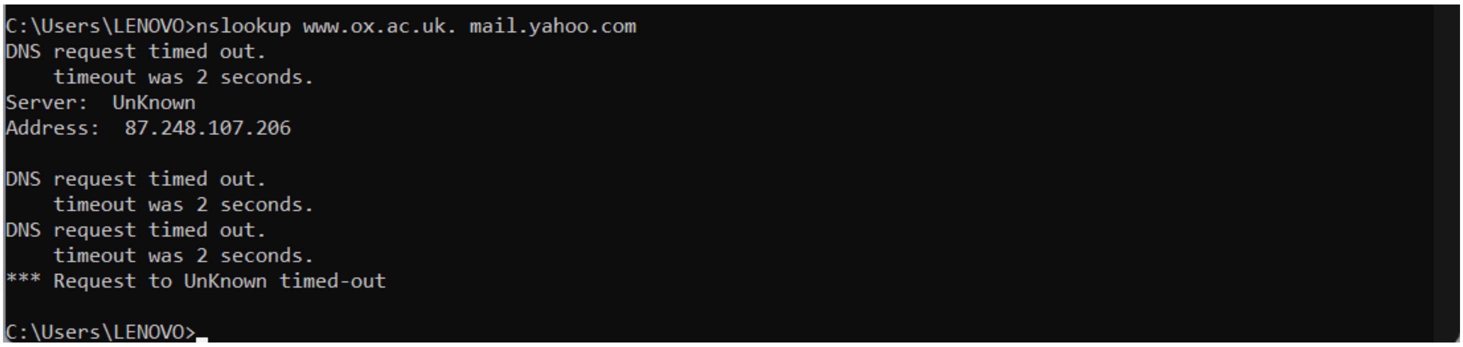


```
C:\Users\LENOVO>nslookup -type=NS  www.ox.ac.uk
Server:  dns.opendns.com
Address:  208.67.222.222

ox.ac.uk
        primary name server = raptor.dns.ox.ac.uk
        responsible mail addr = hostmaster.ox.ac.uk
        serial  = 2021111744
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 900 (15 mins)

C:\Users\LENOVO>
```

raptor.dns.ox.ac.uk

Q3-

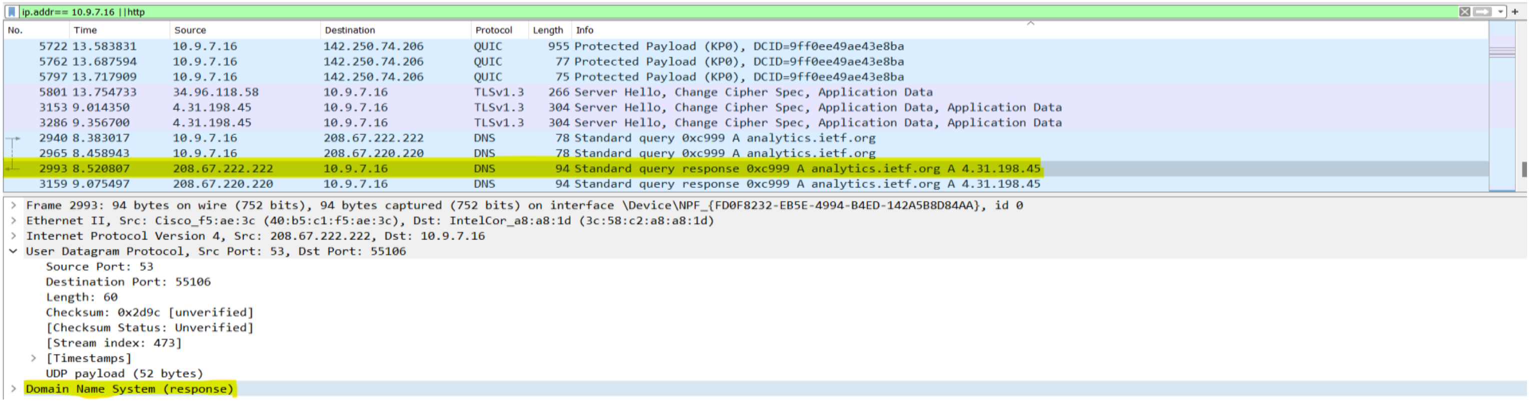
The IP address is 87.248.107.206



```
C:\Users\LENOVO>nslookup www.ox.ac.uk. mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.107.206

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

C:\Users\LENOVO>
```

