CSP334: Computer Networks, Lab Assignment No 6,Application Layer: DNS Wireshark Assignment

Rahul Byas Sherwan
Entry No. : 2016UCS0028

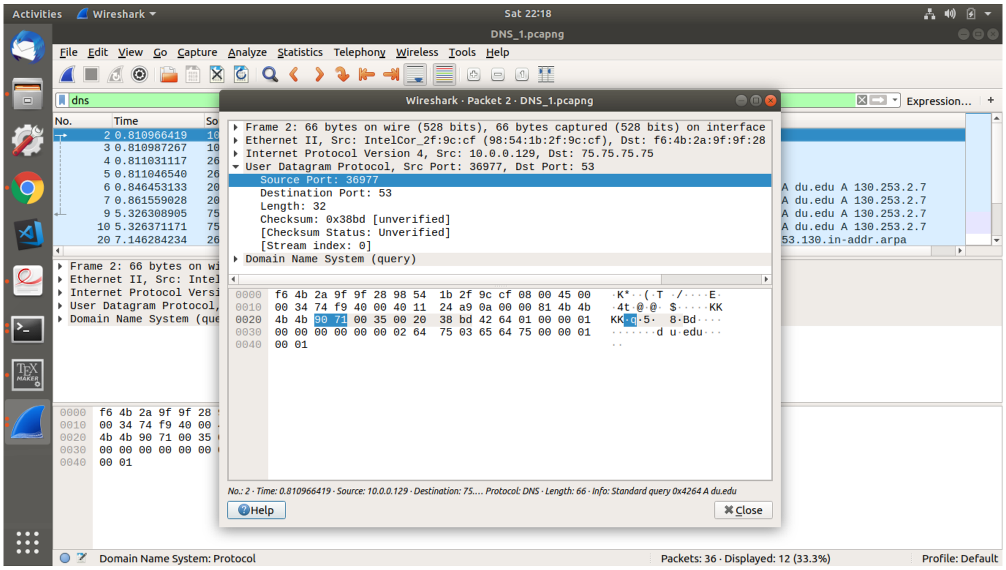
1: SET 1: The Basic DNS

(1) Determine which transport layer protocol was used for sending the DNS queries?

What are the benefits and drawbacks of using that protocol ?
UDP is used as an underlying transport layer protocol for sending the DNS queries.
Drawbacks :
It doesnot do initial handshake unlike what tcp does. That's why, it is not reliable. However, reliability can be added on application layer.
Benefits :
UDP is a faster transport layer protocol . This is because it doesnot do any sort of handshakes like tcp.
DNS requests are small requests and fits well within UDP segments.
DNS server is less loaded because of UDP since it doesnot have to maintain any connections.

(2) What port numbers are used for sending and receiving the packet in packet 2 ?

As we can see in the figure below that following ports numbers are used :
For sending : 36977
For receiving : 53



```
Wireshark · Packet 2 · DNS_1.pcapng
▸ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
▸ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: f6:4b:2a:9f:9f:28
▸ Internet Protocol Version 4, Src: 10.0.0.129, Dst: 75.75.75.75
▾ User Datagram Protocol, Src Port: 36977, Dst Port: 53
    Source Port: 36977
    Destination Port: 53
    Length: 32
    Checksum: 0x38bd [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▸ Domain Name System (query)

0000  f6 4b 2a 9f 9f 28 98 54  1b 2f 9c cf 08 00 45 00   ·K*··(·T ·/····E·
0010  00 34 74 f9 40 00 40 11  24 a9 0a 00 00 81 4b 4b   ·4t·@·@· $·····KK
0020  4b 4b 90 71 00 35 00 20  38 bd 42 64 01 00 00 01   KK·q·5·  8·Bd····
0030  00 00 00 00 00 00 02 64  75 03 65 64 75 00 00 01   ·······d u·edu···
0040  00 01                                              ··

No.: 2 · Time: 0.810966419 · Source: 10.0.0.129 · Destination: 75.... Protocol: DNS · Length: 66 · Info: Standard query 0x4264 A du.edu
```

Activities
Wireshark
Sat 22:18
DNS_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
Help
Close
Domain Name System: Protocol
Packets: 36 · Displayed: 12 (33.3%)
Profile: Default

Figure 1: port numbers

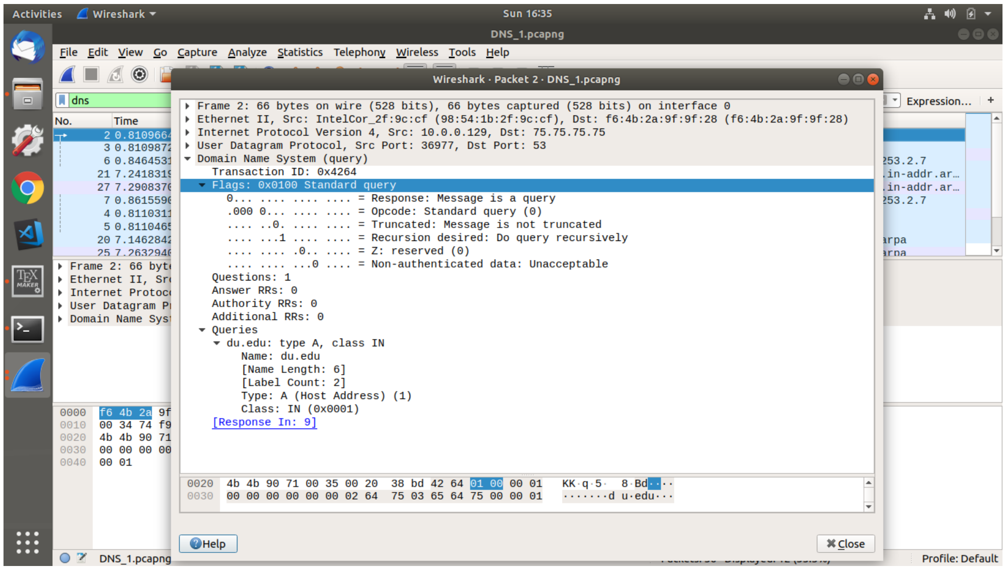
(3) What is the destination address of packet 2? What type of DNS query it is? What type of DNS server it is? What flags are set in the query ?

Destination address : 75.75.75.75

DNS query type : A

DNS server : Non - authoritative server

Flags that are set in the query is: Recursion desired (as we can verify it from the figure below.)

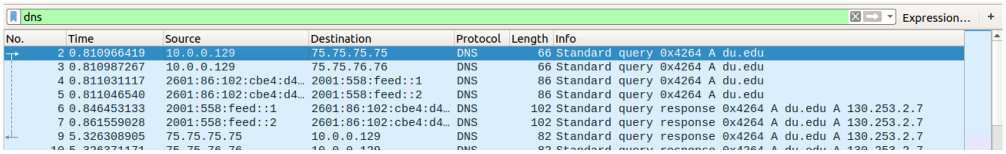


```
Wireshark · Packet 2 · DNS_1.pcapng
▸ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: f6:4b:2a:9f:9f:28 (f6:4b:2a:9f:9f:28)
▸ Internet Protocol Version 4, Src: 10.0.0.129, Dst: 75.75.75.75
▸ User Datagram Protocol, Src Port: 36977, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x4264
  ▾ 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
    ▾ du.edu: type A, class IN
        Name: du.edu
        [Name Length: 6]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 9]

0020  4b 4b 90 71 00 35 00 20  38 bd 42 64 01 00 00 01   KK·q·5·  8·Bd····
0030  00 00 00 00 00 00 02 64  75 03 65 64 75 00 00 01   ·······d u·edu···
```

Figure 2: packet 2 query

(4) How many DNS servers are queried to for resolving the domain name du.edu.?

4 DNS servers are queried to for resolving the domain name du.edu.

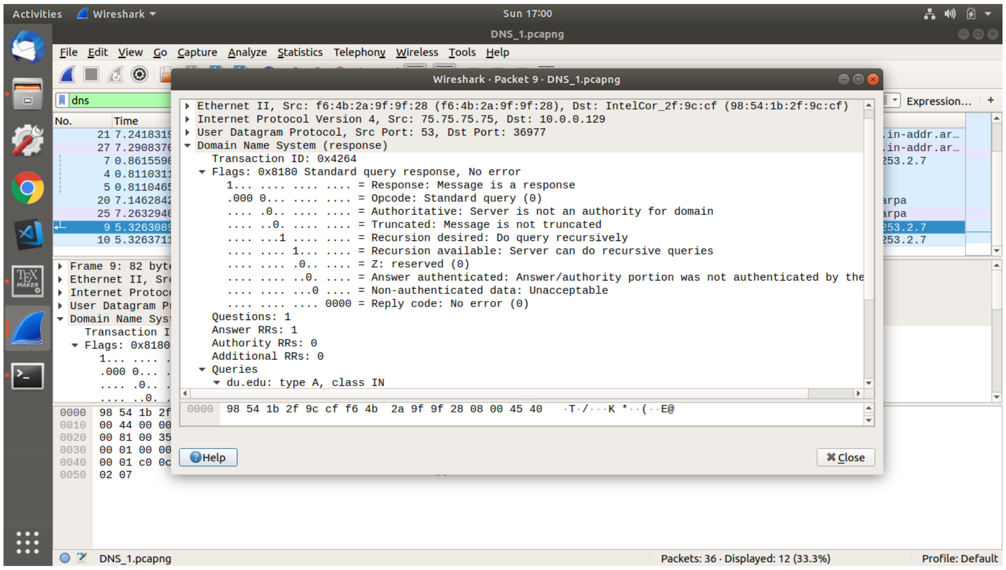


No.	Time	Source	Destination	Protocol	Length	Info
2	0.810966419	10.0.0.129	75.75.75.75	DNS	66	Standard query 0x4264 A du.edu
3	0.810987267	10.0.0.129	75.75.76.76	DNS	66	Standard query 0x4264 A du.edu
4	0.811031117	2601:86:102:cbe4:d4…	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu
5	0.811046540	2601:86:102:cbe4:d4…	2001:558:feed::2	DNS	86	Standard query 0x4264 A du.edu
6	0.846453133	2001:558:feed::1	2601:86:102:cbe4:d4…	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
7	0.861559028	2001:558:feed::2	2601:86:102:cbe4:d4…	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
9	5.326308905	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
10	5.326371171	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7

Figure 3: DNS servers

(5) Which packet contains the response of the query sent in packet 2 ? Which flags are set in the response ?

