Lab_2b_Wireshark_DNS_v8.0

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

```
tuandat@tuandatHP ~ nslookup www.vnexpress.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.vnexpress.net       canonical name = vnexpress.net.
Name:   vnexpress.net
Address: 111.65.250.2
```

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

```
tuandat@tuandatHP ~ nslookup -type=NS uoi.gr
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
uoi.gr  nameserver = marina.noc.uoi.gr.
uoi.gr  nameserver = sns1.grnet.gr.
uoi.gr  nameserver = kouzina.noc.uoi.gr.
uoi.gr  nameserver = sns0.grnet.gr.

Authoritative answers can be found from:
```

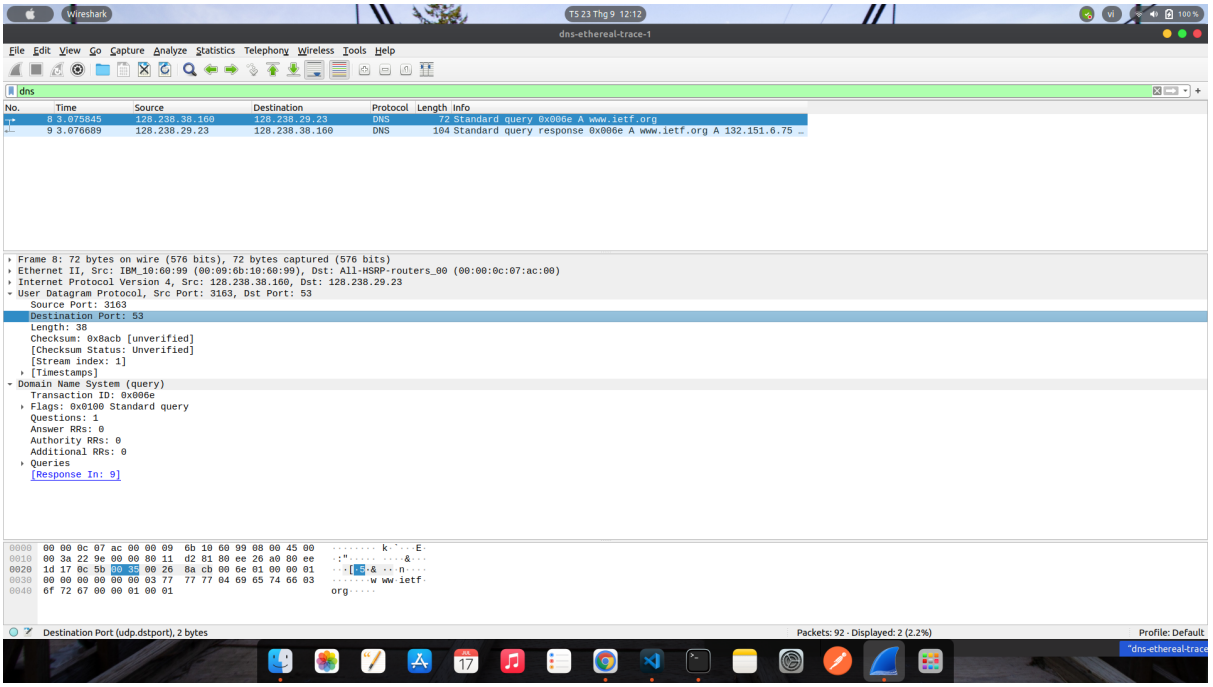
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

