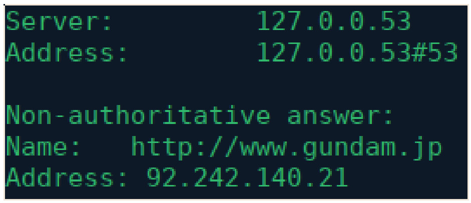
Computer Networks Lab 1

Shane Cincotta

March 30, 2020

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



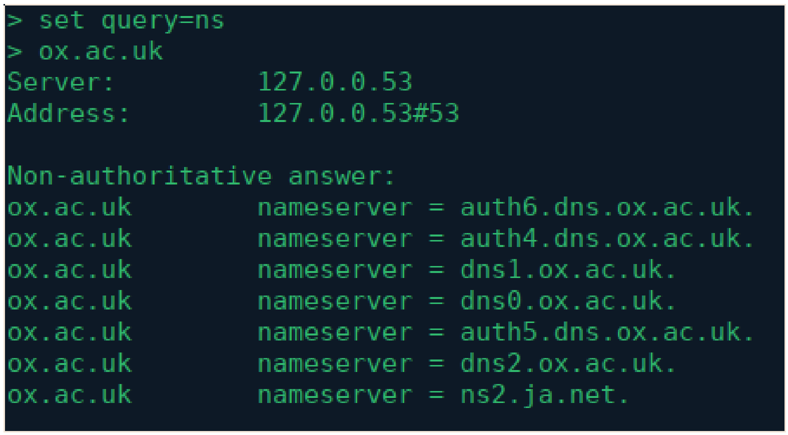
```
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   http://www.gundam.jp
Address: 92.242.140.21
```

Figure 1:

According to figure 1, I used the server http://www.gundam.jp, the IP address is 92.242.140.21

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



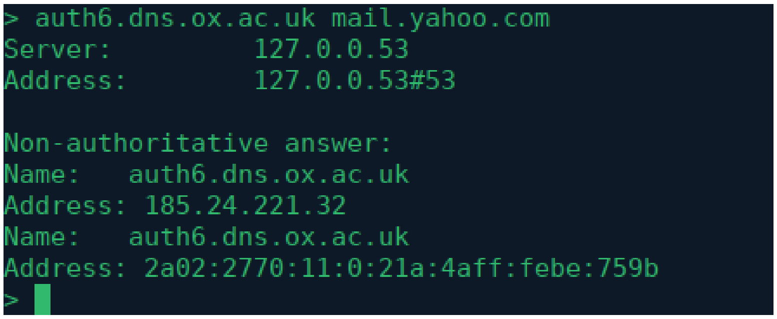
```
> set query=ns
> ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.
```

Figure 2:

According to figure 2, the authoritative DNS server for ox.ac.uk is auth6.dns.ox.ac.uk.

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?