Q4-

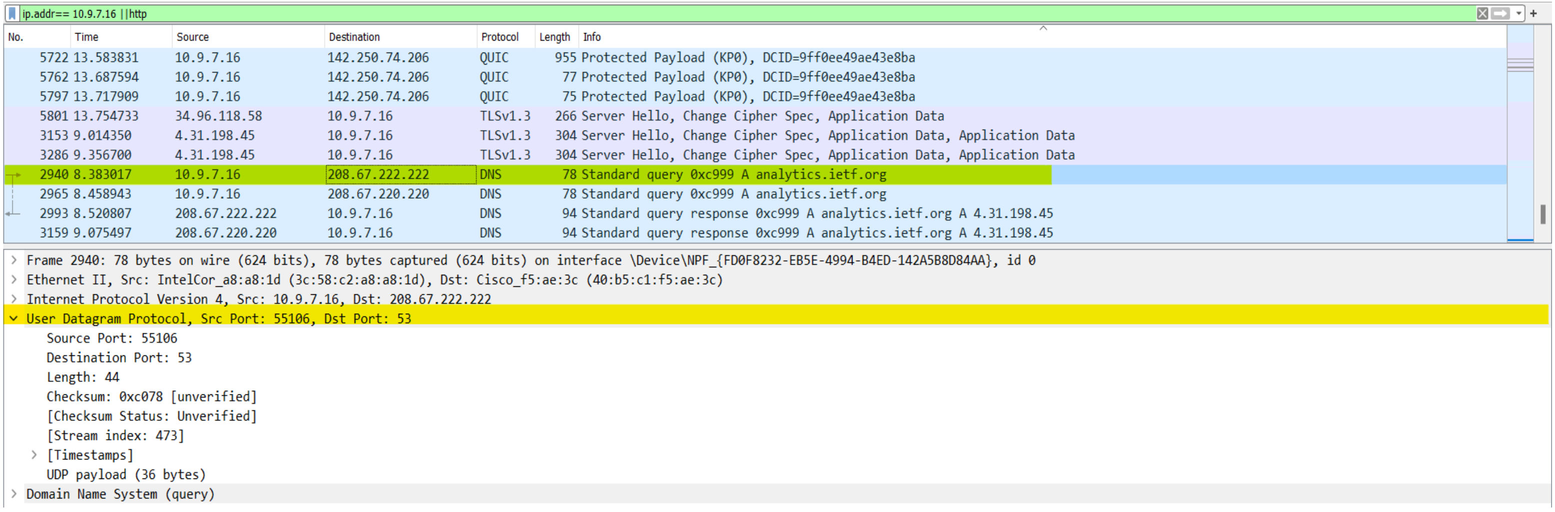
The DNS request uses UDP protocol.



```
ip.addr== 10.9.7.16 ||http

No.  Time       Source          Destination     Protocol Length Info
5722 13.583831  10.9.7.16       142.250.74.206  QUIC      955 Protected Payload (KP0), DCID=9ff0ee49ae43e8ba
5762 13.687594  10.9.7.16       142.250.74.206  QUIC       77 Protected Payload (KP0), DCID=9ff0ee49ae43e8ba
5797 13.717909  10.9.7.16       142.250.74.206  QUIC       75 Protected Payload (KP0), DCID=9ff0ee49ae43e8ba
5801 13.754733  34.96.118.58    10.9.7.16       TLSv1.3   266 Server Hello, Change Cipher Spec, Application Data
3153 9.014350   4.31.198.45     10.9.7.16       TLSv1.3   304 Server Hello, Change Cipher Spec, Application Data, Application Data
3286 9.356700   4.31.198.45     10.9.7.16       TLSv1.3   304 Server Hello, Change Cipher Spec, Application Data, Application Data
2940 8.383017   10.9.7.16       208.67.222.222  DNS        78 Standard query 0xc999 A analytics.ietf.org
2965 8.458943   10.9.7.16       208.67.220.220  DNS        78 Standard query 0xc999 A analytics.ietf.org
2993 8.520807   208.67.222.222  10.9.7.16       DNS        94 Standard query response 0xc999 A analytics.ietf.org A 4.31.198.45
3159 9.075497   208.67.220.220  10.9.7.16       DNS        94 Standard query response 0xc999 A analytics.ietf.org A 4.31.198.45

> Frame 2993: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Cisco_f5:ae:3c (40:b5:c1:f5:ae:3c), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 208.67.222.222, Dst: 10.9.7.16
v User Datagram Protocol, Src Port: 53, Dst Port: 55106
    Source Port: 53
    Destination Port: 55106
    Length: 60
    Checksum: 0x2d9c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 473]
  > [Timestamps]
    UDP payload (52 bytes)
> Domain Name System (response)
```