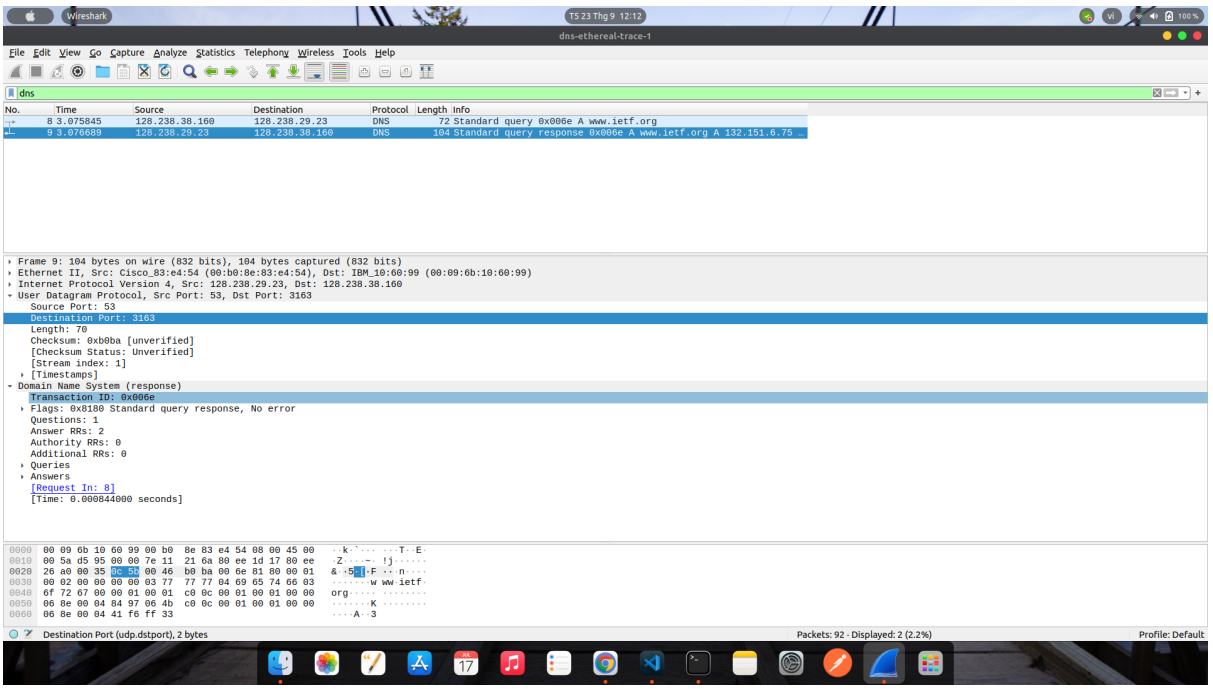
```
tuandat@tuandatHP ~/MMT nslookup mail.yahoo.com gong.ci.uv.es
Server:         gong.ci.uv.es
Address:        147.156.1.1#53

** server can't find mail.yahoo.com: REFUSED
```

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

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





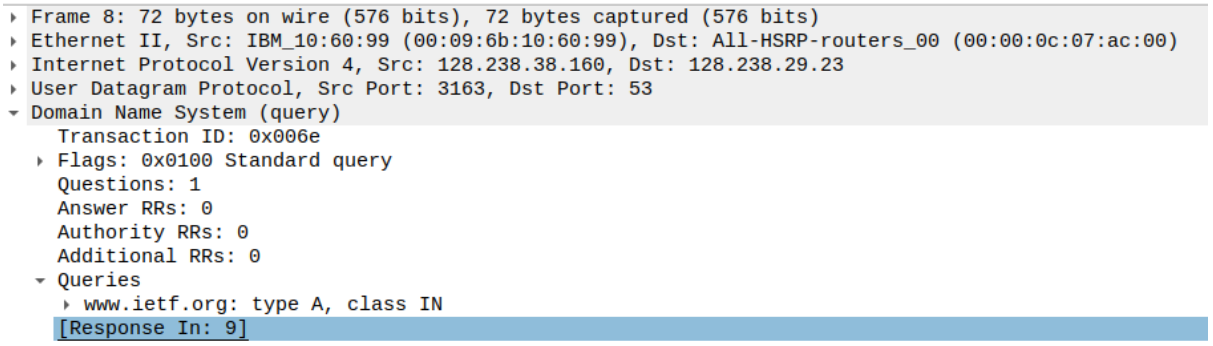
The destination port for the DNS query is 53 and the source port of the DNS response is 53.

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?

