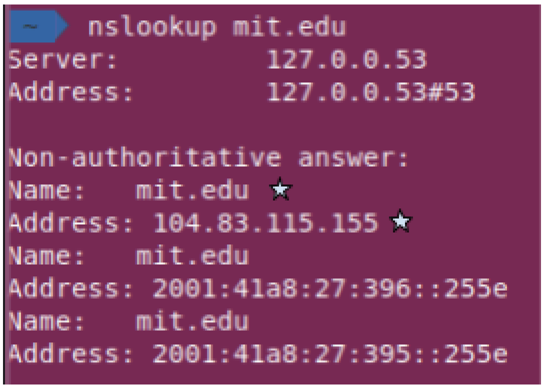
150116884 - Esra Polat

CSE4074 Homework 2

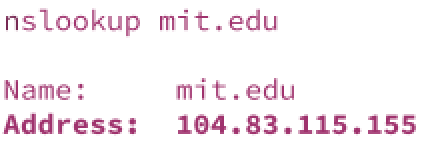
Wireshark Lab: DNS Solutions

1. nslookup

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

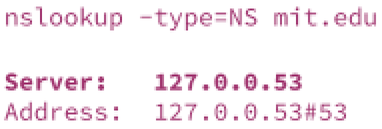


```
 ~  nslookup mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mit.edu ☆
Address: 104.83.115.155 ☆
Name:   mit.edu
Address: 2001:41a8:27:396::255e
Name:   mit.edu
Address: 2001:41a8:27:395::255e
```

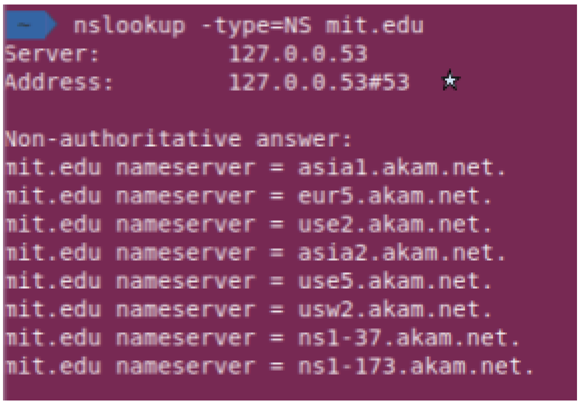


```
nslookup mit.edu

Name:      mit.edu
Address:   104.83.115.155
```

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

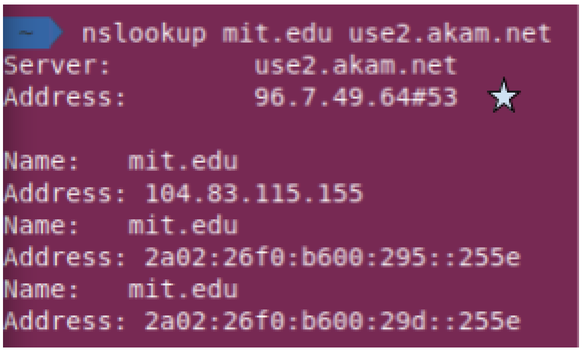


```
nslookup -type=NS mit.edu

Server:    127.0.0.53
Address:   127.0.0.53#53
```

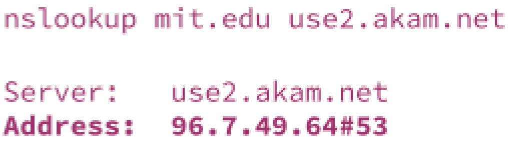


```
 ~  nslookup -type=NS mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53   ☆

Non-authoritative answer:
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = ns1-173.akam.net.
```

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?



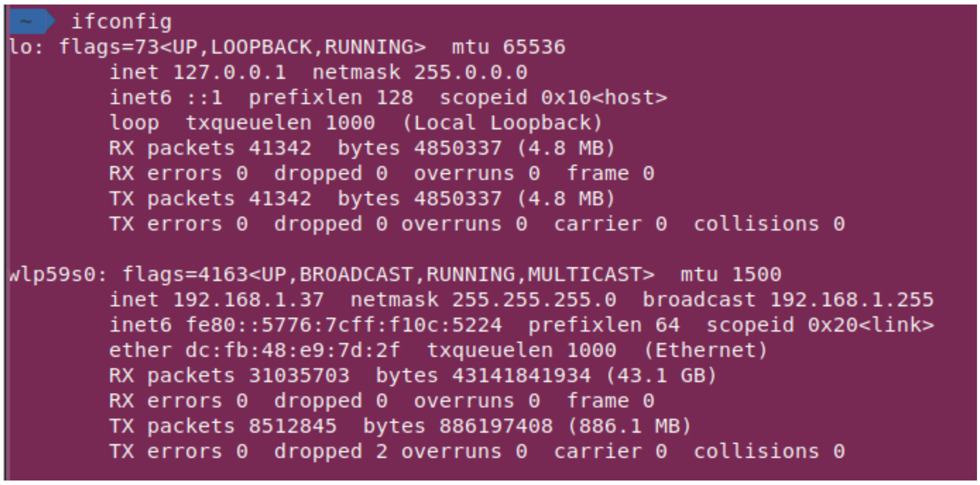
```
 ~  nslookup mit.edu use2.akam.net
Server:         use2.akam.net
Address:        96.7.49.64#53  ☆

Name:   mit.edu
Address: 104.83.115.155
Name:   mit.edu
Address: 2a02:26f0:b600:295::255e
Name:   mit.edu
Address: 2a02:26f0:b600:29d::255e
```



```
nslookup mit.edu use2.akam.net

Server:    use2.akam.net
Address:   96.7.49.64#53
```

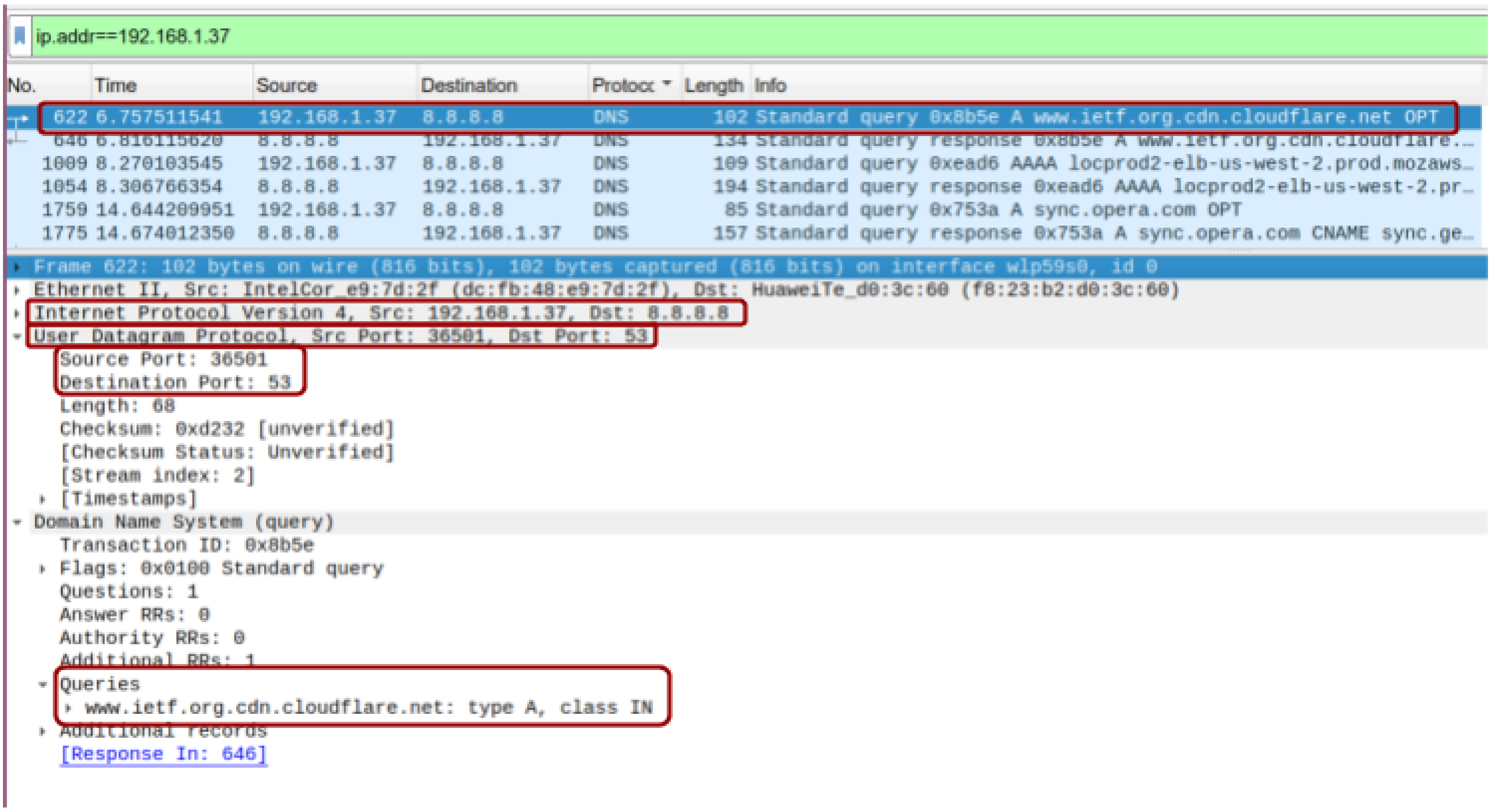
2. ifconfig

I use Linux Ubuntu. Therefore, I will use "ifconfig" in this homework.



```
 ~  ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 41342  bytes 4850337 (4.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41342  bytes 4850337 (4.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp59s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.37  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::5776:7cff:f10c:5224  prefixlen 64  scopeid 0x20<link>
        ether dc:fb:48:e9:7d:2f  txqueuelen 1000  (Ethernet)
        RX packets 31035703  bytes 43141841934 (43.1 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8512845  bytes 886197408 (886.1 MB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0
```

3. Tracing DNS with Wireshark



```
ip.addr==192.168.1.37

No.   Time          Source         Destination    Protocol Length Info
  622 6.757511541   192.168.1.37   8.8.8.8        DNS      102 Standard query 0x8b5e A www.ietf.org.cdn.cloudflare.net OPT
  646 6.816115620   8.8.8.8        192.168.1.37   DNS      134 Standard query response 0x8b5e A www.ietf.org.cdn.cloudflare.…
 1009 8.270103545   192.168.1.37   8.8.8.8        DNS      109 Standard query 0xead6 AAAA locprod2-elb-us-west-2.prod.mozaws…
 1054 8.306766354   8.8.8.8        192.168.1.37   DNS      194 Standard query response 0xead6 AAAA locprod2-elb-us-west-2.pr…
 1759 14.644209951  192.168.1.37   8.8.8.8        DNS       85 Standard query 0x753a A sync.opera.com OPT
 1775 14.674012350  8.8.8.8        192.168.1.37   DNS      157 Standard query response 0x753a A sync.opera.com CNAME sync.ge…

▸ Frame 622: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f), Dst: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60)
▸ Internet Protocol Version 4, Src: 192.168.1.37, Dst: 8.8.8.8
▾ User Datagram Protocol, Src Port: 36501, Dst Port: 53
    Source Port: 36501
    Destination Port: 53
    Length: 68
    Checksum: 0xd232 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  ▸ [Timestamps]
▾ Domain Name System (query)
    Transaction ID: 0x8b5e
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN
  ▸ Additional records
    [Response In: 646]
```

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

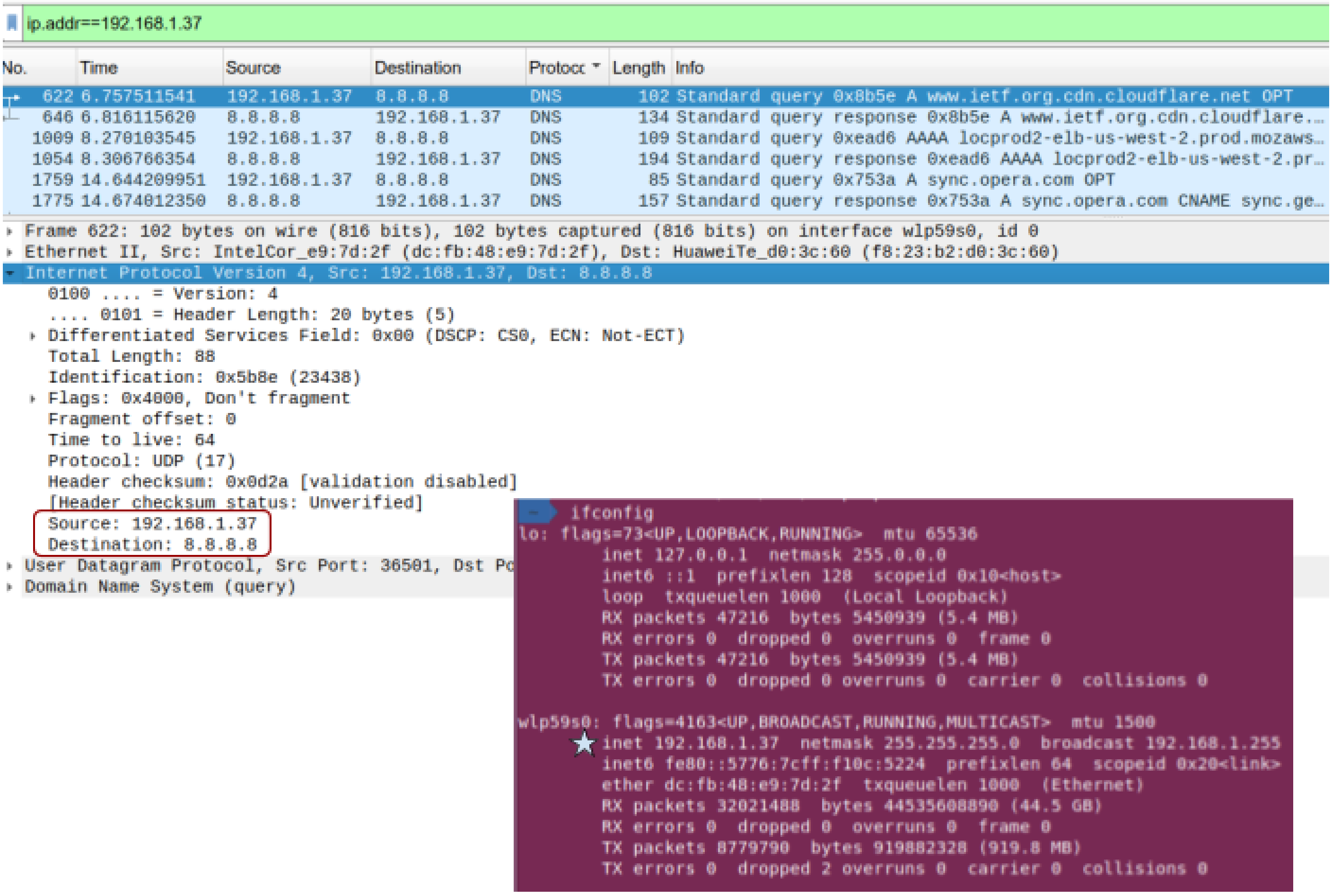
They are sent over UDP.