Packet number 9 contains the response of the query sent in packet number 2.
Flags which are set in the response packet are:
1) Response
2) Recursion desired
3) Recursion available

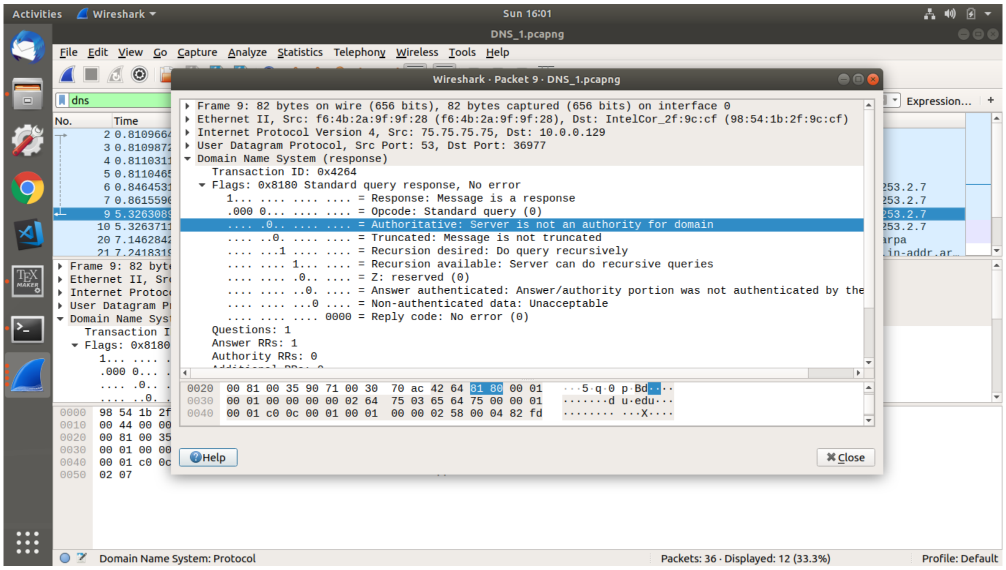

Activities
Wireshark
Sun 17:00
DNS_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
Wireshark · Packet 9 · DNS_1.pcapng
Help
Close
DNS_1.pcapng
Packets: 36 · Displayed: 12 (33.3%)
Profile: Default

```
▸ Ethernet II, Src: f6:4b:2a:9f:9f:28 (f6:4b:2a:9f:9f:28), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
▸ Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.129
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36977
▾ Domain Name System (response)
    Transaction ID: 0x4264
  ▾ 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
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ du.edu: type A, class IN

0000  98 54 1b 2f 9c cf f6 4b  2a 9f 9f 28 08 00 45 40   ·T·/···K *··(··E@
```

Figure 4: response packet of #2

(6) How many answers do you get in the response? Is the response from authoritative server ?

We get 1 answer in the response. It was not from the authoritative server as we can see the flag status.

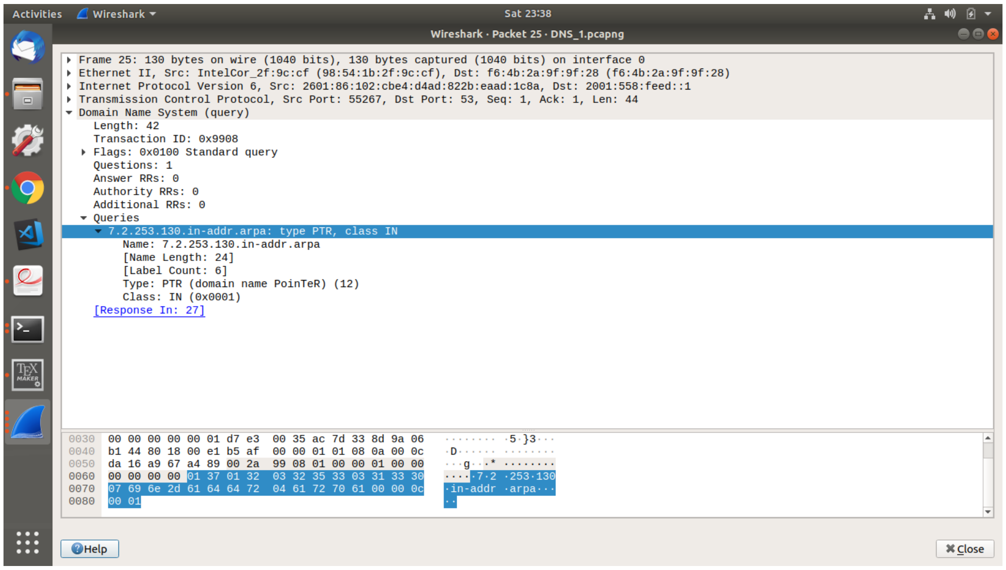

Activities
Wireshark
Sun 16:01
DNS_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression…
Wireshark · Packet 9 · DNS_1.pcapng
Help
Close
Domain Name System: Protocol
Packets: 36 · Displayed: 12 (33.3%)
Profile: Default

```
▸ Frame 9: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▸ Ethernet II, Src: f6:4b:2a:9f:9f:28 (f6:4b:2a:9f:9f:28), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
▸ Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.129
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36977
▾ Domain Name System (response)
    Transaction ID: 0x4264
  ▾ 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
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0

0020  00 81 00 35 90 71 00 30  70 ac 42 64 81 80 00 01   ···5·q·0 p·Bd····
0030  00 01 00 00 00 00 02 64  75 03 65 64 75 00 00 01   ·······d u·edu···
0040  00 01 c0 0c 00 01 00 01  00 00 02 58 00 04 82 fd   ········ ···X····
```

Figure 5: response answer of #2

(7) What does the query in the packet number 25 do ?

Packet Number 25 is a request query for an inverse domain lookings.

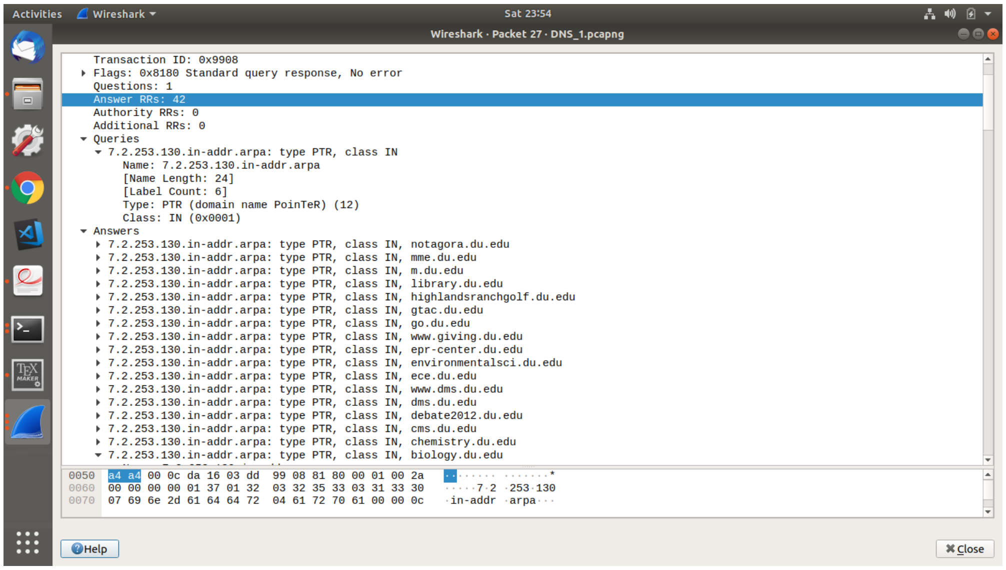


```
▸ Frame 25: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
▸ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: f6:4b:2a:9f:9f:28 (f6:4b:2a:9f:9f:28)
▸ Internet Protocol Version 6, Src: 2601:86:102:cbe4:d4ad:822b:eaad:1c8a, Dst: 2001:558:feed::1
▸ Transmission Control Protocol, Src Port: 55267, Dst Port: 53, Seq: 1, Ack: 1, Len: 44
▾ Domain Name System (query)
    Length: 42
    Transaction ID: 0x9908
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ 7.2.253.130.in-addr.arpa: type PTR, class IN
        Name: 7.2.253.130.in-addr.arpa
        [Name Length: 24]
        [Label Count: 6]
        Type: PTR (domain name PointeR) (12)
        Class: IN (0x0001)
    [Response In: 27]

0030  00 00 00 00 00 01 d7 e3  00 35 ac 7d 33 8d 9a 06   ········ ·5·}3···
0040  b1 44 80 18 00 e1 b5 af  00 00 01 01 08 0a 00 0c   ·D······ ········
0050  da 16 a9 67 a4 89 00 2a  99 08 01 00 00 01 00 00   ···g···* ········
0060  00 00 00 00 01 37 01 32  03 32 35 33 03 31 33 30   ·····7·2 ·253·130
0070  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00 0c   ·in-addr ·arpa···
0080  00 01                                              ··
```

Figure 6: query of packet #25

(8) Which packet contains the response of the query sent ? What is the response ?