Answer

It's sent to 128.238.29.22, is not the default local DNS server because i use file dns-ethereal-trace-1 in zip file

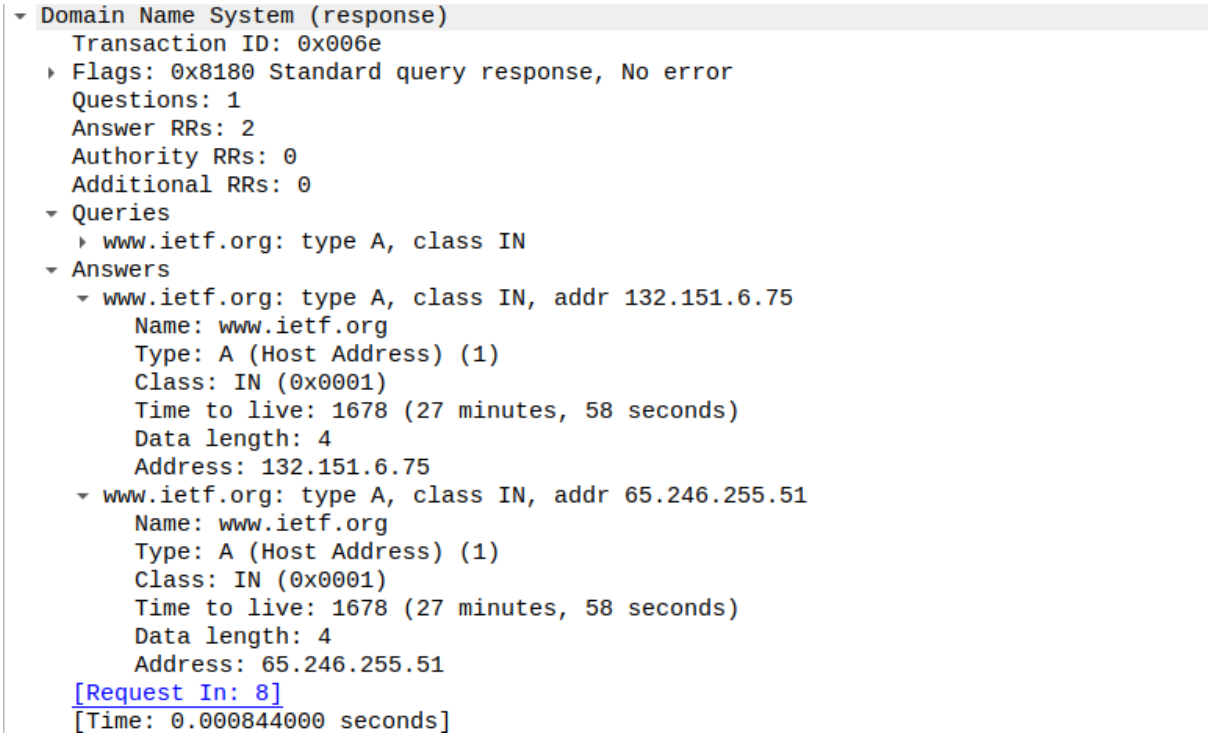
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



Answer:

It's a type A Standard Query and it doesn't contain any answers.

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



Answer:

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?

