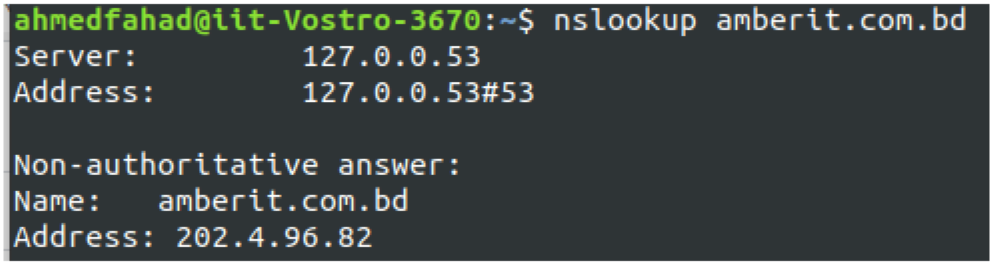
Wireshark Lab 3 (DNS)
BSSE 1204

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

Ans:

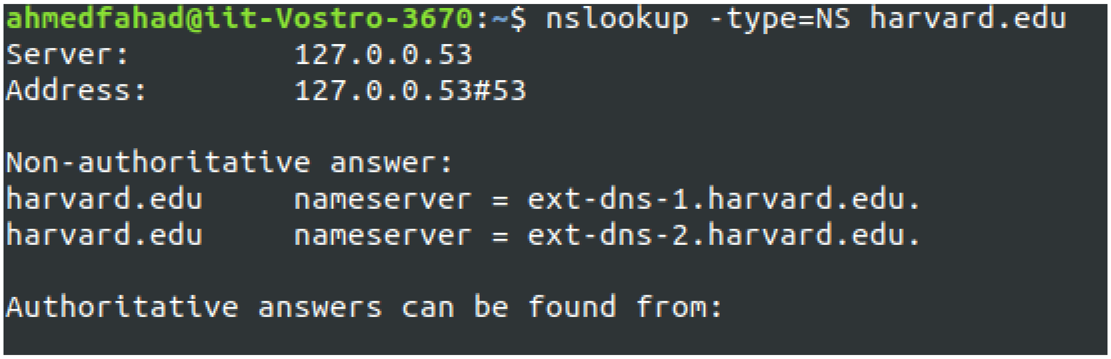


```
ahmedfahad@iit-Vostro-3670:~$ nslookup amberit.com.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   amberit.com.bd
Address: 202.4.96.82
```

The IP address: **202.4.96.82**

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

Ans:

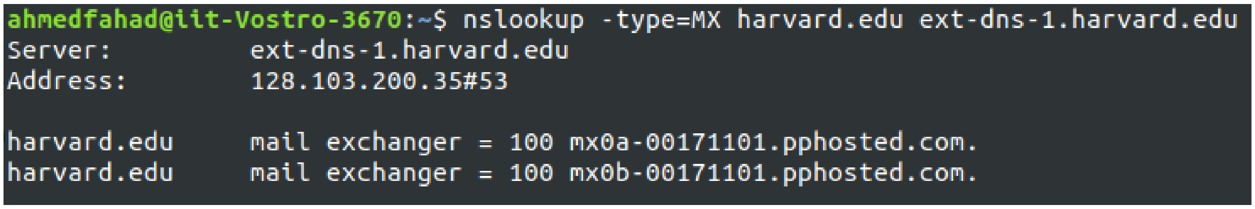


```
ahmedfahad@iit-Vostro-3670:~$ nslookup -type=NS harvard.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
harvard.edu     nameserver = ext-dns-1.harvard.edu.
harvard.edu     nameserver = ext-dns-2.harvard.edu.

Authoritative answers can be found from:
```