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

The destination port is port 53, and the source port is port 36501.

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?

It’s sent to 192.168.1.37, which is the IP address of one of my local DNS servers.



```
ip.addr==192.168.1.37

No.   Time         Source         Destination    Protocc  Length Info
  622 6.757511541  192.168.1.37   8.8.8.8        DNS         102 Standard query 0x8b5e A www.ietf.org.cdn.cloudflare.net OPT
  646 6.816115620  8.8.8.8        192.168.1.37   DNS         134 Standard query response 0x8b5e A www.ietf.org.cdn.cloudflare.…
 1009 8.270103545  192.168.1.37   8.8.8.8        DNS         109 Standard query 0xead6 AAAA locprod2-elb-us-west-2.prod.mozaws…
 1054 8.306766354  8.8.8.8        192.168.1.37   DNS         194 Standard query response 0xead6 AAAA locprod2-elb-us-west-2.pr…
 1759 14.644209951 192.168.1.37   8.8.8.8        DNS          85 Standard query 0x753a A sync.opera.com OPT
 1775 14.674012350 8.8.8.8        192.168.1.37   DNS         157 Standard query response 0x753a A sync.opera.com CNAME sync.ge…

▸ Frame 622: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f), Dst: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60)
▾ Internet Protocol Version 4, Src: 192.168.1.37, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 88
    Identification: 0x5b8e (23438)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x0d2a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.37
    Destination: 8.8.8.8
▸ User Datagram Protocol, Src Port: 36501, Dst Po
▸ Domain Name System (query)
```

```
~ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 47216  bytes 5450939 (5.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47216  bytes 5450939 (5.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp59s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      ★ inet 192.168.1.37  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::5776:7cff:f10c:5224  prefixlen 64  scopeid 0x20<link>
        ether dc:fb:48:e9:7d:2f  txqueuelen 1000  (Ethernet)
        RX packets 32021488  bytes 44535608890 (44.5 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8779790  bytes 919882328 (919.8 MB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0
```

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

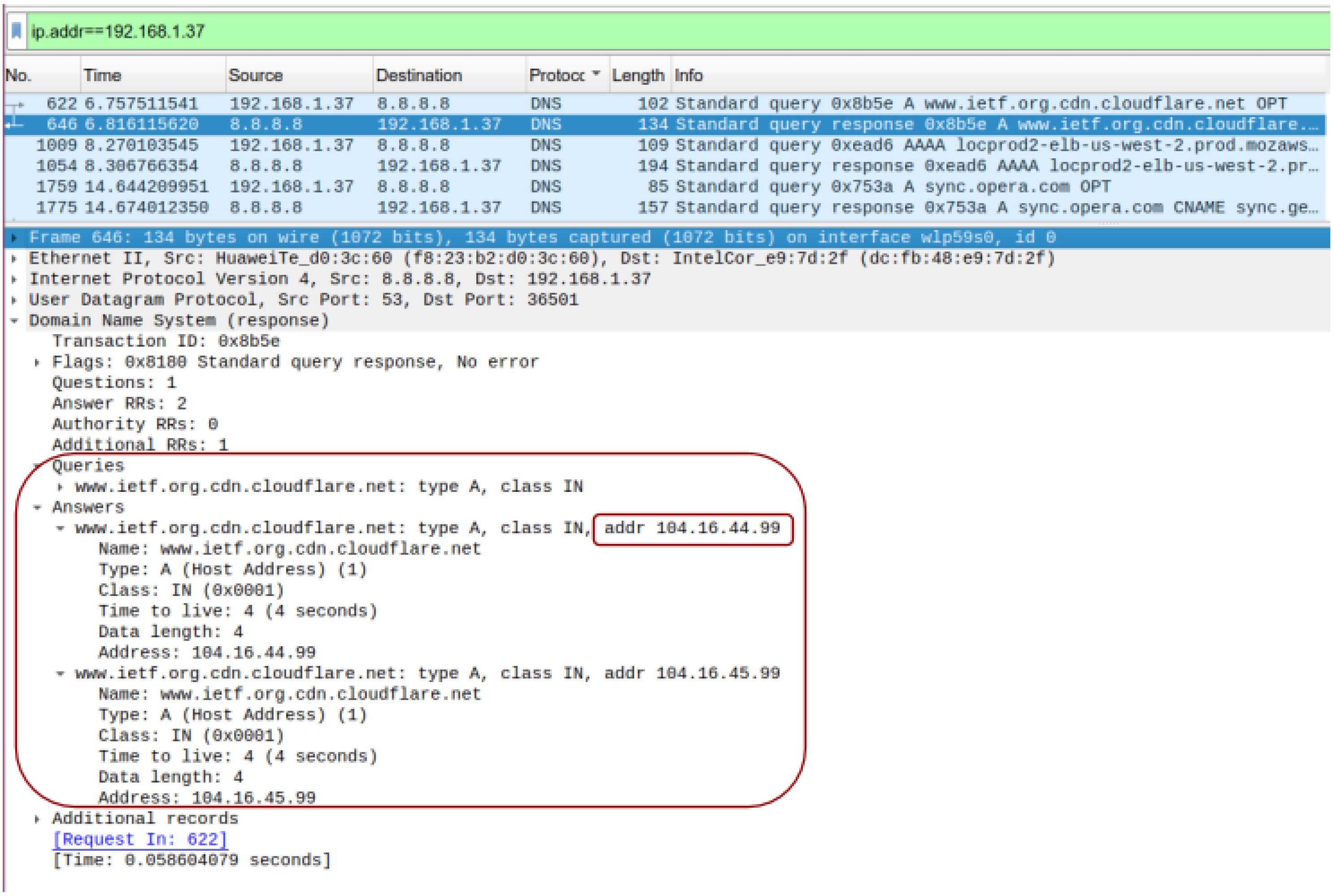
This query was a type A query. It did not contain any “answers”.

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

There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.

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

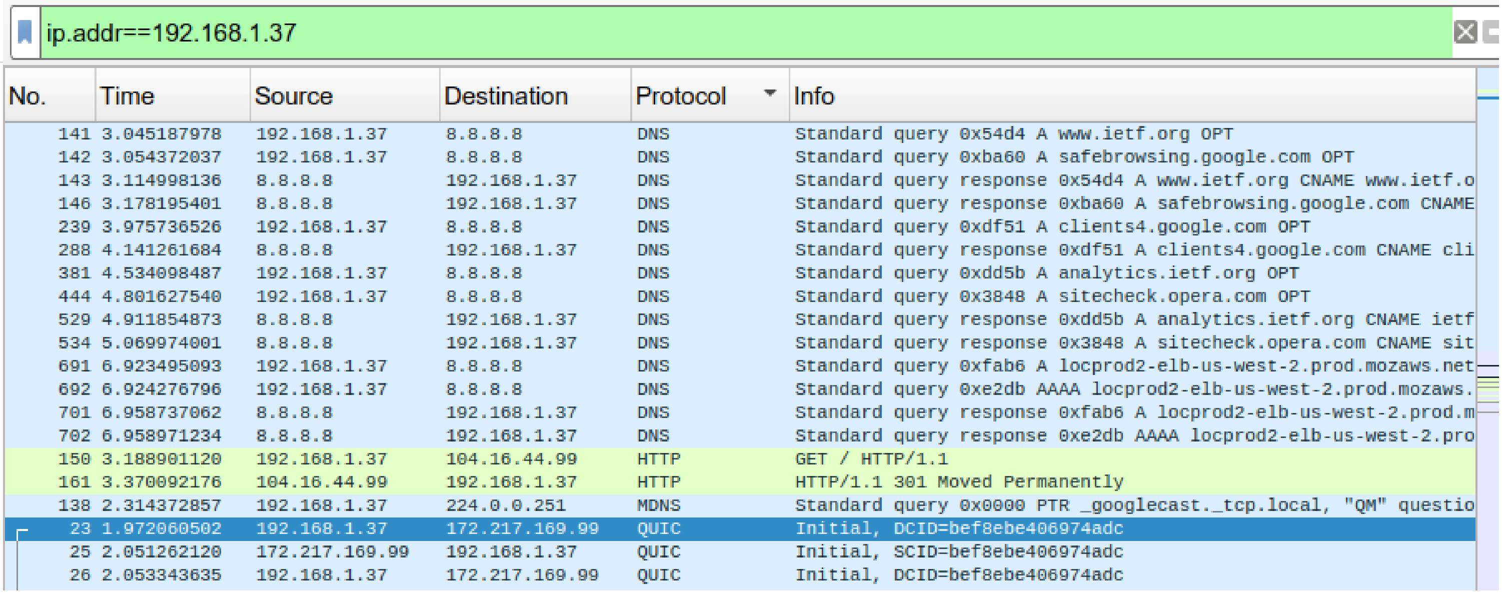
Yes, the destination IP address of the SYN packet corresponds to the address provided by the DNS response, 104.16.45.99.



```
ip.addr==192.168.1.37

No.   Time          Source         Destination    Protocc  Length Info
  622 6.757511541   192.168.1.37   8.8.8.8        DNS      102 Standard query 0x8b5e A www.ietf.org.cdn.cloudflare.net OPT
  646 6.816115620   8.8.8.8        192.168.1.37   DNS      134 Standard query response 0x8b5e A www.ietf.org.cdn.cloudflare.…
 1009 8.270103545   192.168.1.37   8.8.8.8        DNS      109 Standard query 0xead6 AAAA locprod2-elb-us-west-2.prod.mozaws…
 1054 8.306766354   8.8.8.8        192.168.1.37   DNS      194 Standard query response 0xead6 AAAA locprod2-elb-us-west-2.pr…
 1759 14.644209951  192.168.1.37   8.8.8.8        DNS       85 Standard query 0x753a A sync.opera.com OPT
 1775 14.674012350  8.8.8.8        192.168.1.37   DNS      157 Standard query response 0x753a A sync.opera.com CNAME sync.ge…

▸ Frame 646: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60), Dst: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.37
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36501
▾ Domain Name System (response)
    Transaction ID: 0x8b5e
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN
  ▾ Answers
    ▾ 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: 4 (4 seconds)
        Data length: 4
        Address: 104.16.44.99
    ▾ 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: 4 (4 seconds)
        Data length: 4
        Address: 104.16.45.99
  ▸ Additional records
    [Request In: 622]
    [Time: 0.058604079 seconds]
```

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

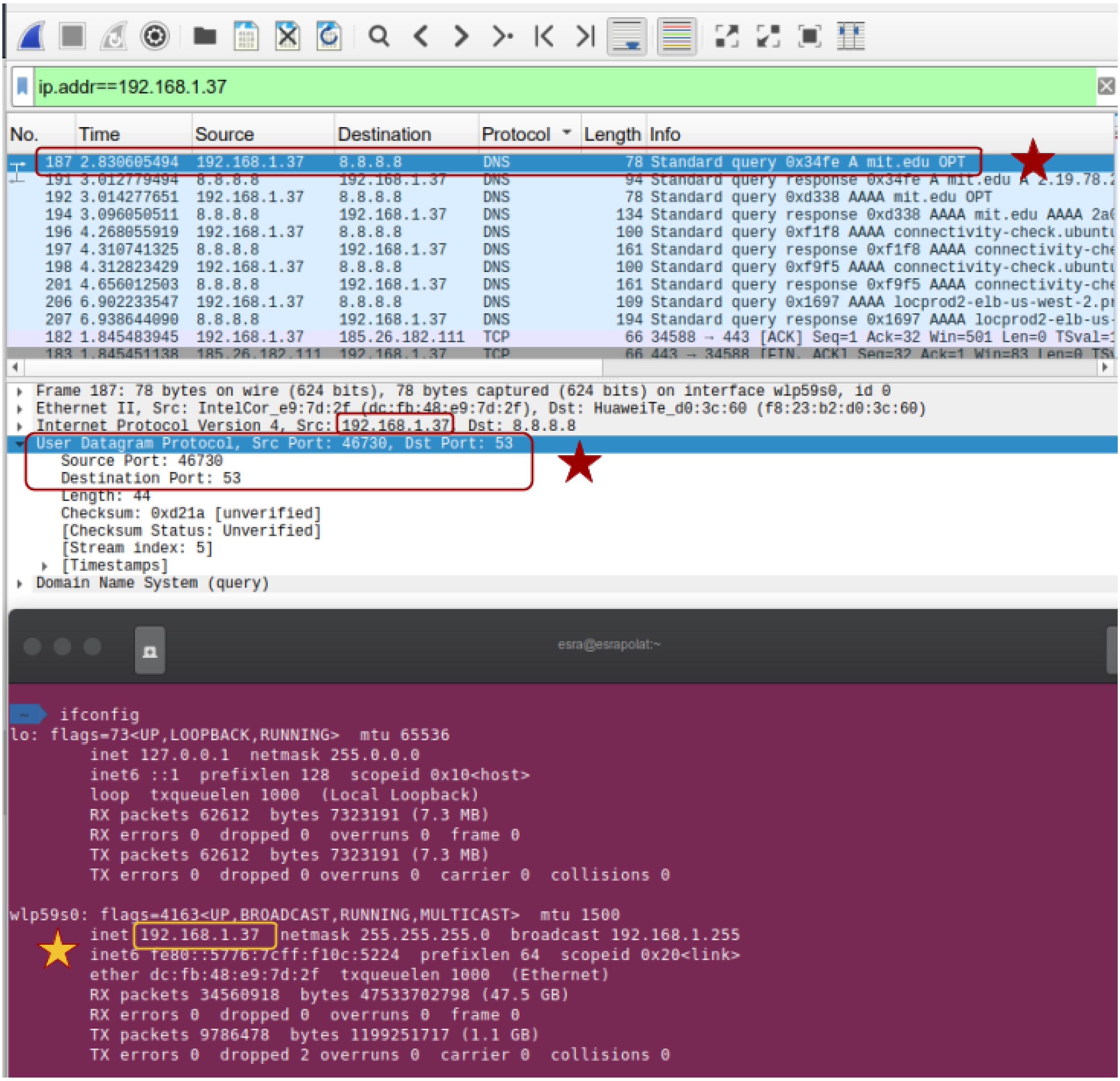
No, the host issues new DNS queries for each image.



```
ip.addr==192.168.1.37

No.   Time          Source          Destination     Protocol   Info
  141 3.045187978   192.168.1.37    8.8.8.8         DNS        Standard query 0x54d4 A www.ietf.org OPT
  142 3.054372037   192.168.1.37    8.8.8.8         DNS        Standard query 0xba60 A safebrowsing.google.com OPT
  143 3.114998136   8.8.8.8         192.168.1.37    DNS        Standard query response 0x54d4 A www.ietf.org CNAME www.ietf.o
  146 3.178195401   8.8.8.8         192.168.1.37    DNS        Standard query response 0xba60 A safebrowsing.google.com CNAME
  239 3.975736526   192.168.1.37    8.8.8.8         DNS        Standard query 0xdf51 A clients4.google.com OPT
  288 4.141261684   8.8.8.8         192.168.1.37    DNS        Standard query response 0xdf51 A clients4.google.com CNAME cli
  381 4.534098487   192.168.1.37    8.8.8.8         DNS        Standard query 0xdd5b A analytics.ietf.org OPT
  444 4.801627540   192.168.1.37    8.8.8.8         DNS        Standard query 0x3848 A sitecheck.opera.com OPT
  529 4.911854873   8.8.8.8         192.168.1.37    DNS        Standard query response 0xdd5b A analytics.ietf.org CNAME ietf
  534 5.069974001   8.8.8.8         192.168.1.37    DNS        Standard query response 0x3848 A sitecheck.opera.com CNAME sit
  691 6.923495093   192.168.1.37    8.8.8.8         DNS        Standard query 0xfab6 A locprod2-elb-us-west-2.prod.mozaws.net
  692 6.924276796   192.168.1.37    8.8.8.8         DNS        Standard query 0xe2db AAAA locprod2-elb-us-west-2.prod.mozaws.
  701 6.958737062   8.8.8.8         192.168.1.37    DNS        Standard query response 0xfab6 A locprod2-elb-us-west-2.prod.m
  702 6.958971234   8.8.8.8         192.168.1.37    DNS        Standard query response 0xe2db AAAA locprod2-elb-us-west-2.pro
  150 3.188901120   192.168.1.37    104.16.44.99    HTTP       GET / HTTP/1.1
  161 3.370092176   104.16.44.99    192.168.1.37    HTTP       HTTP/1.1 301 Moved Permanently
  138 2.314372857   192.168.1.37    224.0.0.251     MDNS       Standard query 0x0000 PTR _googlecast._tcp.local, "QM" questio
   23 1.972060502   192.168.1.37    172.217.169.99  QUIC       Initial, DCID=bef8ebe406974adc
   25 2.051262120   172.217.169.99  192.168.1.37    QUIC       Initial, SCID=bef8ebe406974adc
   26 2.053343635   192.168.1.37    172.217.169.99  QUIC       Initial, DCID=bef8ebe406974adc
```

