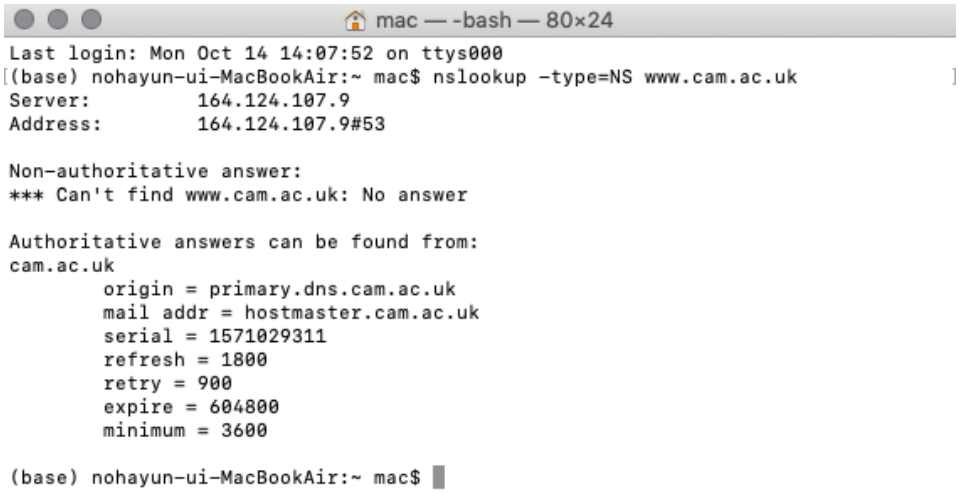
Wireshark Lab : DNS

17011588 노하윤
17011599 안정연

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

We queried the webpage for the Asian Institute of Technology in Thailand. The IP address of that server was 164.124.107.9

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



We used the webpage for Cambridge University in England. This webpage is http://www.cam.ac.uk. The authoritative DNS server is authdns0.csx.ac.uk.

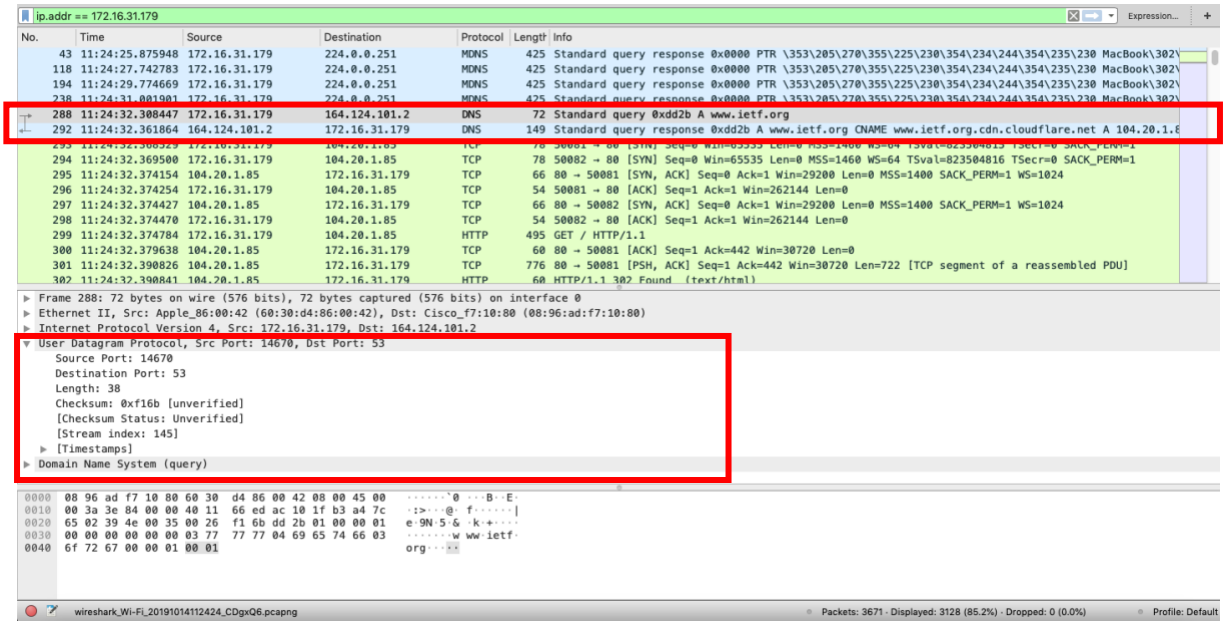
3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

```
mac — -bash — 80×24
Last login: Mon Oct 14 14:12:22 on ttys000
(base) nohayun-ui-MacBookAir:~ mac$ nslookup www.cam.ac.uk mail.yahoo.com
;; connection timed out; no servers could be reached

(base) nohayun-ui-MacBookAir:~ mac$
```