Packet number 27 contains the response of the query sent. The response message contains 42 answers which are 42 machine names.



```
Transaction ID: 0x9908
▸ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 42
  Authority RRs: 0
  Additional RRs: 0
▾ Queries
  ▾ 7.2.253.130.in-addr.arpa: type PTR, class IN
      Name: 7.2.253.130.in-addr.arpa
      [Name Length: 24]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
▾ Answers
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, notagora.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, mme.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, m.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, library.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, highlandsranchgolf.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, gtac.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, go.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, www.giving.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, epr-center.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, environmentalsci.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, ece.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, www.dms.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, dms.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, debate2012.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, cms.du.edu
  ▸ 7.2.253.130.in-addr.arpa: type PTR, class IN, chemistry.du.edu
  ▾ 7.2.253.130.in-addr.arpa: type PTR, class IN, biology.du.edu

0050  a4 a4 00 0c da 16 03 dd  99 08 81 80 00 01 00 2a   ········ ·······*
0060  00 00 00 00 01 37 01 32  03 32 35 33 03 31 33 30   ·····7·2 ·253·130
0070  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00 0c   ·in-addr ·arpa···
```

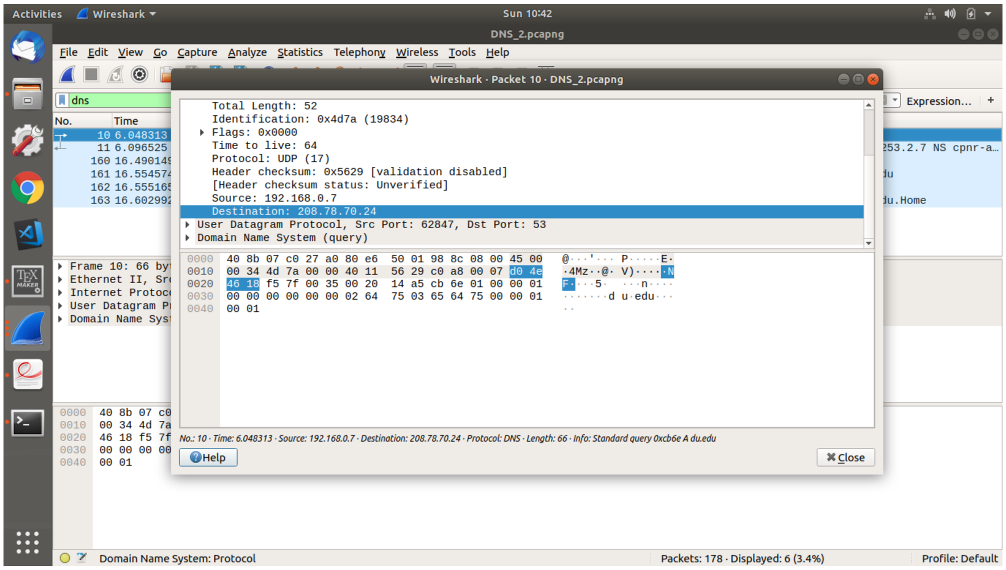
Figure 7: Response answer of packet #25

2: SET 2: Using the DNS 2.pcapng :

(1) In packet number 10, what is the destination IP address of the server? To which DNS server request is being sent to?

Destination IPA : 208.78.70.24

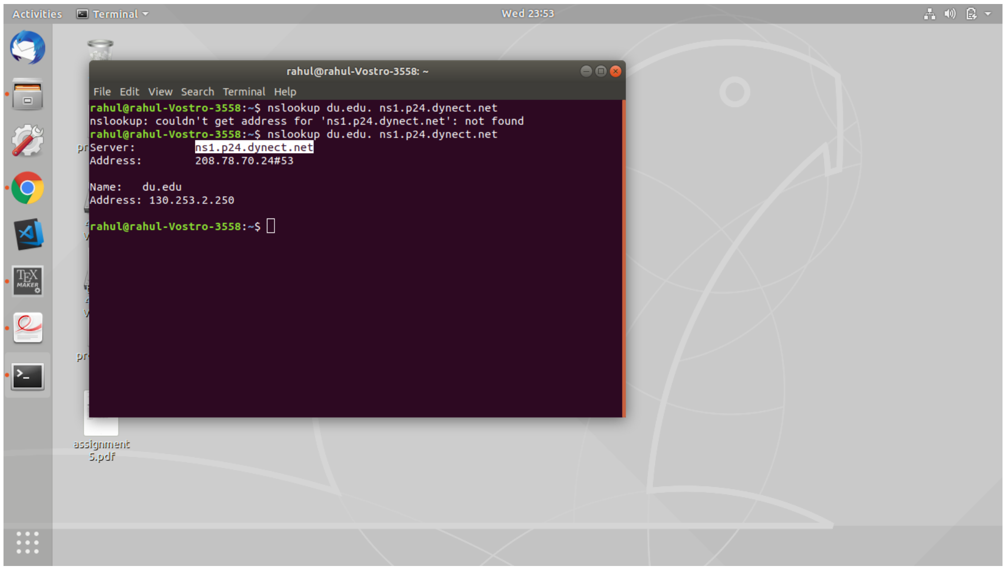
DNS server request to which it is being sent to : ns1.p24.dynect.net.



```
  Total Length: 52
  Identification: 0x4d7a (19834)
▸ Flags: 0x0000
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x5629 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.7
  Destination: 208.78.70.24
▸ User Datagram Protocol, Src Port: 62847, Dst Port: 53
▸ Domain Name System (query)

0000  40 8b 07 c0 27 a0 80 e6  50 01 98 8c 08 00 45 00   @···'··· P·····E·
0010  00 34 4d 7a 00 00 40 11  56 29 c0 a8 00 07 d0 4e   ·4Mz··@· V)·····N
0020  46 18 f5 7f 00 35 00 20  14 a5 cb 6e 01 00 00 01   F····5·  ···n····
0030  00 00 00 00 00 00 02 64  75 03 65 64 75 00 00 01   ·······d u·edu···
0040  00 01                                              ··

No.: 10 · Time: 6.048313 · Source: 192.168.0.7 · Destination: 208.78.70.24 · Protocol: DNS · Length: 66 · Info: Standard query 0xcb6e A du.edu
```

Activities
Wireshark
Sun 10:42
DNS_2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 10 · DNS_2.pcapng
dns
Expression…
No.
Time
Help
Close
Domain Name System: Protocol
Packets: 178 · Displayed: 6 (3.4%)
Profile: Default

Figure 8: Destination IPA of the server

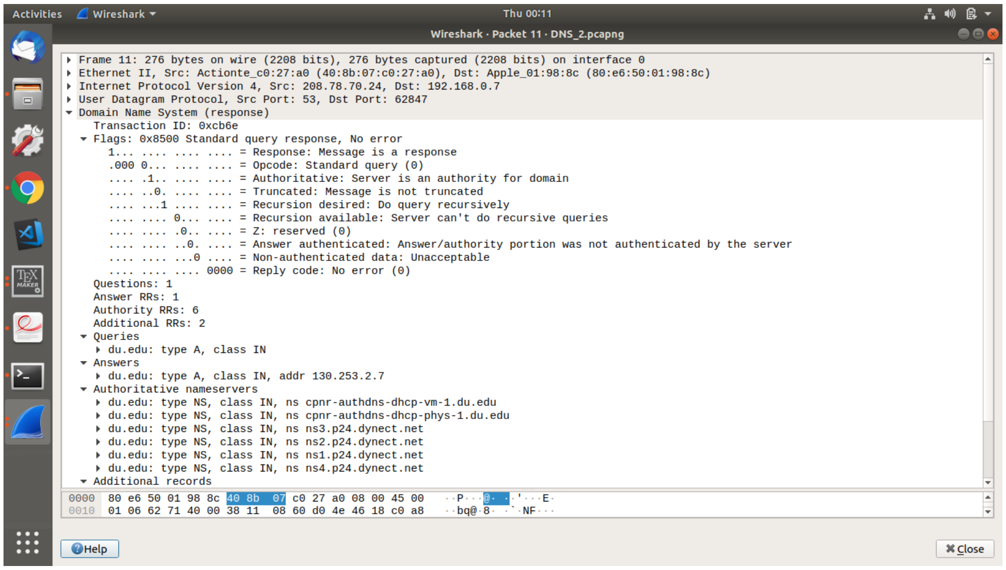


Activities
Terminal
Wed 23:53
rahul@rahul-Vostro-3558: ~
File Edit View Search Terminal Help
assignment 5.pdf

```
rahul@rahul-Vostro-3558:~$ nslookup du.edu. ns1.p24.dynect.net
nslookup: couldn't get address for 'ns1.p24.dynect.net': not found
rahul@rahul-Vostro-3558:~$ nslookup du.edu. ns1.p24.dynect.net
Server:         ns1.p24.dynect.net
Address:        208.78.70.24#53

Name:   du.edu
Address: 130.253.2.250

rahul@rahul-Vostro-3558:~$ 
```

Figure 9: DNS server

(2) Which packet contains the reply of the query that is sent in packet #10? Did DNS server reply ? Examine the flags of the response and what you infer from the flags? Packet number 11 contains the response of the query sent in packet number 10. Yes DNS server replied. Flag responses : Following labels are set in flag:
1) Response
2) Authoritative
3) Recursion desired
We can draw some useful conclusion by looking at the flag response which are as follows:
The nameserver which handled the query was an authoritative server for du.edu since the authoritative label is set in the flag.