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

The destination port is 53 and the source port is 46730.



```
No.  Time         Source          Destination     Protocol  Length Info
 187 2.830605494  192.168.1.37    8.8.8.8         DNS           78 Standard query 0x34fe A mit.edu OPT
 191 3.012779494  8.8.8.8         192.168.1.37    DNS           94 Standard query response 0x34fe A mit.edu A 2.19.78.2
 192 3.014277651  192.168.1.37    8.8.8.8         DNS           78 Standard query 0xd338 AAAA mit.edu OPT
 194 3.096050511  8.8.8.8         192.168.1.37    DNS          134 Standard query response 0xd338 AAAA mit.edu AAAA 2a(
 196 4.268055919  192.168.1.37    8.8.8.8         DNS          100 Standard query 0xf1f8 AAAA connectivity-check.ubuntu
 197 4.310741325  8.8.8.8         192.168.1.37    DNS          161 Standard query response 0xf1f8 AAAA connectivity-che
 198 4.312823429  192.168.1.37    8.8.8.8         DNS          100 Standard query 0xf9f5 AAAA connectivity-check.ubuntu
 201 4.656012503  8.8.8.8         192.168.1.37    DNS          161 Standard query response 0xf9f5 AAAA connectivity-che
 206 6.902233547  192.168.1.37    8.8.8.8         DNS          109 Standard query 0x1697 AAAA locprod2-elb-us-west-2.pr
 207 6.938644090  8.8.8.8         192.168.1.37    DNS          194 Standard query response 0x1697 AAAA locprod2-elb-us-
 182 1.845483945  192.168.1.37    185.26.182.111  TCP           66 34588 → 443 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=1
 183 1.845451138  185.26.182.111  192.168.1.37    TCP           66 443 → 34588 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0 TSv
```

```
▸ Frame 187: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f), Dst: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60)
▸ Internet Protocol Version 4, Src: 192.168.1.37, Dst: 8.8.8.8
▾ User Datagram Protocol, Src Port: 46730, Dst Port: 53
    Source Port: 46730
    Destination Port: 53
    Length: 44
    Checksum: 0xd21a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  ▸ [Timestamps]
▸ Domain Name System (query)
```

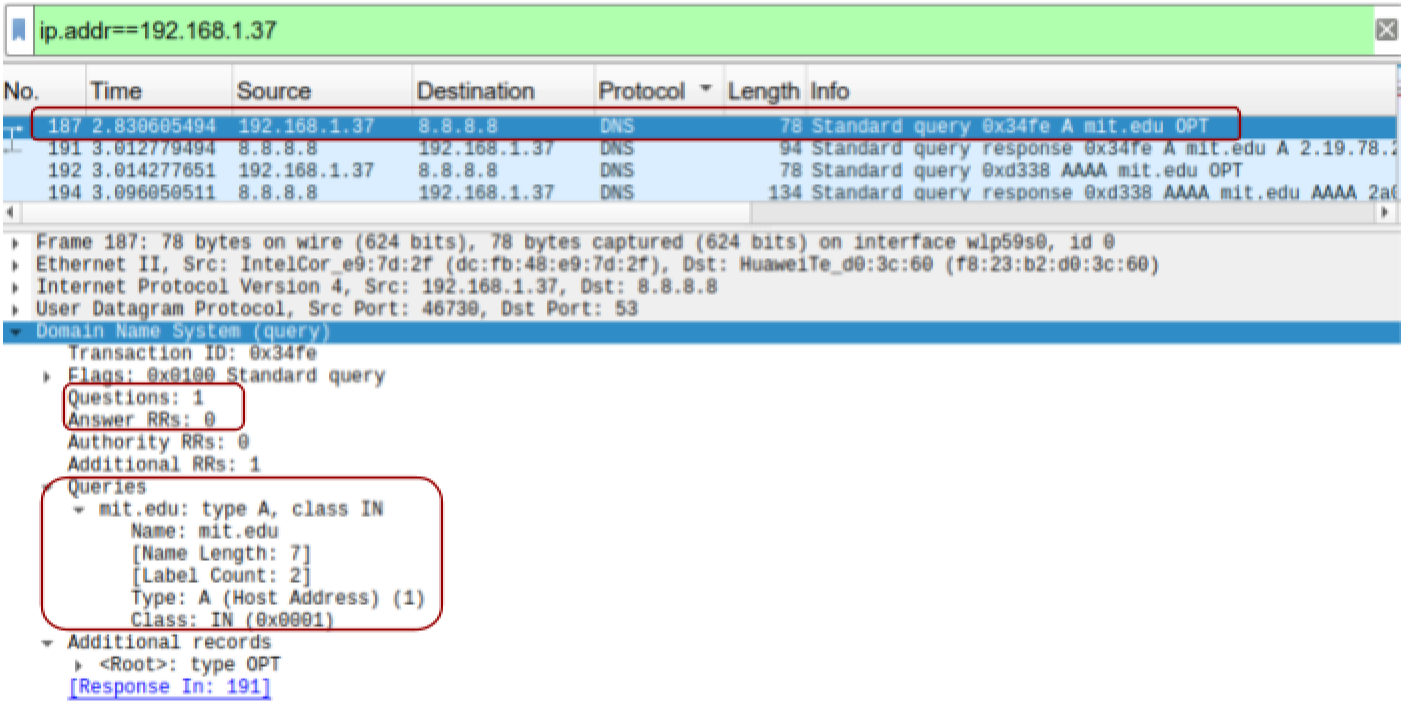
```
~  ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 62612  bytes 7323191 (7.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62612  bytes 7323191 (7.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp59s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.37  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::5776:7cff:f10c:5224  prefixlen 64  scopeid 0x20<link>
        ether dc:fb:48:e9:7d:2f  txqueuelen 1000  (Ethernet)
        RX packets 34560918  bytes 47533702798 (47.5 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9786478  bytes 1199251717 (1.1 GB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0
```

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

It's sent to 192.168.1.37 which as we can see from the ifconfig screenshot is 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”?

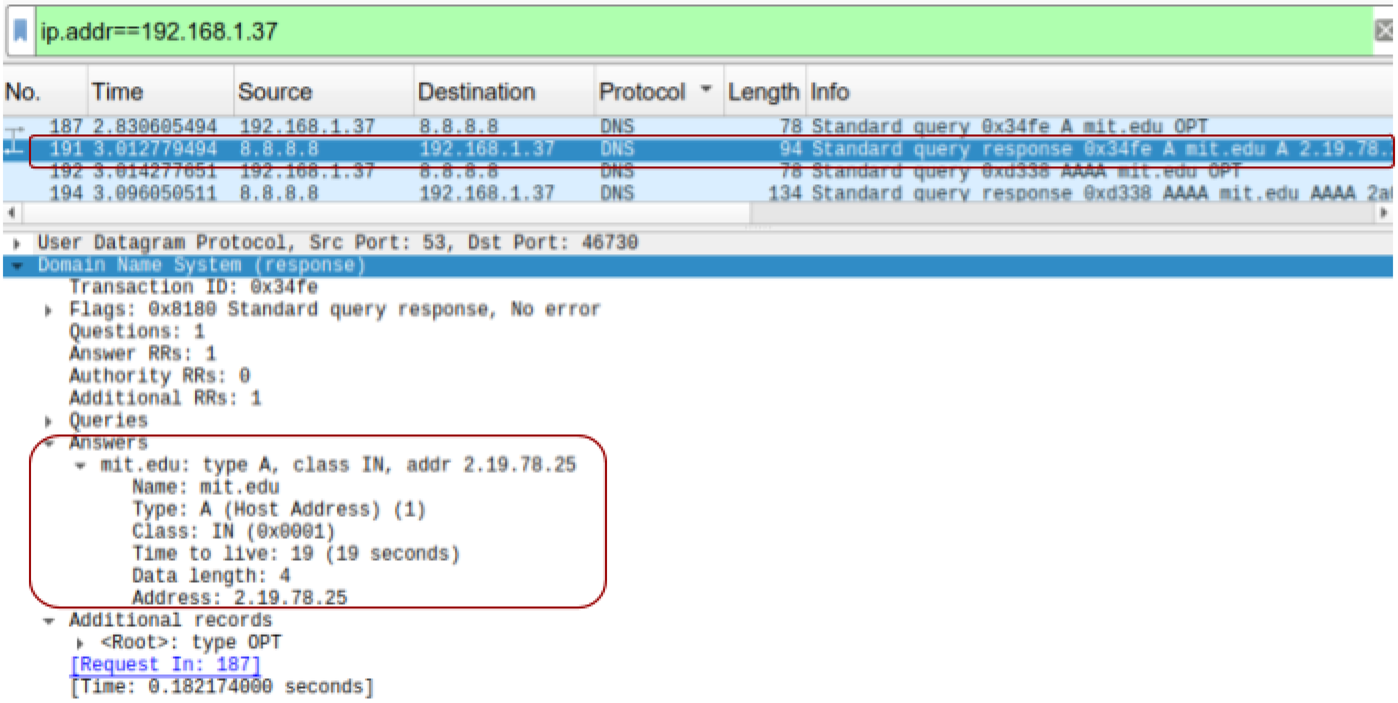
The DNS query message is a type “A” query, containing only one question and not containing any answers.



```
ip.addr==192.168.1.37

No.  Time         Source        Destination   Protocol  Length Info
 187 2.830605494  192.168.1.37  8.8.8.8       DNS           78 Standard query 0x34fe A mit.edu OPT
 191 3.012779494  8.8.8.8       192.168.1.37  DNS           94 Standard query response 0x34fe A mit.edu A 2.19.78.
 192 3.014277651  192.168.1.37  8.8.8.8       DNS           78 Standard query 0xd338 AAAA mit.edu OPT
 194 3.096050511  8.8.8.8       192.168.1.37  DNS          134 Standard query response 0xd338 AAAA mit.edu AAAA 2a

▸ Frame 187: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f), Dst: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60)
▸ Internet Protocol Version 4, Src: 192.168.1.37, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 46730, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x34fe
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ mit.edu: type A, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Additional records
    ▸ <Root>: type OPT
    [Response In: 191]
```

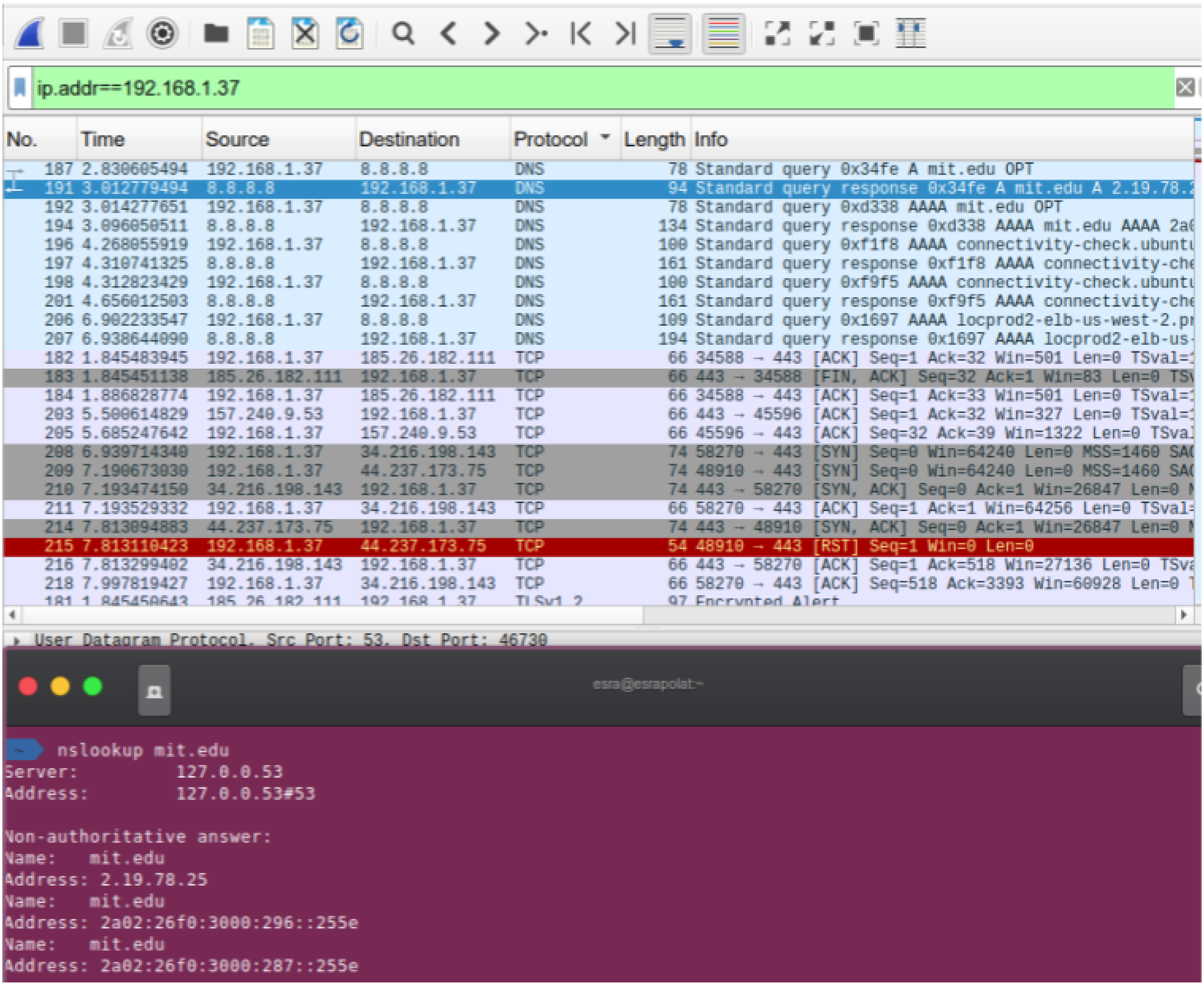
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