The IP address for the DNS server if queried for the Yahoo! mail server is 209.191.122.42

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



The DNS query and response messages are sent over UDP.

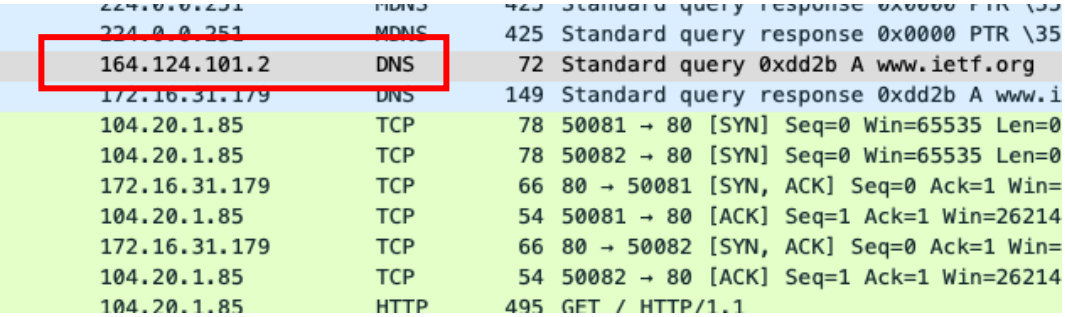
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

```
▼ User Datagram Protocol, Src Port: 14670, Dst Port: 53
    Source Port: 14670
    Destination Port: 53
    Length: 38
    Checksum: 0xf16b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 145]
  ▶ [Timestamps]
▶ Domain Name System (query)
```

The destination port is 53

The source port is 14670

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?