Q5-

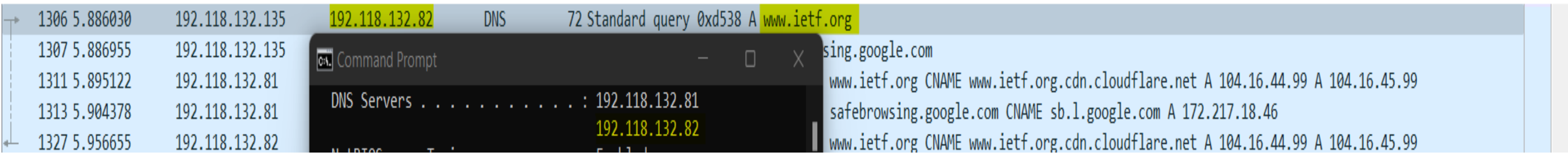
The source port is 55106, the destination port is 53.



```
ip.addr== 10.9.7.16 ||http

No.   Time       Source          Destination     Protocol Length Info
 5722 13.583831  10.9.7.16       142.250.74.206  QUIC      955 Protected Payload (KP0), DCID=9ff0ee49ae43e8ba
 5762 13.687594  10.9.7.16       142.250.74.206  QUIC       77 Protected Payload (KP0), DCID=9ff0ee49ae43e8ba
 5797 13.717909  10.9.7.16       142.250.74.206  QUIC       75 Protected Payload (KP0), DCID=9ff0ee49ae43e8ba
 5801 13.754733  34.96.118.58    10.9.7.16       TLSv1.3   266 Server Hello, Change Cipher Spec, Application Data
 3153 9.014350   4.31.198.45     10.9.7.16       TLSv1.3   304 Server Hello, Change Cipher Spec, Application Data, Application Data
 3286 9.356700   4.31.198.45     10.9.7.16       TLSv1.3   304 Server Hello, Change Cipher Spec, Application Data, Application Data
 2940 8.383017   10.9.7.16       208.67.222.222  DNS        78 Standard query 0xc999 A analytics.ietf.org
 2965 8.458943   10.9.7.16       208.67.220.220  DNS        78 Standard query 0xc999 A analytics.ietf.org
 2993 8.520807   208.67.222.222  10.9.7.16       DNS        94 Standard query response 0xc999 A analytics.ietf.org A 4.31.198.45
 3159 9.075497   208.67.220.220  10.9.7.16       DNS        94 Standard query response 0xc999 A analytics.ietf.org A 4.31.198.45

> Frame 2940: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: Cisco_f5:ae:3c (40:b5:c1:f5:ae:3c)
> Internet Protocol Version 4, Src: 10.9.7.16, Dst: 208.67.222.222
v User Datagram Protocol, Src Port: 55106, Dst Port: 53
    Source Port: 55106
    Destination Port: 53
    Length: 44
    Checksum: 0xc078 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 473]
  > [Timestamps]
    UDP payload (36 bytes)
> Domain Name System (query)
```

Q6-

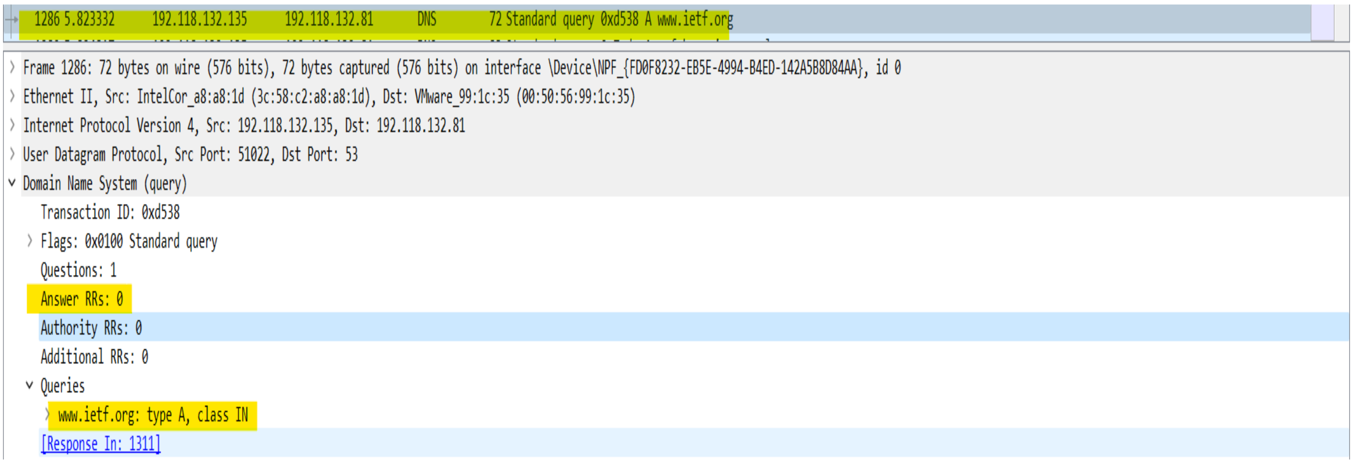
Yes, this 2 IP addresses are the same, The IP address of the DNS query is 192.118.132.82, and the message which has been sent is my local DNS server.



```
1306 5.886030  192.118.132.135  192.118.132.82  DNS  72 Standard query 0xd538 A www.ietf.org
1307 5.886955  192.118.132.135                                 sing.google.com
1311 5.895122  192.118.132.81                                   www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
1313 5.904378  192.118.132.81                                   safebrowsing.google.com CNAME sb.l.google.com A 172.217.18.46
1327 5.956655  192.118.132.82                                   www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
```