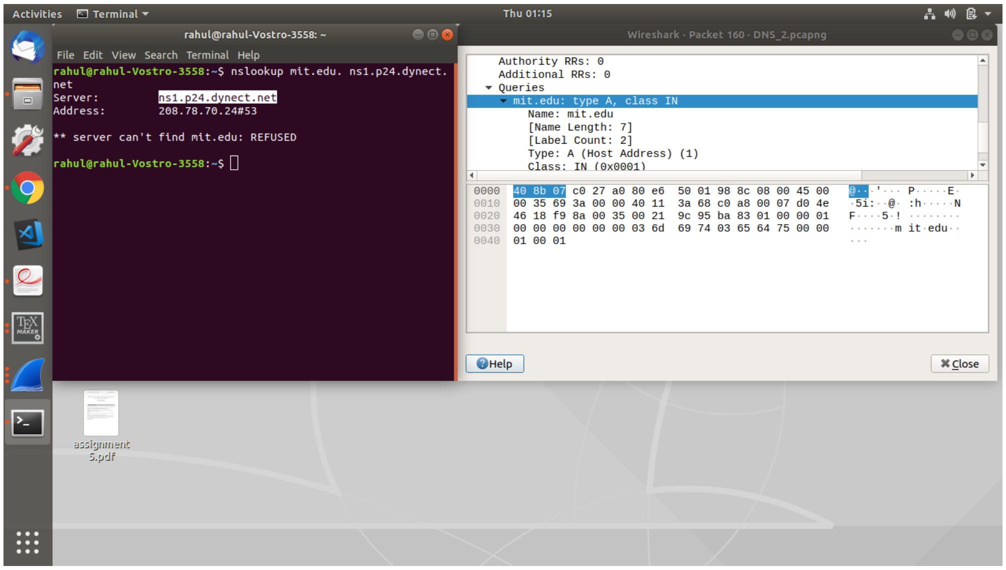


```
▸ Frame 11: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits) on interface 0
▸ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: Apple_01:98:8c (80:e6:50:01:98:8c)
▸ Internet Protocol Version 4, Src: 208.78.70.24, Dst: 192.168.0.7
▸ User Datagram Protocol, Src Port: 53, Dst Port: 62847
▾ Domain Name System (response)
    Transaction ID: 0xcb6e
  ▾ Flags: 0x8500 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 0... .... = Recursion available: Server can't 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: 6
    Additional RRs: 2
  ▾ Queries
    ▸ du.edu: type A, class IN
  ▾ Answers
    ▸ du.edu: type A, class IN, addr 130.253.2.7
  ▾ Authoritative nameservers
    ▸ du.edu: type NS, class IN, ns cpnr-authdns-dhcp-vm-1.du.edu
    ▸ du.edu: type NS, class IN, ns cpnr-authdns-dhcp-phys-1.du.edu
    ▸ du.edu: type NS, class IN, ns ns3.p24.dynect.net
    ▸ du.edu: type NS, class IN, ns ns2.p24.dynect.net
    ▸ du.edu: type NS, class IN, ns ns1.p24.dynect.net
    ▸ du.edu: type NS, class IN, ns ns4.p24.dynect.net
  ▾ Additional records

0000  80 e6 50 01 98 8c 40 8b  07 c0 27 a0 08 00 45 00   ··P···@· ··'···E·
0010  01 06 62 71 40 00 38 11  08 60 d0 4e 46 18 c0 a8   ··bq@·8· ·`·NF···
```

Figure 10: packet number 11

(3) To which DNS server, is the DNS request in #160 sent to? What does the DNS request ask from the DNS server?

The DNS request in #160 is being sent to ns1.p24.dynect.net .
It asked about the IPA of mit.edu domain.



Activities
Terminal
Thu 01:15
rahul@rahul-Vostro-3558: ~
File Edit View Search Terminal Help
Wireshark · Packet 160 · DNS_2.pcapng
Help
Close
assignment 5.pdf

```
rahul@rahul-Vostro-3558:~$ nslookup mit.edu. ns1.p24.dynect.
net
Server:         ns1.p24.dynect.net
Address:        208.78.70.24#53

** server can't find mit.edu: REFUSED

rahul@rahul-Vostro-3558:~$ 
```

```
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ mit.edu: type A, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

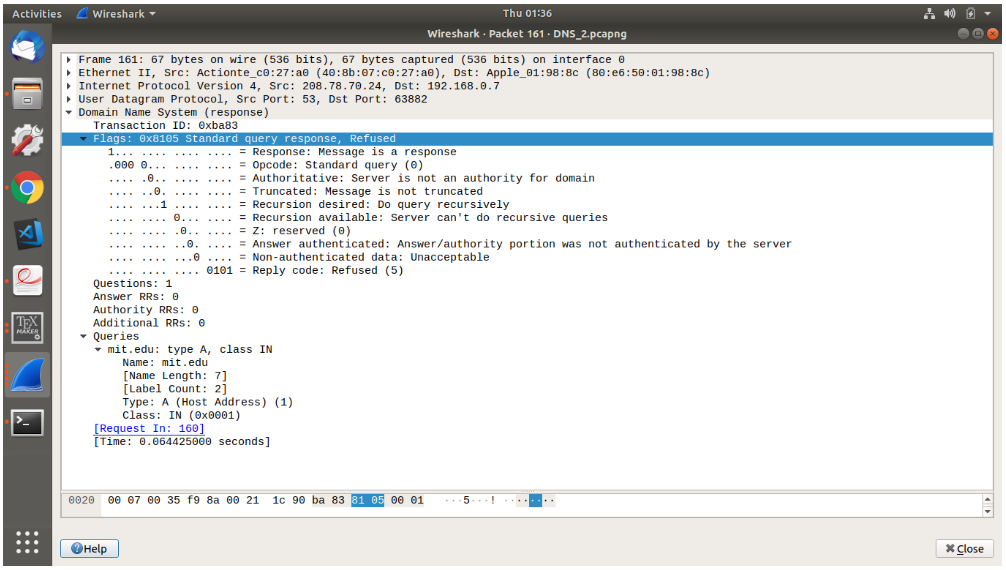
```
0000  40 8b 07 c0 27 a0 80 e6  50 01 98 8c 08 00 45 00   @··'···  P·····E·
0010  00 35 69 3a 00 00 40 11  3a 68 c0 a8 00 07 d0 4e   ·5i:··@· :h·····N
0020  46 18 f9 8a 00 35 00 21  9c 95 ba 83 01 00 00 01   F····5·! ········
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  01 00 01                                           ···
```

Figure 11: packet number 160 query and nslookup

(4) What is the response from the DNS server in packet #160 ? Did the server resolve the DNS request? Explain in brief?

The DNS server refused the query asked in packet #160. No, the server didn't resolved the DNS request.

Over here the nameserver might not be able to find the information related to mit.edu which results in rejecting the query.



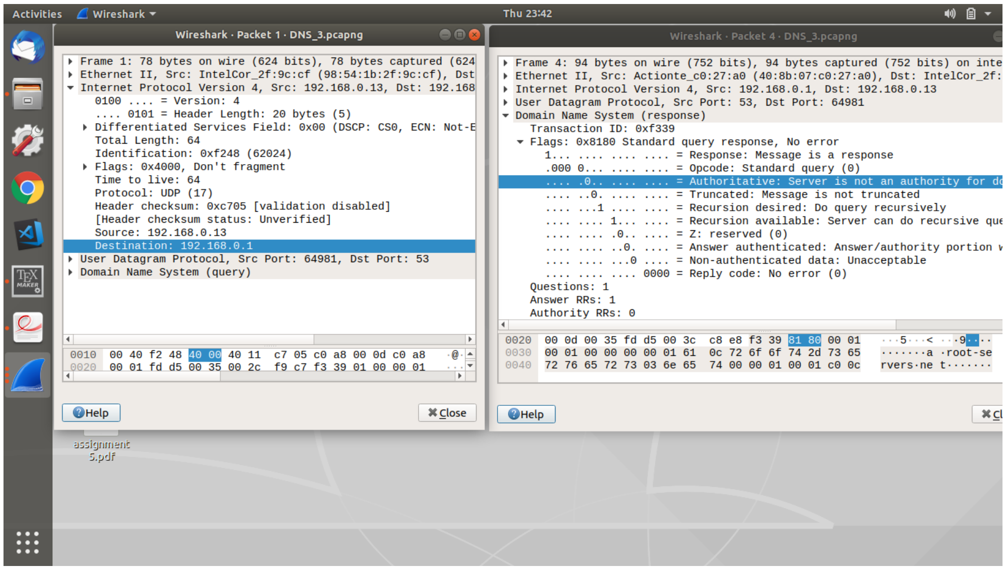
```
▸ Frame 161: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: Apple_01:98:8c (80:e6:50:01:98:8c)
▸ Internet Protocol Version 4, Src: 208.78.70.24, Dst: 192.168.0.7
▸ User Datagram Protocol, Src Port: 53, Dst Port: 63882
▾ Domain Name System (response)
    Transaction ID: 0xba83
  ▾ Flags: 0x8105 Standard query response, Refused
      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
      .... .... 0... .... = Recursion available: Server can't do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0101 = Reply code: Refused (5)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ mit.edu: type A, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Request In: 160]
    [Time: 0.064425000 seconds]