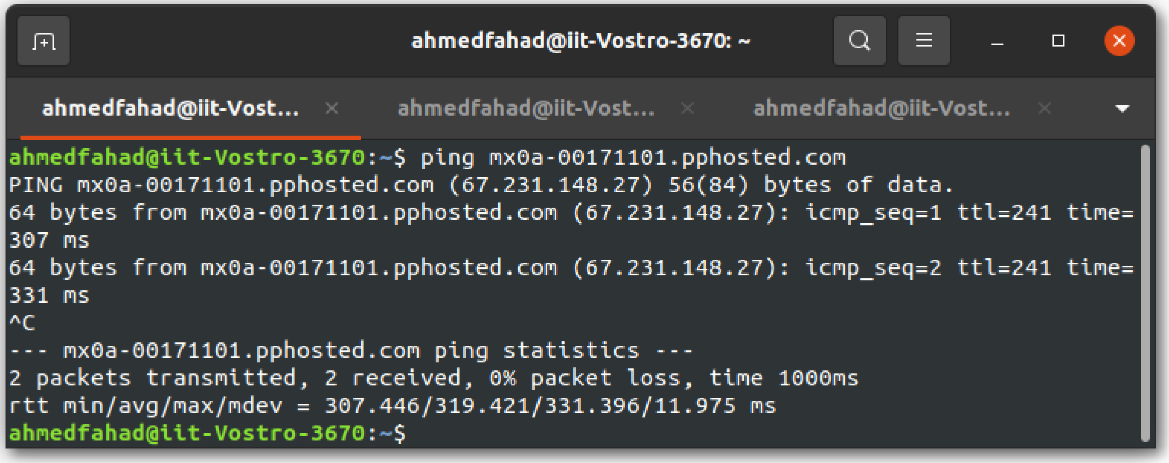
Authoritative DNS Server: **ext-dns-2.harvard.edu**

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?

Ans:



```
ahmedfahad@iit-Vostro-3670:~$ nslookup -type=MX harvard.edu ext-dns-1.harvard.edu
Server:         ext-dns-1.harvard.edu
Address:        128.103.200.35#53

harvard.edu     mail exchanger = 100 mx0a-00171101.pphosted.com.
harvard.edu     mail exchanger = 100 mx0b-00171101.pphosted.com.
```



```
ahmedfahad@iit-Vostro-3670:~$ ping mx0a-00171101.pphosted.com
PING mx0a-00171101.pphosted.com (67.231.148.27) 56(84) bytes of data.
64 bytes from mx0a-00171101.pphosted.com (67.231.148.27): icmp_seq=1 ttl=241 time=
307 ms
64 bytes from mx0a-00171101.pphosted.com (67.231.148.27): icmp_seq=2 ttl=241 time=
331 ms
^C
--- mx0a-00171101.pphosted.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 307.446/319.421/331.396/11.975 ms
ahmedfahad@iit-Vostro-3670:~$
```

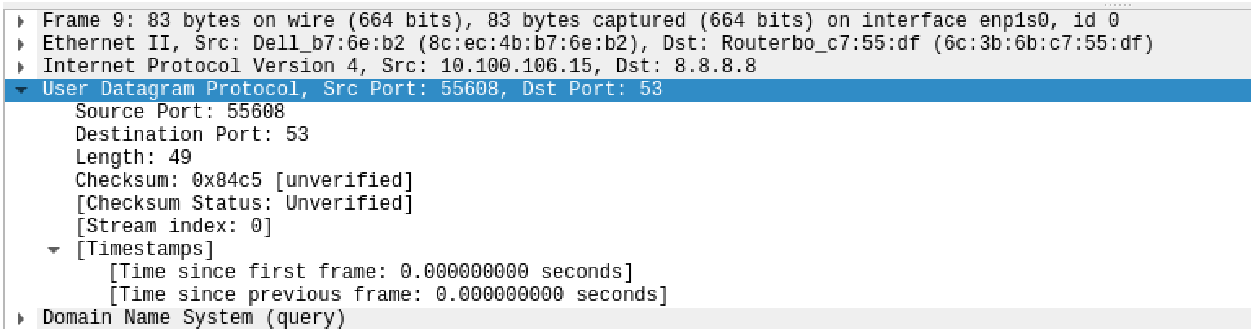
I didn't find the yahoo mail server. Rather I got **mx0a-00171101.pphosted.com** as the mail server of **harvard.edu**. IP of that server is collected from pinging the address and **67.231.148.27.**

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

Ans: 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?