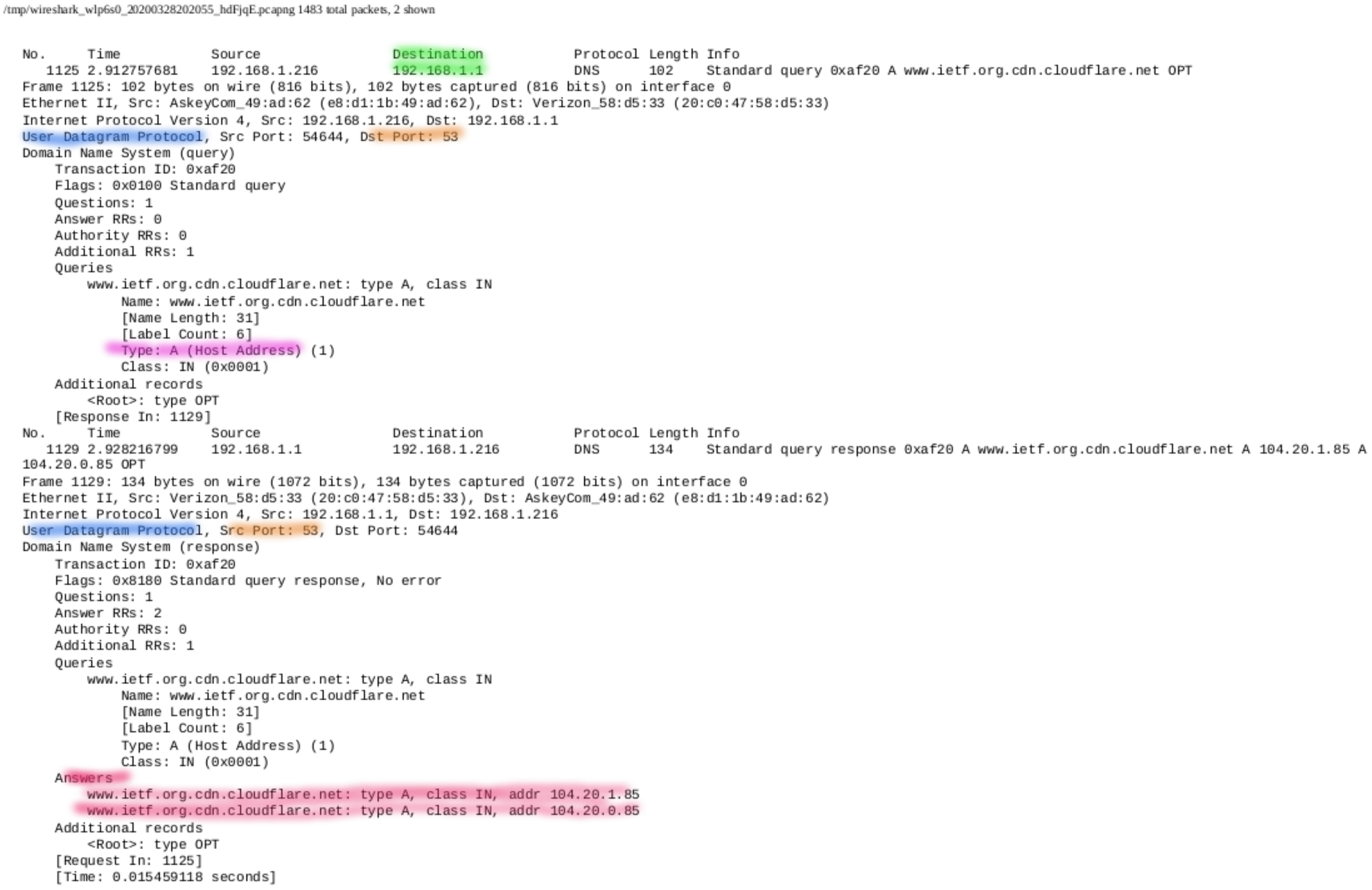


```
> auth6.dns.ox.ac.uk mail.yahoo.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   auth6.dns.ox.ac.uk
Address: 185.24.221.32
Name:   auth6.dns.ox.ac.uk
Address: 2a02:2770:11:0:21a:4aff:febe:759b
> 
```

Figure 3:

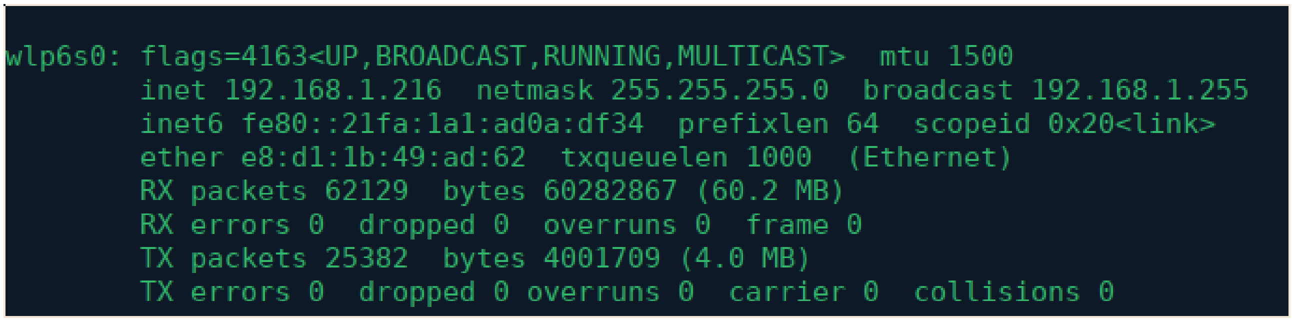
According to figure 3, the IP address is 185.24.221.32



```
/tmp/wireshark_wlp6s0_20200328202055_hdFjqE.pcapng 1483 total packets, 2 shown

No.     Time           Source                Destination           Protocol Length Info
   1125 2.912757681    192.168.1.216         192.168.1.1           DNS      102    Standard query 0xaf20 A www.ietf.org.cdn.cloudflare.net OPT
Frame 1125: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 54644, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xaf20
    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
            Name: www.ietf.org.cdn.cloudflare.net
            [Name Length: 31]
            [Label Count: 6]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Additional records
        <Root>: type OPT
    [Response In: 1129]
No.     Time           Source                Destination           Protocol Length Info
   1129 2.928216799    192.168.1.1           192.168.1.216         DNS      134    Standard query response 0xaf20 A www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 
104.20.0.85 OPT
Frame 1129: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.216
User Datagram Protocol, Src Port: 53, Dst Port: 54644
Domain Name System (response)
    Transaction ID: 0xaf20
    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
            Name: www.ietf.org.cdn.cloudflare.net
            [Name Length: 31]
            [Label Count: 6]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Answers
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    Additional records
        <Root>: type OPT
    [Request In: 1125]
    [Time: 0.015459118 seconds]
```