0020  00 07 00 35 f9 8a 00 21  1c 90 ba 83 81 05 00 01   ···5···! ········
```

Figure 12: response packet of #160

3: SET 3: Working with the DNS 3.pcapng :

(1) 1. To what IP address, is the DNS query sent in packet #1? What typeof DNS server is that?

The DNS query is sent to a server with IPA : 192.168.0.1 (shown in the screen dump below)
It is a non-authoritative server (local DNS server).
We can verify it by looking at the response packet which is in our case is packet #4 where the flag label of authority part is not set.


Activities
Wireshark
Thu 23:42
Wireshark · Packet 1 · DNS_3.pcapng
Help
Close
assignment 5.pdf
Wireshark · Packet 4 · DNS_3.pcapng
Help
Cl

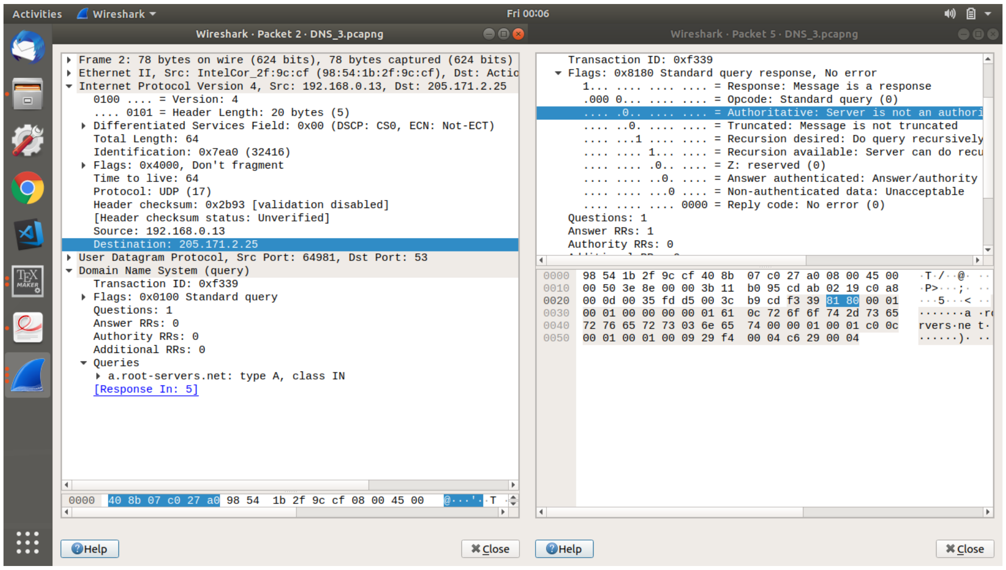
```
▸ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624
▸ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst
▾ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 192.168
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E
    Total Length: 64
    Identification: 0xf248 (62024)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xc705 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.13
    Destination: 192.168.0.1
▸ User Datagram Protocol, Src Port: 64981, Dst Port: 53
▸ Domain Name System (query)

0010  00 40 f2 48 40 00 40 11  c7 05 c0 a8 00 0d c0 a8   ·@·
0020  00 01 fd d5 00 35 00 2c  f9 c7 f3 39 01 00 00 01   ···
```

```
▸ Frame 4: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on inte
▸ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: IntelCor_2f:
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.13
▸ User Datagram Protocol, Src Port: 53, Dst Port: 64981
▾ Domain Name System (response)
    Transaction ID: 0xf339
  ▾ 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 do
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive que
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion w
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0

0020  00 0d 00 35 fd d5 00 3c  c8 e8 f3 39 81 80 00 01   ···5···< ···9····
0030  00 01 00 00 00 00 01 61  0c 72 6f 6f 74 2d 73 65   ·······a ·root-se
0040  72 76 65 72 73 03 6e 65  74 00 00 01 00 01 c0 0c   rvers·ne t·······
```

Figure 13: screenshot of IPA and DNS server flag for the query

(2) To what IP address is the DNS query sent in packet #2? What typeof DNS server is that?

The DNS query is sent to a server with IPA :205.171.2.25 (shown in the screen dump below)
It is a non-authoritative server (and is a TLD server).


Activities
Wireshark
Fri 00:06
Wireshark · Packet 2 · DNS_3.pcapng
Wireshark · Packet 5 · DNS_3.pcapng
Help
Close
Help
Close

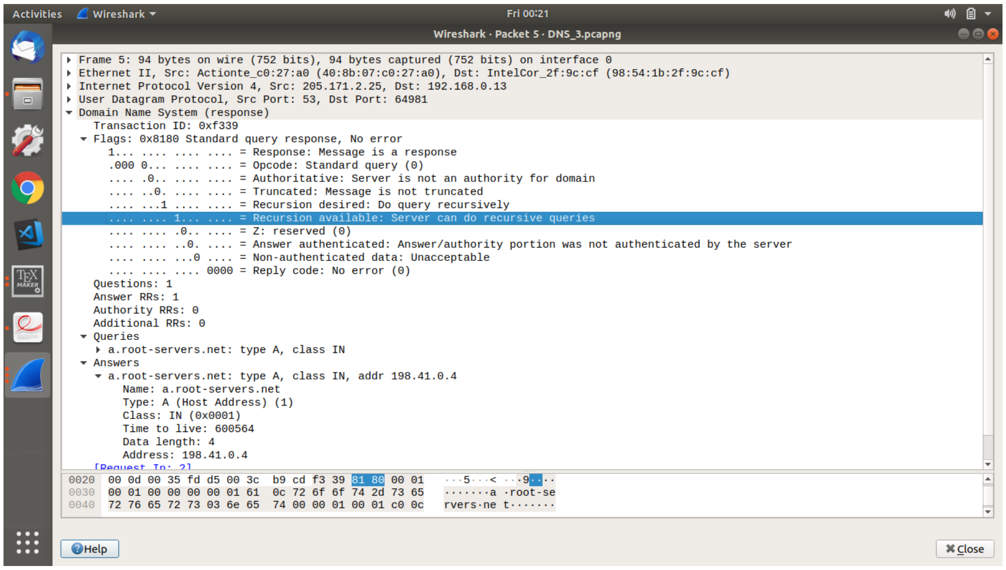
```
▸ Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▸ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actic
▾ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 205.171.2.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 64
    Identification: 0x7ea0 (32416)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x2b93 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.13
    Destination: 205.171.2.25
▸ User Datagram Protocol, Src Port: 64981, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xf339
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ a.root-servers.net: type A, class IN
    [Response In: 5]

0000  40 8b 07 c0 27 a0 98 54  1b 2f 9c cf 08 00 45 00   @···'··T
```

```
    Transaction ID: 0xf339
  ▾ 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 authori
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recu
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0