The first DNS response message contains one answer. This answer contains the next DNS server to query en route to mit.edu.



```
ip.addr==192.168.1.37

No.  Time         Source        Destination   Protocol  Length Info
 187 2.830605494  192.168.1.37  8.8.8.8       DNS           78 Standard query 0x34fe A mit.edu OPT
 191 3.012779494  8.8.8.8       192.168.1.37  DNS           94 Standard query response 0x34fe A mit.edu A 2.19.78.
 192 3.014277651  192.168.1.37  8.8.8.8       DNS           78 Standard query 0xd338 AAAA mit.edu OPT
 194 3.096050511  8.8.8.8       192.168.1.37  DNS          134 Standard query response 0xd338 AAAA mit.edu AAAA 2a

▸ User Datagram Protocol, Src Port: 53, Dst Port: 46730
▾ Domain Name System (response)
    Transaction ID: 0x34fe
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▾ mit.edu: type A, class IN, addr 2.19.78.25
        Name: mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 19 (19 seconds)
        Data length: 4
        Address: 2.19.78.25
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 187]
    [Time: 0.182174000 seconds]
```

15. Provide a screenshot.



ip.addr==192.168.1.37

```
No.  Time         Source          Destination     Protocol  Length Info
 187 2.830605494  192.168.1.37    8.8.8.8         DNS         78 Standard query 0x34fe A mit.edu OPT
 191 3.012779494  8.8.8.8         192.168.1.37    DNS         94 Standard query response 0x34fe A mit.edu A 2.19.78.2
 192 3.014277651  192.168.1.37    8.8.8.8         DNS         78 Standard query 0xd338 AAAA mit.edu OPT
 194 3.096050511  8.8.8.8         192.168.1.37    DNS        134 Standard query response 0xd338 AAAA mit.edu AAAA 2a0
 196 4.268055919  192.168.1.37    8.8.8.8         DNS        100 Standard query 0xf1f8 AAAA connectivity-check.ubuntu
 197 4.310741325  8.8.8.8         192.168.1.37    DNS        161 Standard query response 0xf1f8 AAAA connectivity-che
 198 4.312823429  192.168.1.37    8.8.8.8         DNS        100 Standard query 0xf9f5 AAAA connectivity-check.ubuntu
 201 4.656012503  8.8.8.8         192.168.1.37    DNS        161 Standard query response 0xf9f5 AAAA connectivity-che
 206 6.902233547  192.168.1.37    8.8.8.8         DNS        109 Standard query 0x1697 AAAA locprod2-elb-us-west-2.pr
 207 6.938644090  8.8.8.8         192.168.1.37    DNS        194 Standard query response 0x1697 AAAA locprod2-elb-us-
 182 1.845483945  192.168.1.37    185.26.182.111  TCP         66 34588 → 443 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=1
 183 1.845451138  185.26.182.111  192.168.1.37    TCP         66 443 → 34588 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0 TSv
 184 1.886828774  192.168.1.37    185.26.182.111  TCP         66 34588 → 443 [ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=1
 203 5.500614829  157.240.9.53    192.168.1.37    TCP         66 443 → 45596 [ACK] Seq=1 Ack=32 Win=327 Len=0 TSval=1
 205 5.685247642  192.168.1.37    157.240.9.53    TCP         66 45596 → 443 [ACK] Seq=32 Ack=39 Win=1322 Len=0 TSval
 208 6.939714340  192.168.1.37    34.216.198.143  TCP         74 58270 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
 209 7.190673030  192.168.1.37    44.237.173.75   TCP         74 48910 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
 210 7.193474150  34.216.198.143  192.168.1.37    TCP         74 443 → 58270 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 M
 211 7.193529332  192.168.1.37    34.216.198.143  TCP         66 58270 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
 214 7.813094883  44.237.173.75   192.168.1.37    TCP         74 443 → 48910 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 M
 215 7.813110423  192.168.1.37    44.237.173.75   TCP         54 48910 → 443 [RST] Seq=1 Win=0 Len=0
 216 7.813299402  34.216.198.143  192.168.1.37    TCP         66 443 → 58270 [ACK] Seq=1 Ack=518 Win=27136 Len=0 TSva
 218 7.997819427  192.168.1.37    34.216.198.143  TCP         66 58270 → 443 [ACK] Seq=518 Ack=3393 Win=60928 Len=0 T
 181 1.845450643  185.26.182.111  192.168.1.37    TLSv1.2     97 Encrypted Alert
```

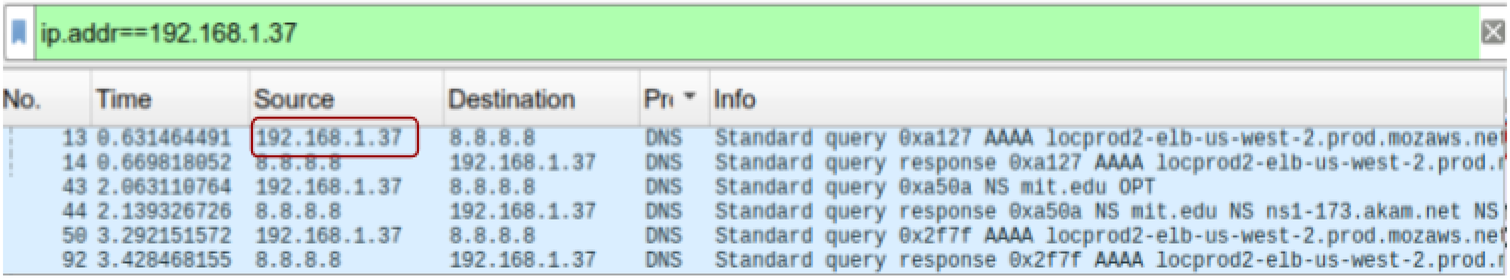
```
▸ User Datagram Protocol, Src Port: 53, Dst Port: 46730
```

esra@esrapolat:~

```
~ nslookup mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mit.edu
Address: 2.19.78.25
Name:   mit.edu
Address: 2a02:26f0:3000:296::255e
Name:   mit.edu
Address: 2a02:26f0:3000:287::255e
```

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

It's sent to 192.168.1.37 which as we can see from the ifconfig screenshot is my default local DNS server.



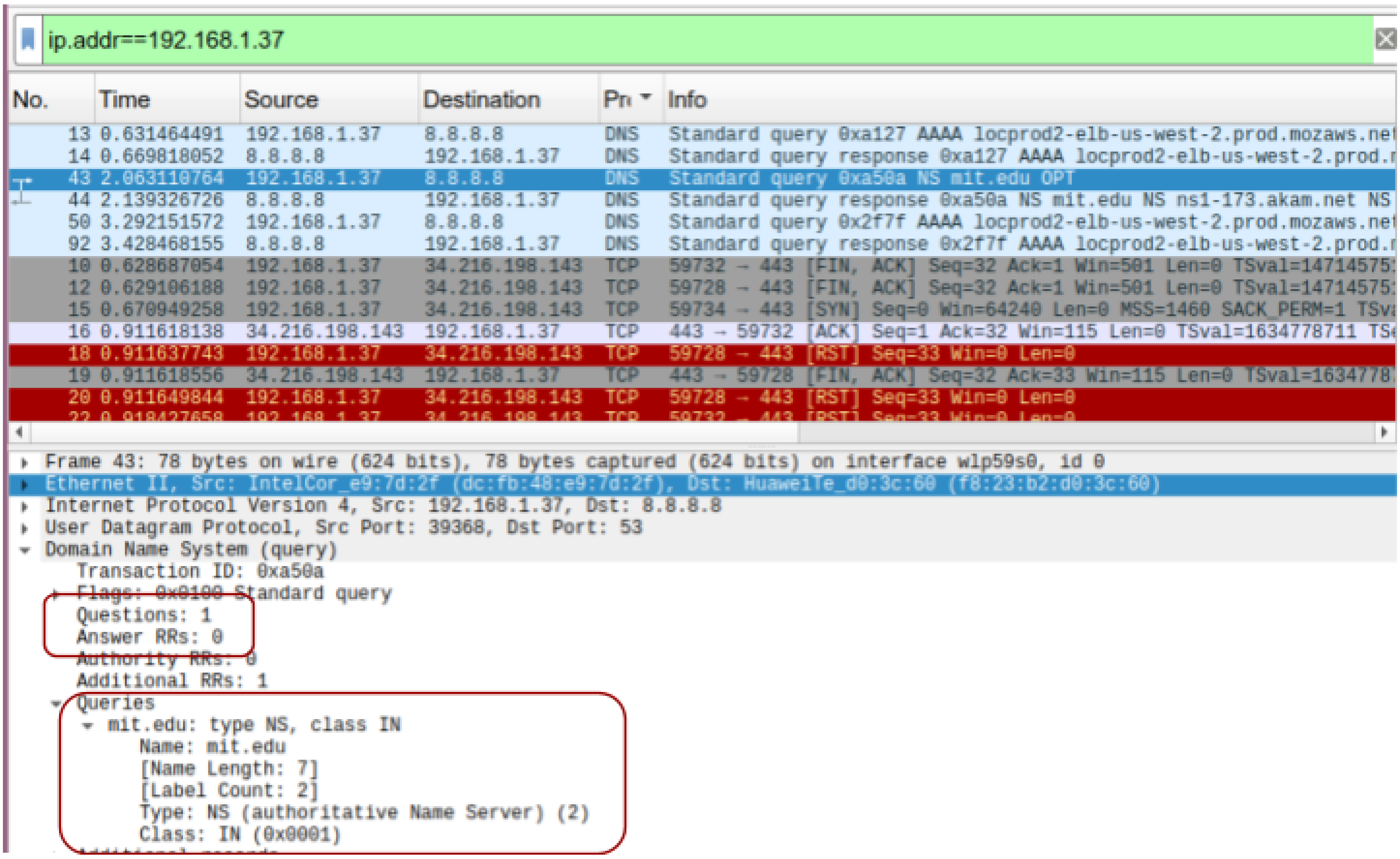
ip.addr==192.168.1.37

```
No.  Time         Source        Destination   Pr  Info
  13 0.631464491  192.168.1.37  8.8.8.8       DNS Standard query 0xa127 AAAA locprod2-elb-us-west-2.prod.mozaws.ne
  14 0.669818052  8.8.8.8       192.168.1.37  DNS Standard query response 0xa127 AAAA locprod2-elb-us-west-2.prod.r
  43 2.063110764  192.168.1.37  8.8.8.8       DNS Standard query 0xa50a NS mit.edu OPT
  44 2.139326726  8.8.8.8       192.168.1.37  DNS Standard query response 0xa50a NS mit.edu NS ns1-173.akam.net NS
  50 3.292151572  192.168.1.37  8.8.8.8       DNS Standard query 0x2f7f AAAA locprod2-elb-us-west-2.prod.mozaws.ne
  92 3.428468155  8.8.8.8       192.168.1.37  DNS Standard query response 0x2f7f AAAA locprod2-elb-us-west-2.prod.r
```

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

The DNS query is a type “NS” message including one question.