Figure 4:



```
wlp6s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.216  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::21fa:1a1:ad0a:df34  prefixlen 64  scopeid 0x20<link>
        ether e8:d1:1b:49:ad:62  txqueuelen 1000  (Ethernet)
        RX packets 62129  bytes 60282867 (60.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25382  bytes 4001709 (4.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 5:

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

According to figure 4, the query and response messages are sent over UDP.

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

According to figure 4, the destination port is 53 and the source port of the response message is also 53.

6 To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

According to figure 4, the DNS query message is being sent to 192.168.1.1. According to figure 5, my IP address is 192.168.1.216, thus they are not the same.

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

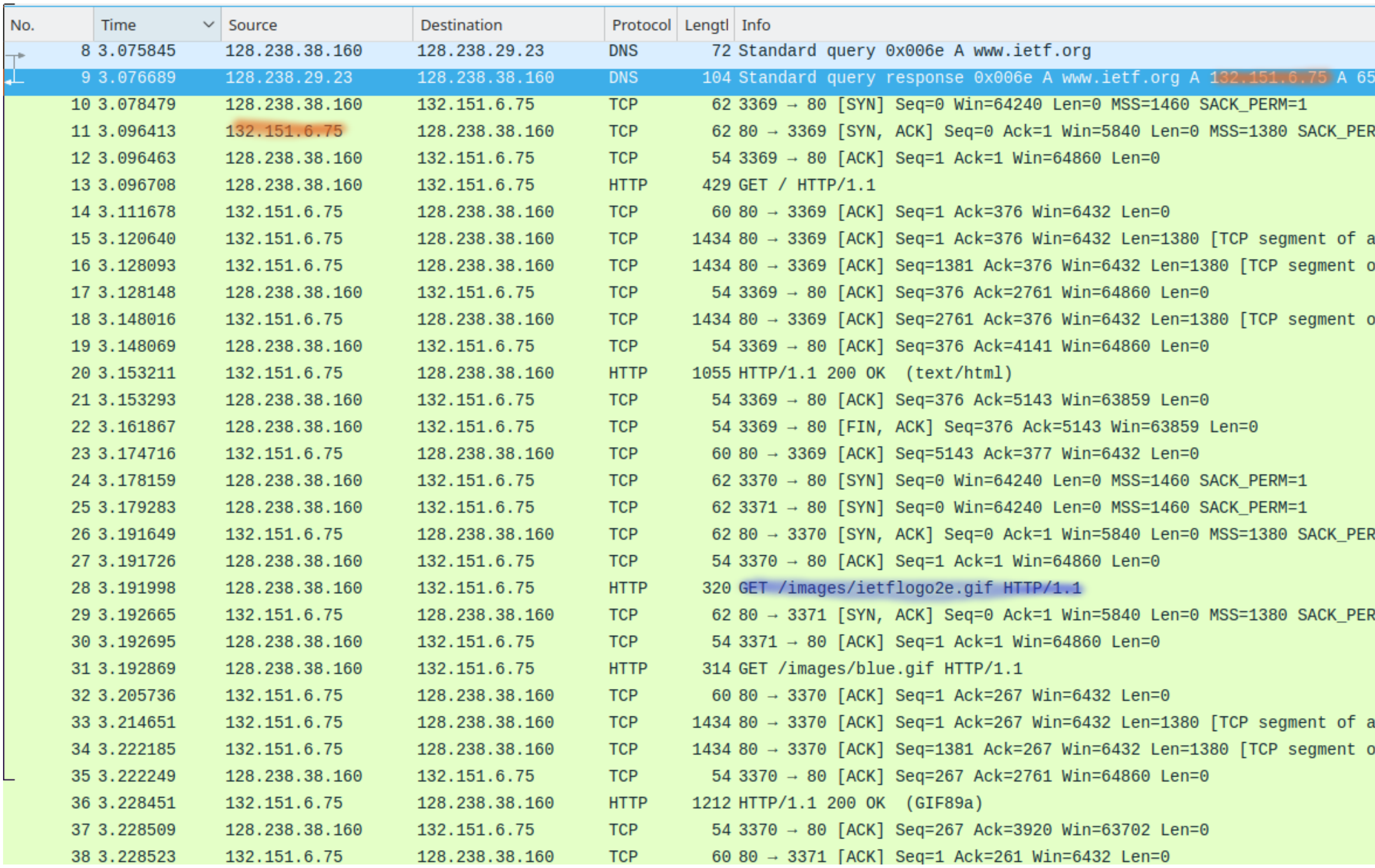
According to figure 4, it is of type A. It does not contain answers.

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

According to figure 4, there are 2 answers provided. The answers contain the address of the website which was queried for.

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?

According to figure 6, the IP address of the SYN packed corresponds to the IP address listed in the DNS response message (132.151.6.75).

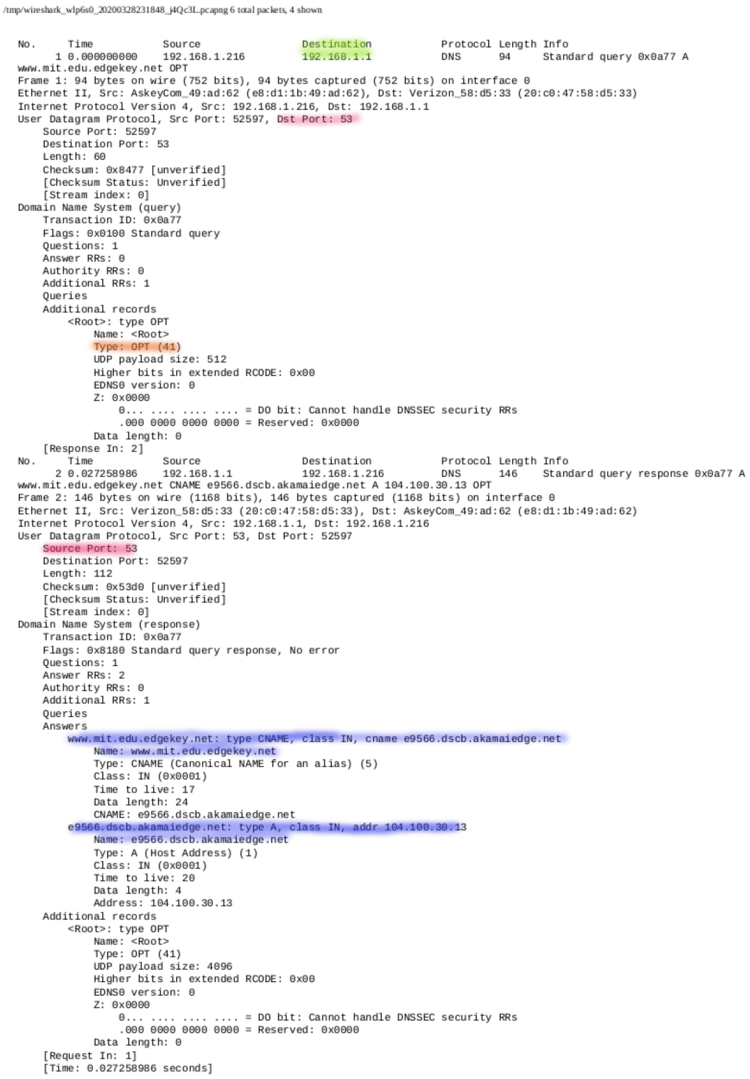


No.	Time	Source	Destination	Protocol	Lengtl	Info