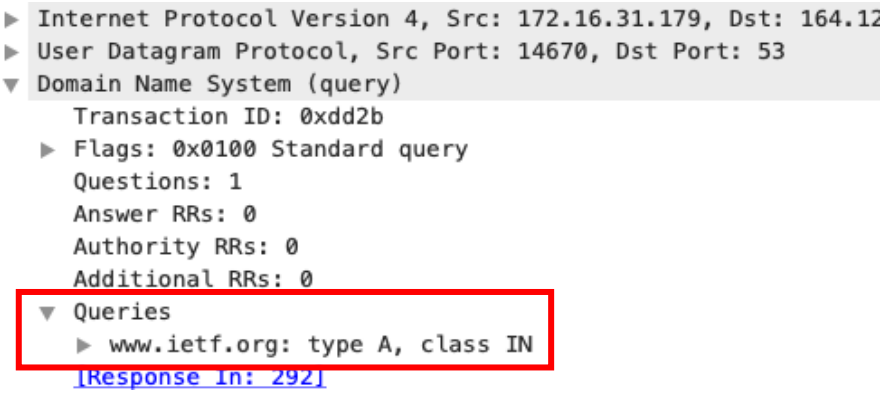


224.0.0.251	MDNS	425	Standard query response 0x0000 PTR \35
164.124.101.2	DNS	72	Standard query 0xdd2b A www.ietf.org
172.16.31.179	DNS	149	Standard query response 0xdd2b A www.i
104.20.1.85	TCP	78	50081 → 80 [SYN] Seq=0 Win=65535 Len=0
104.20.1.85	TCP	78	50082 → 80 [SYN] Seq=0 Win=65535 Len=0
172.16.31.179	TCP	66	80 → 50081 [SYN, ACK] Seq=0 Ack=1 Win=
104.20.1.85	TCP	54	50081 → 80 [ACK] Seq=1 Ack=1 Win=26214
172.16.31.179	TCP	66	80 → 50082 [SYN, ACK] Seq=0 Ack=1 Win=
104.20.1.85	TCP	54	50082 → 80 [ACK] Seq=1 Ack=1 Win=26214
104.20.1.85	HTTP	495	GET / HTTP/1.1

The DNS query was sent to IP address 164.124.101.2.

Yes it is the same IP address ast hat of my local DNS server.

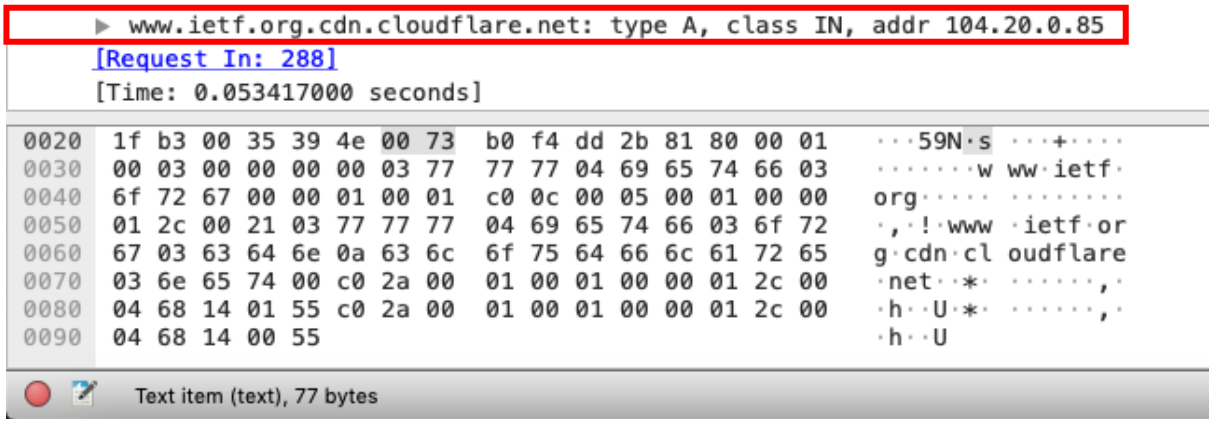
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



```
▶ Internet Protocol Version 4, Src: 172.16.31.179, Dst: 164.12
▶ User Datagram Protocol, Src Port: 14670, Dst Port: 53
▼ Domain Name System (query)
    Transaction ID: 0xdd2b
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.ietf.org: type A, class IN
    [Response In: 292]
```

The query message was a type "A" query, but the message did not contain any "answers."