0000  98 54 1b 2f 9c cf 40 8b  07 c0 27 a0 08 00 45 00   ·T·/··@·  ··
0010  00 50 3e 8e 00 00 3b 11  b0 95 cd ab 02 19 c0 a8   ·P>···;·  ··
0020  00 0d 00 35 fd d5 00 3c  b9 cd f3 39 81 80 00 01   ···5···<  ··
0030  00 01 00 00 00 00 01 61  0c 72 6f 6f 74 2d 73 65   ·······a ·r
0040  72 76 65 72 73 03 6e 65  74 00 00 01 00 01 c0 0c   rvers·ne t·
0050  00 01 00 01 00 09 29 f4  00 04 c6 29 00 04         ······)· ··
```

Figure 14: IPA and type of DNS server

(3) Which packet contains the response of the query that is sent in packet #2? What is your interpretation of the response?

Packet number 5 contains the response of the query that is sent in packet number 2.
We know that 13 root servers are there in the world and in this packet response its IPA is being returned. Now, since the TLD server (from the IPA of the server) is doing a recursive call as we can see from the flag status that recusion desired is set. We can infer that at max 1 recursive call will be there since it is a query regarding root server's IPA.

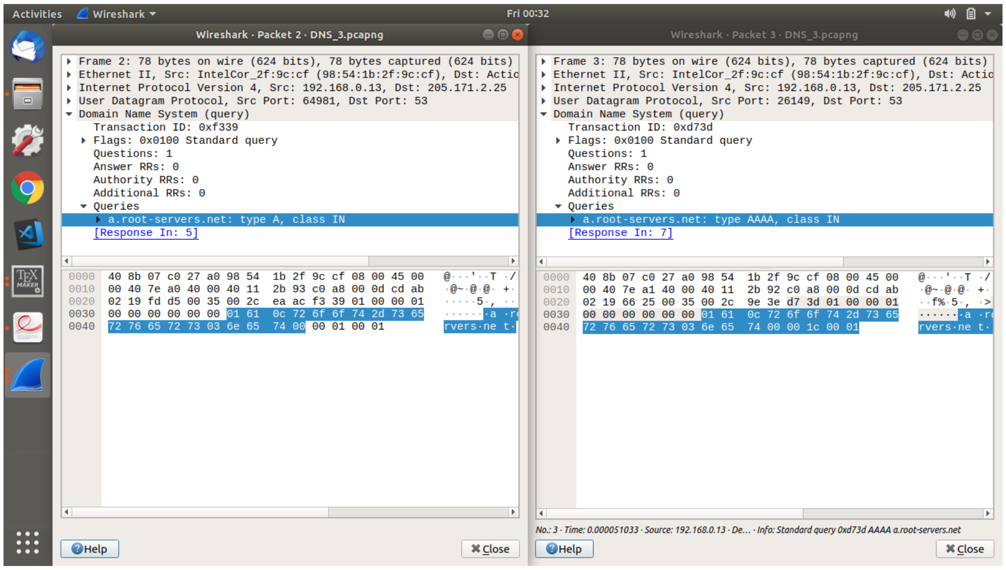


```
Frame 5: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
Internet Protocol Version 4, Src: 205.171.2.25, Dst: 192.168.0.13
User Datagram Protocol, Src Port: 53, Dst Port: 64981
Domain Name System (response)
  Transaction ID: 0xf339
  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: 0
  Additional RRs: 0
  Queries
    a.root-servers.net: type A, class IN
  Answers
    a.root-servers.net: type A, class IN, addr 198.41.0.4
      Name: a.root-servers.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 600564
      Data length: 4
      Address: 198.41.0.4
  [Request In: 2]

0020  00 0d 00 35 fd d5 00 3c  b9 cd f3 39 81 80 00 01   ···5···< ···9····
0030  00 01 00 00 00 00 01 61  0c 72 6f 6f 74 2d 73 65   ·······a ·root-se
0040  72 76 65 72 73 03 6e 65  74 00 00 01 00 01 c0 0c   rvers·ne t·······
```

Figure 15: Packet number 5

(4) What is the difference between query in packet #2 and that in #3 ?

Packet number 2 is asking for A type DNS query which returns an IPv4 address where as packet number 3 is asking for AAAA type query which basically returns an IPv6 address.


Activities
Wireshark
Fri 00:32
Wireshark · Packet 2 · DNS_3.pcapng
Wireshark · Packet 3 · DNS_3.pcapng
Help
Close
Help
Close

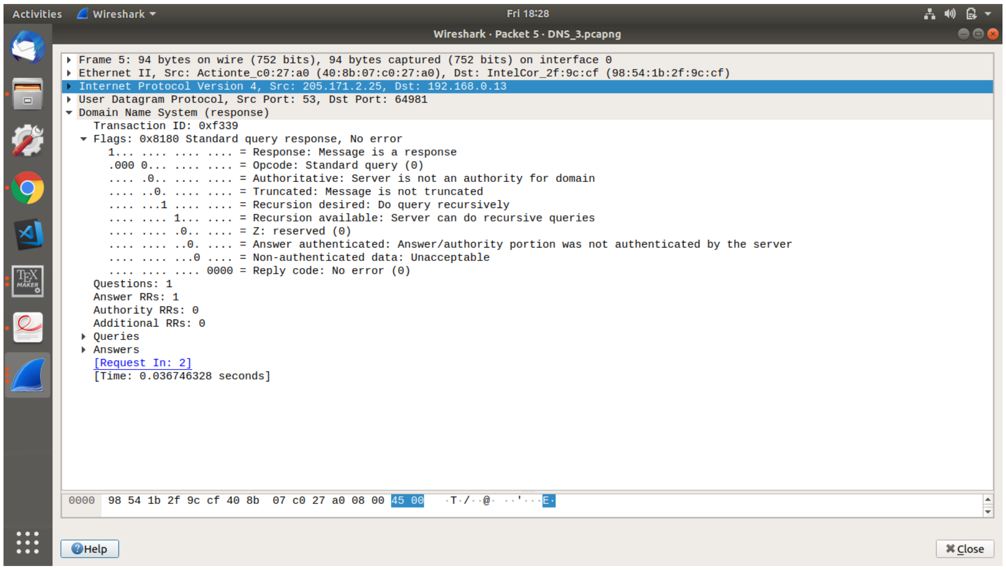
```
Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actio
Internet Protocol Version 4, Src: 192.168.0.13, Dst: 205.171.2.25
User Datagram Protocol, Src Port: 64981, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xf339
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    a.root-servers.net: type A, class IN
  [Response In: 5]

0000  40 8b 07 c0 27 a0 98 54  1b 2f 9c cf 08 00 45 00   @···'··T ·/
0010  00 40 7e a0 40 00 40 11  2b 93 c0 a8 00 0d cd ab   ·@~·@·@· +·
0020  02 19 fd d5 00 35 00 2c  ea ac f3 39 01 00 00 01   ·····5·, ··
0030  00 00 00 00 00 00 01 61  0c 72 6f 6f 74 2d 73 65   ······a ·r
0040  72 76 65 72 73 03 6e 65  74 00 00 01 00 01         rvers·ne t·
```

```
Frame 3: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actio
Internet Protocol Version 4, Src: 192.168.0.13, Dst: 205.171.2.25
User Datagram Protocol, Src Port: 26149, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xd73d
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    a.root-servers.net: type AAAA, class IN
  [Response In: 7]

0000  40 8b 07 c0 27 a0 98 54  1b 2f 9c cf 08 00 45 00   @···'··T ·/
0010  00 40 7e a1 40 00 40 11  2b 92 c0 a8 00 0d cd ab   ·@~·@·@· +·
0020  02 19 66 25 00 35 00 2c  9e 3e d7 3d 01 00 00 01   ··f%·5·, ·>
0030  00 00 00 00 00 00 01 61  0c 72 6f 6f 74 2d 73 65   ······a ·r
0040  72 76 65 72 73 03 6e 65  74 00 00 1c 00 01         rvers·ne t·

No.: 3 · Time: 0.000051033 · Source: 192.168.0.13 · De… · Info: Standard query 0xd73d AAAA a.root-servers.net
```

Figure 16: Packet number 5

(5) What does the query in packet #8 do? Which DNS server is being queried?

The query in packet #8 asks the DNS server about the IPA of the host name mit.edu. The request is not from a local server as we can see that initial netID component of the IPA is not same.

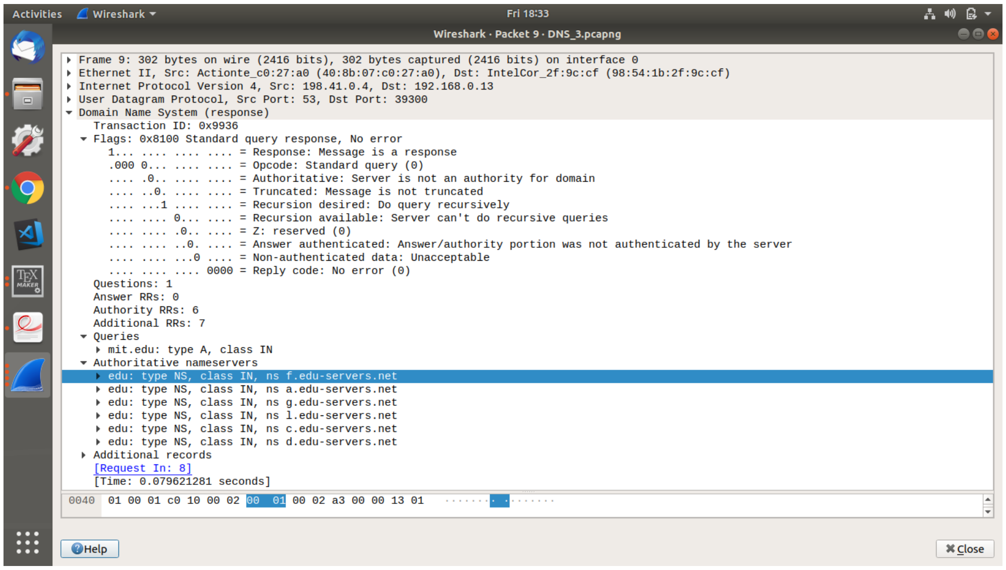


```
▸ Frame 5: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
▸ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
▸ Internet Protocol Version 4, Src: 205.171.2.25, Dst: 192.168.0.13
▸ User Datagram Protocol, Src Port: 53, Dst Port: 64981
▾ Domain Name System (response)
    Transaction ID: 0xf339
  ▾ 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: 0
    Additional RRs: 0
  ▸ Queries
  ▸ Answers
    [Request In: 2]
    [Time: 0.036746328 seconds]