8	3.075845	128.238.38.160	128.238.29.23	DNS	72	Standard query 0x006e A www.ietf.org
9	3.076689	128.238.29.23	128.238.38.160	DNS	104	Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65
10	3.078479	128.238.38.160	132.151.6.75	TCP	62	3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11	3.096413	132.151.6.75	128.238.38.160	TCP	62	80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PER
12	3.096463	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
13	3.096708	128.238.38.160	132.151.6.75	HTTP	429	GET / HTTP/1.1
14	3.111678	132.151.6.75	128.238.38.160	TCP	60	80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=0
15	3.120640	132.151.6.75	128.238.38.160	TCP	1434	80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=1380 [TCP segment of a
16	3.128093	132.151.6.75	128.238.38.160	TCP	1434	80 → 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment o
17	3.128148	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=376 Ack=2761 Win=64860 Len=0
18	3.148016	132.151.6.75	128.238.38.160	TCP	1434	80 → 3369 [ACK] Seq=2761 Ack=376 Win=6432 Len=1380 [TCP segment o
19	3.148069	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=376 Ack=4141 Win=64860 Len=0
20	3.153211	132.151.6.75	128.238.38.160	HTTP	1055	HTTP/1.1 200 OK (text/html)
21	3.153293	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=376 Ack=5143 Win=63859 Len=0
22	3.161867	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [FIN, ACK] Seq=376 Ack=5143 Win=63859 Len=0
23	3.174716	132.151.6.75	128.238.38.160	TCP	60	80 → 3369 [ACK] Seq=5143 Ack=377 Win=6432 Len=0
24	3.178159	128.238.38.160	132.151.6.75	TCP	62	3370 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
