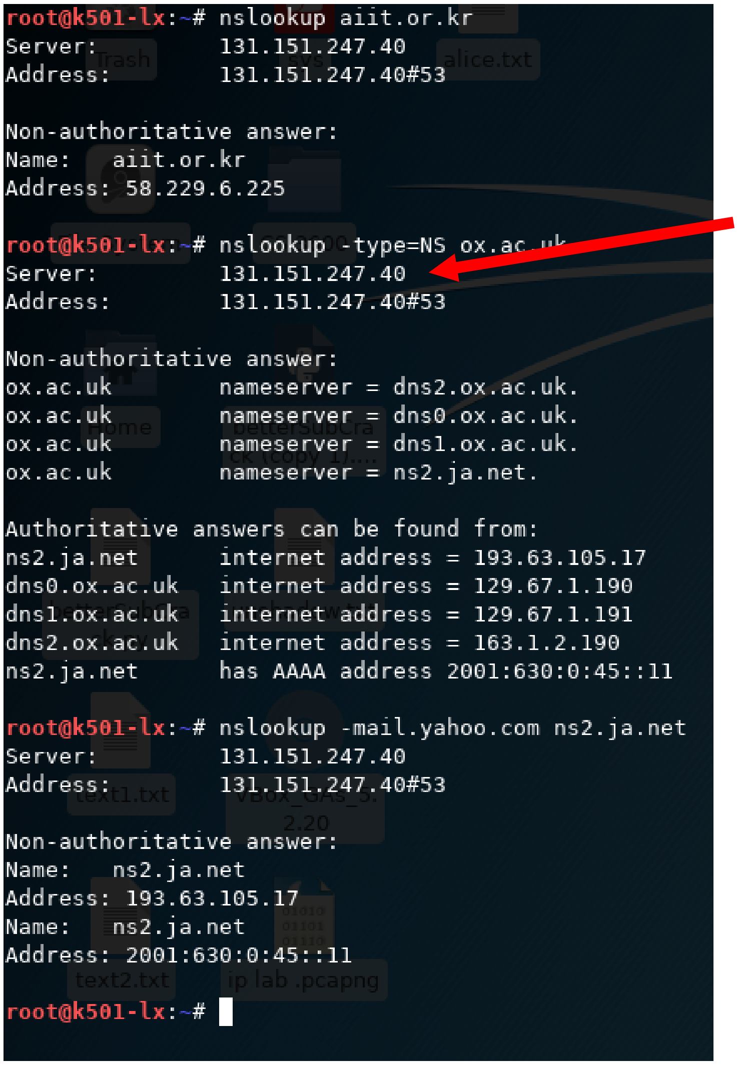
Luke Malloy

Wireshark Lab: DNS

Questions:

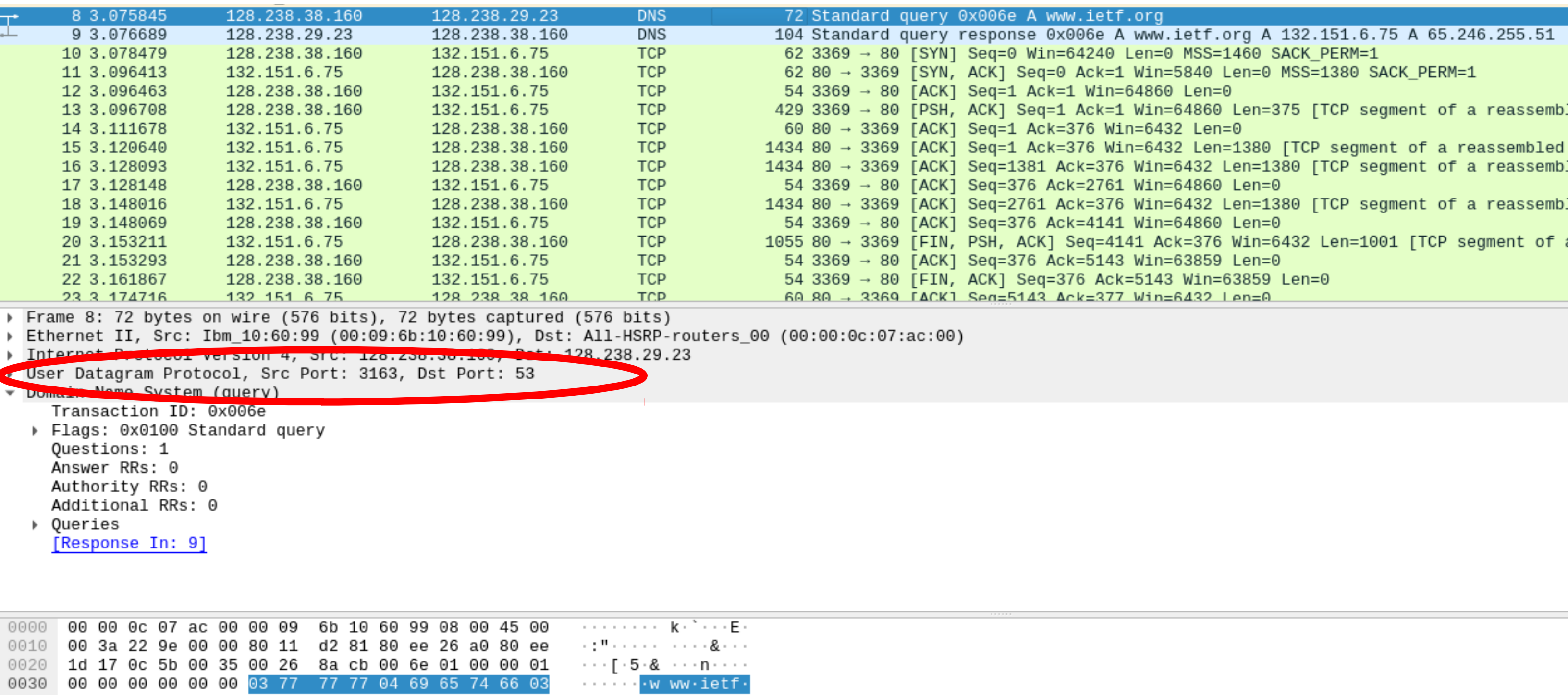


```
root@k501-lx:~# nslookup aiit.or.kr
Server:         131.151.247.40
Address:        131.151.247.40#53

Non-authoritative answer:
Name:   aiit.or.kr
Address: 58.229.6.225

root@k501-lx:~# nslookup -type=NS ox.ac.uk
Server:         131.151.247.40
Address:        131.151.247.40#53

Non-authoritative answer:
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.

Authoritative answers can be found from:
ns2.ja.net      internet address = 193.63.105.17
dns0.ox.ac.uk   internet address = 129.67.1.190
dns1.ox.ac.uk   internet address = 129.67.1.191
dns2.ox.ac.uk   internet address = 163.1.2.190
ns2.ja.net      has AAAA address 2001:630:0:45::11

root@k501-lx:~# nslookup -mail.yahoo.com ns2.ja.net
Server:         131.151.247.40
Address:        131.151.247.40#53

Non-authoritative answer:
Name:   ns2.ja.net
Address: 193.63.105.17
Name:   ns2.ja.net
Address: 2001:630:0:45::11

root@k501-lx:~#
```