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

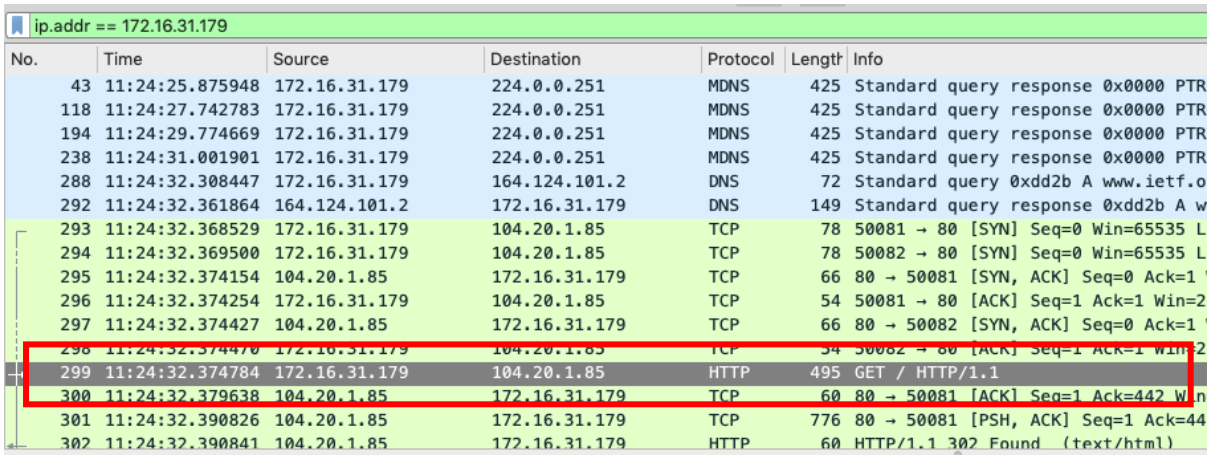


The response message contained one answer to the query which was the sites address [104.20.0.85]. Although it also provided 6 authoritative nameservers, and 11 other responses containing additional information.

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?

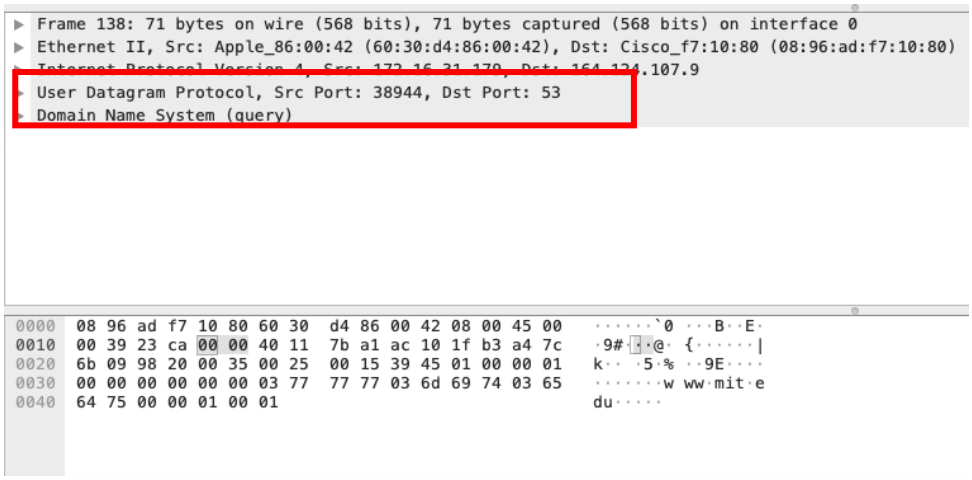
The destination of the SYN packet is [104.20.0.85], the same address that was provided in the DNS response message as the type "A" address of the webpage.

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



Yes, my host did issue new DNS queries before the images were retrieved. For example, one such query was for an image from open-stand.org. The image corresponding to the page was not returned until this query was made.