Command Prompt

```
DNS Servers . . . . . . . . . . . : 192.118.132.81
                                    192.118.132.82
```



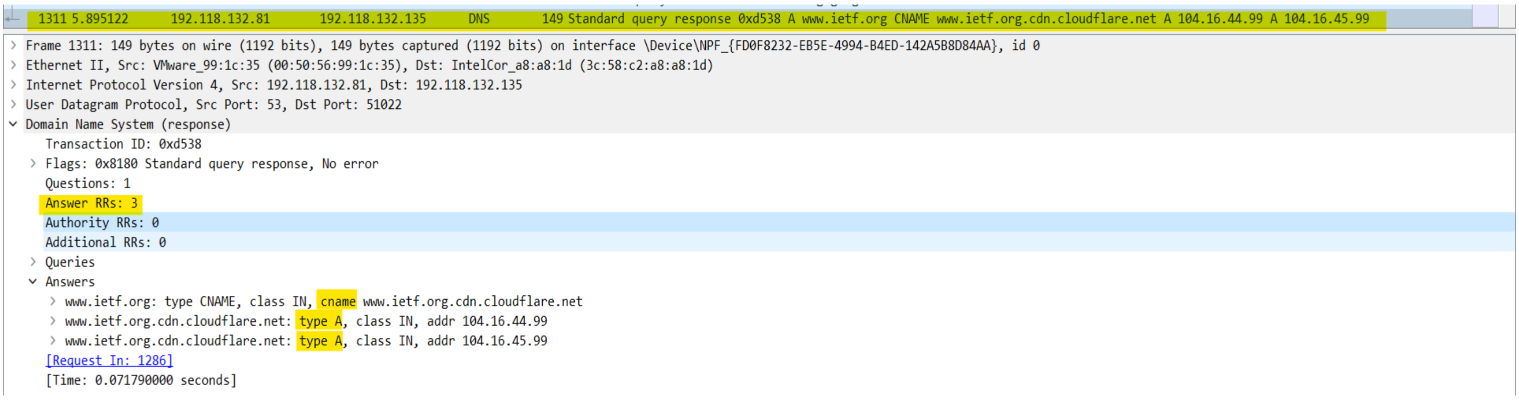
```
1286 5.823332  192.118.132.135  192.118.132.81  DNS  72 Standard query 0xd538 A www.ietf.org

> Frame 1286: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: VMware_99:1c:35 (00:50:56:99:1c:35)
> Internet Protocol Version 4, Src: 192.118.132.135, Dst: 192.118.132.81
> User Datagram Protocol, Src Port: 51022, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xd538
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 1311]
```

Q7-

The "type" of that message is "A", and this query does not contain any answers.

Q8-

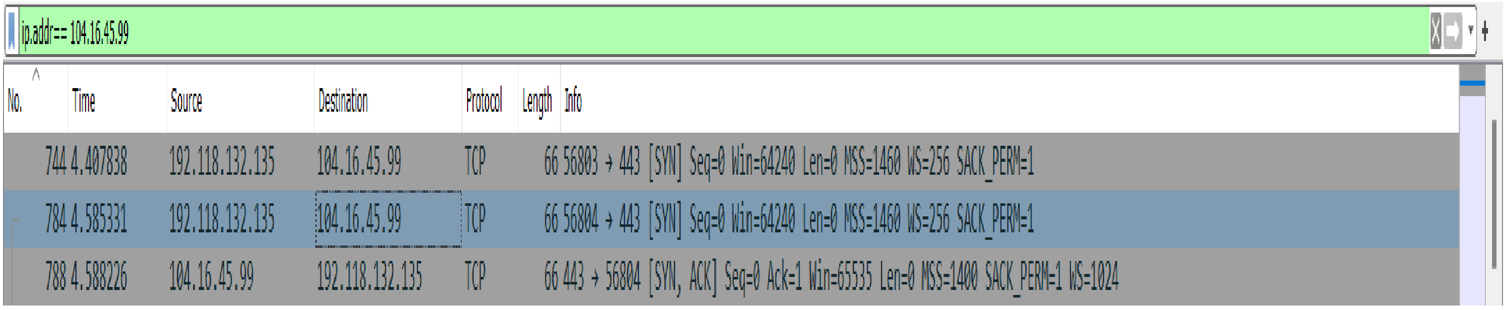
As we see in the image below there are 3 answers, 2 of them is type "A", and the third is "cname"(which contain the name of the website).



```
1311 5.895122    192.118.132.81    192.118.132.135    DNS    149 Standard query response 0xd538 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
> Frame 1311: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: VMware_99:1c:35 (00:50:56:99:1c:35), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 192.118.132.81, Dst: 192.118.132.135
> User Datagram Protocol, Src Port: 53, Dst Port: 51022
v Domain Name System (response)
    Transaction ID: 0xd538
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    [Request In: 1286]
    [Time: 0.071790000 seconds]
```