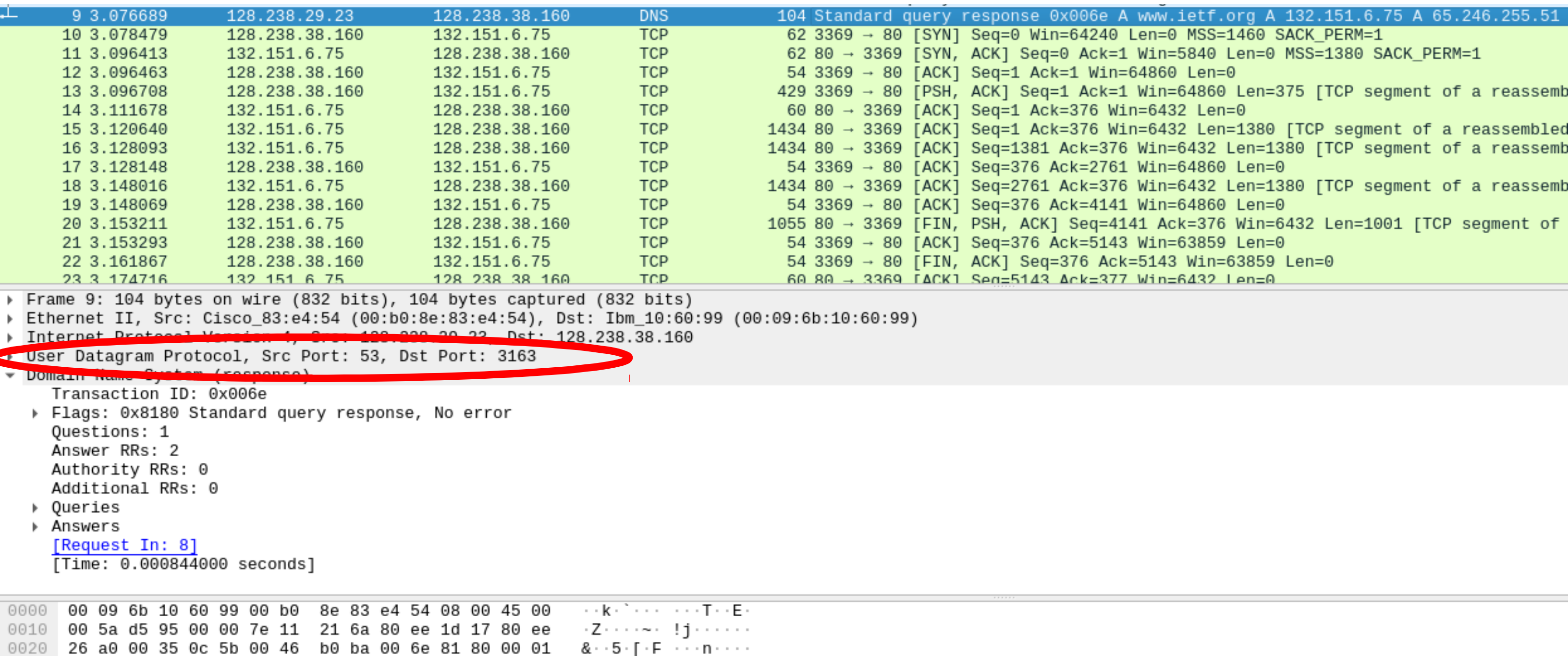
1. 58.229.6.225
2. Instruction only

3. IP of server is 131.151.247.40

4. They are sent over UDP:

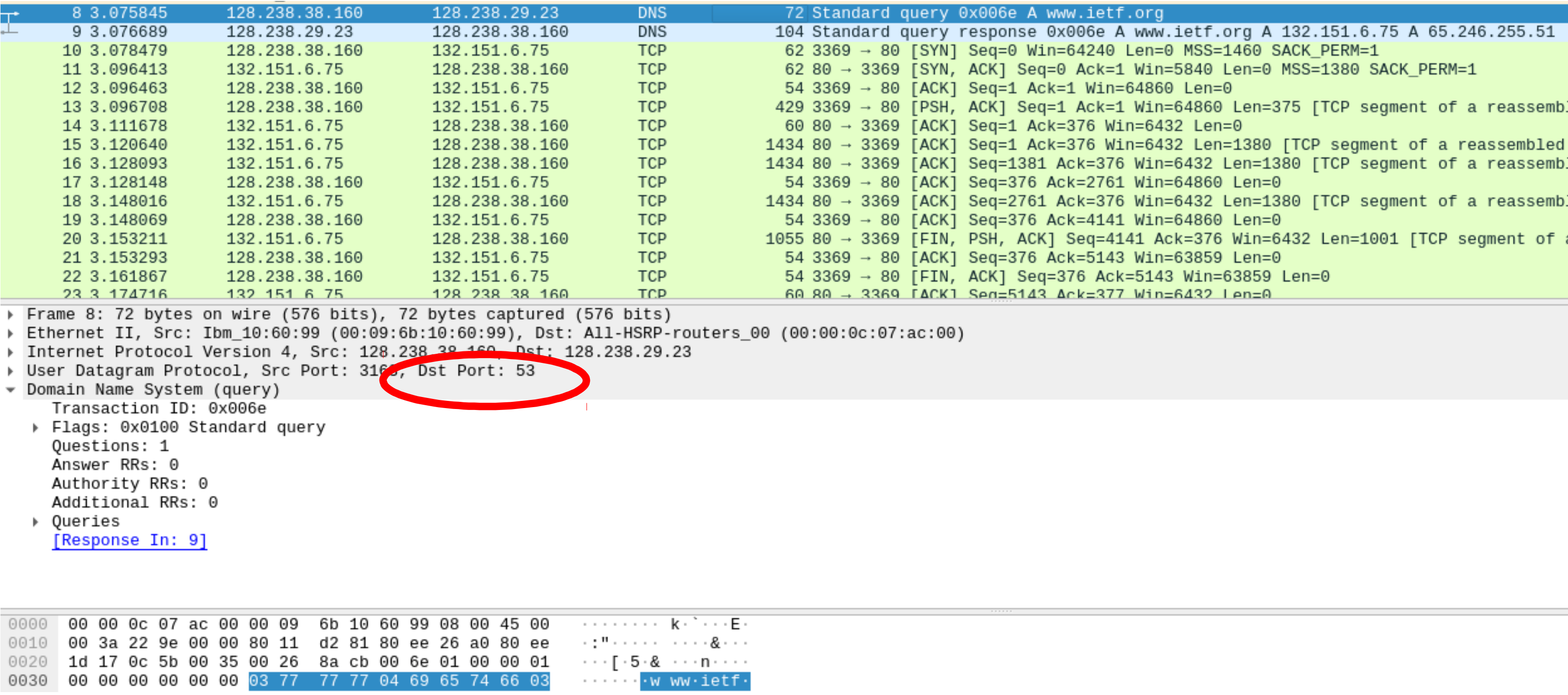


```
  8 3.075845   128.238.38.160   128.238.29.23    DNS     72 Standard query 0x006e A www.ietf.org
  9 3.076689   128.238.29.23    128.238.38.160   DNS    104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
 10 3.078479   128.238.38.160   132.151.6.75     TCP     62 3369 → 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_PERM=1
 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     TCP    429 3369 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64860 Len=375 [TCP segment of a reassembl
 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 reassembled
 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 of a reassembl
 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 of a reassembl
 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   TCP   1055 80 → 3369 [FIN, PSH, ACK] Seq=4141 Ack=376 Win=6432 Len=1001 [TCP segment of a
 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

▸ Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 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: 128.238.29.23
▸ User Datagram Protocol, Src Port: 3163, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x006e
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 9]

0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3a 22 9e 00 00 80 11  d2 81 80 ee 26 a0 80 ee   ·:"····· ····&···
0020  1d 17 0c 5b 00 35 00 26  8a cb 00 6e 01 00 00 01   ···[·5·& ···n····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
```

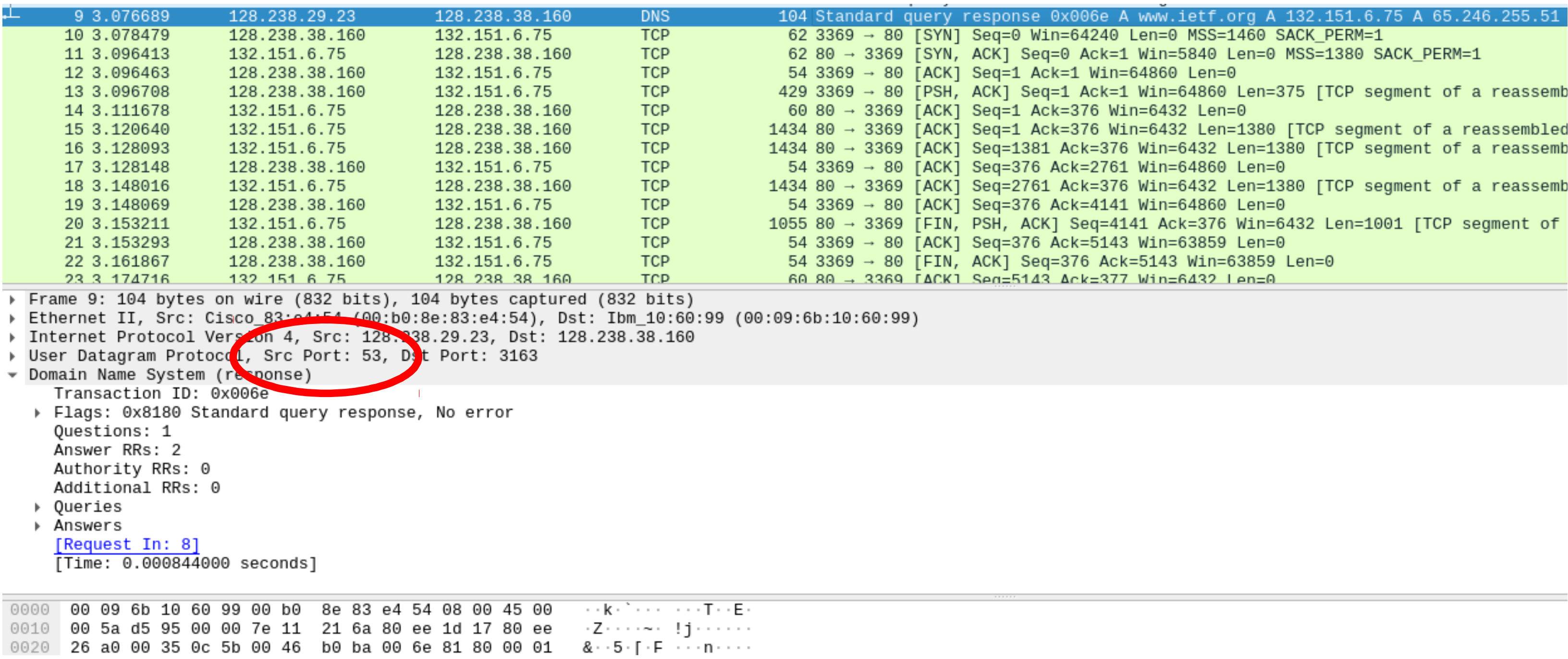


```
  9 3.076689   128.238.29.23    128.238.38.160   DNS    104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
 10 3.078479   128.238.38.160   132.151.6.75     TCP     62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 11 3.096413   132.151.6.75     128.238.38.160   TCP     62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
 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     TCP    429 3369 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64860 Len=375 [TCP segment of a reassemb
 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 reassembled
 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 of a reassemb
 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 of a reassemb
 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   TCP   1055 80 → 3369 [FIN, PSH, ACK] Seq=4141 Ack=376 Win=6432 Len=1001 [TCP segment of
 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

▸ Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 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: 128.238.29.23, Dst: 128.238.38.160
▸ User Datagram Protocol, Src Port: 53, Dst Port: 3163
▾ Domain Name System (response)
    Transaction ID: 0x006e
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▸ Answers
    [Request In: 8]
    [Time: 0.000844000 seconds]

0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 5a d5 95 00 00 7e 11  21 6a 80 ee 1d 17 80 ee   ·Z····~· !j······
0020  26 a0 00 35 0c 5b 00 46  b0 ba 00 6e 81 80 00 01   &··5·[·F ···n····
```

5. The destination port for the DNS query message is 53. The source port for the DNS response message is the same port.

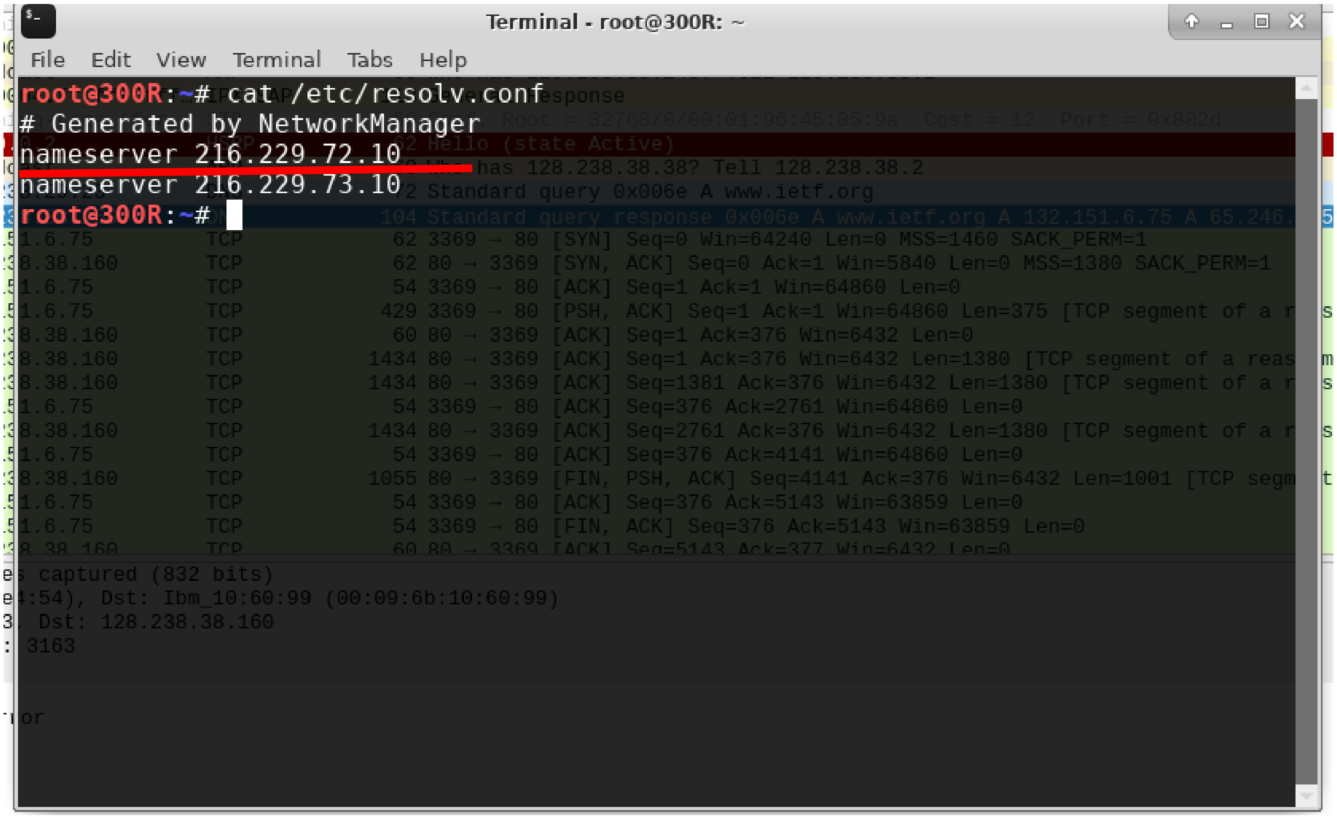


```
 8 3.075845   128.238.38.160   128.238.29.23    DNS     72 Standard query 0x006e A www.ietf.org
 9 3.076689   128.238.29.23    128.238.38.160   DNS    104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
10 3.078479   128.238.38.160   132.151.6.75     TCP     62 3369 → 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_PERM=1
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     TCP    429 3369 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64860 Len=375 [TCP segment of a reassembl
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 reassembled
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 of a reassembl
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 of a reassembl
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   TCP   1055 80 → 3369 [FIN, PSH, ACK] Seq=4141 Ack=376 Win=6432 Len=1001 [TCP segment of a
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

▸ Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 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: 128.238.29.23
▸ User Datagram Protocol, Src Port: 3163, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x006e
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 9]

0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3a 22 9e 00 00 80 11  d2 81 80 ee 26 a0 80 ee   ·:"····· ····&···
0020  1d 17 0c 5b 00 35 00 26  8a cb 00 6e 01 00 00 01   ···[·5·& ···n····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ······ ·w ww·ietf·
```