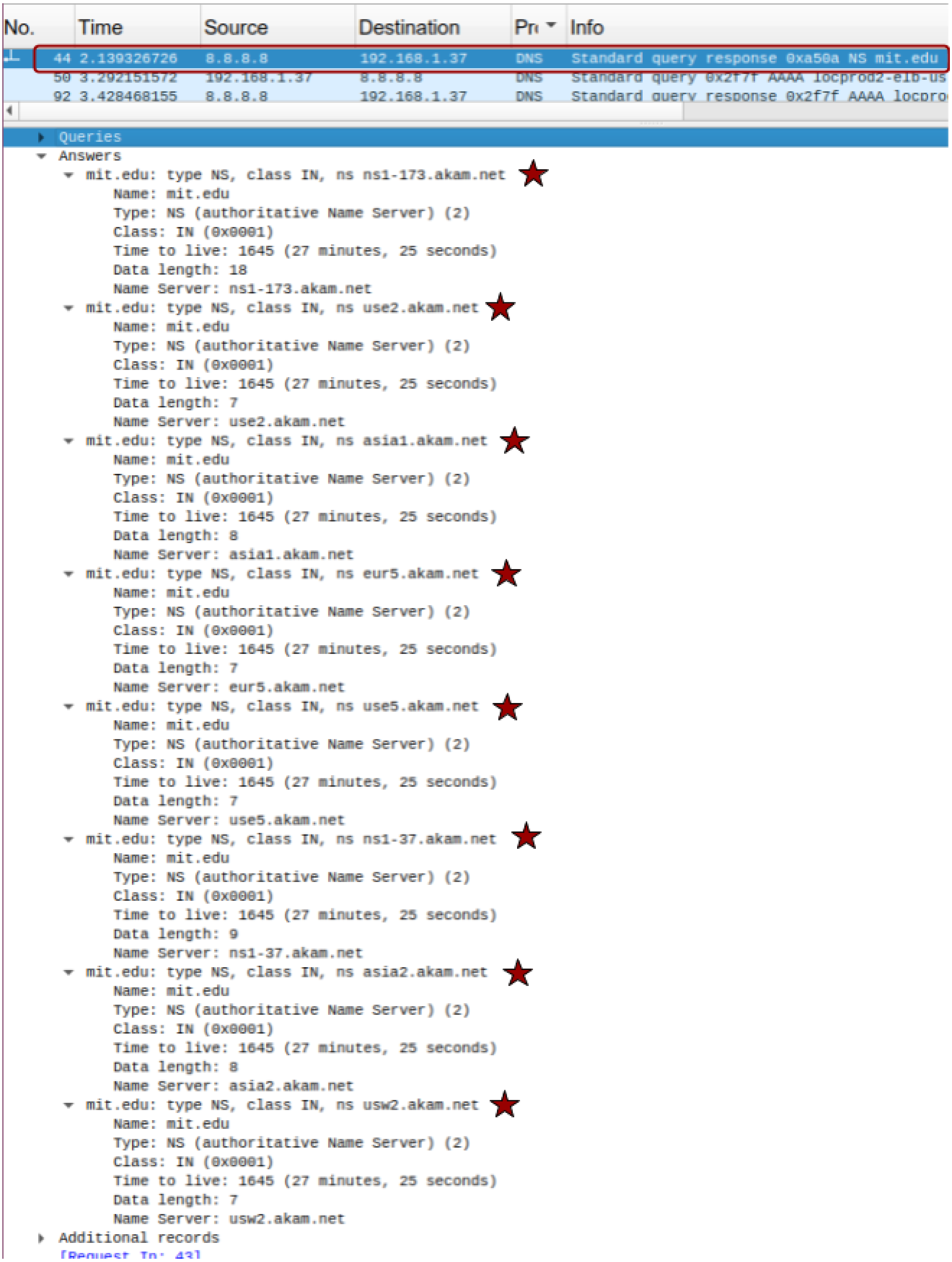
The query message did not contain any answers.



```
ip.addr==192.168.1.37

No.  Time         Source          Destination     Pr  Info
  13 0.631464491  192.168.1.37    8.8.8.8         DNS Standard query 0xa127 AAAA locprod2-elb-us-west-2.prod.mozaws.ne
  14 0.669818052  8.8.8.8         192.168.1.37    DNS Standard query response 0xa127 AAAA locprod2-elb-us-west-2.prod.
  43 2.063110764  192.168.1.37    8.8.8.8         DNS Standard query 0xa50a NS mit.edu OPT
  44 2.139326726  8.8.8.8         192.168.1.37    DNS Standard query response 0xa50a NS mit.edu NS ns1-173.akam.net NS
  50 3.292151572  192.168.1.37    8.8.8.8         DNS Standard query 0x2f7f AAAA locprod2-elb-us-west-2.prod.mozaws.ne
  92 3.428468155  8.8.8.8         192.168.1.37    DNS Standard query response 0x2f7f AAAA locprod2-elb-us-west-2.prod.
  10 0.628687054  192.168.1.37    34.216.198.143  TCP 59732 → 443 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0 TSval=14714575
  12 0.629106188  192.168.1.37    34.216.198.143  TCP 59728 → 443 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0 TSval=14714575
  15 0.670949258  192.168.1.37    34.216.198.143  TCP 59734 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSv
  16 0.911618138  34.216.198.143  192.168.1.37    TCP 443 → 59732 [ACK] Seq=1 Ack=32 Win=115 Len=0 TSval=1634778711 TS
  18 0.911637743  192.168.1.37    34.216.198.143  TCP 59728 → 443 [RST] Seq=33 Win=0 Len=0
  19 0.911618556  34.216.198.143  192.168.1.37    TCP 443 → 59728 [FIN, ACK] Seq=32 Ack=33 Win=115 Len=0 TSval=1634778
  20 0.911649844  192.168.1.37    34.216.198.143  TCP 59728 → 443 [RST] Seq=33 Win=0 Len=0
  22 0.918427658  192.168.1.37    34.216.198.143  TCP 59732 → 443 [RST] Seq=33 Win=0 Len=0

▸ Frame 43: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f), Dst: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60)
▸ Internet Protocol Version 4, Src: 192.168.1.37, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 39368, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xa50a
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ 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)
```

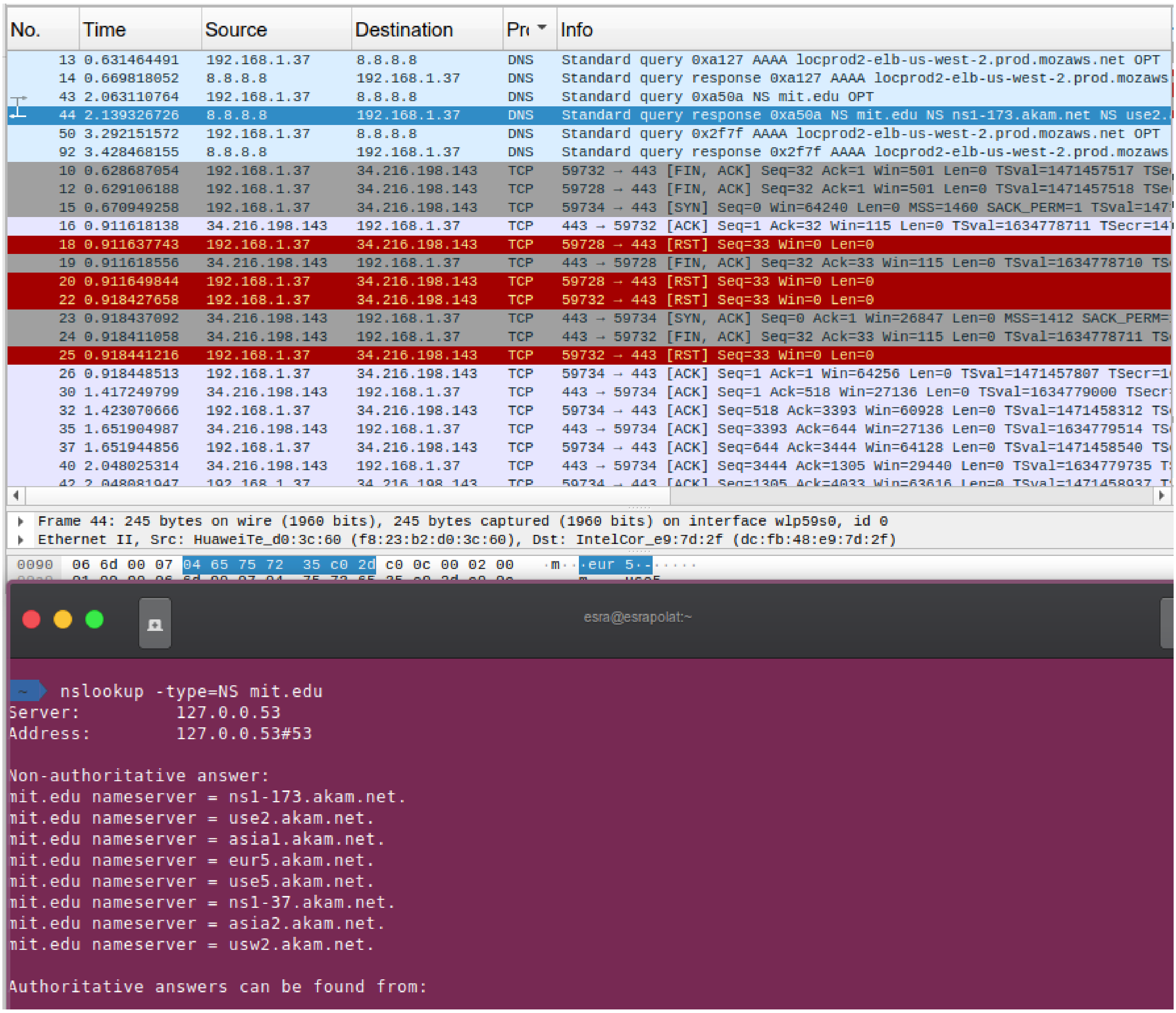
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

It provides mit.edu 8 times for different name servers.



```
No.   Time         Source        Destination   Pr  Info
   44 2.139326726  8.8.8.8       192.168.1.37  DNS Standard query response 0xa50a NS mit.edu
   50 3.292151572  192.168.1.37  8.8.8.8       DNS Standard query 0x2f7f AAAA locprod2-elb-us
   92 3.428468155  8.8.8.8       192.168.1.37  DNS Standard query response 0x2f7f AAAA locpro

  ▸ Queries
  ▾ Answers
    ▾ mit.edu: type NS, class IN, ns ns1-173.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 18
        Name Server: ns1-173.akam.net
    ▾ mit.edu: type NS, class IN, ns use2.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 7
        Name Server: use2.akam.net
    ▾ mit.edu: type NS, class IN, ns asia1.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 8
        Name Server: asia1.akam.net
    ▾ mit.edu: type NS, class IN, ns eur5.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 7
        Name Server: eur5.akam.net
    ▾ mit.edu: type NS, class IN, ns use5.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 7
        Name Server: use5.akam.net
    ▾ mit.edu: type NS, class IN, ns ns1-37.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 9
        Name Server: ns1-37.akam.net
    ▾ mit.edu: type NS, class IN, ns asia2.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 8
        Name Server: asia2.akam.net
    ▾ mit.edu: type NS, class IN, ns usw2.akam.net ★
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1645 (27 minutes, 25 seconds)
        Data length: 7
        Name Server: usw2.akam.net
  ▸ Additional records
    [Request In: 43]
```

19. Provide a screenshot.



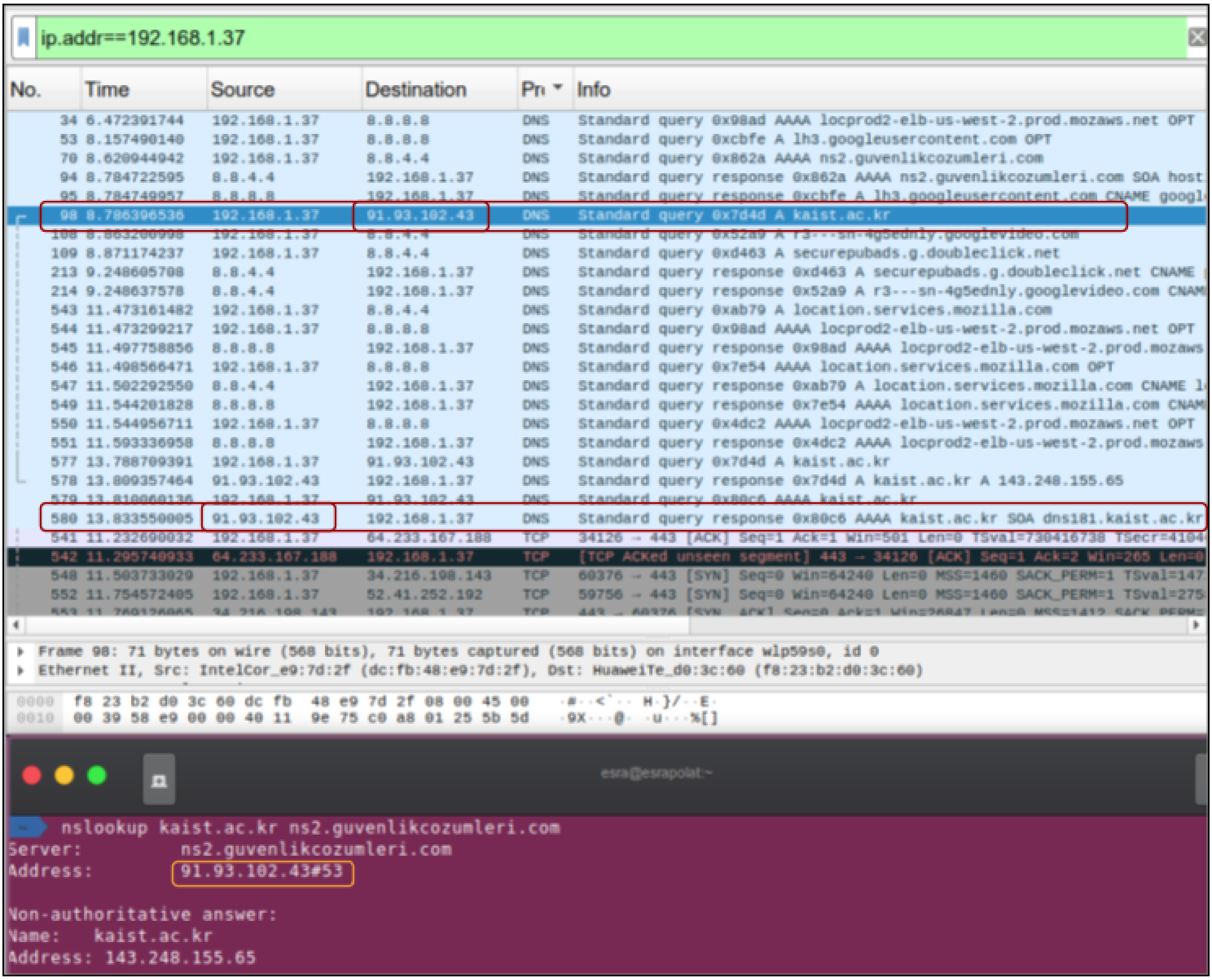
```
No.  Time          Source           Destination      Pr▾  Info
  13 0.631464491  192.168.1.37     8.8.8.8          DNS  Standard query 0xa127 AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
  14 0.669818052  8.8.8.8          192.168.1.37     DNS  Standard query response 0xa127 AAAA locprod2-elb-us-west-2.prod.mozaws
  43 2.063110764  192.168.1.37     8.8.8.8          DNS  Standard query 0xa50a NS mit.edu OPT
  44 2.139326726  8.8.8.8          192.168.1.37     DNS  Standard query response 0xa50a NS mit.edu NS ns1-173.akam.net NS use2.
  50 3.292151572  192.168.1.37     8.8.8.8          DNS  Standard query 0x2f7f AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
  92 3.428468155  8.8.8.8          192.168.1.37     DNS  Standard query response 0x2f7f AAAA locprod2-elb-us-west-2.prod.mozaws
  10 0.628687054  192.168.1.37     34.216.198.143   TCP  59732 → 443 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0 TSval=1471457517 TSe
  12 0.629106188  192.168.1.37     34.216.198.143   TCP  59728 → 443 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0 TSval=1471457518 TSe
  15 0.670949258  192.168.1.37     34.216.198.143   TCP  59734 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=147
  16 0.911618138  34.216.198.143   192.168.1.37     TCP  443 → 59732 [ACK] Seq=1 Ack=32 Win=115 Len=0 TSval=1634778711 TSecr=14
  18 0.911637743  192.168.1.37     34.216.198.143   TCP  59728 → 443 [RST] Seq=33 Win=0 Len=0
  19 0.911618556  34.216.198.143   192.168.1.37     TCP  443 → 59728 [FIN, ACK] Seq=32 Ack=33 Win=115 Len=0 TSval=1634778710 TS
  20 0.911649844  192.168.1.37     34.216.198.143   TCP  59728 → 443 [RST] Seq=33 Win=0 Len=0
  22 0.918427658  192.168.1.37     34.216.198.143   TCP  59732 → 443 [RST] Seq=33 Win=0 Len=0
  23 0.918437092  34.216.198.143   192.168.1.37     TCP  443 → 59734 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1412 SACK_PERM=
  24 0.918411058  34.216.198.143   192.168.1.37     TCP  443 → 59732 [FIN, ACK] Seq=32 Ack=33 Win=115 Len=0 TSval=1634778711 TS
  25 0.918441216  192.168.1.37     34.216.198.143   TCP  59732 → 443 [RST] Seq=33 Win=0 Len=0
  26 0.918448513  192.168.1.37     34.216.198.143   TCP  59734 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1471457807 TSecr=1
  30 1.417249799  34.216.198.143   192.168.1.37     TCP  443 → 59734 [ACK] Seq=1 Ack=518 Win=27136 Len=0 TSval=1634779000 TSecr
  32 1.423070666  192.168.1.37     34.216.198.143   TCP  59734 → 443 [ACK] Seq=518 Ack=3393 Win=60928 Len=0 TSval=1471458312 TS
  35 1.651904987  34.216.198.143   192.168.1.37     TCP  443 → 59734 [ACK] Seq=3393 Ack=644 Win=27136 Len=0 TSval=1634779514 TS
  37 1.651944856  192.168.1.37     34.216.198.143   TCP  59734 → 443 [ACK] Seq=644 Ack=3444 Win=64128 Len=0 TSval=1471458540 TS
  40 2.048025314  34.216.198.143   192.168.1.37     TCP  443 → 59734 [ACK] Seq=3444 Ack=1305 Win=29440 Len=0 TSval=1634779735 T
  42 2.048081947  192.168.1.37     34.216.198.143   TCP  59734 → 443 [ACK] Seq=1305 Ack=4033 Win=63616 Len=0 TSval=1471458937 T

▸ Frame 44: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60), Dst: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f)

0090  06 6d 00 07 04 65 75 72  35 c0 2d c0 0c 00 02 00   ·m···eur 5·-······
```

esra@esrapolat:~

```
~ nslookup -type=NS mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = usw2.akam.net.

Authoritative answers can be found from:
```

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?