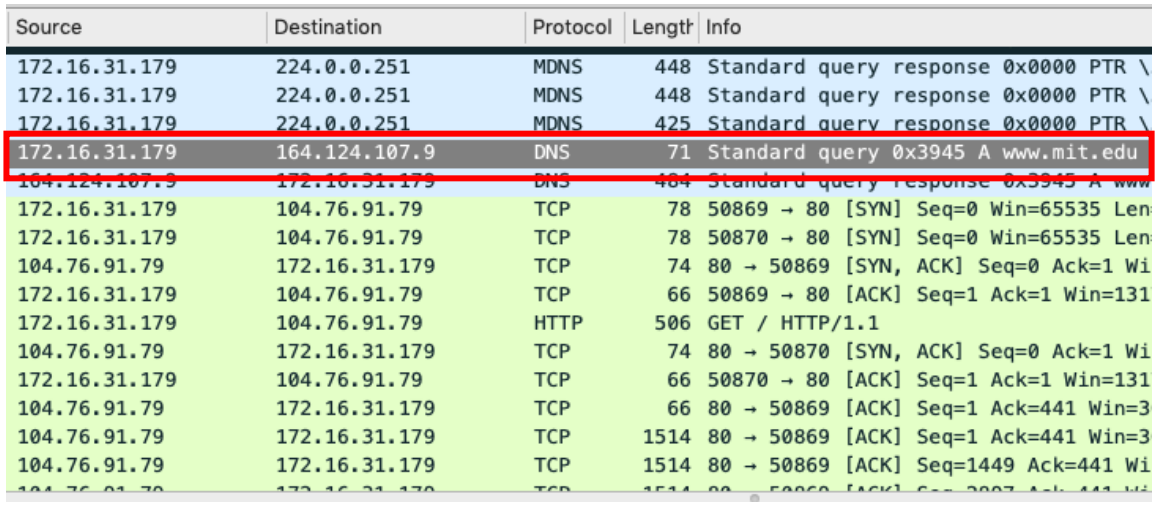
11. What is the destination port for the DNS query message? What is the source port of DNS response message?



Destination Port : 53

Source Port : 38944

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

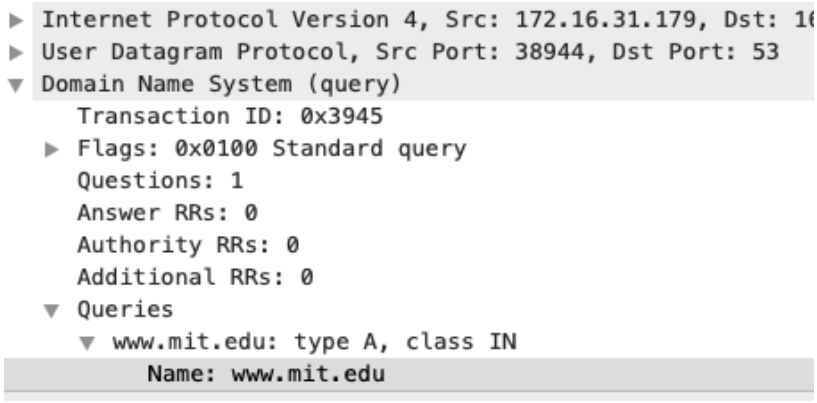


Source	Destination	Protocol	Length	Info
172.16.31.179	224.0.0.251	MDNS	448	Standard query response 0x0000 PTR \
172.16.31.179	224.0.0.251	MDNS	448	Standard query response 0x0000 PTR \
172.16.31.179	224.0.0.251	MDNS	425	Standard query response 0x0000 PTR \
172.16.31.179	164.124.107.9	DNS	71	Standard query 0x3945 A www.mit.edu
172.16.31.179	104.76.91.79	TCP	78	50869 → 80 [SYN] Seq=0 Win=65535 Len
172.16.31.179	104.76.91.79	TCP	78	50870 → 80 [SYN] Seq=0 Win=65535 Len
104.76.91.79	172.16.31.179	TCP	74	80 → 50869 [SYN, ACK] Seq=0 Ack=1 Wi
172.16.31.179	104.76.91.79	TCP	66	50869 → 80 [ACK] Seq=1 Ack=1 Win=131
172.16.31.179	104.76.91.79	HTTP	506	GET / HTTP/1.1
104.76.91.79	172.16.31.179	TCP	74	80 → 50870 [SYN, ACK] Seq=0 Ack=1 Wi
172.16.31.179	104.76.91.79	TCP	66	50870 → 80 [ACK] Seq=1 Ack=1 Win=131
104.76.91.79	172.16.31.179	TCP	66	80 → 50869 [ACK] Seq=1 Ack=441 Win=3
104.76.91.79	172.16.31.179	TCP	1514	80 → 50869 [ACK] Seq=1 Ack=441 Win=3
104.76.91.79	172.16.31.179	TCP	1514	80 → 50869 [ACK] Seq=1449 Ack=441 Wi