Q9-

Yes, the IP which provided is the same IP which we got from the DNS response,



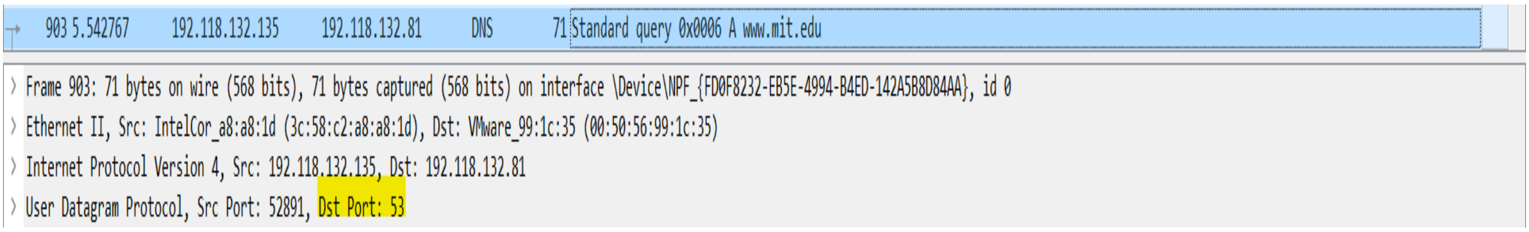
```
ip.addr== 104.16.45.99

No.   Time       Source            Destination       Protocol  Length  Info
744   4.407838   192.118.132.135   104.16.45.99      TCP       66 56803 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
784   4.585331   192.118.132.135   104.16.45.99      TCP       66 56804 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
788   4.588226   104.16.45.99      192.118.132.135   TCP       66 443 → 56804 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
```

Q10-

No, we get all of the images from the web server, and no issue new DNS queries are response.

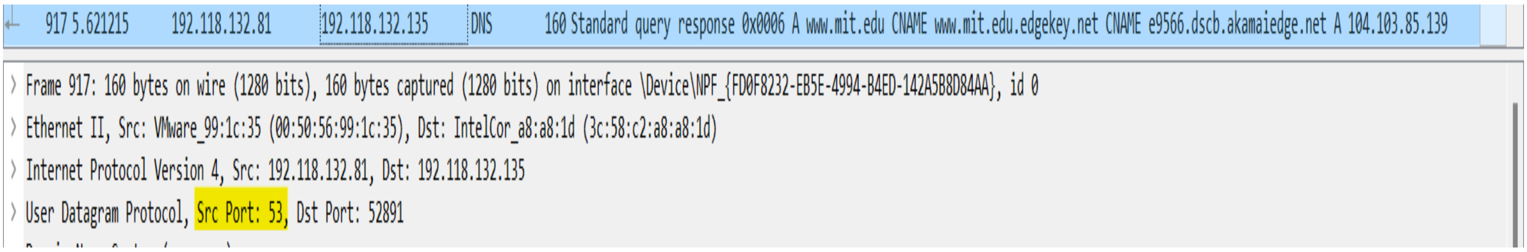
Q11-

As we can see in the image below, the destination port for the DNS query is 53.



```
903 5.542767   192.118.132.135   192.118.132.81   DNS   71 Standard query 0x0006 A www.mit.edu

> Frame 903: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: VMware_99:1c:35 (00:50:56:99:1c:35)
> Internet Protocol Version 4, Src: 192.118.132.135, Dst: 192.118.132.81
> User Datagram Protocol, Src Port: 52891, Dst Port: 53
```

And the source port of the respond DNS query is also 53.