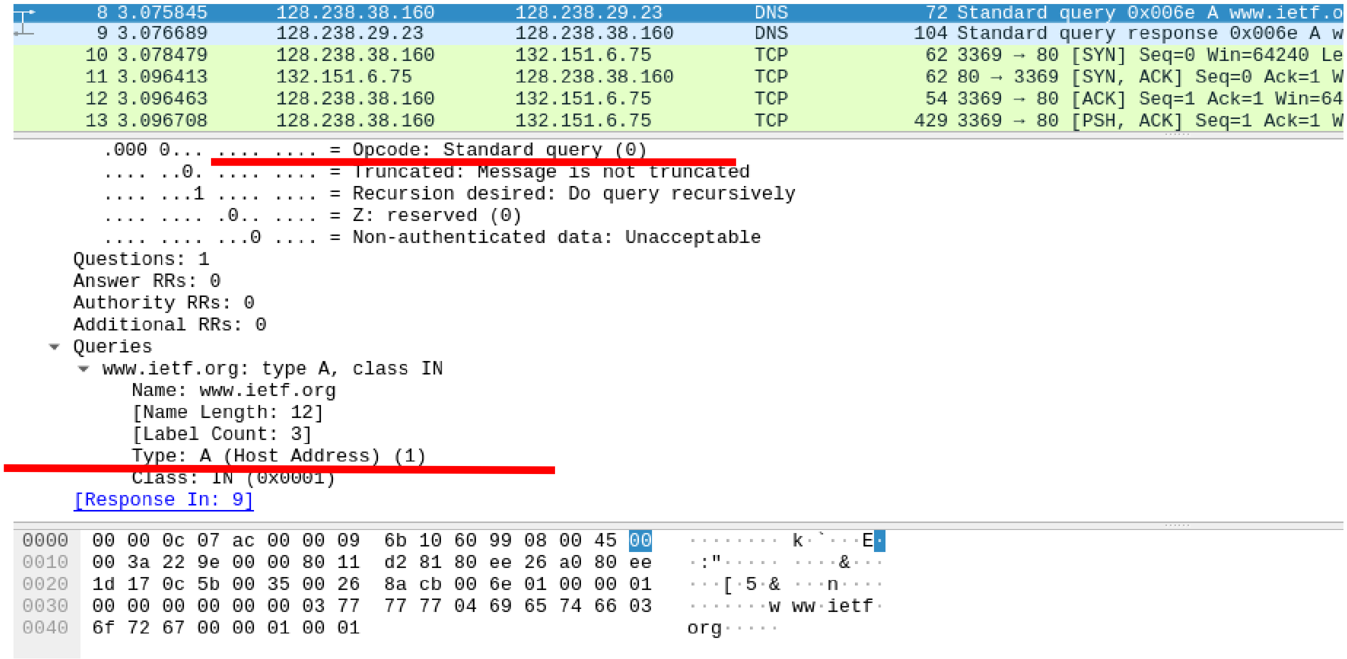
```
 9 3.076689   128.238.29.23    128.238.38.160   DNS    104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
10 3.078479   128.238.38.160   132.151.6.75     TCP     62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11 3.096413   132.151.6.75     128.238.38.160   TCP     62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
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     TCP    429 3369 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64860 Len=375 [TCP segment of a reassemb
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 reassembled
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 of a reassemb
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 of a reassemb
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   TCP   1055 80 → 3369 [FIN, PSH, ACK] Seq=4141 Ack=376 Win=6432 Len=1001 [TCP segment of
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

▸ Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 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: 128.238.29.23, Dst: 128.238.38.160
▸ User Datagram Protocol, Src Port: 53, Dst Port: 3163
▾ Domain Name System (response)
    Transaction ID: 0x006e
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▸ Answers
    [Request In: 8]
    [Time: 0.000844000 seconds]

0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 5a d5 95 00 00 7e 11  21 6a 80 ee 1d 17 80 ee   ·Z····~· !j······
0020  26 a0 00 35 0c 5b 00 46  b0 ba 00 6e 81 80 00 01   &··5·[·F ···n····
```

6. As I used the packet trace, I could not find the DNS server of the local host machine that produced the trace. However, the IP of my local DNS server is 216.229.72.10 inside of my VM.



```
root@300R:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 216.229.72.10
nameserver 216.229.73.10
root@300R:~# 
```

7. The DNS query message is a Type A Standard Query. It does not contain answers, responses contain answers.

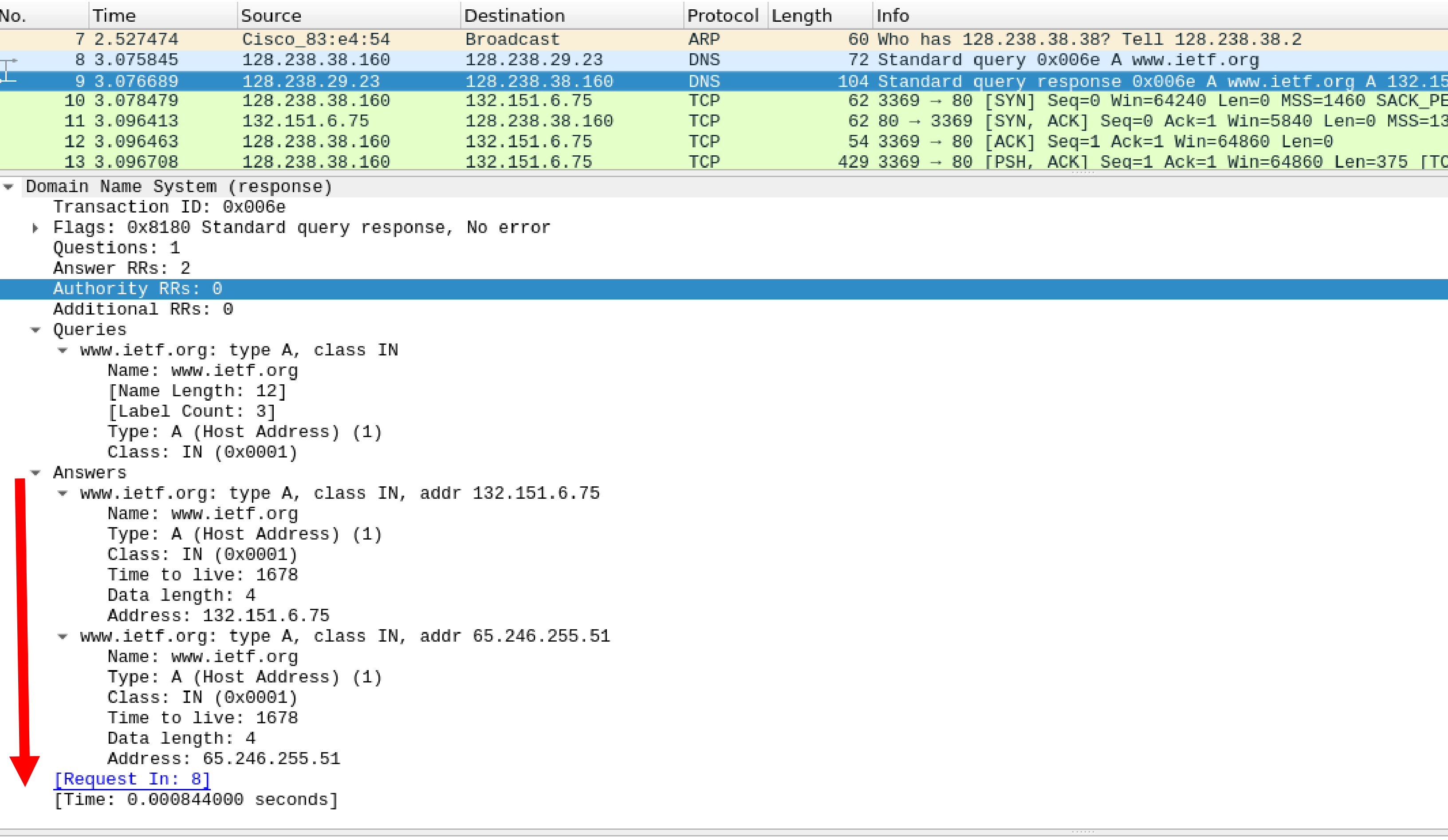


```
    8 3.075845   128.238.38.160    128.238.29.23     DNS      72 Standard query 0x006e A www.ietf.o
    9 3.076689   128.238.29.23     128.238.38.160    DNS     104 Standard query response 0x006e A w
   10 3.078479   128.238.38.160    132.151.6.75      TCP      62 3369 → 80 [SYN] Seq=0 Win=64240 Le
   11 3.096413   132.151.6.75      128.238.38.160    TCP      62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 W
   12 3.096463   128.238.38.160    132.151.6.75      TCP      54 3369 → 80 [ACK] Seq=1 Ack=1 Win=64
   13 3.096708   128.238.38.160    132.151.6.75      TCP     429 3369 → 80 [PSH, ACK] Seq=1 Ack=1 W
```

```
        .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.ietf.org: type A, class IN
          Name: www.ietf.org
          [Name Length: 12]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
     [Response In: 9]
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3a 22 9e 00 00 80 11  d2 81 80 ee 26 a0 80 ee   ·:"····· ····&···
0020  1d 17 0c 5b 00 35 00 26  8a cb 00 6e 01 00 00 01   ···[·5·& ···n····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····
```