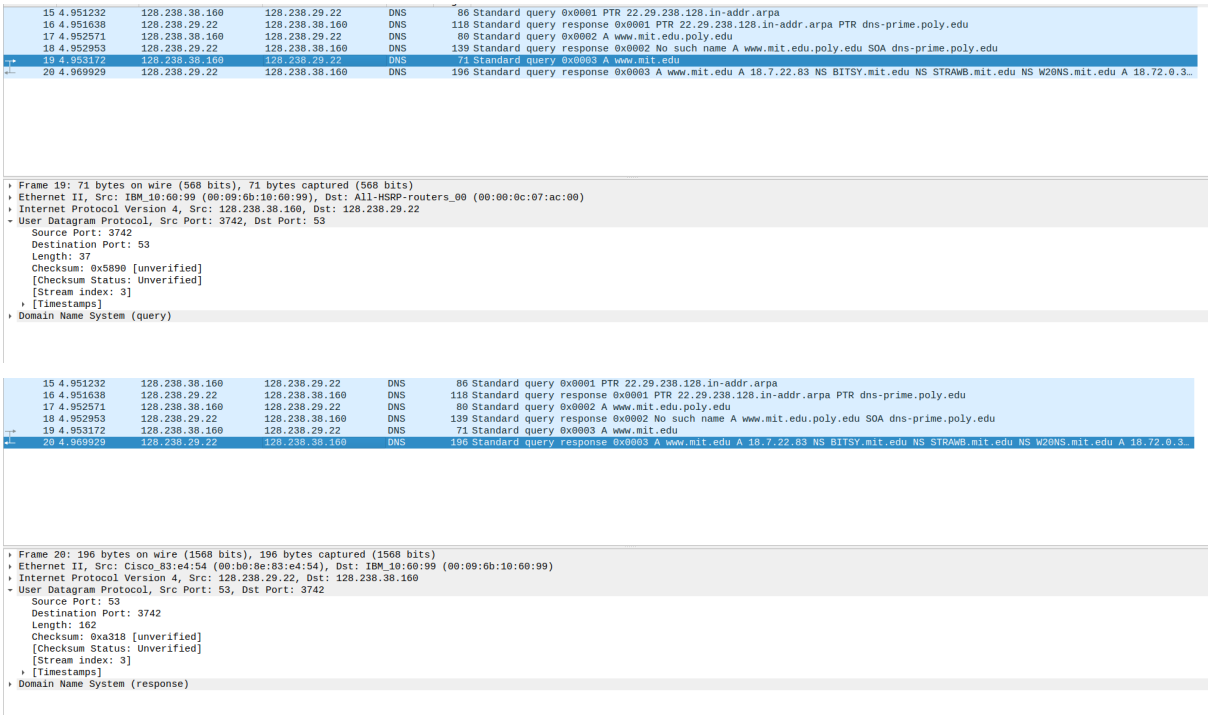
Answer:

The first SYN packet was sent to 132.151.6.75 which corresponds to the first IP address provided in the DNS response message.

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

Answer: No

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



Answer:

The destination port of the DNS query is 53 and the source port of the DNS response is 53.

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

Answer:

It's sent to 128.238.29.22, is not the default local DNS server because i use file dns-ethereal-trace-2 in zip file

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

```
▸ Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
▸ Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
▸ Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
▾ User Datagram Protocol, Src Port: 3742, Dst Port: 53
    Source Port: 3742
    Destination Port: 53
    Length: 37
    Checksum: 0x5890 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  ▸ [Timestamps]
▾ Domain Name System (query)
    Transaction ID: 0x0003
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.mit.edu: type A, class IN
    [Response In: 20]
```

Answer:

The query is of type A and it doesn't contain any answers.

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

```
▸ Frame 20: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits)
▸ Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
▸ Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
▾ User Datagram Protocol, Src Port: 53, Dst Port: 3742
    Source Port: 53
    Destination Port: 3742
    Length: 162
    Checksum: 0xa318 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  ▸ [Timestamps]
▾ Domain Name System (response)
    Transaction ID: 0x0003
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  ▾ Queries
    ▸ www.mit.edu: type A, class IN
  ▾ Answers
    ▾ www.mit.edu: type A, class IN, addr 18.7.22.83
        Name: www.mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 4
        Address: 18.7.22.83
```

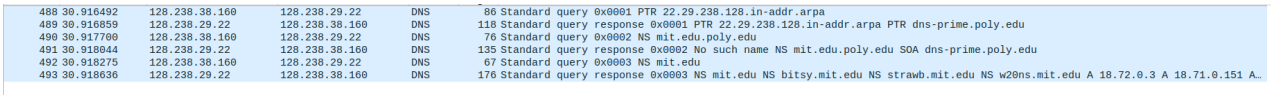
Answer:

The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.