This DNS query message is sent to 91.93.102.43 which is the IP address of the kaist.ac.kr DNS response sender.

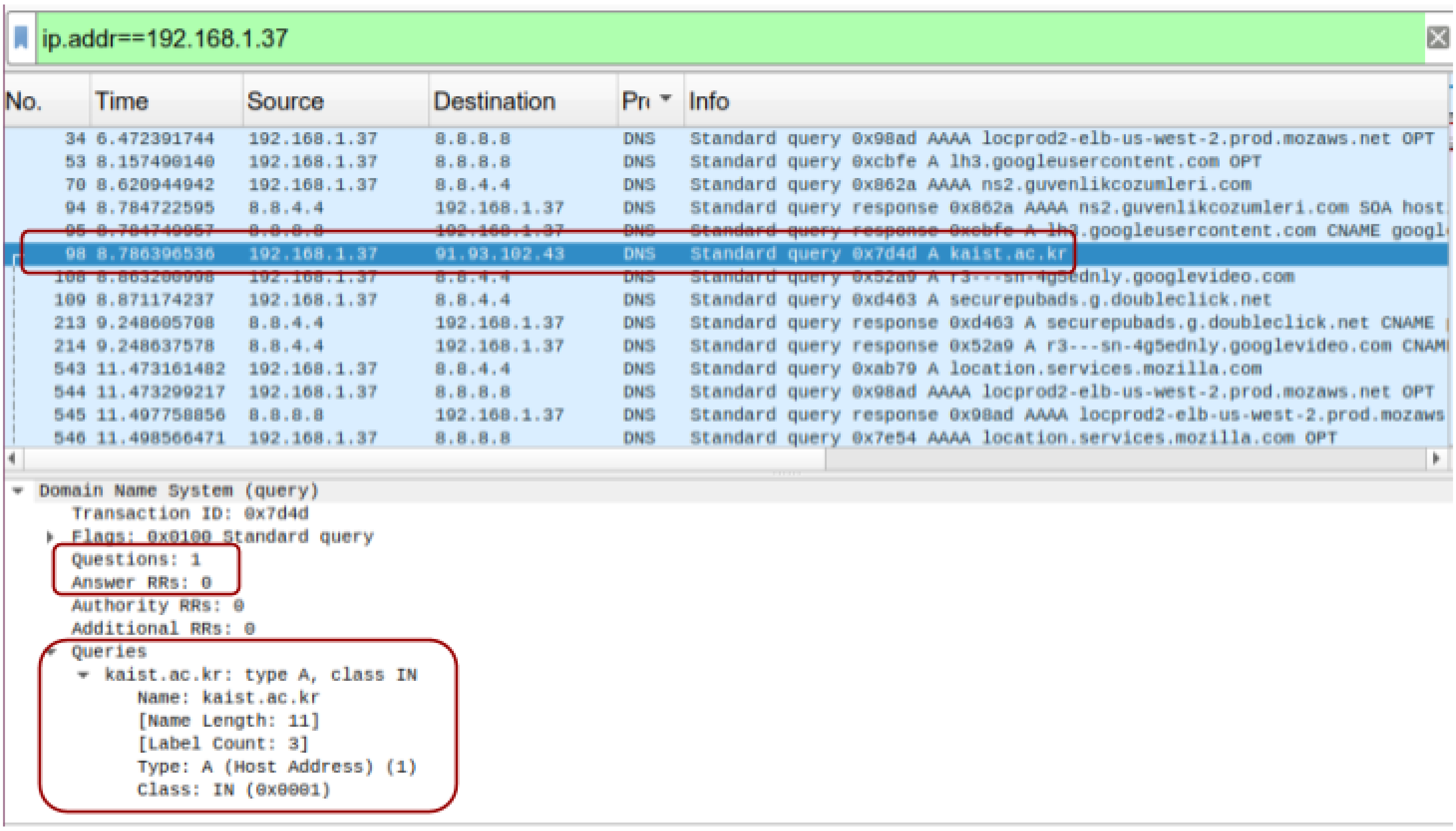


```
No.  Time          Source          Destination     Pr  Info
 34 6.472391744    192.168.1.37    8.8.8.8         DNS Standard query 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
 53 8.157490140    192.168.1.37    8.8.8.8         DNS Standard query 0xcbfe A lh3.googleusercontent.com OPT
 70 8.620944942    192.168.1.37    8.8.4.4         DNS Standard query 0x862a AAAA ns2.guvenlikcozumleri.com
 94 8.784722595    8.8.4.4         192.168.1.37    DNS Standard query response 0x862a AAAA ns2.guvenlikcozumleri.com SOA host
 95 8.784749957    8.8.8.8         192.168.1.37    DNS Standard query response 0xcbfe A lh3.googleusercontent.com CNAME googl
 98 8.786396536    192.168.1.37    91.93.102.43    DNS Standard query 0x7d4d A kaist.ac.kr
108 8.863200998    192.168.1.37    8.8.4.4         DNS Standard query 0x52a9 A r3---sn-4g5ednly.googlevideo.com
109 8.871174237    192.168.1.37    8.8.4.4         DNS Standard query 0xd463 A securepubads.g.doubleclick.net
213 9.248605708    8.8.4.4         192.168.1.37    DNS Standard query response 0xd463 A securepubads.g.doubleclick.net CNAME
214 9.248637578    8.8.4.4         192.168.1.37    DNS Standard query response 0x52a9 A r3---sn-4g5ednly.googlevideo.com CNAM
543 11.473161482   192.168.1.37    8.8.4.4         DNS Standard query 0xab79 A location.services.mozilla.com
544 11.473299217   192.168.1.37    8.8.8.8         DNS Standard query 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
545 11.497758856   8.8.8.8         192.168.1.37    DNS Standard query response 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws
546 11.498566471   192.168.1.37    8.8.8.8         DNS Standard query 0x7e54 AAAA location.services.mozilla.com OPT
547 11.502292550   8.8.4.4         192.168.1.37    DNS Standard query response 0xab79 A location.services.mozilla.com CNAME l
549 11.544201828   8.8.8.8         192.168.1.37    DNS Standard query response 0x7e54 AAAA location.services.mozilla.com CNAM
550 11.544956711   192.168.1.37    8.8.8.8         DNS Standard query 0x4dc2 AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
551 11.593336958   8.8.8.8         192.168.1.37    DNS Standard query response 0x4dc2 AAAA locprod2-elb-us-west-2.prod.mozaws
577 13.788709391   192.168.1.37    91.93.102.43    DNS Standard query 0x7d4d A kaist.ac.kr
578 13.809357464   91.93.102.43    192.168.1.37    DNS Standard query response 0x7d4d A kaist.ac.kr A 143.248.155.65
579 13.810060136   192.168.1.37    91.93.102.43    DNS Standard query 0x80c6 AAAA kaist.ac.kr
580 13.833550005   91.93.102.43    192.168.1.37    DNS Standard query response 0x80c6 AAAA kaist.ac.kr SOA dns181.kaist.ac.kr
541 11.232690032   192.168.1.37    64.233.167.188  TCP 34126 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=730416738 TSecr=4104
542 11.295740933   64.233.167.188  192.168.1.37    TCP [TCP ACKed unseen segment] 443 → 34126 [ACK] Seq=1 Ack=2 Win=265 Len=0
548 11.503733029   192.168.1.37    34.216.198.143  TCP 60376 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=147
552 11.754572405   192.168.1.37    52.41.252.192   TCP 59756 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=275
553 11.769126065   34.216.198.143  192.168.1.37    TCP 443 → 60376 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1412 SACK_PERM=

▸ Frame 98: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface wlp59s0, id 0
▸ Ethernet II, Src: IntelCor_e9:7d:2f (dc:fb:48:e9:7d:2f), Dst: HuaweiTe_d0:3c:60 (f8:23:b2:d0:3c:60)

0000  f8 23 b2 d0 3c 60 dc fb  48 e9 7d 2f 08 00 45 00   ·#··<`·· H·}/··E·
0010  00 39 58 e9 00 00 40 11  9e 75 c0 a8 01 25 5b 5d   ·9X···@· ·u···%[]
```

```
~ nslookup kaist.ac.kr ns2.guvenlikcozumleri.com
Server:         ns2.guvenlikcozumleri.com
Address:        91.93.102.43#53

Non-authoritative answer:
Name:   kaist.ac.kr
Address: 143.248.155.65
```