Ans:

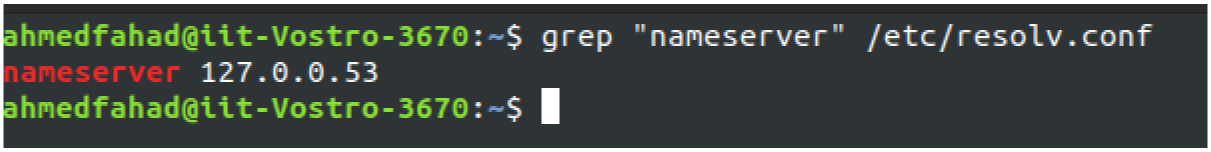


```
▸ Frame 9: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface enp1s0, id 0
▸ Ethernet II, Src: Dell_b7:6e:b2 (8c:ec:4b:b7:6e:b2), Dst: Routerbo_c7:55:df (6c:3b:6b:c7:55:df)
▸ Internet Protocol Version 4, Src: 10.100.106.15, Dst: 8.8.8.8
▾ User Datagram Protocol, Src Port: 55608, Dst Port: 53
     Source Port: 55608
     Destination Port: 53
     Length: 49
     Checksum: 0x84c5 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
   ▾ [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
▸ Domain Name System (query)
```

Source Port of DNS response message: **53**
Destination Port of DNS query message: **53**

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

Ans: DNS query message was sent to **8.8.8.8**



```
ahmedfahad@iit-Vostro-3670:~$ grep "nameserver" /etc/resolv.conf
nameserver 127.0.0.53
ahmedfahad@iit-Vostro-3670:~$ 
```

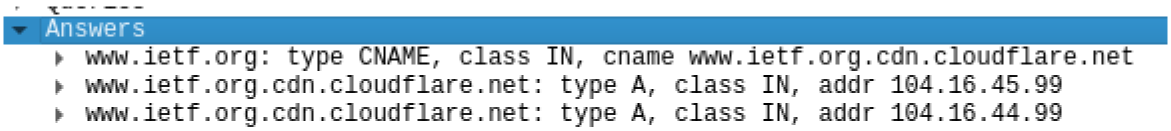
Local DNS Server IP address: **127.0.0.53.** No, these two IP addresses are not the same.

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

Ans: It’s of Type **A. No**, the query message doesn’t contain any “answers”. It’s in the DNS response message.

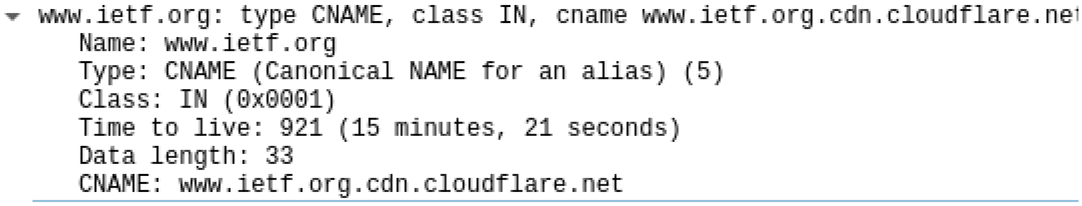
8. Examine the DNS response message. How many “answers” are provided? What Do each of these answers contain?

Ans:



```
▾ 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 104.16.45.99
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
```

3 answers are provided.

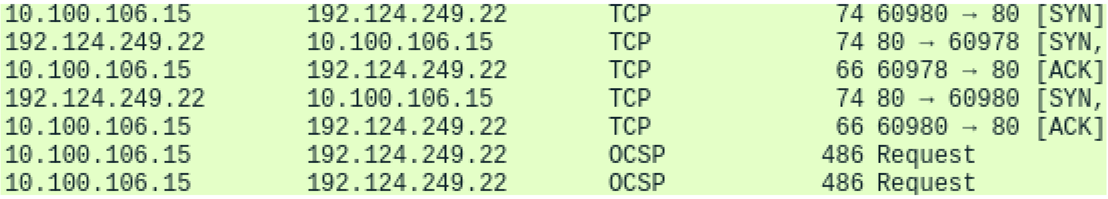


```
▾ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
     Name: www.ietf.org
     Type: CNAME (Canonical NAME for an alias) (5)
     Class: IN (0x0001)
     Time to live: 921 (15 minutes, 21 seconds)
     Data length: 33
     CNAME: www.ietf.org.cdn.cloudflare.net
```

Each of the answers contain **Name, Type, Class, Time to live(TTL), Data length and CNAME.**