15. Provide a screenshot.

Answer: In answer for questions 12, 13, 14

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

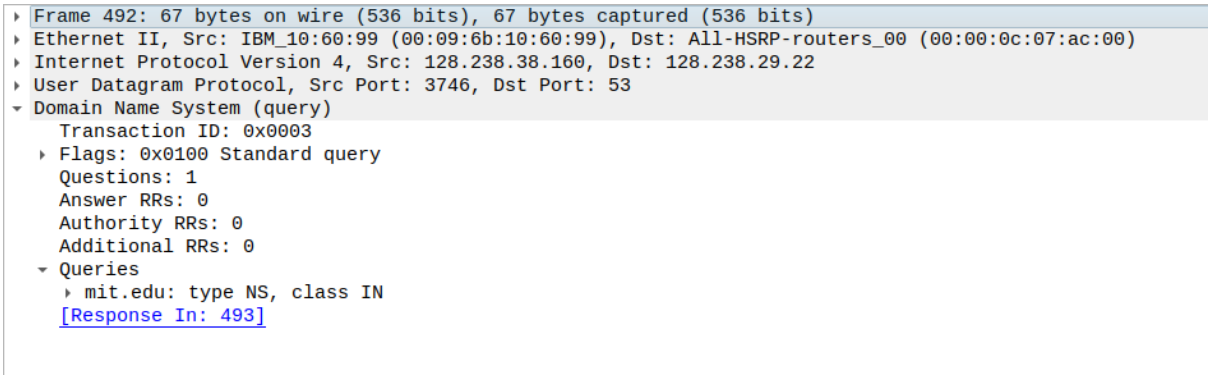


```
488 30.916492   128.238.38.160   128.238.29.22    DNS   86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489 30.916859   128.238.29.22    128.238.38.160   DNS  118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490 30.917700   128.238.38.160   128.238.29.22    DNS   76 Standard query 0x0002 NS mit.edu.poly.edu
491 30.918044   128.238.29.22    128.238.38.160   DNS  135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492 30.918275   128.238.38.160   128.238.29.22    DNS   67 Standard query 0x0003 NS mit.edu
493 30.918636   128.238.29.22    128.238.38.160   DNS  176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71.0.151 A…
```

Answer:

It's sent to 128.238.29.22, is not the default local DNS server because i use file dns-ethereal-trace-3 in zip file

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

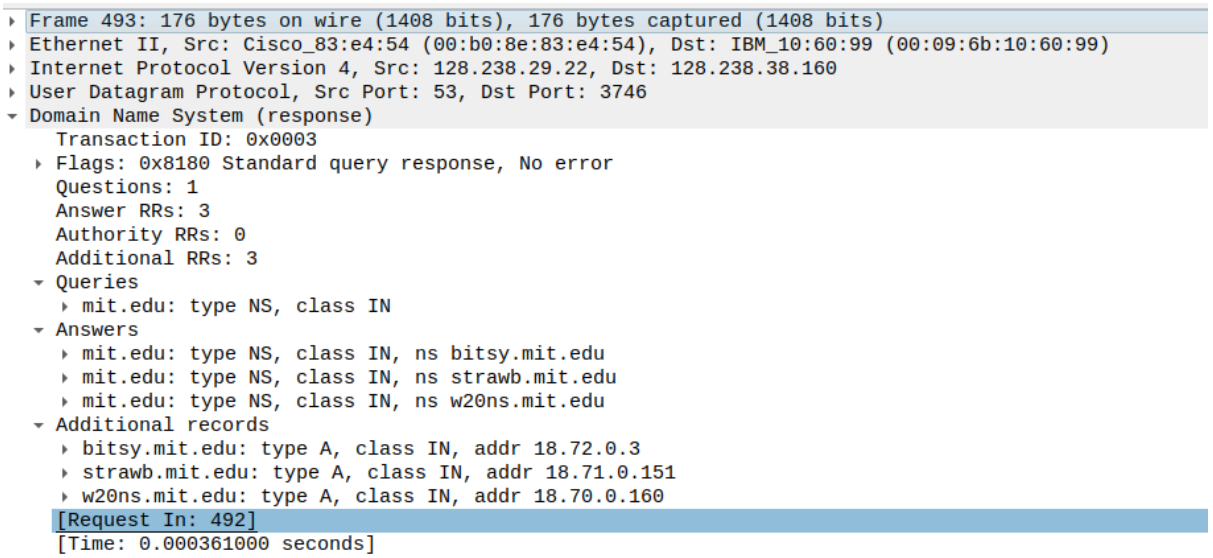


```
▸ Frame 492: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
▸ Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
▸ Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
▸ User Datagram Protocol, Src Port: 3746, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x0003
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mit.edu: type NS, class IN
    [Response In: 493]
```