25	3.179283	128.238.38.160	132.151.6.75	TCP	62	3371 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
26	3.191649	132.151.6.75	128.238.38.160	TCP	62	80 → 3370 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PER
27	3.191726	128.238.38.160	132.151.6.75	TCP	54	3370 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
28	3.191998	128.238.38.160	132.151.6.75	HTTP	320	GET /images/ietflogo2e.gif HTTP/1.1
29	3.192665	132.151.6.75	128.238.38.160	TCP	62	80 → 3371 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PER
30	3.192695	128.238.38.160	132.151.6.75	TCP	54	3371 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
31	3.192869	128.238.38.160	132.151.6.75	HTTP	314	GET /images/blue.gif HTTP/1.1
32	3.205736	132.151.6.75	128.238.38.160	TCP	60	80 → 3370 [ACK] Seq=1 Ack=267 Win=6432 Len=0
33	3.214651	132.151.6.75	128.238.38.160	TCP	1434	80 → 3370 [ACK] Seq=1 Ack=267 Win=6432 Len=1380 [TCP segment of a
34	3.222185	132.151.6.75	128.238.38.160	TCP	1434	80 → 3370 [ACK] Seq=1381 Ack=267 Win=6432 Len=1380 [TCP segment o
35	3.222249	128.238.38.160	132.151.6.75	TCP	54	3370 → 80 [ACK] Seq=267 Ack=2761 Win=64860 Len=0
36	3.228451	132.151.6.75	128.238.38.160	HTTP	1212	HTTP/1.1 200 OK (GIF89a)
37	3.228509	128.238.38.160	132.151.6.75	TCP	54	3370 → 80 [ACK] Seq=267 Ack=3920 Win=63702 Len=0
38	3.228523	132.151.6.75	128.238.38.160	TCP	60	80 → 3371 [ACK] Seq=1 Ack=261 Win=6432 Len=0

Figure 6:

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

According to figure 6, my host does issue new DNS queries after each get request.