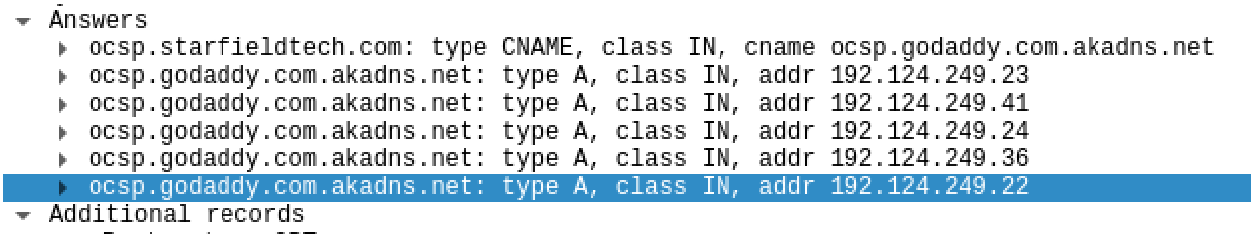
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans:



```
10.100.106.15       192.124.249.22      TCP          74 60980 → 80 [SYN]
192.124.249.22      10.100.106.15       TCP          74 80 → 60978 [SYN,
10.100.106.15       192.124.249.22      TCP          66 60978 → 80 [ACK]
192.124.249.22      10.100.106.15       TCP          74 80 → 60980 [SYN,
10.100.106.15       192.124.249.22      TCP          66 60980 → 80 [ACK]
10.100.106.15       192.124.249.22      OCSP        486 Request
10.100.106.15       192.124.249.22      OCSP        486 Request
```

Destination IP of the SYN packet is **192.124.249.22**



```
▾ Answers
    ▸ ocsp.starfieldtech.com: type CNAME, class IN, cname ocsp.godaddy.com.akadns.net
    ▸ ocsp.godaddy.com.akadns.net: type A, class IN, addr 192.124.249.23
    ▸ ocsp.godaddy.com.akadns.net: type A, class IN, addr 192.124.249.41
    ▸ ocsp.godaddy.com.akadns.net: type A, class IN, addr 192.124.249.24
    ▸ ocsp.godaddy.com.akadns.net: type A, class IN, addr 192.124.249.36
    ▸ ocsp.godaddy.com.akadns.net: type A, class IN, addr 192.124.249.22
▾ Additional records
```

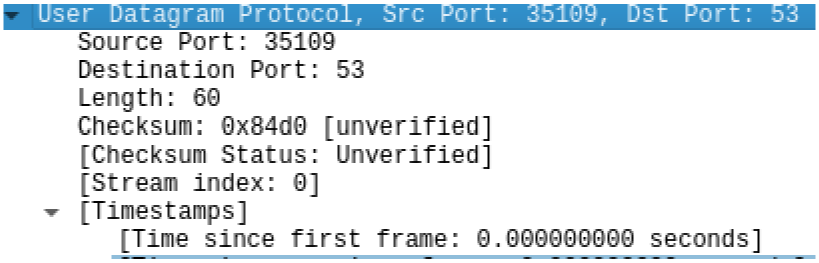
According to the above screenshot **192.124.249.22** corresponds to any of the DNS response messages.

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

Ans: No.

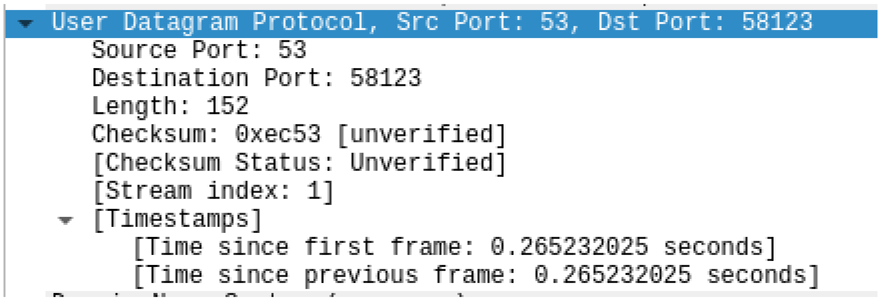
11. What is the destination port for the DNS query message? What is the source port of a DNS response message?