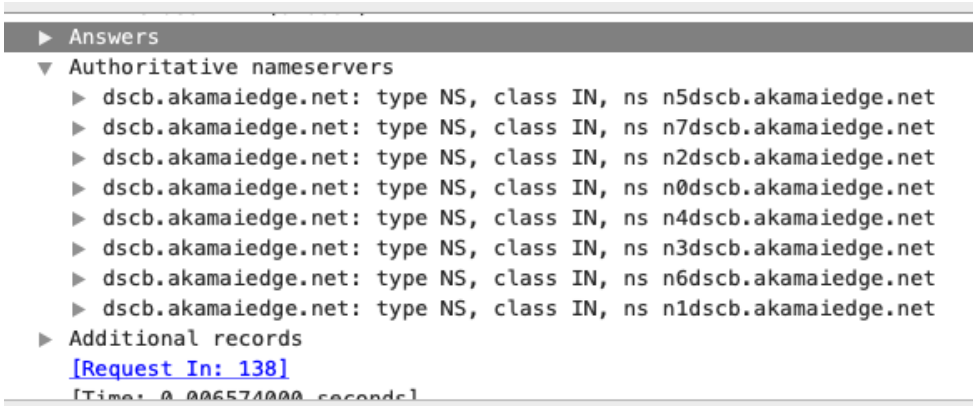
The DNS query message is sent to IP address [164.124.107.9], the same address as my default local DNS server.

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.

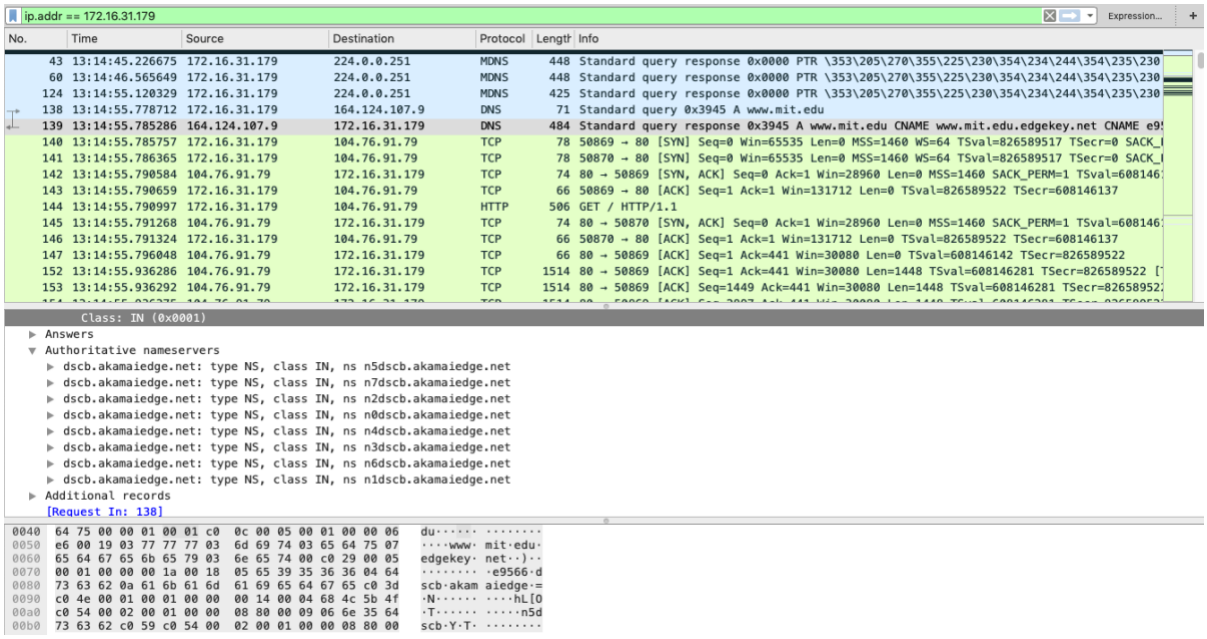


14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?