0000  98 54 1b 2f 9c cf 40 8b  07 c0 27 a0 08 00 45 00   ·T·/··@· ··'···E·
```

Figure 17: Packet number 8

(6) Which packet contains the response of the query sent in packet #8? What flags are set in this response? Does it have the answer user wants? What information does it provide?

Packet #9.
Flags :response and recurision are set.
No, it does not have the answer that user wants.
The dns server responded with a additional records and authoritative name servers list but didn't replied anything about the desired query.

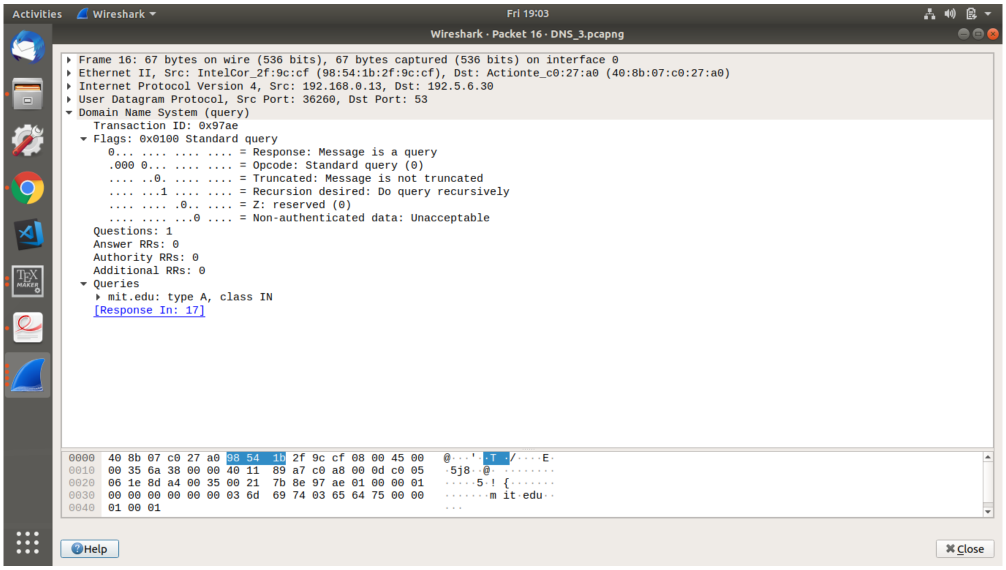


```
▸ Frame 9: 302 bytes on wire (2416 bits), 302 bytes captured (2416 bits) on interface 0
▸ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
▸ Internet Protocol Version 4, Src: 198.41.0.4, Dst: 192.168.0.13
▸ User Datagram Protocol, Src Port: 53, Dst Port: 39300
▾ Domain Name System (response)
    Transaction ID: 0x9936
  ▾ Flags: 0x8100 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
      .... .... 0... .... = Recursion available: Server can't 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: 0
    Authority RRs: 6
    Additional RRs: 7
  ▾ Queries
    ▸ mit.edu: type A, class IN
  ▾ Authoritative nameservers
    ▸ edu: type NS, class IN, ns f.edu-servers.net
    ▸ edu: type NS, class IN, ns a.edu-servers.net
    ▸ edu: type NS, class IN, ns g.edu-servers.net
    ▸ edu: type NS, class IN, ns l.edu-servers.net
    ▸ edu: type NS, class IN, ns c.edu-servers.net
    ▸ edu: type NS, class IN, ns d.edu-servers.net
  ▸ Additional records
    [Request In: 8]
    [Time: 0.079621281 seconds]

0040  01 00 01 c0 10 00 02 00  01 00 02 a3 00 00 13 01   ················
```

Figure 18: Packet number 9

(7) Which DNS server is being queried in the query of packet #16 ? Is it a local DNS server ?

TLD DNS server is being queried in the query of packet #16.
No, It is not a local server since .edu type request is from TLD DNS server.

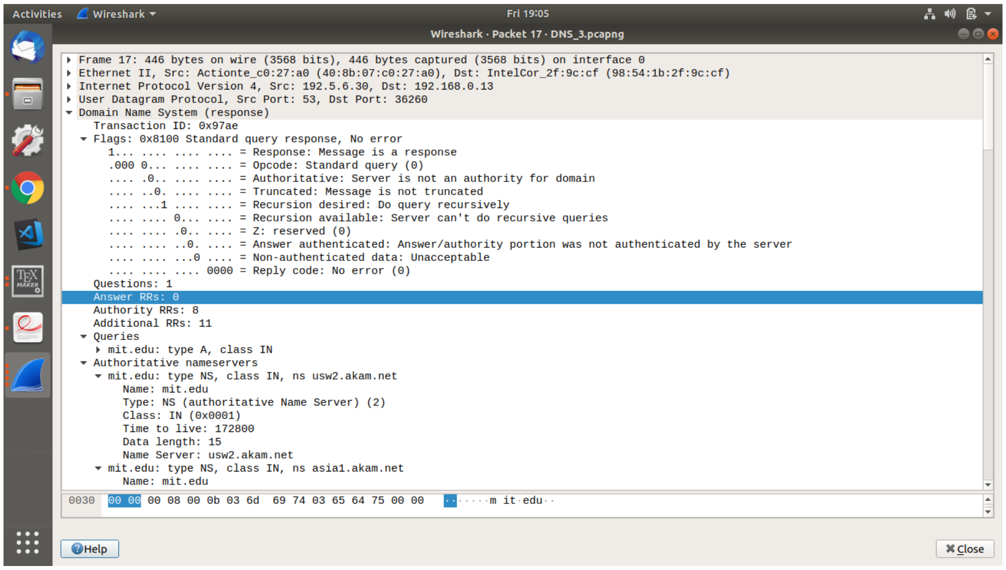


```
▸ Frame 16: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actionte_c0:27:a0 (40:8b:07:c0:27:a0)
▸ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 192.5.6.30
▸ User Datagram Protocol, Src Port: 36260, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x97ae
  ▾ 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: 17]

0000  40 8b 07 c0 27 a0 98 54  1b 2f 9c cf 08 00 45 00   @···'··T ·/····E·
0010  00 35 6a 38 00 00 40 11  89 a7 c0 a8 00 0d c0 05   ·5j8··@· ········
0020  06 1e 8d a4 00 35 00 21  7b 8e 97 ae 01 00 00 01   ·····5·! {·······
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  01 00 01                                           ···
```

Figure 19: Packet number 16

(8) Which packet contains the response of the query sent in packet #16? What flags are set in this response? Does it have the answer user wants? What information does it provide?

Packet #17 .
Flags : response and recurision are set.
No, it does not have the answer that user wants.
The dns server responded with a list of authoritative servers along with the IPA withou any answer.

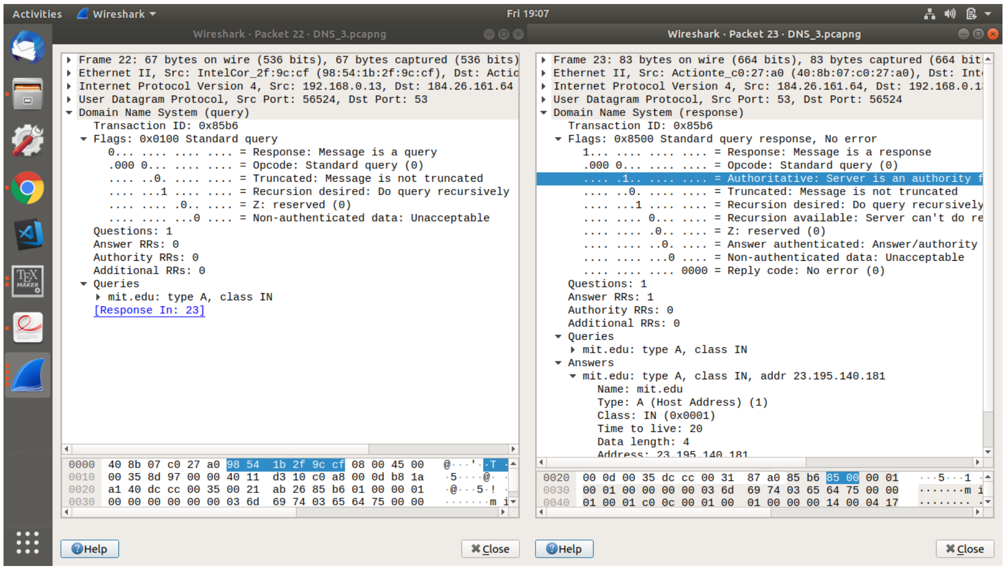


```
Wireshark · Packet 17 · DNS_3.pcapng
▸ Frame 17: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0
▸ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
▸ Internet Protocol Version 4, Src: 192.5.6.30, Dst: 192.168.0.13
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36260
▾ Domain Name System (response)
    Transaction ID: 0x97ae
  ▾ Flags: 0x8100 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
      .... .... 0... .... = Recursion available: Server can't 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: 0
    Authority RRs: 8
    Additional RRs: 11
  ▾ Queries
    ▸ mit.edu: type A, class IN
  ▾ Authoritative nameservers
    ▾ mit.edu: type NS, class IN, ns usw2.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 172800
        Data length: 15
        Name Server: usw2.akam.net
    ▾ mit.edu: type NS, class IN, ns asia1.akam.net
        Name: mit.edu
0030  00 00 00 08 00 0b 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
```

Figure 20: Packet number 17

(9) What does the query in packet #22 actually do? Which DNS server is being queried?

Asks the DNS server the IPA of the mit.edu.
Authoritative DNS server is being queried .