Answer:

_____ It's a type NS DNS query that doesn't contain any answer.

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?



```
▸ Frame 493: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
▸ Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
▸ Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
▸ User Datagram Protocol, Src Port: 53, Dst Port: 3746
▾ Domain Name System (response)
    Transaction ID: 0x0003
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
  ▾ Queries
    ▸ mit.edu: type NS, class IN
  ▾ Answers
    ▸ mit.edu: type NS, class IN, ns bitsy.mit.edu
    ▸ mit.edu: type NS, class IN, ns strawb.mit.edu
    ▸ mit.edu: type NS, class IN, ns w20ns.mit.edu
  ▾ Additional records
    ▸ bitsy.mit.edu: type A, class IN, addr 18.72.0.3
    ▸ strawb.mit.edu: type A, class IN, addr 18.71.0.151
    ▸ w20ns.mit.edu: type A, class IN, addr 18.70.0.160
    [Request In: 492]
    [Time: 0.000361000 seconds]
```

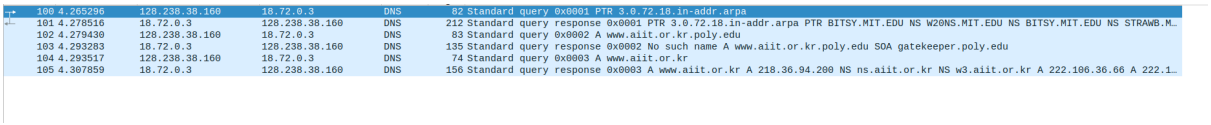
Answer:

The response message provides 3 MIT nameservers: w20ns.mit.edu[18.70.0.160], strawb.mit.edu[18.71.0.150], and bitsy.mit.edu[18.72.0.3]. The IP addresses for the name servers were included under the additional records category sent back as part of the response message.

19. Provide a screenshot.

Answer: In answer 16, 17, 18

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?



```
100 4.265296    128.238.38.160  18.72.0.3       DNS   82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101 4.278516    18.72.0.3       128.238.38.160  DNS  212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.M…
102 4.279430    128.238.38.160  18.72.0.3       DNS   83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
103 4.293283    18.72.0.3       128.238.38.160  DNS  135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
104 4.293517    128.238.38.160  18.72.0.3       DNS   74 Standard query 0x0003 A www.aiit.or.kr
105 4.307859    18.72.0.3       128.238.38.160  DNS  156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A 222.1…
```

Answer:

This DNS query message is sent to 18.72.0.3 which is the IP address of the MIT DNS response sender.

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

```
▸ Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
▸ Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
▸ User Datagram Protocol, Src Port: 3753, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x0003
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.aiit.or.kr: type A, class IN
    [Response In: 105]
```

Answer:

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

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

```
▸ Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
▸ Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
▸ Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
▸ User Datagram Protocol, Src Port: 53, Dst Port: 3753
▾ Domain Name System (response)
    Transaction ID: 0x0003
  ▾ 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: 2
    Additional RRs: 2
  ▾ Queries
    ▸ www.aiit.or.kr: type A, class IN
  ▾ Answers
    ▸ www.aiit.or.kr: type A, class IN, addr 218.36.94.200
```

Answer:

_____It only provided one “answer” containing the servers IP address, however, the server also returned a flag that stated that it could complete a recursive query.

23. Provide a screenshot.

Answer: In answer for questions 20, 21, 22