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

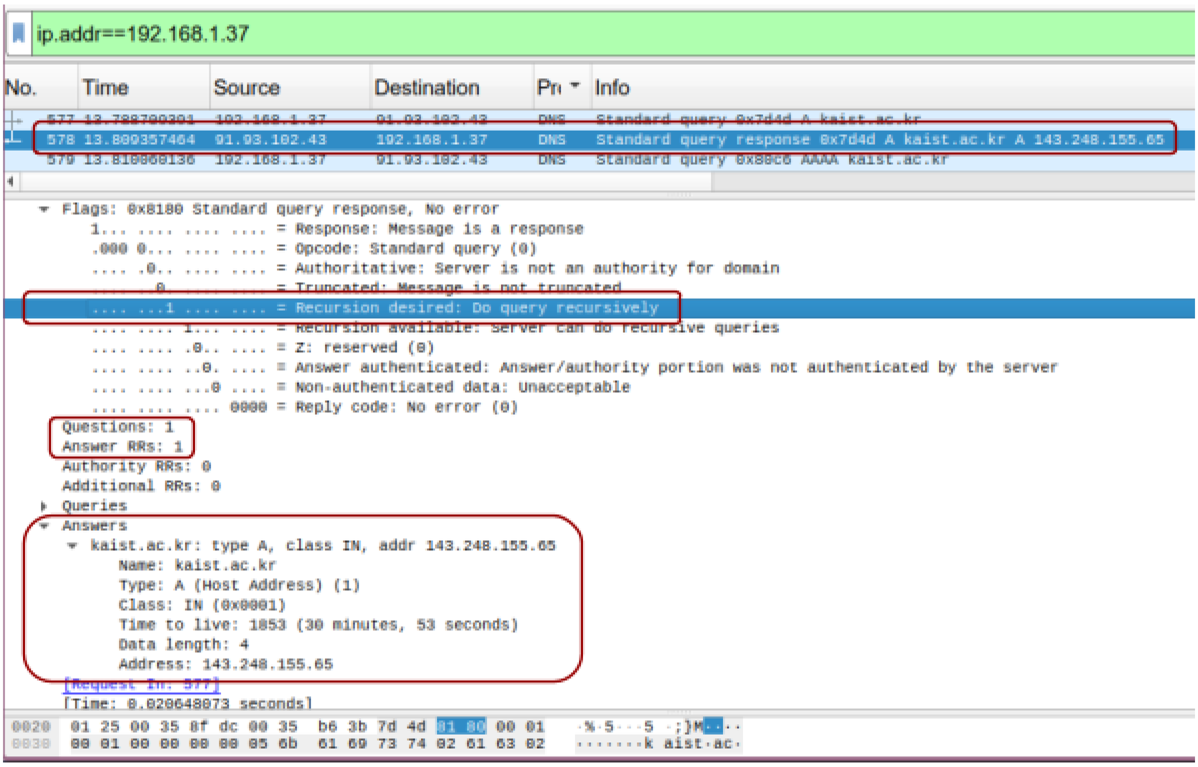
This DNS query is a type “A” query. The message does not contain any answers.



```
ip.addr==192.168.1.37

No.  Time          Source         Destination    Pr  Info
  34 6.472391744   192.168.1.37   8.8.8.8        DNS Standard query 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
  53 8.157490140   192.168.1.37   8.8.8.8        DNS Standard query 0xcbfe A lh3.googleusercontent.com OPT
  70 8.620944942   192.168.1.37   8.8.4.4        DNS Standard query 0x862a AAAA ns2.guvenlikcozumleri.com
  94 8.784722595   8.8.4.4        192.168.1.37   DNS Standard query response 0x862a AAAA ns2.guvenlikcozumleri.com SOA host
  95 8.784749957   8.8.8.8        192.168.1.37   DNS Standard query response 0xcbfe A lh3.googleusercontent.com CNAME googl
  98 8.786396536   192.168.1.37   91.93.102.43   DNS Standard query 0x7d4d A kaist.ac.kr
 108 8.863200998   192.168.1.37   8.8.4.4        DNS Standard query 0x52a9 A r3---sn-4g5ednly.googlevideo.com
 109 8.871174237   192.168.1.37   8.8.4.4        DNS Standard query 0xd463 A securepubads.g.doubleclick.net
 213 9.248605708   8.8.4.4        192.168.1.37   DNS Standard query response 0xd463 A securepubads.g.doubleclick.net CNAME
 214 9.248637578   8.8.4.4        192.168.1.37   DNS Standard query response 0x52a9 A r3---sn-4g5ednly.googlevideo.com CNAM
 543 11.473161482  192.168.1.37   8.8.4.4        DNS Standard query 0xab79 A location.services.mozilla.com
 544 11.473299217  192.168.1.37   8.8.8.8        DNS Standard query 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
 545 11.497758856  8.8.8.8        192.168.1.37   DNS Standard query response 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws
 546 11.498566471  192.168.1.37   8.8.8.8        DNS Standard query 0x7e54 AAAA location.services.mozilla.com OPT

▾ Domain Name System (query)
    Transaction ID: 0x7d4d
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ kaist.ac.kr: type A, class IN
        Name: kaist.ac.kr
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

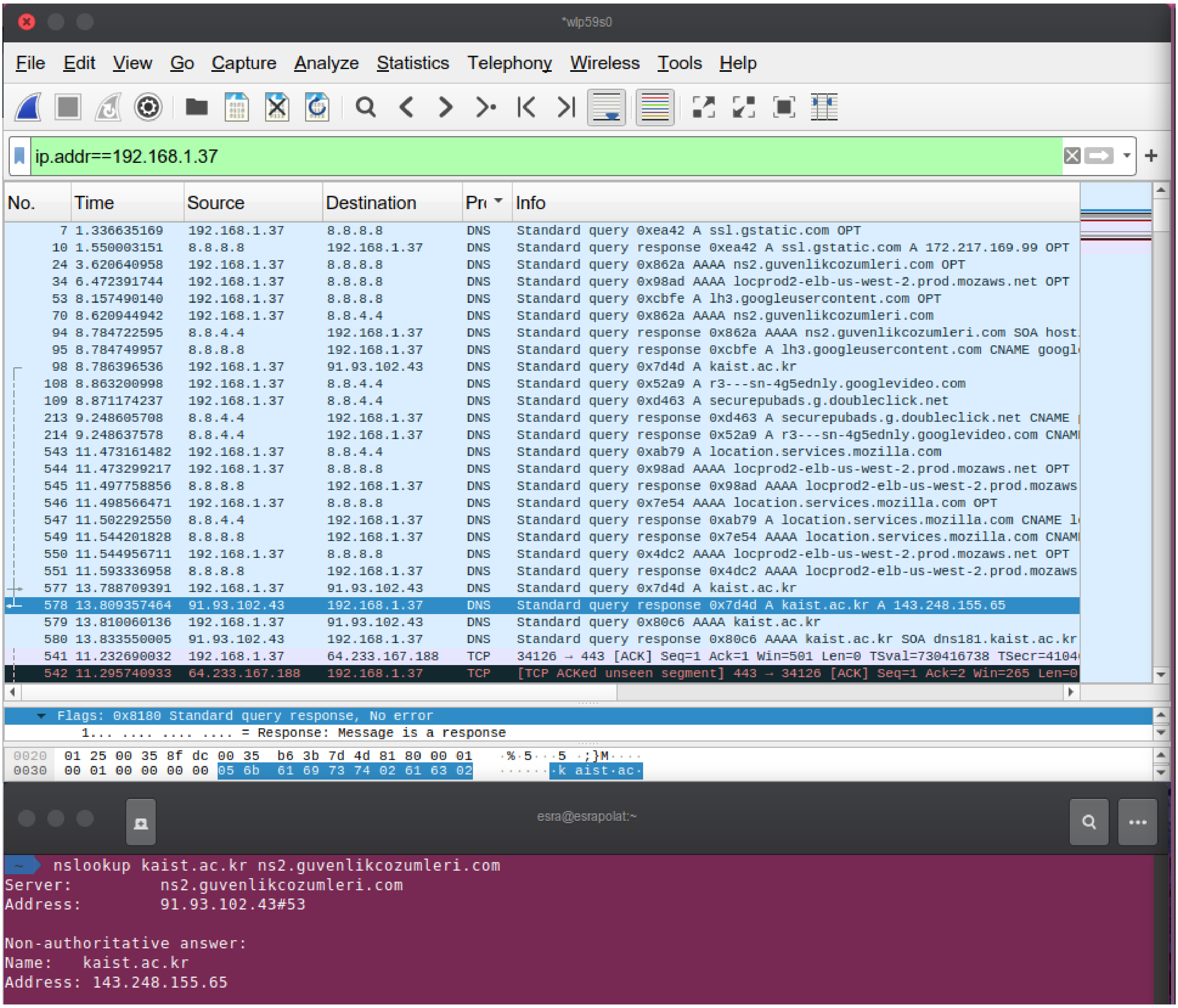
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

One answer is provided in the DNS response message. It contains the following:



```
ip.addr==192.168.1.37

No.  Time          Source         Destination    Pr  Info
 577 13.788709391  192.168.1.37   91.93.102.43   DNS Standard query 0x7d4d A kaist.ac.kr
 578 13.809357464  91.93.102.43   192.168.1.37   DNS Standard query response 0x7d4d A kaist.ac.kr A 143.248.155.65
 579 13.810060136  192.168.1.37   91.93.102.43   DNS Standard query 0x88c6 AAAA kaist.ac.kr

  ▾ Flags: 0x8180 Standard query response, No error
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▾ kaist.ac.kr: type A, class IN, addr 143.248.155.65
        Name: kaist.ac.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1853 (30 minutes, 53 seconds)
        Data length: 4
        Address: 143.248.155.65
    [Request In: 577]
    [Time: 0.020648073 seconds]

0020  01 25 00 35 8f dc 00 35  b6 3b 7d 4d 81 80 00 01   ·%·5···5 ·;}M····
0030  00 01 00 00 00 00 05 6b  61 69 73 74 02 61 63 02   ·······k aist·ac·
```

23. Provide a screenshot.


*wlp59s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
esra@esrapolat:~

```
ip.addr==192.168.1.37

No.  Time          Source          Destination     Pr  Info
   7 1.336635169   192.168.1.37    8.8.8.8         DNS Standard query 0xea42 A ssl.gstatic.com OPT
  10 1.550003151   8.8.8.8         192.168.1.37    DNS Standard query response 0xea42 A ssl.gstatic.com A 172.217.169.99 OPT
  24 3.620640958   192.168.1.37    8.8.8.8         DNS Standard query 0x862a AAAA ns2.guvenlikcozumleri.com OPT
  34 6.472391744   192.168.1.37    8.8.8.8         DNS Standard query 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
  53 8.157490140   192.168.1.37    8.8.8.8         DNS Standard query 0xcbfe A lh3.googleusercontent.com OPT
  70 8.620944942   192.168.1.37    8.8.4.4         DNS Standard query 0x862a AAAA ns2.guvenlikcozumleri.com
  94 8.784722595   8.8.4.4         192.168.1.37    DNS Standard query response 0x862a AAAA ns2.guvenlikcozumleri.com SOA host
  95 8.784749957   8.8.8.8         192.168.1.37    DNS Standard query response 0xcbfe A lh3.googleusercontent.com CNAME googl
  98 8.786396536   192.168.1.37    91.93.102.43    DNS Standard query 0x7d4d A kaist.ac.kr
 108 8.863200998   192.168.1.37    8.8.4.4         DNS Standard query 0x52a9 A r3---sn-4g5ednly.googlevideo.com
 109 8.871174237   192.168.1.37    8.8.4.4         DNS Standard query 0xd463 A securepubads.g.doubleclick.net
 213 9.248605708   8.8.4.4         192.168.1.37    DNS Standard query response 0xd463 A securepubads.g.doubleclick.net CNAME
 214 9.248637578   8.8.4.4         192.168.1.37    DNS Standard query response 0x52a9 A r3---sn-4g5ednly.googlevideo.com CNAM
 543 11.473161482  192.168.1.37    8.8.4.4         DNS Standard query 0xab79 A location.services.mozilla.com
 544 11.473299217  192.168.1.37    8.8.8.8         DNS Standard query 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
 545 11.497758856  8.8.8.8         192.168.1.37    DNS Standard query response 0x98ad AAAA locprod2-elb-us-west-2.prod.mozaws
 546 11.498566471  192.168.1.37    8.8.8.8         DNS Standard query 0x7e54 AAAA location.services.mozilla.com OPT
 547 11.502292550  8.8.4.4         192.168.1.37    DNS Standard query response 0xab79 A location.services.mozilla.com CNAME l
 549 11.544201828  8.8.8.8         192.168.1.37    DNS Standard query response 0x7e54 AAAA location.services.mozilla.com CNAM
 550 11.544956711  192.168.1.37    8.8.8.8         DNS Standard query 0x4dc2 AAAA locprod2-elb-us-west-2.prod.mozaws.net OPT
 551 11.593336958  8.8.8.8         192.168.1.37    DNS Standard query response 0x4dc2 AAAA locprod2-elb-us-west-2.prod.mozaws
 577 13.788709391  192.168.1.37    91.93.102.43    DNS Standard query 0x7d4d A kaist.ac.kr
 578 13.809357464  91.93.102.43    192.168.1.37    DNS Standard query response 0x7d4d A kaist.ac.kr A 143.248.155.65
 579 13.810060136  192.168.1.37    91.93.102.43    DNS Standard query 0x80c6 AAAA kaist.ac.kr
 580 13.833550005  91.93.102.43    192.168.1.37    DNS Standard query response 0x80c6 AAAA kaist.ac.kr SOA dns181.kaist.ac.kr
 541 11.232690032  192.168.1.37    64.233.167.188  TCP 34126 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=730416738 TSecr=4104
 542 11.295740933  64.233.167.188  192.168.1.37    TCP [TCP ACKed unseen segment] 443 → 34126 [ACK] Seq=1 Ack=2 Win=265 Len=0

    Flags: 0x8180 Standard query response, No error
        1... .... .... .... = Response: Message is a response

0020  01 25 00 35 8f dc 00 35  b6 3b 7d 4d 81 80 00 01   ·%·5···5 ·;}M····
0030  00 01 00 00 00 00 05 6b  61 69 73 74 02 61 63 02   ······k aist·ac·
```

```
~ nslookup kaist.ac.kr ns2.guvenlikcozumleri.com
Server:         ns2.guvenlikcozumleri.com
Address:        91.93.102.43#53