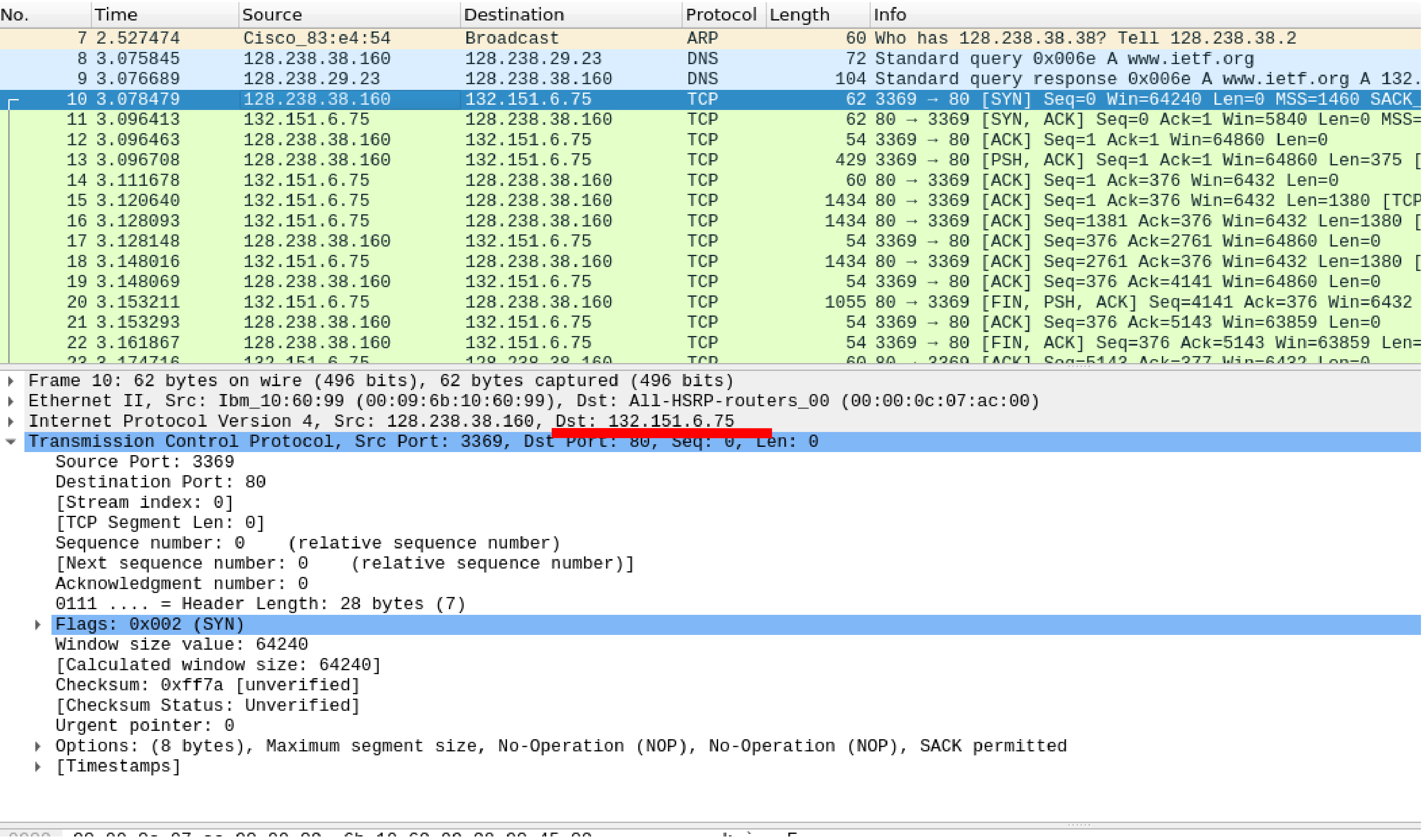
8. There are 2 answers provided. These answers contain the following fields for the IP addresses of 132.151.6.75 and 65.246.255.51: Name, Type, Class, TTL, Data Length and Address.



```
No.    Time       Source             Destination        Protocol Length Info
     7 2.527474   Cisco_83:e4:54     Broadcast          ARP       60 Who has 128.238.38.38? Tell 128.238.38.2
     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 132.15
    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_PE
    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=13
    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       TCP      429 3369 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64860 Len=375 [TC
```

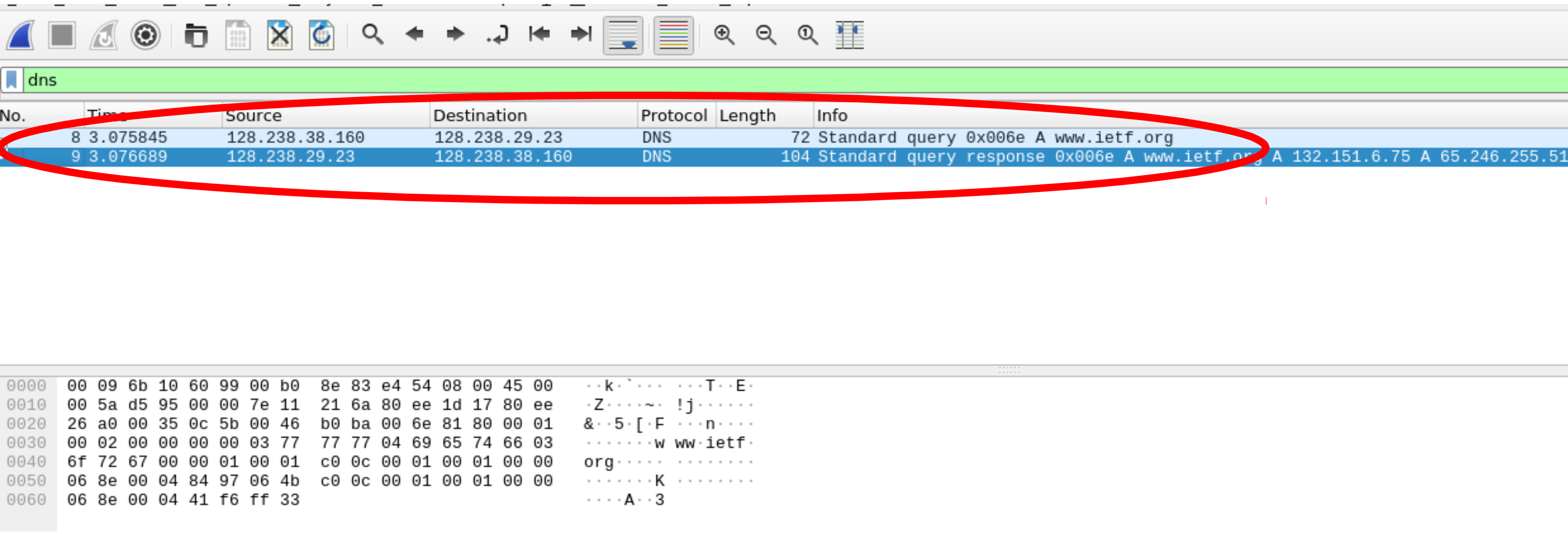
```
Domain Name System (response)
    Transaction ID: 0x006e
  Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    www.ietf.org: type A, class IN, addr 132.151.6.75
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1678
        Data length: 4
        Address: 132.151.6.75
    www.ietf.org: type A, class IN, addr 65.246.255.51
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1678
        Data length: 4
        Address: 65.246.255.51
    [Request In: 8]
    [Time: 0.000844000 seconds]
```

9. The subsequent TCP SYN packet came from 128.238.38.160. The destination address of this SYN packet, 132.151.6.75 corresponds to the first answer IP in the DNS response message.



```
No.   Time       Source          Destination      Protocol Length Info
    7 2.527474   Cisco_83:e4:54  Broadcast        ARP          60 Who has 128.238.38.38? Tell 128.238.38.2
    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.
   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_
   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=
   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     TCP         429 3369 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64860 Len=375 [
   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
   16 3.128093   132.151.6.75    128.238.38.160   TCP        1434 80 → 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [
   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 [
   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   TCP        1055 80 → 3369 [FIN, PSH, ACK] Seq=4141 Ack=376 Win=6432
   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=
   23 3.174716   132.151.6.75    128.238.38.160   TCP          60 80 → 3369 [ACK] Seq=5143 Ack=377 Win=6432 Len=0

▸ Frame 10: 62 bytes on wire (496 bits), 62 bytes captured (496 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: 132.151.6.75
▾ Transmission Control Protocol, Src Port: 3369, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 3369
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
  ▸ Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0xff7a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
  ▸ [Timestamps]
```

10. No, the host does not issue new DNS queries before retrieving each image. There is only one DNS query and one DNS response in the trace.



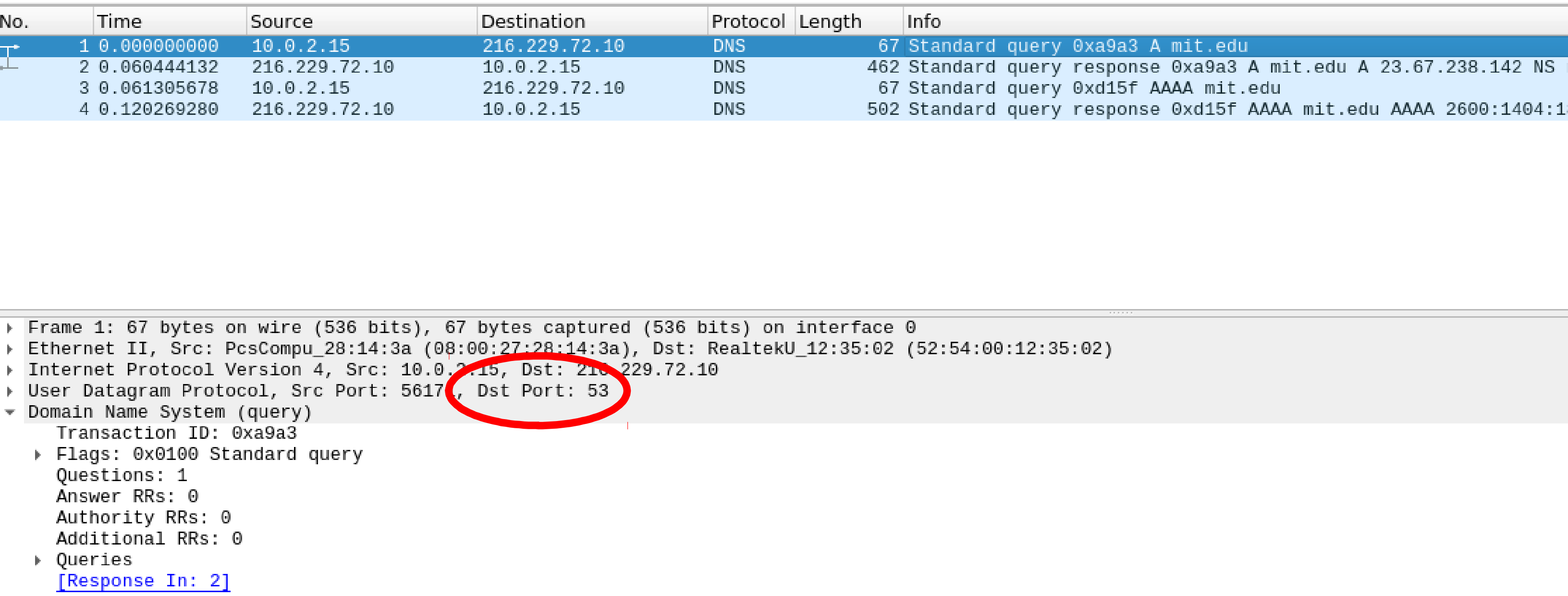
dns

No.	Time	Source	Destination	Protocol	Length	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 65.246.255.51