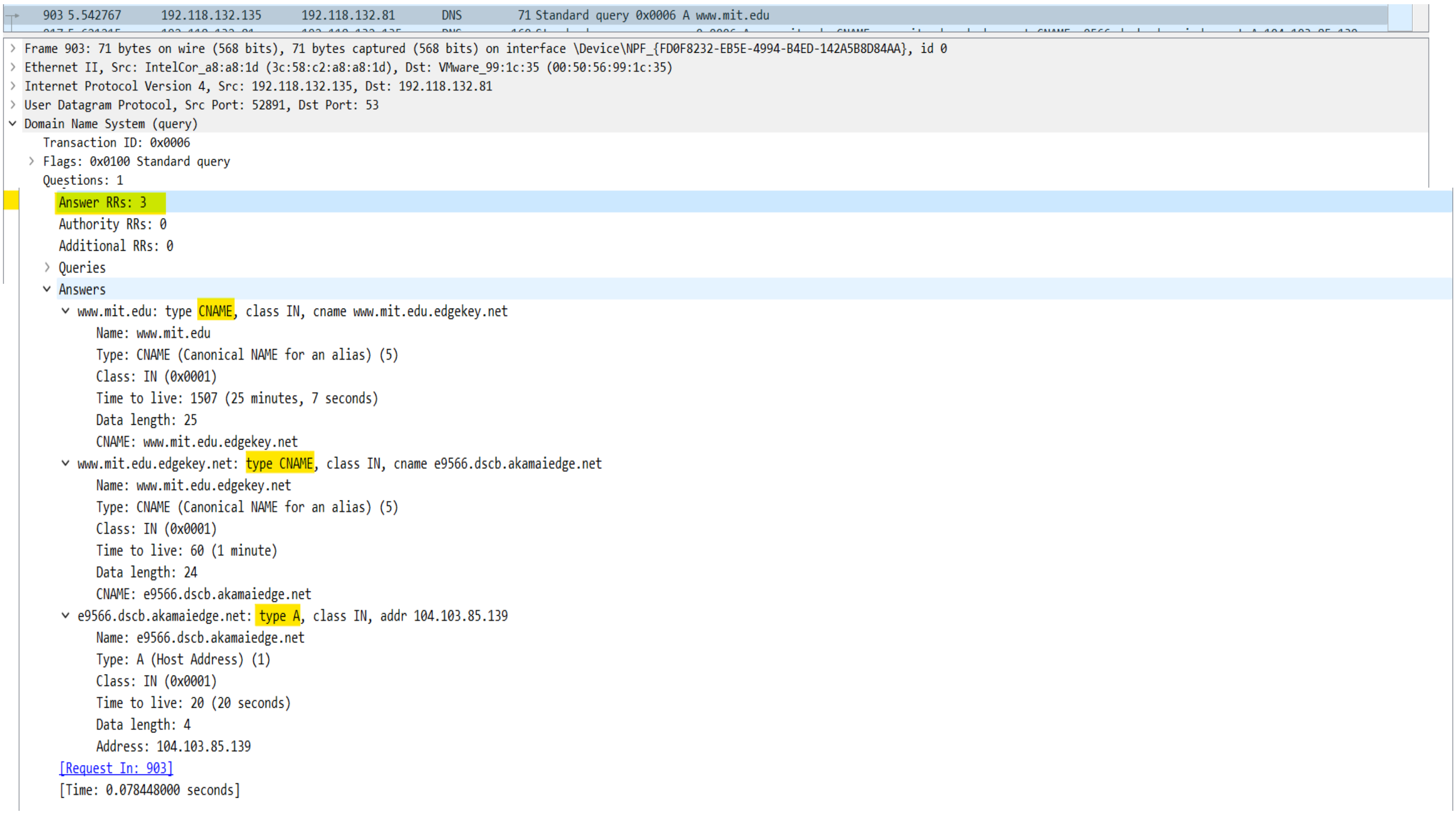
```
917 5.621215   192.118.132.81   192.118.132.135   DNS   160 Standard query response 0x0006 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.103.85.139

> Frame 917: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: VMware_99:1c:35 (00:50:56:99:1c:35), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 192.118.132.81, Dst: 192.118.132.135
> User Datagram Protocol, Src Port: 53, Dst Port: 52891
```

Q12-

The IP address of the DNS query that sent is 192.118.132.81, and this is my local DNS IP.

Q13-

The type of the DNS query is "A" and there are no answers.