Non-authoritative answer:
Name:   kaist.ac.kr
Address: 143.248.155.65
```

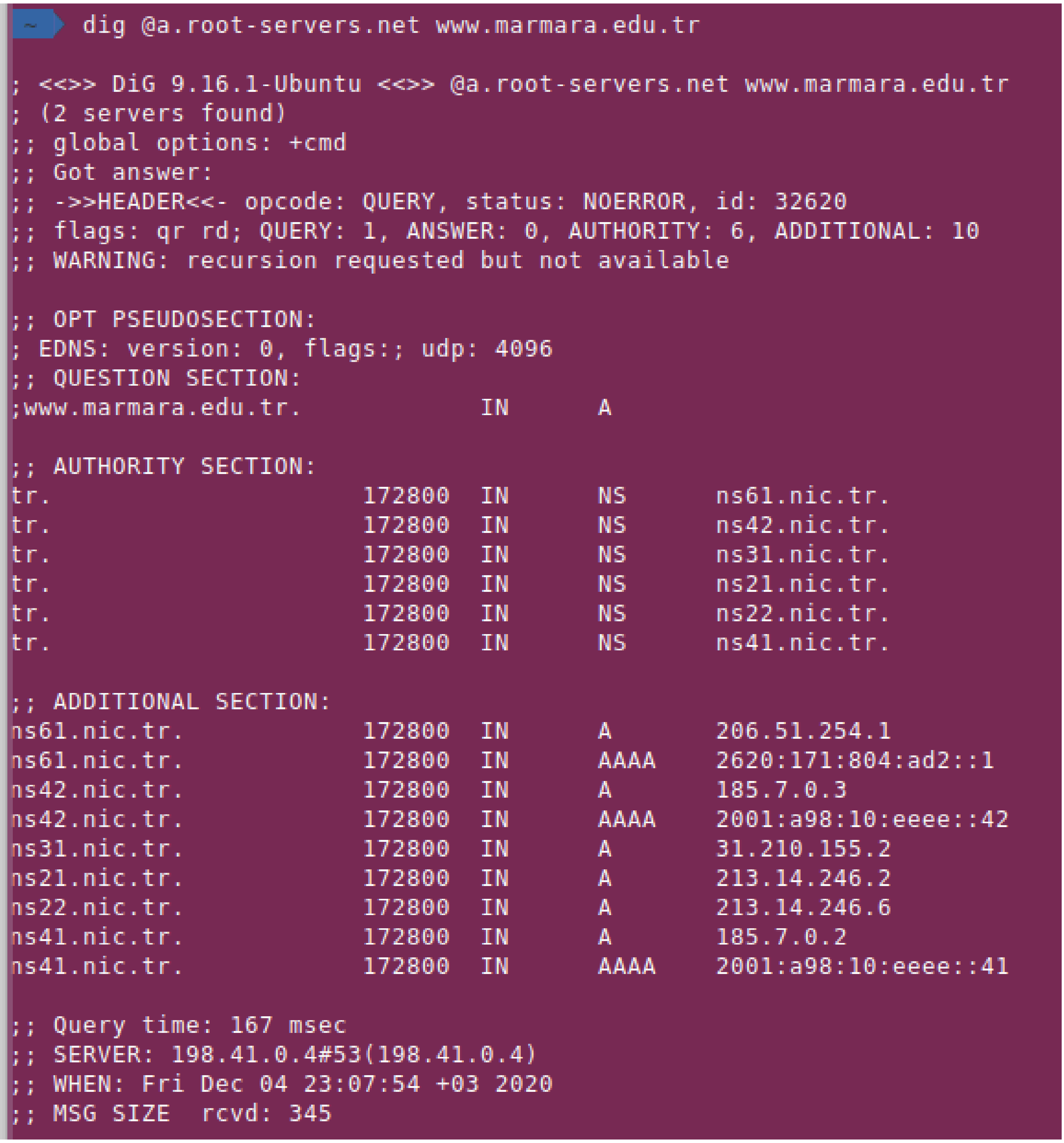
4. Extra Questions

24. You may send queries to root DNS servers and see what you get. You may try the following root server: a.root-servers.net

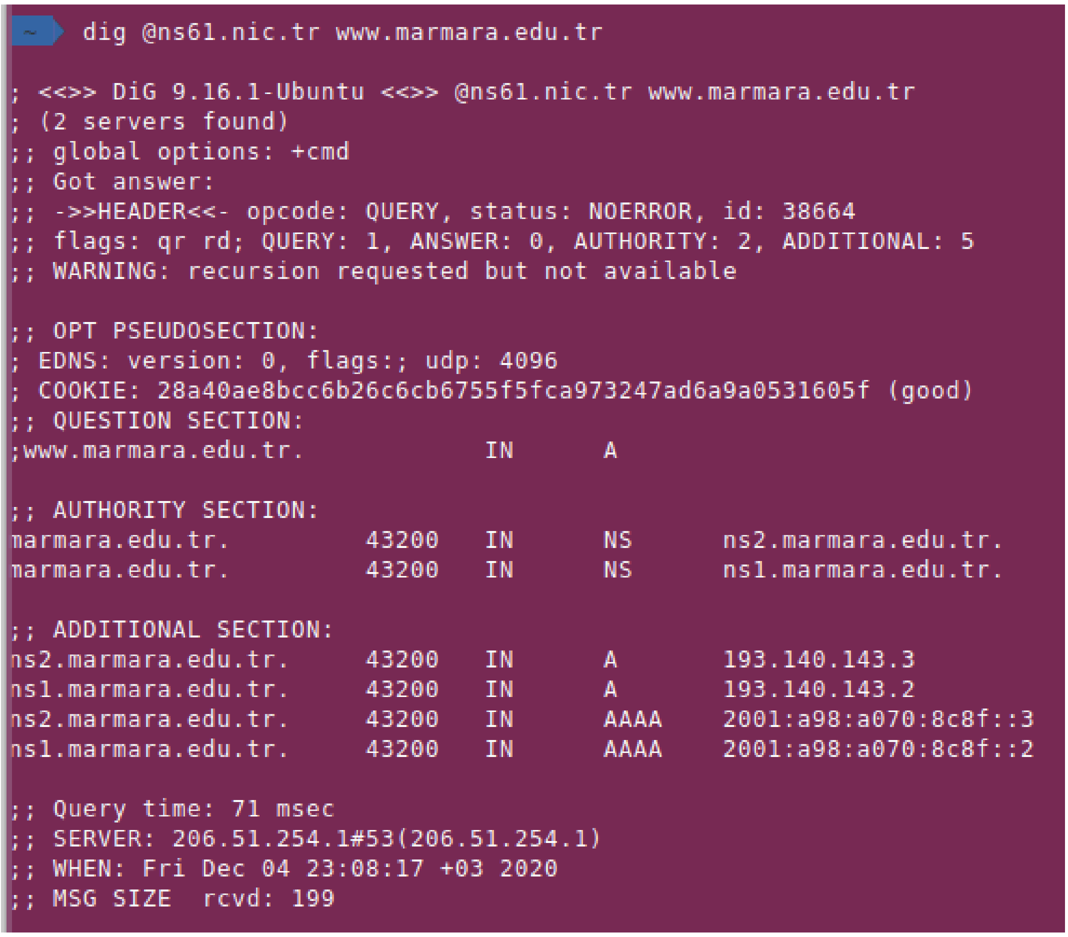
- Please try the following: "nslookup www.marmara.edu.tr a.root-servers.net"
- You will get a list of TLD servers
- Then please send the same query to one of the TLD servers.
- You will get a list of authoritative DNS servers of marmara.edu.tr
- Then please send the same query to authoritative DNS server of marmara.edu.tr

- You will get the IP address of www.marmara.edu.tr

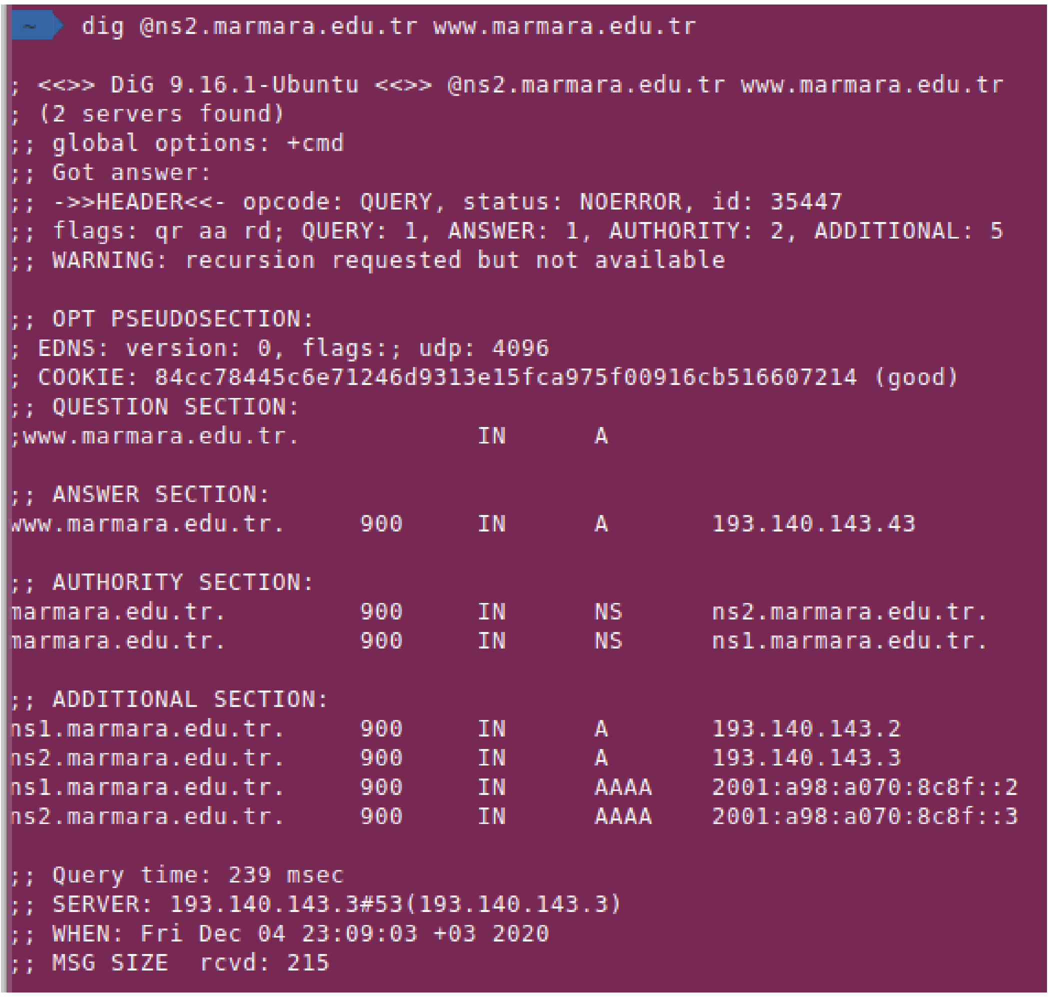
- Repeat the above steps for any address in Asia.



```
 ~   dig @a.root-servers.net www.marmara.edu.tr

; <<>> DiG 9.16.1-Ubuntu <<>> @a.root-servers.net www.marmara.edu.tr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32620
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.marmara.edu.tr.            IN      A

;; AUTHORITY SECTION:
tr.                     172800  IN      NS      ns61.nic.tr.
tr.                     172800  IN      NS      ns42.nic.tr.
tr.                     172800  IN      NS      ns31.nic.tr.
tr.                     172800  IN      NS      ns21.nic.tr.
tr.                     172800  IN      NS      ns22.nic.tr.
tr.                     172800  IN      NS      ns41.nic.tr.

;; ADDITIONAL SECTION:
ns61.nic.tr.            172800  IN      A       206.51.254.1
ns61.nic.tr.            172800  IN      AAAA    2620:171:804:ad2::1
ns42.nic.tr.            172800  IN      A       185.7.0.3
ns42.nic.tr.            172800  IN      AAAA    2001:a98:10:eeee::42
ns31.nic.tr.            172800  IN      A       31.210.155.2
ns21.nic.tr.            172800  IN      A       213.14.246.2
ns22.nic.tr.            172800  IN      A       213.14.246.6
ns41.nic.tr.            172800  IN      A       185.7.0.2
ns41.nic.tr.            172800  IN      AAAA    2001:a98:10:eeee::41

;; Query time: 167 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Fri Dec 04 23:07:54 +03 2020
;; MSG SIZE  rcvd: 345
```



```
~  dig @ns61.nic.tr www.marmara.edu.tr

; <<>> DiG 9.16.1-Ubuntu <<>> @ns61.nic.tr www.marmara.edu.tr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38664
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 28a40ae8bcc6b26c6cb6755f5fca973247ad6a9a0531605f (good)
;; QUESTION SECTION:
;www.marmara.edu.tr.            IN      A

;; AUTHORITY SECTION:
narmara.edu.tr.         43200   IN      NS      ns2.marmara.edu.tr.
narmara.edu.tr.         43200   IN      NS      ns1.marmara.edu.tr.

;; ADDITIONAL SECTION:
ns2.marmara.edu.tr.     43200   IN      A       193.140.143.3
ns1.marmara.edu.tr.     43200   IN      A       193.140.143.2
ns2.marmara.edu.tr.     43200   IN      AAAA    2001:a98:a070:8c8f::3
ns1.marmara.edu.tr.     43200   IN      AAAA    2001:a98:a070:8c8f::2

;; Query time: 71 msec
;; SERVER: 206.51.254.1#53(206.51.254.1)
;; WHEN: Fri Dec 04 23:08:17 +03 2020
;; MSG SIZE  rcvd: 199
```

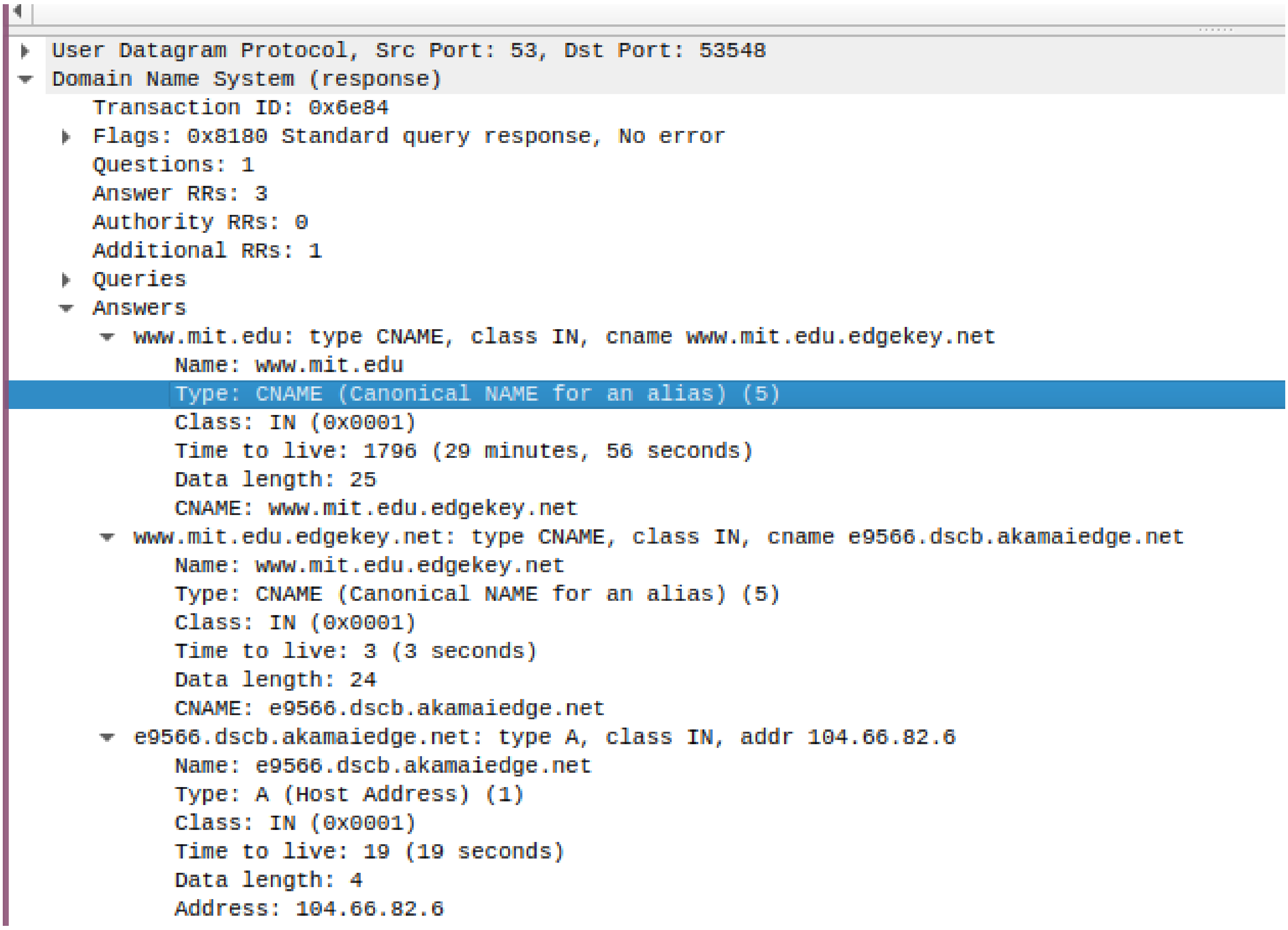


```
~  dig @ns2.marmara.edu.tr www.marmara.edu.tr

; <<>> DiG 9.16.1-Ubuntu <<>> @ns2.marmara.edu.tr www.marmara.edu.tr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35447
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 84cc78445c6e71246d9313e15fca975f00916cb516607214 (good)
;; QUESTION SECTION:
;www.marmara.edu.tr.            IN      A

;; ANSWER SECTION:
www.marmara.edu.tr.     900     IN      A       193.140.143.43

;; AUTHORITY SECTION:
narmara.edu.tr.         900     IN      NS      ns2.marmara.edu.tr.
narmara.edu.tr.         900     IN      NS      ns1.marmara.edu.tr.

;; ADDITIONAL SECTION:
ns1.marmara.edu.tr.     900     IN      A       193.140.143.2
ns2.marmara.edu.tr.     900     IN      A       193.140.143.3
ns1.marmara.edu.tr.     900     IN      AAAA    2001:a98:a070:8c8f::2
ns2.marmara.edu.tr.     900     IN      AAAA    2001:a98:a070:8c8f::3

;; Query time: 239 msec
;; SERVER: 193.140.143.3#53(193.140.143.3)
;; WHEN: Fri Dec 04 23:09:03 +03 2020
;; MSG SIZE  rcvd: 215
```

25. You may also try other types, such as CNAME and MX.

- What is the canonical name of www.mit.edu? What about "satlab.cmpe.boun.edu.tr" (my previous lab)? Or "netlab.cmpe.boun.edu.tr" (another lab that I worked in)?
- What is the name of the mail server (mail exchanger) of marmara.edu.tr? What about "cmpe.boun.edu.tr"? or "boun.edu.tr"?
- Please repeat the above for any web server and mail domain, respectively.

We can observe CNAME for mit.edu in the picture.



```
▸ User Datagram Protocol, Src Port: 53, Dst Port: 53548
▾ Domain Name System (response)
    Transaction ID: 0x6e84
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ 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: 1796 (29 minutes, 56 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: 3 (3 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    ▾ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.66.82.6
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 19 (19 seconds)
        Data length: 4
        Address: 104.66.82.6
```

150116884

Esra Polat