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`···  ···T··E·
0010  00 5a d5 95 00 00 7e 11  21 6a 80 ee 1d 17 80 ee   ·Z····~·  !j······
0020  26 a0 00 35 0c 5b 00 46  b0 ba 00 6e 81 80 00 01   &··5·[·F  ···n····
0030  00 02 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w  ww·ietf·
0040  6f 72 67 00 00 01 00 01  c0 0c 00 01 00 01 00 00   org·····  ········
0050  06 8e 00 04 84 97 06 4b  c0 0c 00 01 00 01 00 00   ·······K  ········
0060  06 8e 00 04 41 f6 ff 33                            ····A··3
```

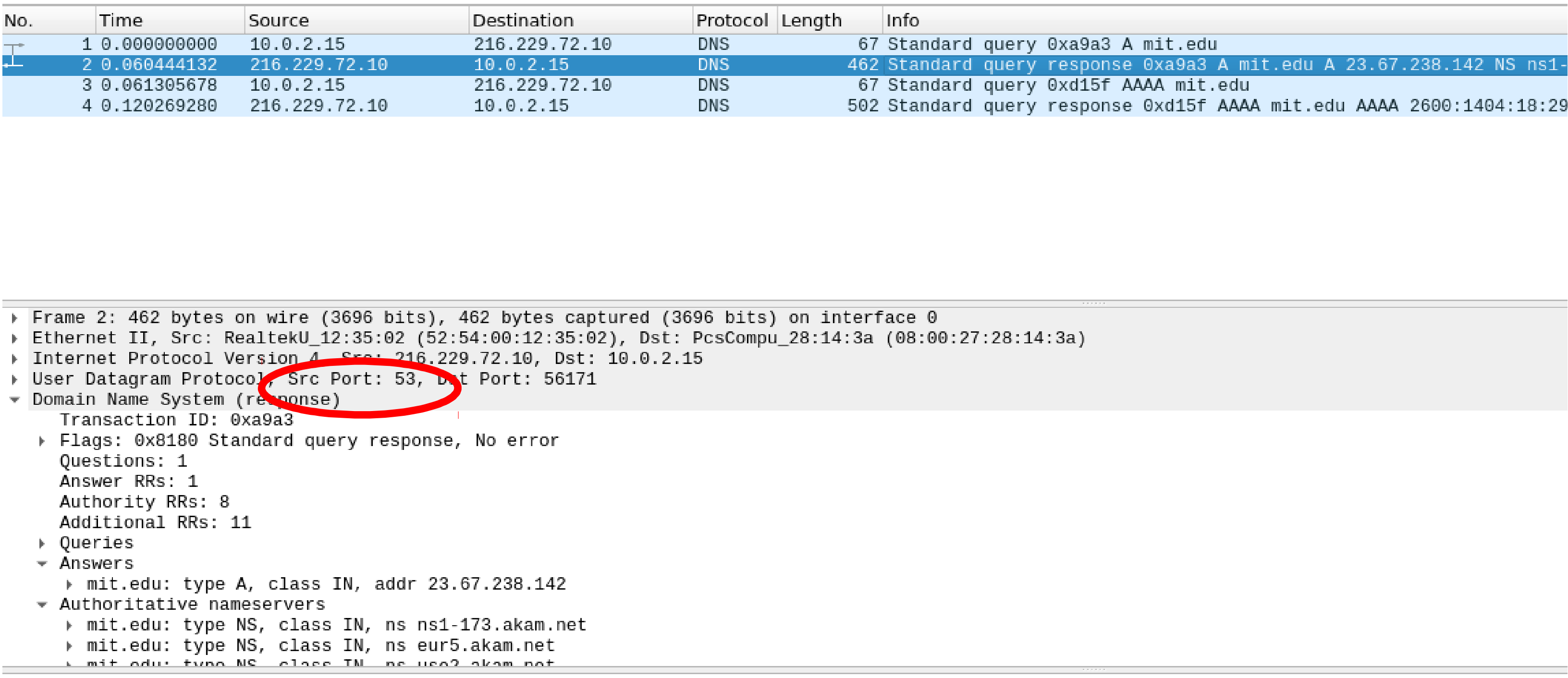
11. I actually have two sets of DNS query/responses instead of the promised 3 in the lab. I am more familiar with the addresses in the first set as they appear to be regular IPV4 addresses, and will use this set for the questions 11-15.

The dest port for the DNS query message is 53, the source port for the response is 53, as expected.



```
No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  10.0.2.15       216.229.72.10   DNS        67 Standard query 0xa9a3 A mit.edu
   2 0.060444132  216.229.72.10   10.0.2.15       DNS       462 Standard query response 0xa9a3 A mit.edu A 23.67.238.142 NS
   3 0.061305678  10.0.2.15       216.229.72.10   DNS        67 Standard query 0xd15f AAAA mit.edu
   4 0.120269280  216.229.72.10   10.0.2.15       DNS       502 Standard query response 0xd15f AAAA mit.edu AAAA 2600:1404:1
```

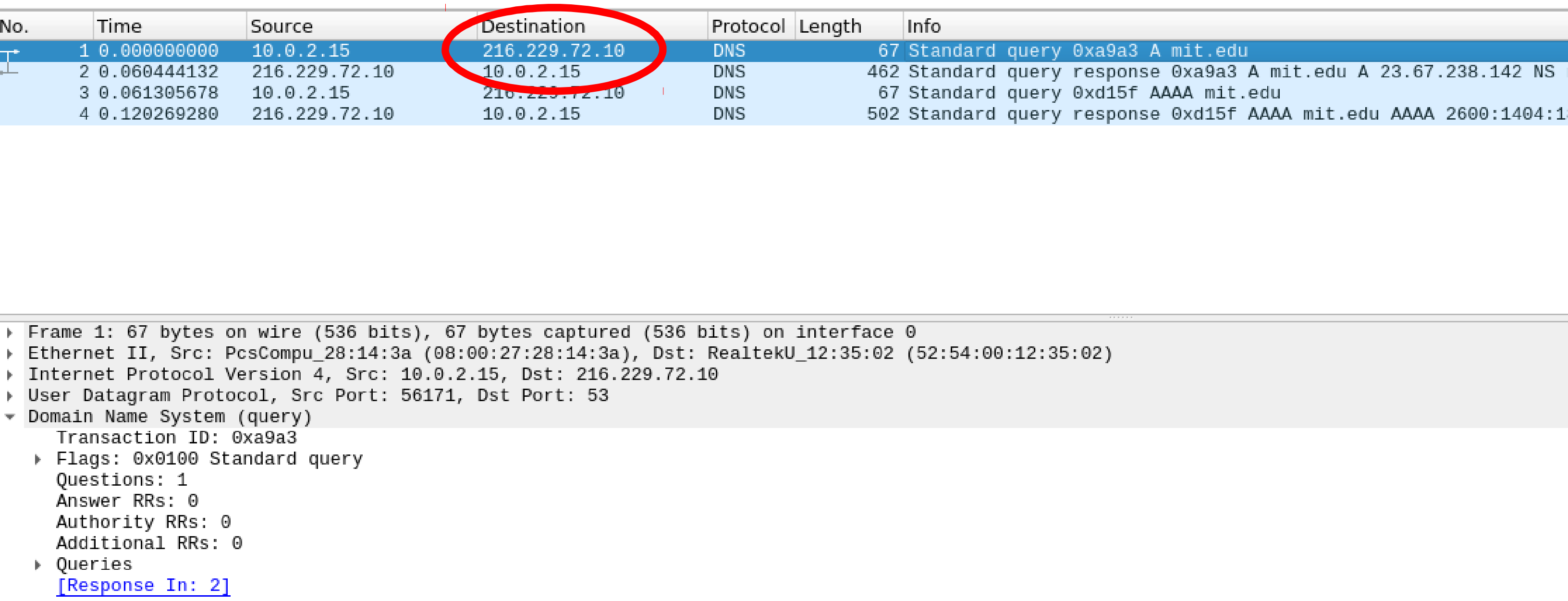
```
▸ Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.229.72.10
▸ User Datagram Protocol, Src Port: 56171, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xa9a3
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 2]
```



```
No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  10.0.2.15       216.229.72.10   DNS        67 Standard query 0xa9a3 A mit.edu
   2 0.060444132  216.229.72.10   10.0.2.15       DNS       462 Standard query response 0xa9a3 A mit.edu A 23.67.238.142 NS ns1-
   3 0.061305678  10.0.2.15       216.229.72.10   DNS        67 Standard query 0xd15f AAAA mit.edu
   4 0.120269280  216.229.72.10   10.0.2.15       DNS       502 Standard query response 0xd15f AAAA mit.edu AAAA 2600:1404:18:29
```

```
▸ Frame 2: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_28:14:3a (08:00:27:28:14:3a)
▸ Internet Protocol Version 4, Src: 216.229.72.10, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 56171
▾ Domain Name System (response)
    Transaction ID: 0xa9a3
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 8
    Additional RRs: 11
  ▸ Queries
  ▾ Answers
    ▸ mit.edu: type A, class IN, addr 23.67.238.142
  ▾ Authoritative nameservers
    ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▸ mit.edu: type NS, class IN, ns eur5.akam.net
    ▸ mit.edu: type NS, class IN, ns use2.akam.net
```

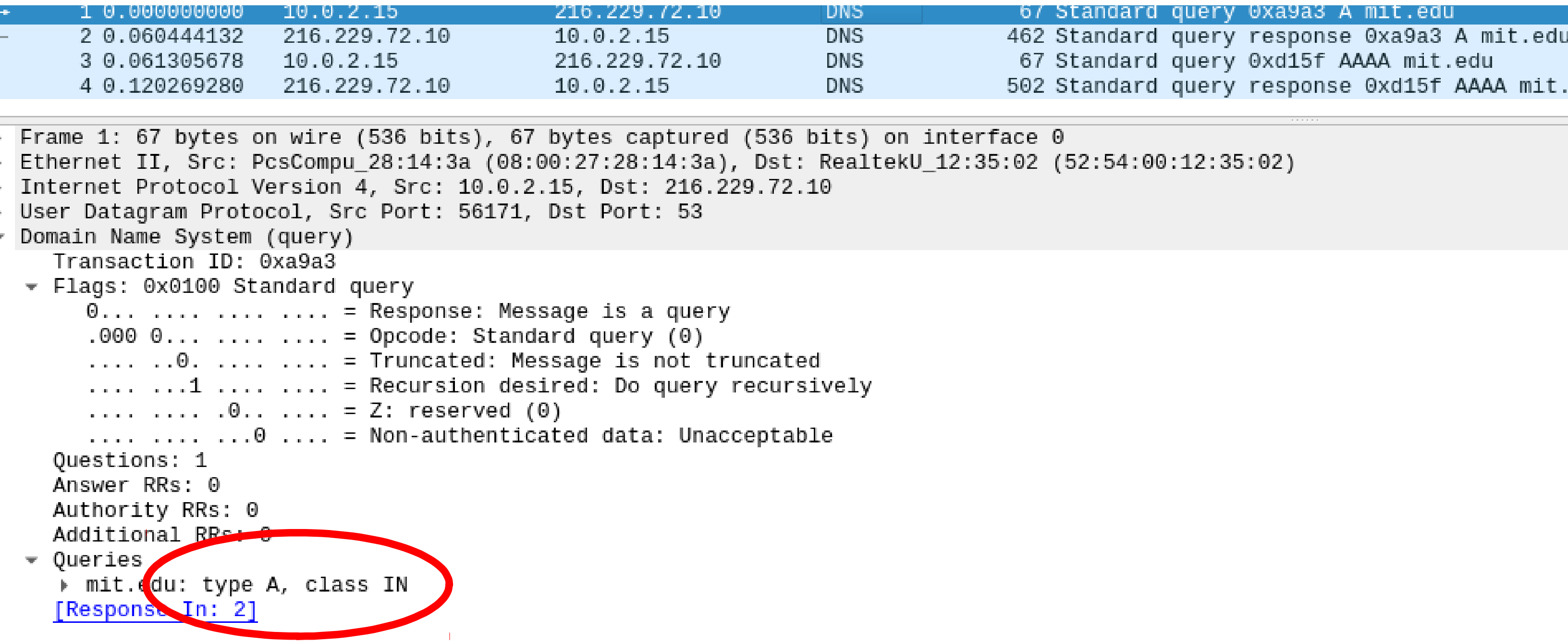
12. The query is sent to 216.229.72.10 and is indeed the same IP address of my default DNS server as found in question 6.