Ans:



```
▾ User Datagram Protocol, Src Port: 35109, Dst Port: 53
      Source Port: 35109
      Destination Port: 53
      Length: 60
      Checksum: 0x84d0 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
    ▾ [Timestamps]
         [Time since first frame: 0.000000000 seconds]
```

Destination port for the DNS query message is **53**

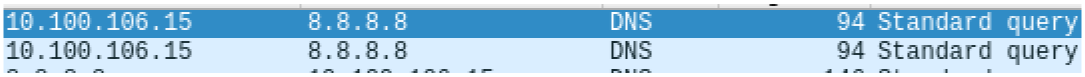


```
▾ User Datagram Protocol, Src Port: 53, Dst Port: 58123
      Source Port: 53
      Destination Port: 58123
      Length: 152
      Checksum: 0xec53 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 1]
    ▾ [Timestamps]
         [Time since first frame: 0.265232025 seconds]
         [Time since previous frame: 0.265232025 seconds]
```

Source port for the DNS response message is **53**

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

Ans:

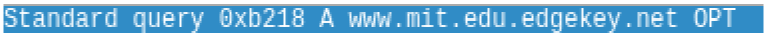


```
10.100.106.15      8.8.8.8           DNS          94 Standard query
10.100.106.15      8.8.8.8           DNS          94 Standard query
```

DNS query message was sent to **8.8.8.8.** No, this is not the IP address of my default local DNS server.

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

Ans:

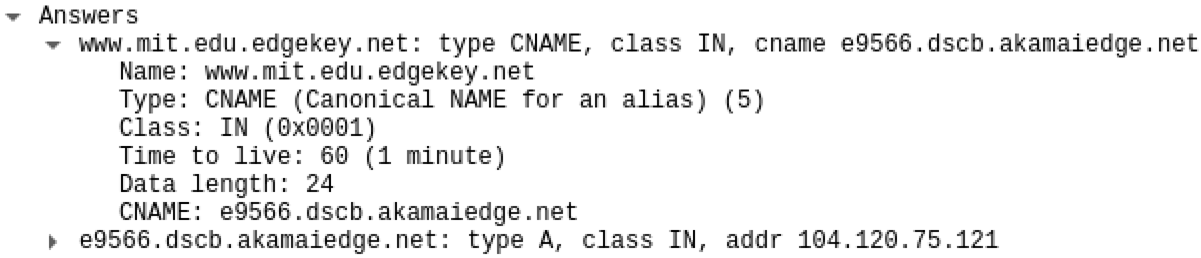


```
Standard query 0xb218 A www.mit.edu.edgekey.net OPT
```

It’s a Type **A** DNS query message. No, it doesn’t contain any “answers”.

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

Ans:

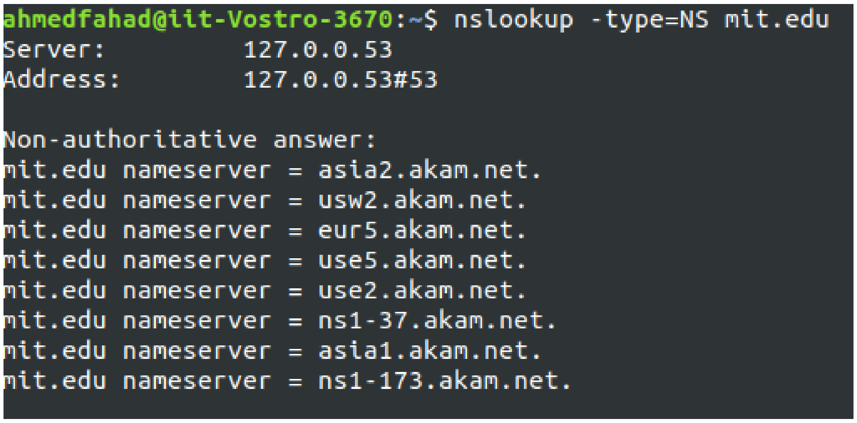


```
▾ Answers
  ▾ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▸ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.120.75.121
```