```
/tmp/wireshark_wlp6s0_20200328231848_j4Qc3L.pcapng 6 total packets, 4 shown

No.     Time           Source                Destination           Protocol Length Info
      1 0.000000000    192.168.1.216         192.168.1.1           DNS      94     Standard query 0x0a77 A
www.mit.edu.edgekey.net OPT
Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 52597, Dst Port: 53
    Source Port: 52597
    Destination Port: 53
    Length: 60
    Checksum: 0x8477 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (query)
    Transaction ID: 0x0a77
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
    Queries
    Additional records
        <Root>: type OPT
            Name: <Root>
            Type: OPT (41)
            UDP payload size: 512
            Higher bits in extended RCODE: 0x00
            EDNS0 version: 0
            Z: 0x0000
                0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
                .000 0000 0000 0000 = Reserved: 0x0000
            Data length: 0
    [Response In: 2]
No.     Time           Source                Destination           Protocol Length Info
      2 0.027258986    192.168.1.1           192.168.1.216         DNS      146    Standard query response 0x0a77 A
www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.100.30.13 OPT
Frame 2: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.216
User Datagram Protocol, Src Port: 53, Dst Port: 52597
    Source Port: 53
    Destination Port: 52597
    Length: 112
    Checksum: 0x53d0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (response)
    Transaction ID: 0x0a77
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
    Queries
    Answers
        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: 17
            Data length: 24
            CNAME: e9566.dscb.akamaiedge.net
        e9566.dscb.akamaiedge.net: type A, class IN, addr 104.100.30.13
            Name: e9566.dscb.akamaiedge.net
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 20
            Data length: 4
            Address: 104.100.30.13
    Additional records
        <Root>: type OPT
            Name: <Root>
            Type: OPT (41)
            UDP payload size: 4096
            Higher bits in extended RCODE: 0x00
            EDNS0 version: 0
            Z: 0x0000
                0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
                .000 0000 0000 0000 = Reserved: 0x0000
            Data length: 0
    [Request In: 1]
    [Time: 0.027258986 seconds]
```

Figure 7:

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

According to figure 7, the destination port for the DNS query message is 53, and the source port for the DNS response message is also 53.

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

According to figure 7, the DNS query message is being sent to 192.168.1.1. This is not my IP address, as shown in figure 6, my IP is 192.168.1.216.

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

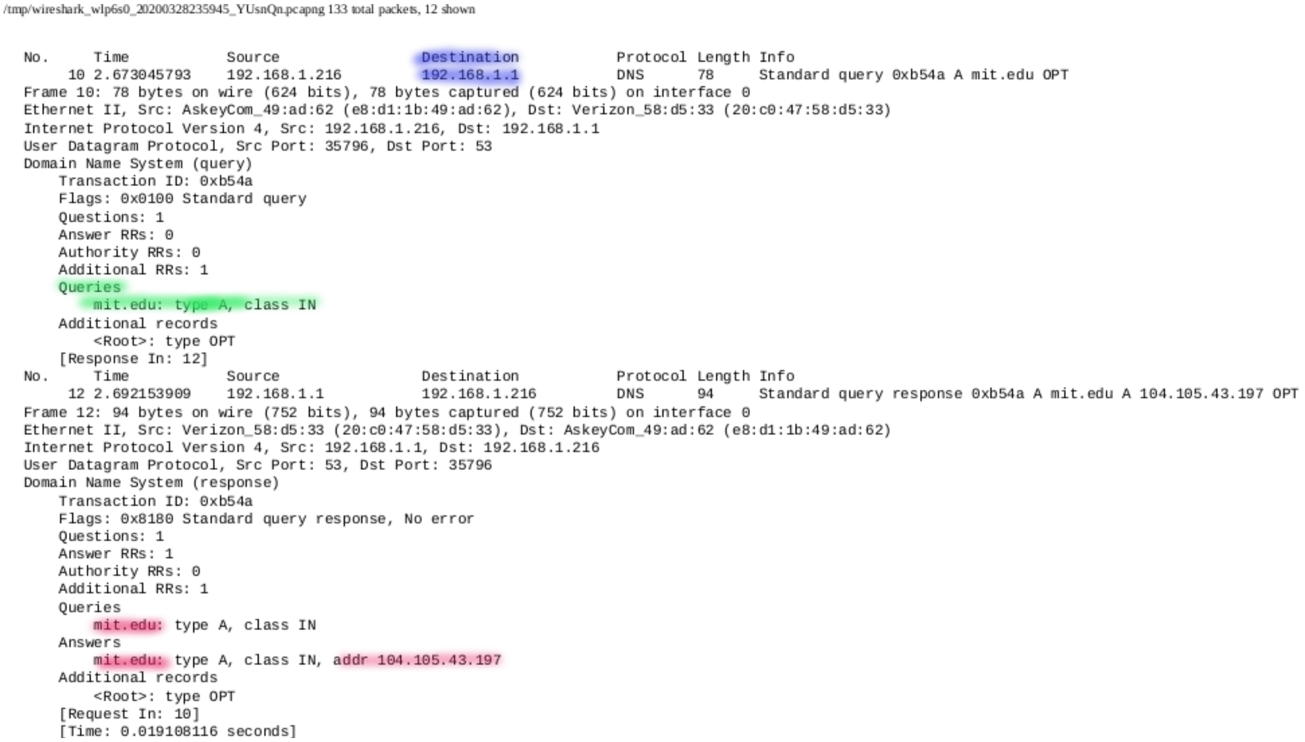
According to figure 7, the query message is of type OPT. It contains no answers.

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

According to figure 7, there are two answers. The answers contain a canonical name for an alias, as well as the host address. The answers also contain the name, type, class, time to live, data length and address.

15 Provide a screenshot

See figure 7.