```
No.   Time          Source          Destination     Protocol  Length  Info
    1 0.000000000   10.0.2.15       216.229.72.10   DNS           67  Standard query 0xa9a3 A mit.edu
    2 0.060444132   216.229.72.10   10.0.2.15       DNS          462  Standard query response 0xa9a3 A mit.edu A 23.67.238.142 NS
    3 0.061305678   10.0.2.15       216.229.72.10   DNS           67  Standard query 0xd15f AAAA mit.edu
    4 0.120269280   216.229.72.10   10.0.2.15       DNS          502  Standard query response 0xd15f AAAA mit.edu AAAA 2600:1404:1
```

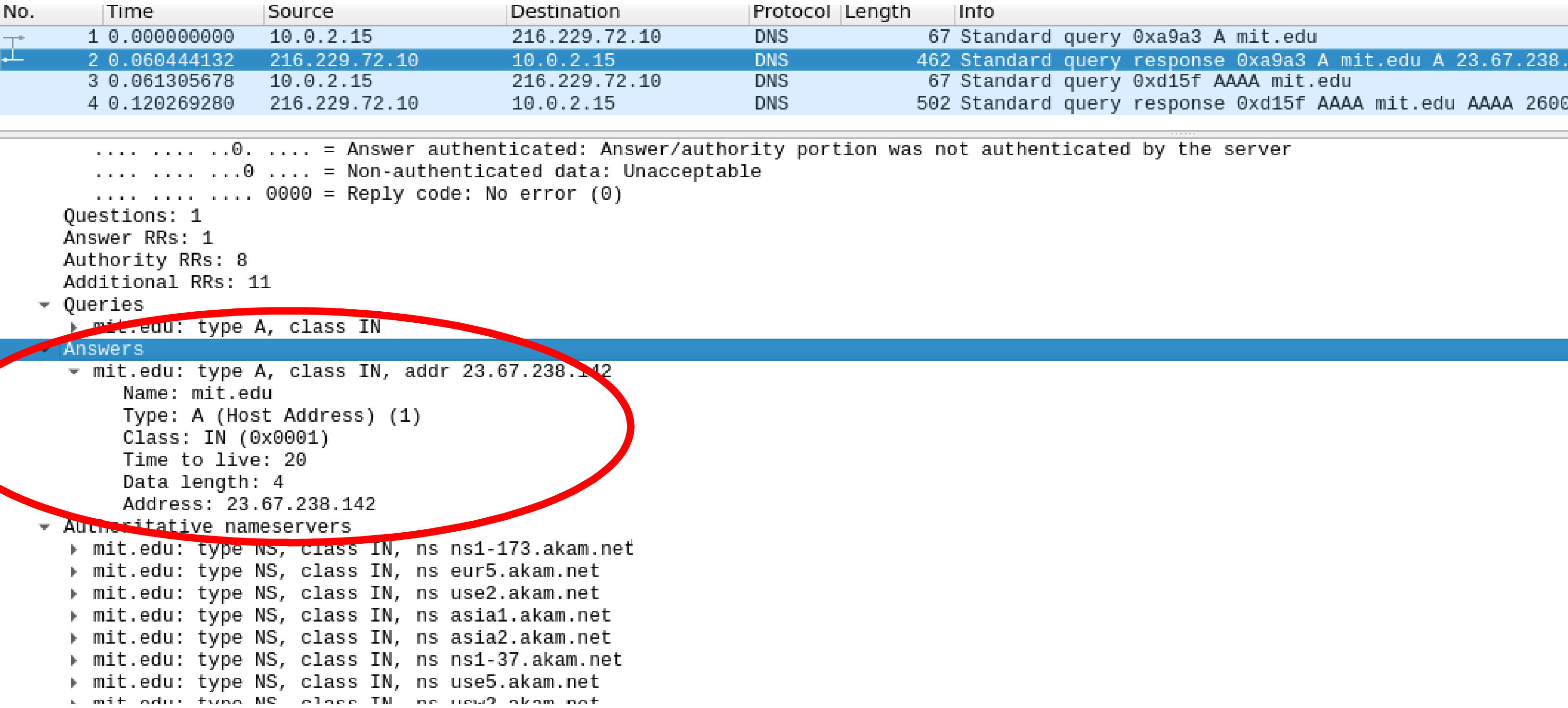
```
▸ Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.229.72.10
▸ User Datagram Protocol, Src Port: 56171, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xa9a3
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 2]
```

13. The query is of type A, standard query. A query will not have answers.



```
  1 0.000000000   10.0.2.15         216.229.72.10     DNS         67 Standard query 0xa9a3 A mit.edu
  2 0.060444132   216.229.72.10     10.0.2.15         DNS        462 Standard query response 0xa9a3 A mit.edu
  3 0.061305678   10.0.2.15         216.229.72.10     DNS         67 Standard query 0xd15f AAAA mit.edu
  4 0.120269280   216.229.72.10     10.0.2.15         DNS        502 Standard query response 0xd15f AAAA mit.

Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.229.72.10
User Datagram Protocol, Src Port: 56171, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xa9a3
    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
        mit.edu: type A, class IN
    [Response In: 2]
```

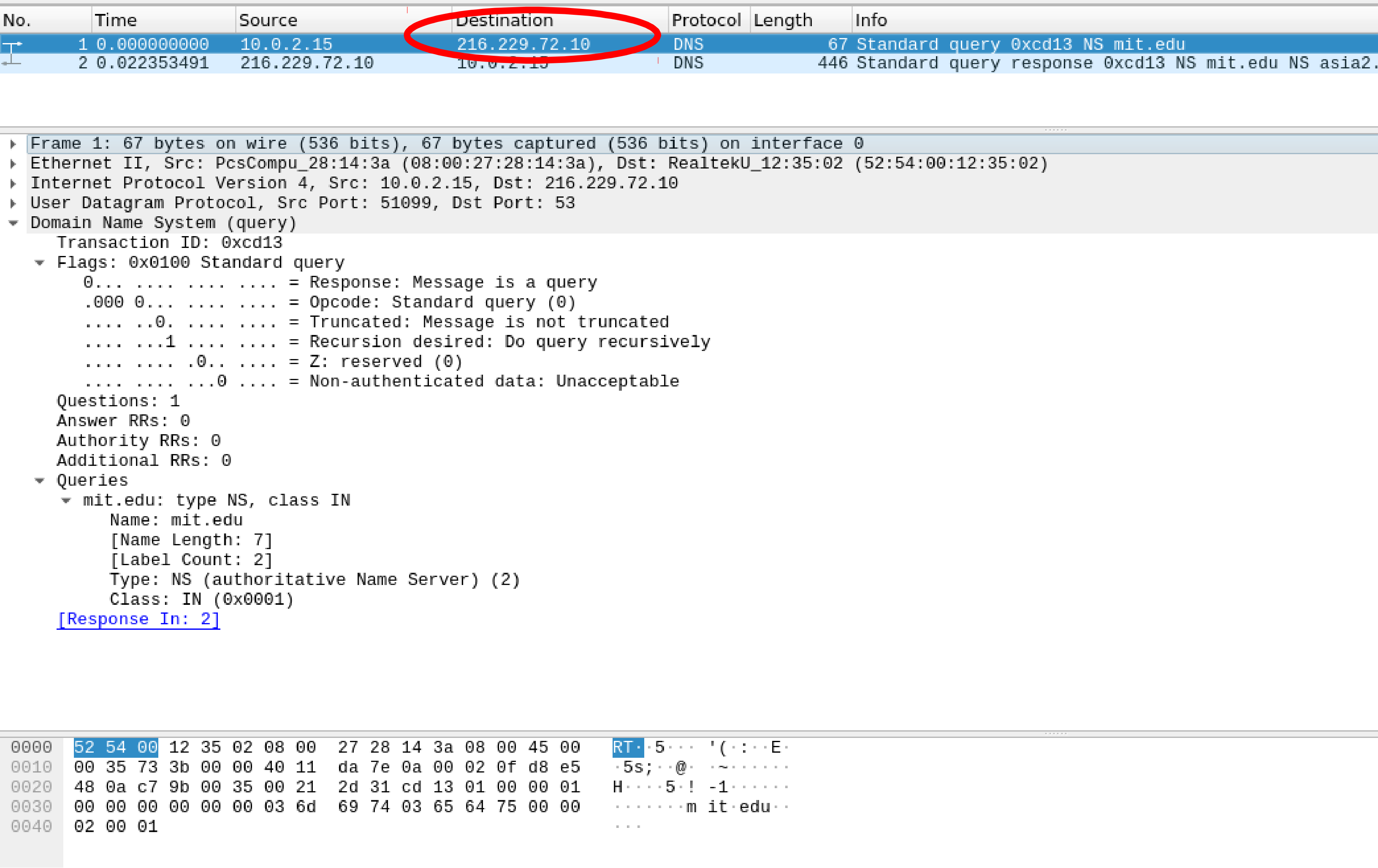
14. There is one answer. This answer contains the following: (same fields as previous question)
15. Screenshot provided, instruction only.



```
No.   Time          Source          Destination     Protocol Length Info
    1 0.000000000   10.0.2.15       216.229.72.10   DNS          67 Standard query 0xa9a3 A mit.edu
    2 0.060444132   216.229.72.10   10.0.2.15       DNS         462 Standard query response 0xa9a3 A mit.edu A 23.67.238.
    3 0.061305678   10.0.2.15       216.229.72.10   DNS          67 Standard query 0xd15f AAAA mit.edu
    4 0.120269280   216.229.72.10   10.0.2.15       DNS         502 Standard query response 0xd15f AAAA mit.edu AAAA 2600
```

```
        .... .... ..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: 8
    Additional RRs: 11
  ▾ Queries
      ▸ mit.edu: type A, class IN
  ▾ Answers
      ▾ mit.edu: type A, class IN, addr 23.67.238.142
            Name: mit.edu
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 20
            Data length: 4
            Address: 23.67.238.142
  ▾ Authoritative nameservers
      ▸ mit.edu: type NS, class IN, ns ns1-173.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 asia1.akam.net
      ▸ mit.edu: type NS, class IN, ns asia2.akam.net
      ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
      ▸ mit.edu: type NS, class IN, ns use5.akam.net
      ▸ mit.edu: type NS, class IN, ns usw2.akam.net
```

16. The query is sent to 216.229.72.10 and yes this is the IP of my local DNS server

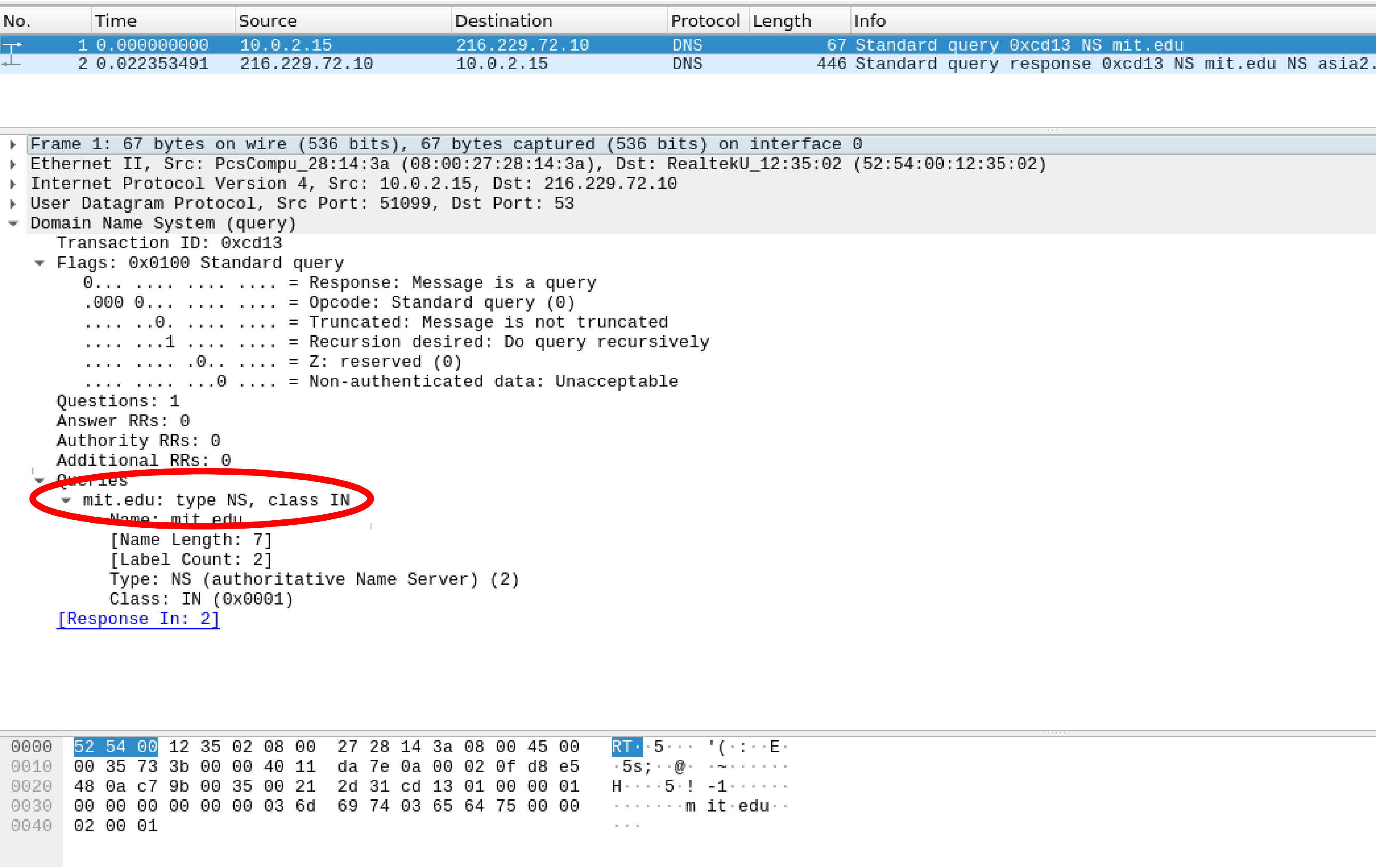