2 Answers in DNS response message. Each of the answers contains Name, Type, Class, Time to live, Data length, CNAME.

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

Ans:



```
ahmedfahad@iit-Vostro-3670:~$ nslookup -type=NS mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

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

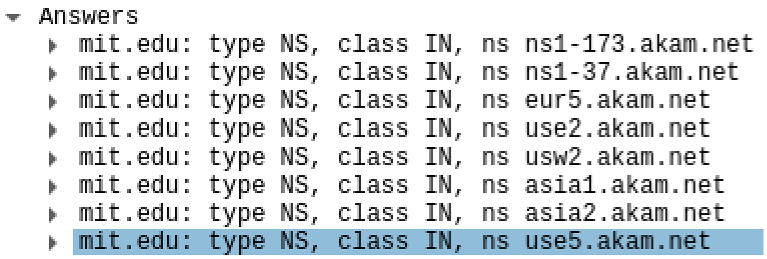
The IP address is **127.0.0.53** which is the IP of my default local DNS address.

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

Ans: DNS query type is **NS.** No, it doesn't.

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

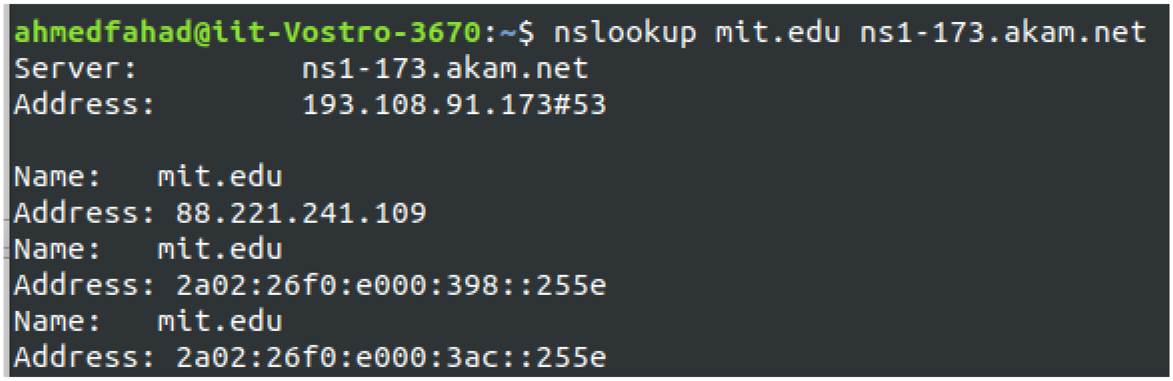
Ans: MIT nameservers provided with the response message are **ns1-173.akam.net, ns1-37.akam.net, eur5.akam.net, use2.akam.net, usw2.akam.net, asia1.akam.net, asia1.akam.net, asia1.akam.net**. No, it doesn't provide any IP address.



```
▾ Answers
  ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
  ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
  ▸ mit.edu: type NS, class IN, ns eur5.akam.net
  ▸ mit.edu: type NS, class IN, ns use2.akam.net
  ▸ mit.edu: type NS, class IN, ns usw2.akam.net
  ▸ mit.edu: type NS, class IN, ns asia1.akam.net
  ▸ mit.edu: type NS, class IN, ns asia2.akam.net
  ▸ mit.edu: type NS, class IN, ns use5.akam.net
```

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

Ans:



```
ahmedfahad@iit-Vostro-3670:~$ nslookup mit.edu ns1-173.akam.net
Server:         ns1-173.akam.net
Address:        193.108.91.173#53

Name:   mit.edu
Address: 88.221.241.109
Name:   mit.edu
Address: 2a02:26f0:e000:398::255e
Name:   mit.edu
Address: 2a02:26f0:e000:3ac::255e
```

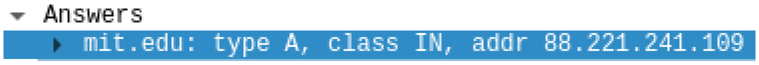
The IP address is **193.108.91.173.** This is not the default local DNS server. The IP address corresponds to ns1-173.akam.net.

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

Ans: DNS query type is **A.** No, it doesn't.

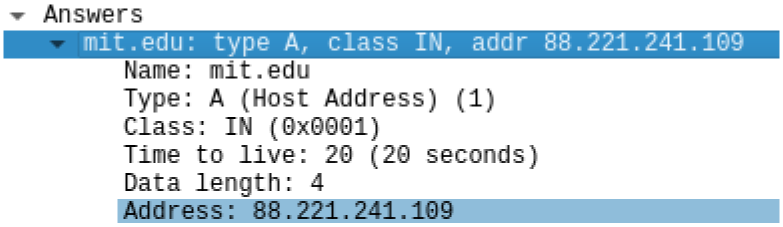
22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

Ans:



```
▾ Answers
   ▸ mit.edu: type A, class IN, addr 88.221.241.109
```

Only **1 answer** is provided here.



```
▾ Answers
   ▾ mit.edu: type A, class IN, addr 88.221.241.109
         Name: mit.edu
         Type: A (Host Address) (1)
         Class: IN (0x0001)
         Time to live: 20 (20 seconds)
         Data length: 4
         Address: 88.221.241.109
```

Each of the answers contains Name, Type, Class, Time to live, Data length, Address.