```
/tmp/wireshark_wlp6s0_20200328235945_YUsnQn.pcapng 133 total packets, 12 shown

No.     Time           Source                Destination           Protocol Length Info
     10 2.673045793    192.168.1.216         192.168.1.1           DNS      78     Standard query 0xb54a A mit.edu OPT
Frame 10: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 35796, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xb54a
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
    Queries
        mit.edu: type A, class IN
    Additional records
        <Root>: type OPT
    [Response In: 12]
No.     Time           Source                Destination           Protocol Length Info
     12 2.692153909    192.168.1.1           192.168.1.216         DNS      94     Standard query response 0xb54a A mit.edu A 104.105.43.197 OPT
Frame 12: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.216
User Datagram Protocol, Src Port: 53, Dst Port: 35796
Domain Name System (response)
    Transaction ID: 0xb54a
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
    Queries
        mit.edu: type A, class IN
    Answers
        mit.edu: type A, class IN, addr 104.105.43.197
    Additional records
        <Root>: type OPT
    [Request In: 10]
    [Time: 0.019108116 seconds]
```

Figure 8:

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

According to figure 8, the DNS query message is being sent to 192.168.1.1. This is not the IP of my local default DNS server.

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

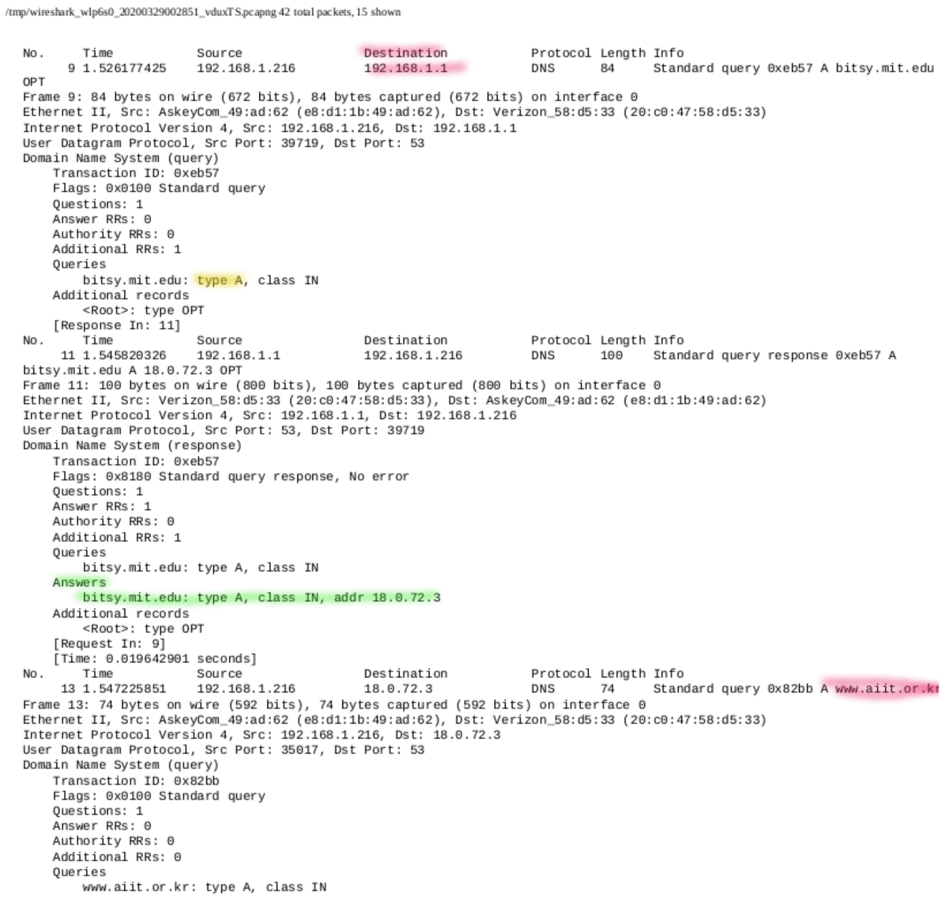
According to figure 8, the query is type A. It doesn't contain any answers.

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?

According to figure 8, the response message provides mit.edu, as well as an IP address of 104.105.43.197.

19 Provide a screenshot.

See figure 8.



/tmp/wireshark_wlp6s0_20200329002851_vduxTS.pcapng 42 total packets, 15 shown

```
No.     Time           Source                Destination           Protocol Length Info
      9 1.526177425    192.168.1.216         192.168.1.1           DNS      84     Standard query 0xeb57 A bitsy.mit.edu
OPT
Frame 9: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 39719, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xeb57
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
    Queries
        bitsy.mit.edu: type A, class IN
    Additional records
        <Root>: type OPT
    [Response In: 11]
No.     Time           Source                Destination           Protocol Length Info
     11 1.545820326    192.168.1.1           192.168.1.216         DNS      100    Standard query response 0xeb57 A
bitsy.mit.edu A 18.0.72.3 OPT
Frame 11: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.216
User Datagram Protocol, Src Port: 53, Dst Port: 39719
Domain Name System (response)
    Transaction ID: 0xeb57
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
    Queries
        bitsy.mit.edu: type A, class IN
    Answers
        bitsy.mit.edu: type A, class IN, addr 18.0.72.3
    Additional records
        <Root>: type OPT
    [Request In: 9]
    [Time: 0.019642901 seconds]
No.     Time           Source                Destination           Protocol Length Info
     13 1.547225851    192.168.1.216         18.0.72.3             DNS      74     Standard query 0x82bb A www.aiit.or.kr
Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 18.0.72.3
User Datagram Protocol, Src Port: 35017, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x82bb
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.aiit.or.kr: type A, class IN
```

Figure 9:

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?

According to figure 9, the DNS query message is being sent to 192.168.1.1, this is not the IP address of my defauly local DNS server. This IP address corresponds to www.aiit.or.kr

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

According to figure 9, it is of type A. It contains no answers.

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

According to figure 9 there is one answer which contains the IP address 18.0.72.3.

23 Provide a screenshot

See figure 9.