```
No.    Time          Source           Destination      Protocol  Length  Info
     1 0.000000000   10.0.2.15        216.229.72.10    DNS            67 Standard query 0xcd13 NS mit.edu
     2 0.022353491   216.229.72.10    10.0.2.15        DNS           446 Standard query response 0xcd13 NS mit.edu NS asia2.
```

```
▸ Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.229.72.10
▸ User Datagram Protocol, Src Port: 51099, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xcd13
  ▾ 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
    ▾ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 2]
```

```
0000  52 54 00 12 35 02 08 00  27 28 14 3a 08 00 45 00   RT··5···'(·:··E·
0010  00 35 73 3b 00 00 40 11  da 7e 0a 00 02 0f d8 e5   ·5s;··@··~······
0020  48 0a c7 9b 00 35 00 21  2d 31 cd 13 01 00 00 01   H····5·!-1······
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······mit·edu··
0040  02 00 01                                           ···
```

17. The query is of Type NS. It is a query and does not contain answers.

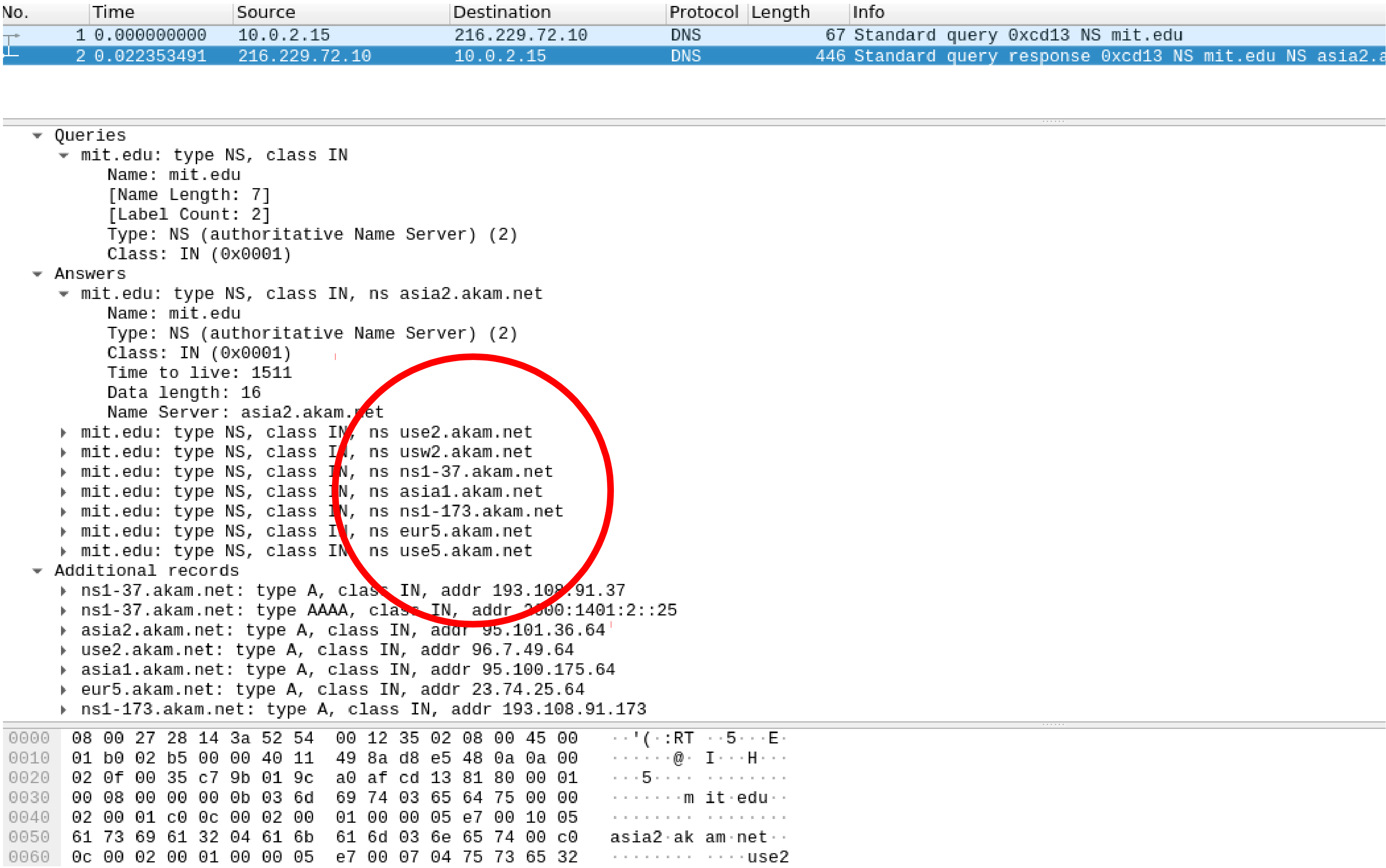


```
No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  10.0.2.15       216.229.72.10   DNS          67 Standard query 0xcd13 NS mit.edu
   2 0.022353491  216.229.72.10   10.0.2.15       DNS         446 Standard query response 0xcd13 NS mit.edu NS asia2.
```

```
▸ Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.229.72.10
▸ User Datagram Protocol, Src Port: 51099, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xcd13
  ▾ 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
    ▾ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 2]
```

```
0000  52 54 00 12 35 02 08 00  27 28 14 3a 08 00 45 00   RT··5··· '(·:··E·
0010  00 35 73 3b 00 00 40 11  da 7e 0a 00 02 0f d8 e5   ·5s;··@· ·~······
0020  48 0a c7 9b 00 35 00 21  2d 31 cd 13 01 00 00 01   H····5·! -1······
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01                                           ···
```

18. The response provides the following nameservers:
It does not provide the IP when expanded, however.
19. Screenshot provided, instruction only.

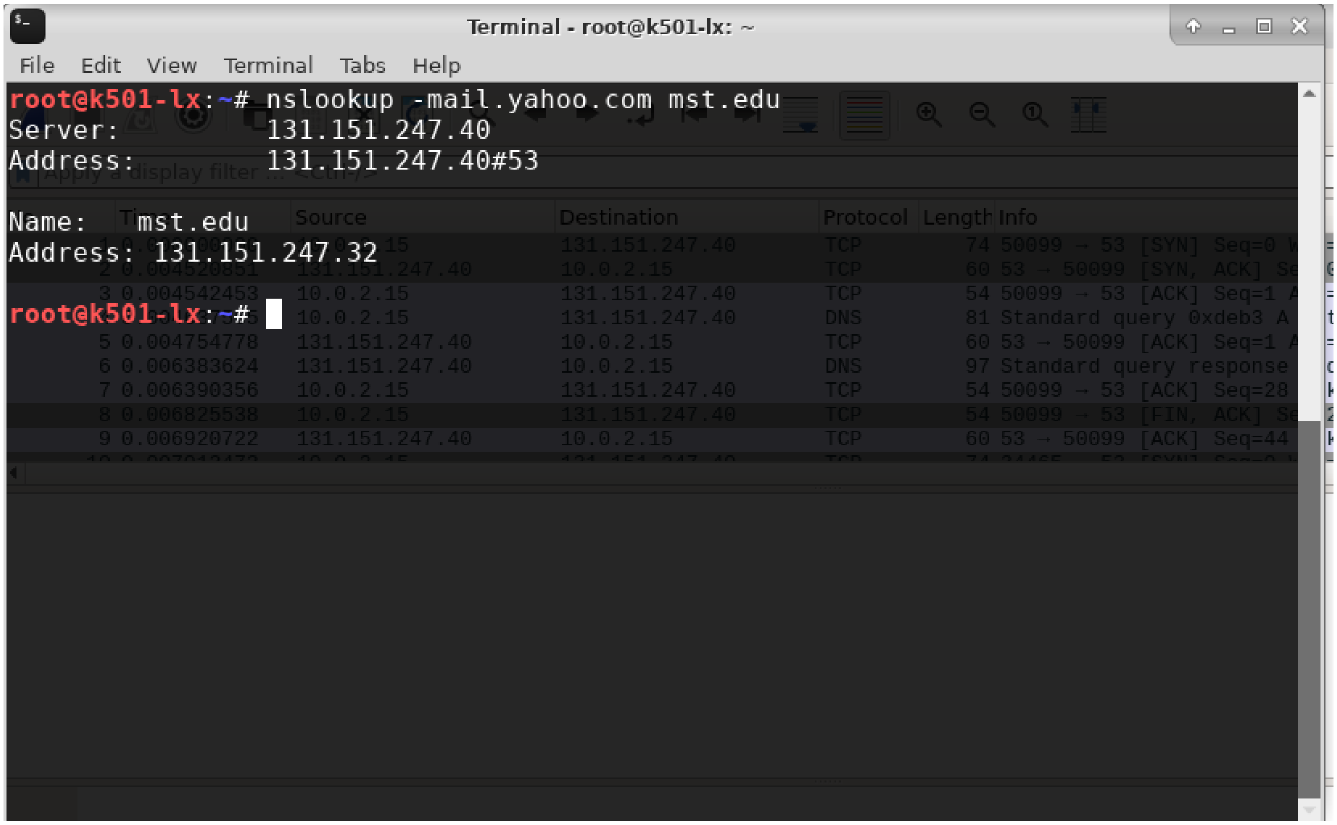


```
No.   Time          Source          Destination     Protocol Length Info
    1 0.000000000   10.0.2.15       216.229.72.10   DNS          67 Standard query 0xcd13 NS mit.edu
    2 0.022353491   216.229.72.10   10.0.2.15       DNS         446 Standard query response 0xcd13 NS mit.edu NS asia2.a
```