The response message contains one answer to the aforementioned query which the type "A" address of http://www.mit.edu or 18.9.22.169. It also contained information on 3 authoritative nameservers and 3 additional records.

15. Provide a screenshot.



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

The query is sent to 164.124.107.9, the same IP address as that of my default local DNS server.

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.

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?

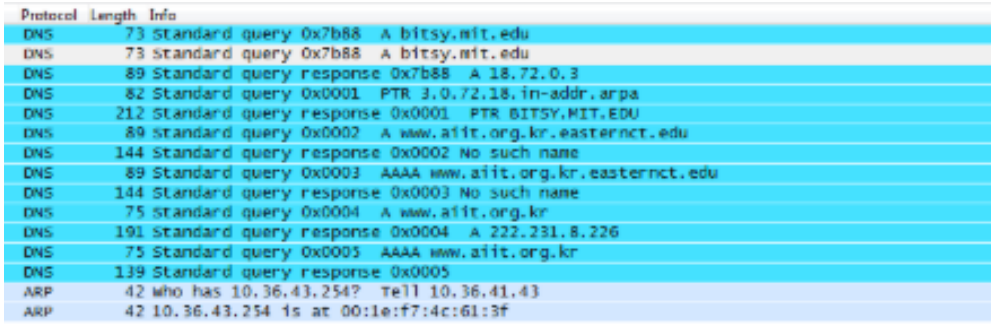
The response message provides 3 MIT nameservers :

w20ns.mit.edu[18.70.0.160] , strawb.mit.edu[18.1.0.150]

bitsy.mit.edu[18.72.0.3].

The IP addresses for the nameservers was included under the additional records category sent back as part of the response message.

19. Provide a screenshot.

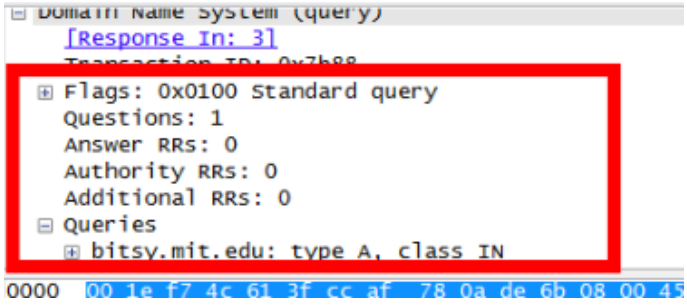


20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

This DNS query message is sent to 149.152.136.65 which is the IP address of the MIT DNS response sender.

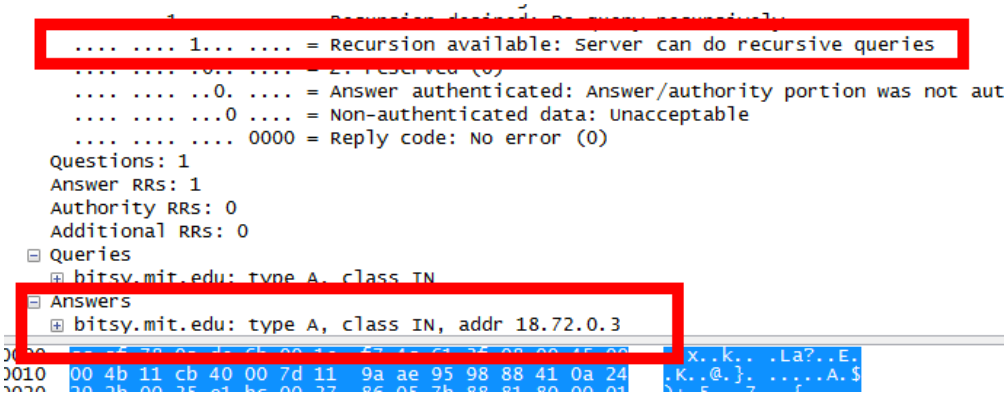
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

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



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

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.