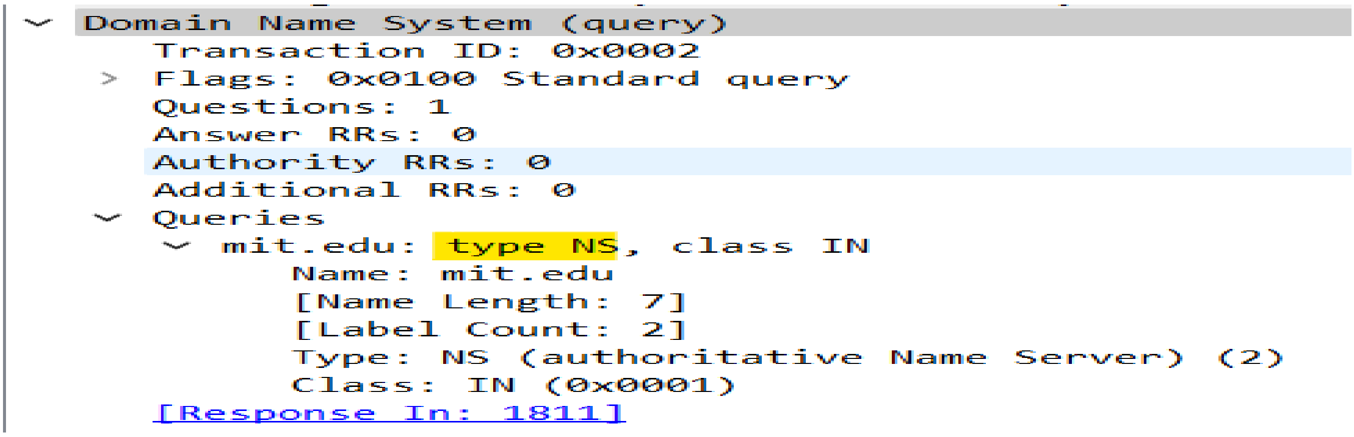
```
903 5.542767      192.118.132.135      192.118.132.81      DNS      71 Standard query 0x0006 A www.mit.edu
> Frame 903: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: VMware_99:1c:35 (00:50:56:99:1c:35)
> Internet Protocol Version 4, Src: 192.118.132.135, Dst: 192.118.132.81
> User Datagram Protocol, Src Port: 52891, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0006
  > Flags: 0x0100 Standard query
    Questions: 1
      Answer RRs: 3
      Authority RRs: 0
      Additional RRs: 0
    > Queries
    v Answers
      v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
            Name: www.mit.edu
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 1507 (25 minutes, 7 seconds)
            Data length: 25
            CNAME: www.mit.edu.edgekey.net
      v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
            Name: www.mit.edu.edgekey.net
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 60 (1 minute)
            Data length: 24
            CNAME: e9566.dscb.akamaiedge.net
      v e9566.dscb.akamaiedge.net: type A, class IN, addr 104.103.85.139
            Name: e9566.dscb.akamaiedge.net
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 20 (20 seconds)
            Data length: 4
            Address: 104.103.85.139
      [Request In: 903]
      [Time: 0.078448000 seconds]
```

Q14-

As we can see in the image below there are 3 answers to the query and 2 of them are type "CName" and the last one is type "A".

Q16-

The IP address of the DNS query that sent is 192.118.132.81, and this is my local DNS IP.



```
⌄ Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    ⌄ mit.edu: type NS, class IN
          Name: mit.edu
          [Name Length: 7]
          [Label Count: 2]
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
    [Response In: 1811]
```

Q17-

The type of the DNS query is "NS" type.

Q18-

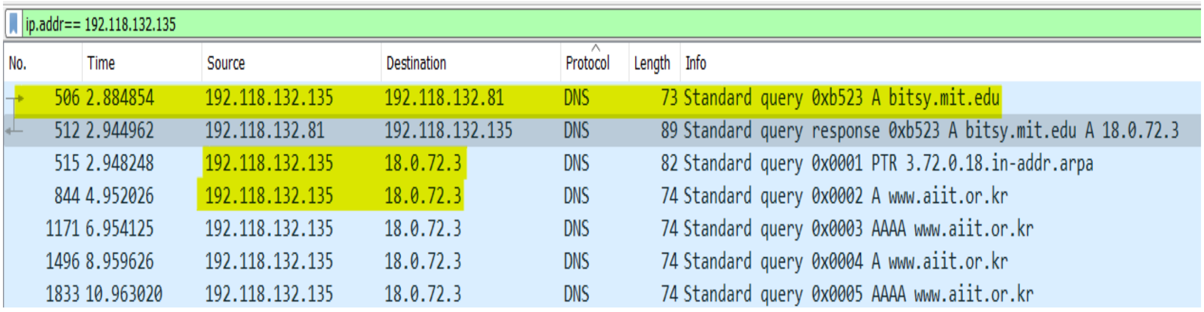
As we can see in the image below I got the nameservers and I got the IP of each of them.

In addition I got extra 3 IP which is IPV6.

<u>Q20-</u>

Bitsy.mit.edu- the message that sent to this website is sent to my local DNS server.