```
▾ 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)
▾ Answers
  ▾ 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: 1511
      Data length: 16
      Name Server: asia2.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 ns1-37.akam.net
  ▸ mit.edu: type NS, class IN, ns asia1.akam.net
  ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
  ▸ mit.edu: type NS, class IN, ns eur5.akam.net
  ▸ mit.edu: type NS, class IN, ns use5.akam.net
▾ Additional records
  ▸ ns1-37.akam.net: type A, class IN, addr 193.108.91.37
  ▸ ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
  ▸ asia2.akam.net: type A, class IN, addr 95.101.36.64
  ▸ use2.akam.net: type A, class IN, addr 96.7.49.64
  ▸ asia1.akam.net: type A, class IN, addr 95.100.175.64
  ▸ eur5.akam.net: type A, class IN, addr 23.74.25.64
  ▸ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
```

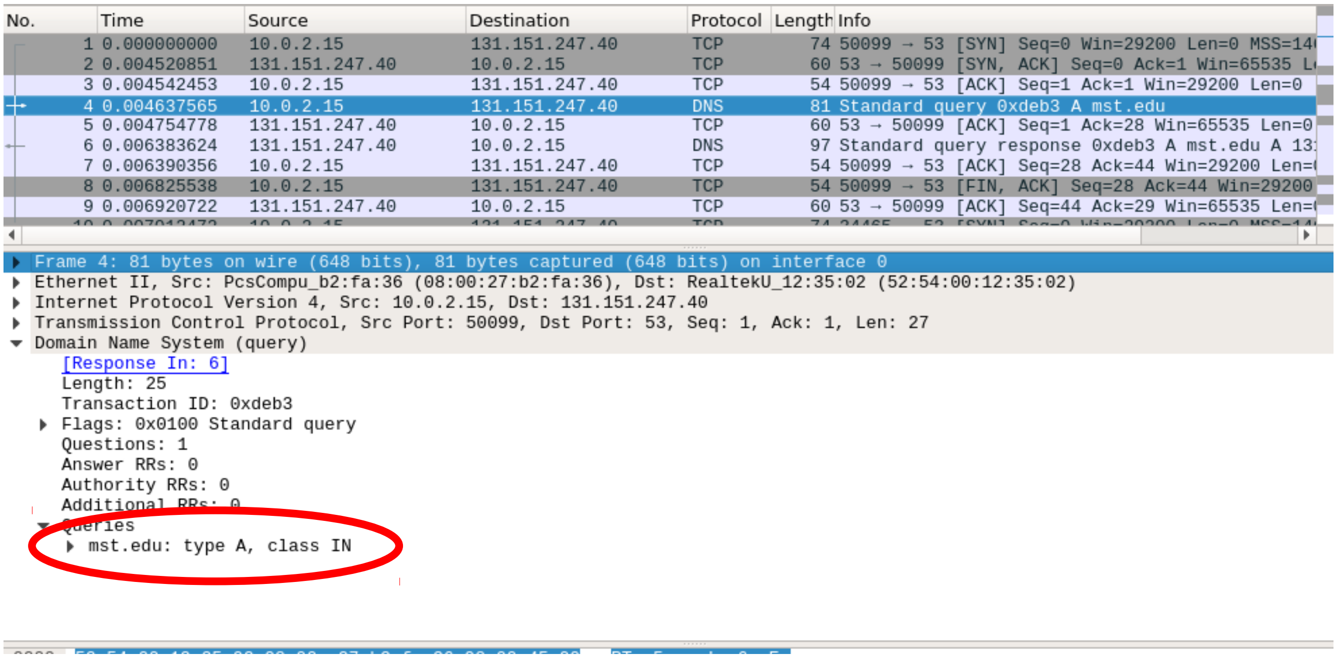
```
0000  08 00 27 28 14 3a 52 54  00 12 35 02 08 00 45 00   ··'(·:RT ··5···E·
0010  01 b0 02 b5 00 00 40 11  49 8a d8 e5 48 0a 0a 00   ······@· I···H···
0020  02 0f 00 35 c7 9b 01 9c  a0 af cd 13 81 80 00 01   ···5···· ········
0030  00 08 00 00 00 0b 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01 c0 0c 00 02 00  01 00 00 05 e7 00 10 05   ········ ········
0050  61 73 69 61 32 04 61 6b  61 6d 03 6e 65 74 00 c0   asia2·ak am·net··
0060  0c 00 02 00 01 00 00 05  e7 00 07 04 75 73 65 32   ········ ····use2
```

20. The query is sent to IP 131.151.247.40. This is not the address of my local DNS server, but the address of one of mst.edu’s DNS servers.



```
root@k501-lx:~# nslookup -mail.yahoo.com mst.edu
Server:         131.151.247.40
Address:        131.151.247.40#53

Name:    mst.edu
Address: 131.151.247.32

root@k501-lx:~# 
```

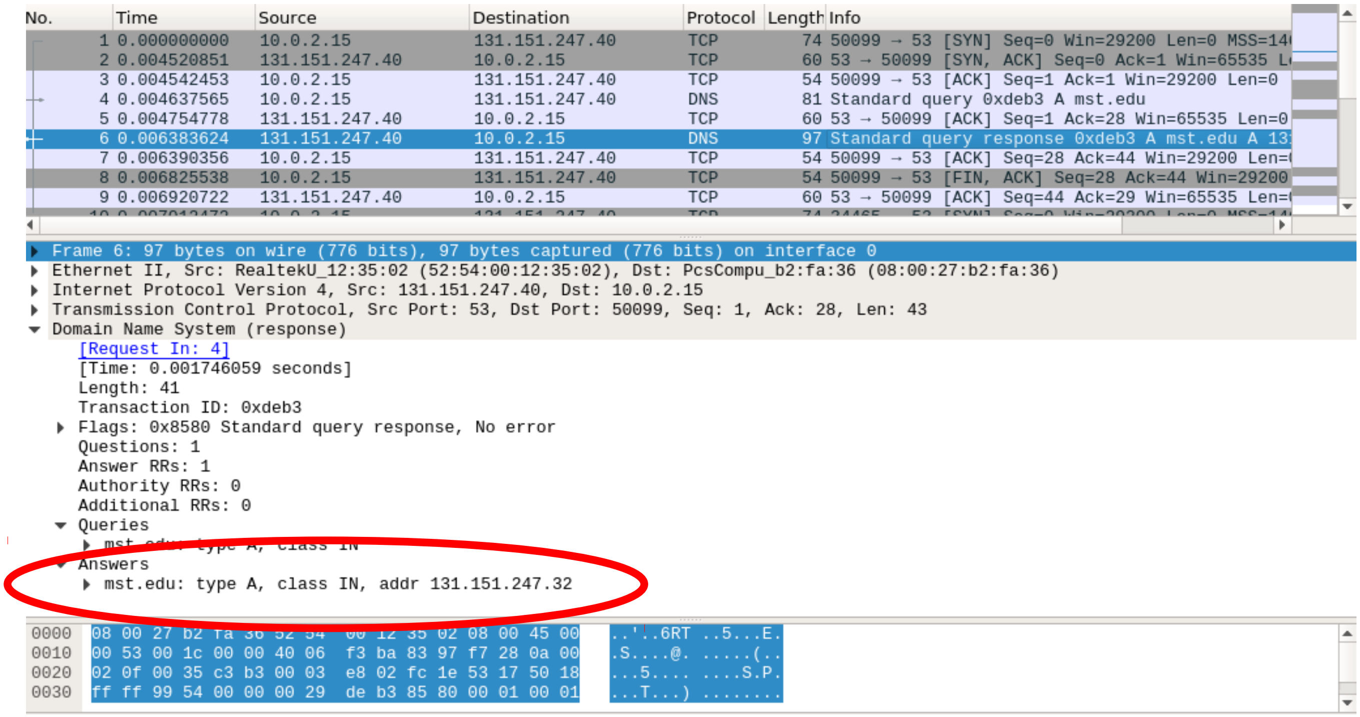
21. The query message is a type A standard query. The query does not contain answers.



```
No.  Time          Source           Destination      Protocol Length Info
   1 0.000000000   10.0.2.15        131.151.247.40   TCP        74 50099 → 53 [SYN] Seq=0 Win=29200 Len=0 MSS=14
   2 0.004520851   131.151.247.40   10.0.2.15        TCP        60 53 → 50099 [SYN, ACK] Seq=0 Ack=1 Win=65535 L
   3 0.004542453   10.0.2.15        131.151.247.40   TCP        54 50099 → 53 [ACK] Seq=1 Ack=1 Win=29200 Len=0
   4 0.004637565   10.0.2.15        131.151.247.40   DNS        81 Standard query 0xdeb3 A mst.edu
   5 0.004754778   131.151.247.40   10.0.2.15        TCP        60 53 → 50099 [ACK] Seq=1 Ack=28 Win=65535 Len=0
   6 0.006383624   131.151.247.40   10.0.2.15        DNS        97 Standard query response 0xdeb3 A mst.edu A 13
   7 0.006390356   10.0.2.15        131.151.247.40   TCP        54 50099 → 53 [ACK] Seq=28 Ack=44 Win=29200 Len=
   8 0.006825538   10.0.2.15        131.151.247.40   TCP        54 50099 → 53 [FIN, ACK] Seq=28 Ack=44 Win=29200
   9 0.006920722   131.151.247.40   10.0.2.15        TCP        60 53 → 50099 [ACK] Seq=44 Ack=29 Win=65535 Len=
```

```
▸ Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 131.151.247.40
▸ Transmission Control Protocol, Src Port: 50099, Dst Port: 53, Seq: 1, Ack: 1, Len: 27
▾ Domain Name System (query)
    [Response In: 6]
    Length: 25
    Transaction ID: 0xdeb3
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mst.edu: type A, class IN
```

22. There is one answer in the response, this contains the type of query, class and IP address.



```
No.   Time          Source            Destination       Protocol Length Info
    1 0.000000000   10.0.2.15         131.151.247.40    TCP        74 50099 → 53 [SYN] Seq=0 Win=29200 Len=0 MSS=14
    2 0.004520851   131.151.247.40    10.0.2.15         TCP        60 53 → 50099 [SYN, ACK] Seq=0 Ack=1 Win=65535 L
    3 0.004542453   10.0.2.15         131.151.247.40    TCP        54 50099 → 53 [ACK] Seq=1 Ack=1 Win=29200 Len=0
    4 0.004637565   10.0.2.15         131.151.247.40    DNS        81 Standard query 0xdeb3 A mst.edu
    5 0.004754778   131.151.247.40    10.0.2.15         TCP        60 53 → 50099 [ACK] Seq=1 Ack=28 Win=65535 Len=0
    6 0.006383624   131.151.247.40    10.0.2.15         DNS        97 Standard query response 0xdeb3 A mst.edu A 13
    7 0.006390356   10.0.2.15         131.151.247.40    TCP        54 50099 → 53 [ACK] Seq=28 Ack=44 Win=29200 Len=
    8 0.006825538   10.0.2.15         131.151.247.40    TCP        54 50099 → 53 [FIN, ACK] Seq=28 Ack=44 Win=29200
    9 0.006920722   131.151.247.40    10.0.2.15         TCP        60 53 → 50099 [ACK] Seq=44 Ack=29 Win=65535 Len=
   10 0.007013472   10.0.2.15         131.151.247.40    TCP        74 34465 → 53 [SYN] Seq=0 Win=29200 Len=0 MSS=14

Frame 6: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_b2:fa:36 (08:00:27:b2:fa:36)
Internet Protocol Version 4, Src: 131.151.247.40, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 53, Dst Port: 50099, Seq: 1, Ack: 28, Len: 43
Domain Name System (response)
    [Request In: 4]
    [Time: 0.001746059 seconds]
    Length: 41
    Transaction ID: 0xdeb3
    Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        mst.edu: type A, class IN
    Answers
        mst.edu: type A, class IN, addr 131.151.247.32

0000  08 00 27 b2 fa 36 52 54  00 12 35 02 08 00 45 00   ..'..6RT ..5...E.
0010  00 53 00 1c 00 00 40 06  f3 ba 83 97 f7 28 0a 00   .S....@. .....(..
0020  02 0f 00 35 c3 b3 00 03  e8 02 fc 1e 53 17 50 18   ...5.... ....S.P.
0030  ff ff 99 54 00 00 00 29  de b3 85 80 00 01 00 01   ...T...) ........
```