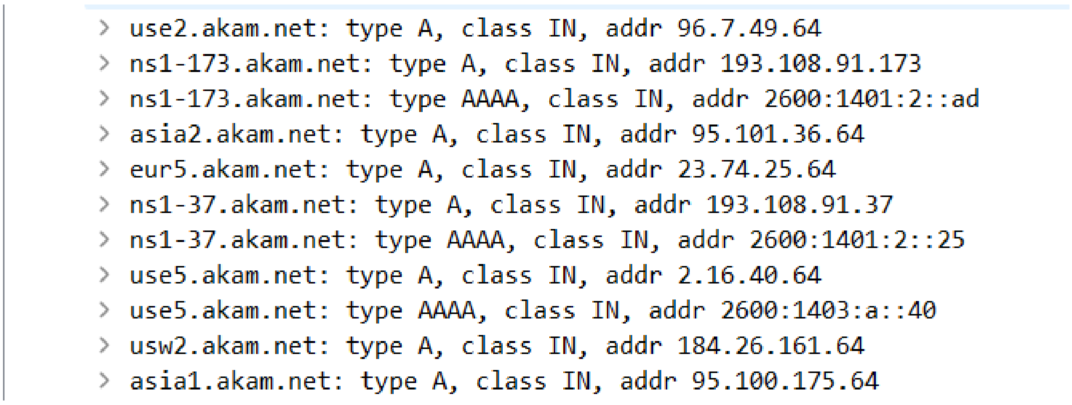
aiit.or.kr- the message that sent to this website sent to different IP address which is 18.0.72.3.



ip.addr== 192.118.132.135

No.	Time	Source	Destination	Protocol	Length	Info
506	2.884854	192.118.132.135	192.118.132.81	DNS	73	Standard query 0xb523 A bitsy.mit.edu
512	2.944962	192.118.132.81	192.118.132.135	DNS	89	Standard query response 0xb523 A bitsy.mit.edu A 18.0.72.3
515	2.948248	192.118.132.135	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
844	4.952026	192.118.132.135	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
1171	6.954125	192.118.132.135	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
1496	8.959626	192.118.132.135	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
1833	10.963020	192.118.132.135	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

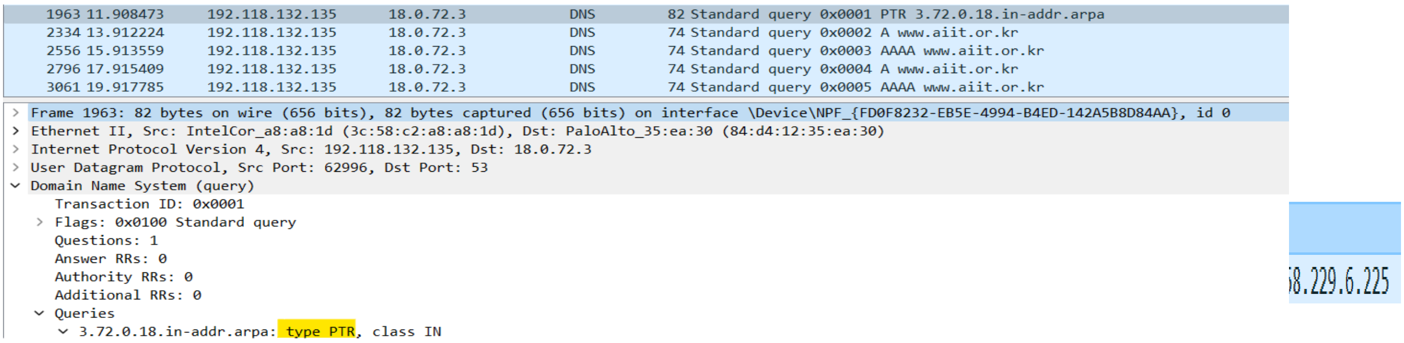
When I used this two IP together, the aiit.or.kr wasn’t response to my local DNS server, but when I changed bitsy.mit.edu to google's primary DNS server (8.8.8.8) I got my local DNS server.



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

aiit.or.kr is not responding.

aiit.or.kr is responding.



```
1963 11.908473   192.118.132.135   18.0.72.3   DNS   82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
2334 13.912224   192.118.132.135   18.0.72.3   DNS   74 Standard query 0x0002 A www.aiit.or.kr
2556 15.913559   192.118.132.135   18.0.72.3   DNS   74 Standard query 0x0003 AAAA www.aiit.or.kr
2796 17.915409   192.118.132.135   18.0.72.3   DNS   74 Standard query 0x0004 A www.aiit.or.kr
3061 19.917785   192.118.132.135   18.0.72.3   DNS   74 Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 1963: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: PaloAlto_35:ea:30 (84:d4:12:35:ea:30)
> Internet Protocol Version 4, Src: 192.118.132.135, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 62996, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 3.72.0.18.in-addr.arpa: type PTR, class IN
```

Q21-

As we can see in the image below the type of the query is PTR and does not contain any answers.

Q22-

There are no responses from aiit.or.kr because the this query doesn't sent to my local DNS servers.