```
Wireshark · Packet 22 · DNS_3.pcapng
▸ Frame 22: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
▸ Ethernet II, Src: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf), Dst: Actio
▸ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 184.26.161.64
▸ User Datagram Protocol, Src Port: 56524, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x85b6
  ▾ 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: 23]
0000  40 8b 07 c0 27 a0 98 54  1b 2f 9c cf 08 00 45 00   @···'··T ··
0010  00 35 8d 97 00 00 40 11  d3 10 c0 a8 00 0d b8 1a   ·5····@· ··
0020  a1 40 dc cc 00 35 00 21  ab 26 85 b6 01 00 00 01   ·@···5·! ··
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m i
```

```
Wireshark · Packet 23 · DNS_3.pcapng
▸ Frame 23: 83 bytes on wire (664 bits), 83 bytes captured (664 bit
▸ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: Int
▸ Internet Protocol Version 4, Src: 184.26.161.64, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 56524
▾ Domain Name System (response)
    Transaction ID: 0x85b6
  ▾ Flags: 0x8500 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority f
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 0... .... = Recursion available: Server can't do re
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mit.edu: type A, class IN
  ▾ Answers
    ▾ mit.edu: type A, class IN, addr 23.195.140.181
        Name: mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20
        Data length: 4
        Address: 23.195.140.181
0020  00 0d 00 35 dc cc 00 31  87 a0 85 b6 85 00 00 01   ···5···1 ·
0030  00 01 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m i
0040  01 00 01 c0 0c 00 01 00  01 00 00 00 14 00 04 17   ········ ·
```

Figure 21: Packet number 22 and 23

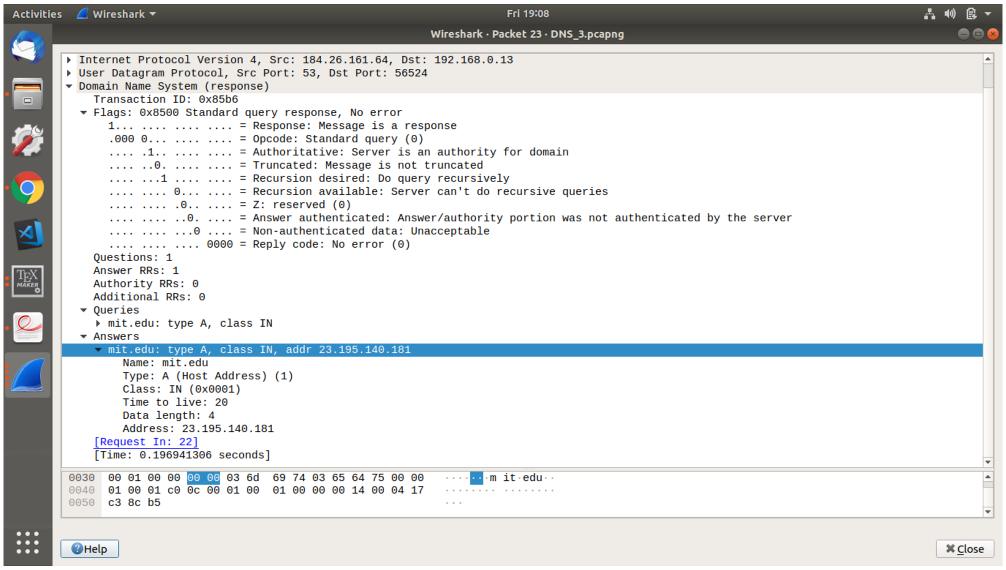
(10) Which packet contains the response to the query sent in packet #22? What flags are set in this response? Does it have the answer user wants? What information does it provide?

Packet #23

Flags: response, authoritative and recursion are set.

Yes, it have the answer that the user wants.

The DNS server responded with the IPA of mit.edu .



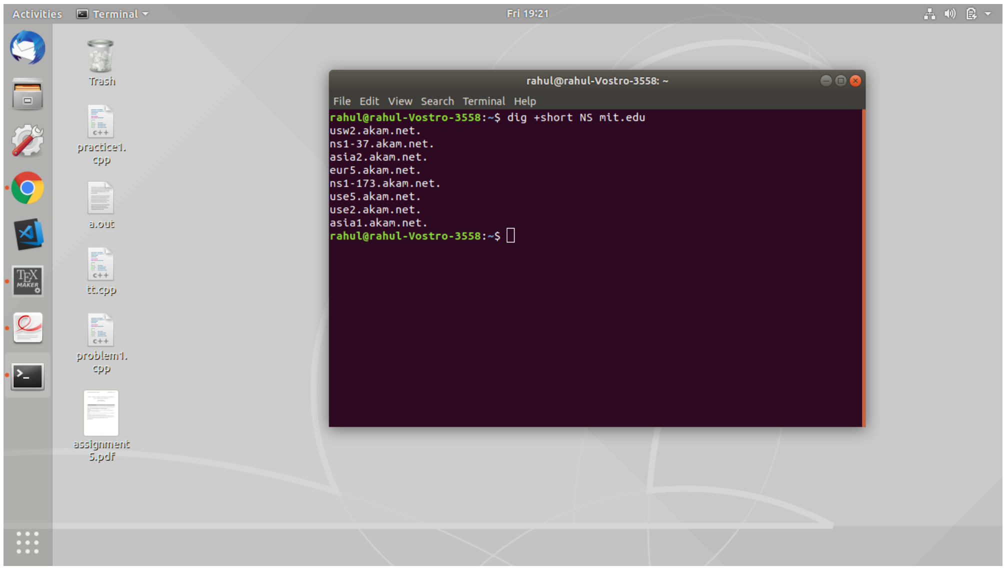
```
▸ Internet Protocol Version 4, Src: 184.26.161.64, Dst: 192.168.0.13
▸ User Datagram Protocol, Src Port: 53, Dst Port: 56524
▾ Domain Name System (response)
    Transaction ID: 0x85b6
  ▾ Flags: 0x8500 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 0... .... = Recursion available: Server can't 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: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mit.edu: type A, class IN
  ▾ Answers
    ▾ mit.edu: type A, class IN, addr 23.195.140.181
        Name: mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20
        Data length: 4
        Address: 23.195.140.181
    [Request In: 22]
    [Time: 0.196941306 seconds]

0030  00 01 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  01 00 01 c0 0c 00 01 00  01 00 00 00 14 00 04 17   ········ ········
0050  c3 8c b5                                           ···
```

Figure 22: Packet number 23

4: SET 4 - Using dig command :

(1) What is the dig command used to determine the authoritative DNS servers for www.mit.edu?

command : dig +short NS mit.edu

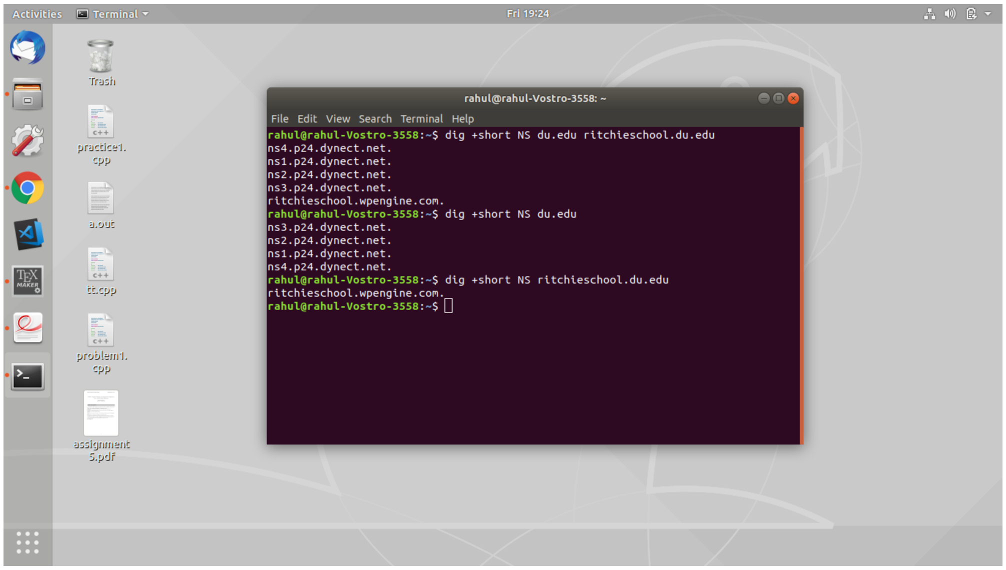


```
rahul@rahul-Vostro-3558:~$ dig +short NS mit.edu
usw2.akam.net.
ns1-37.akam.net.
asia2.akam.net.
eur5.akam.net.
ns1-173.akam.net.
use5.akam.net.
use2.akam.net.
asia1.akam.net.
rahul@rahul-Vostro-3558:~$
```

Figure 23: dig command

(2) Using dig command determine the authoritative DNS servers for www.du.edu and www.ritchieschool.du.edu in a single dig command? Are DNS servers for both different?

Yes, DNS server for both are different. One can verify it from the screenshot given below.

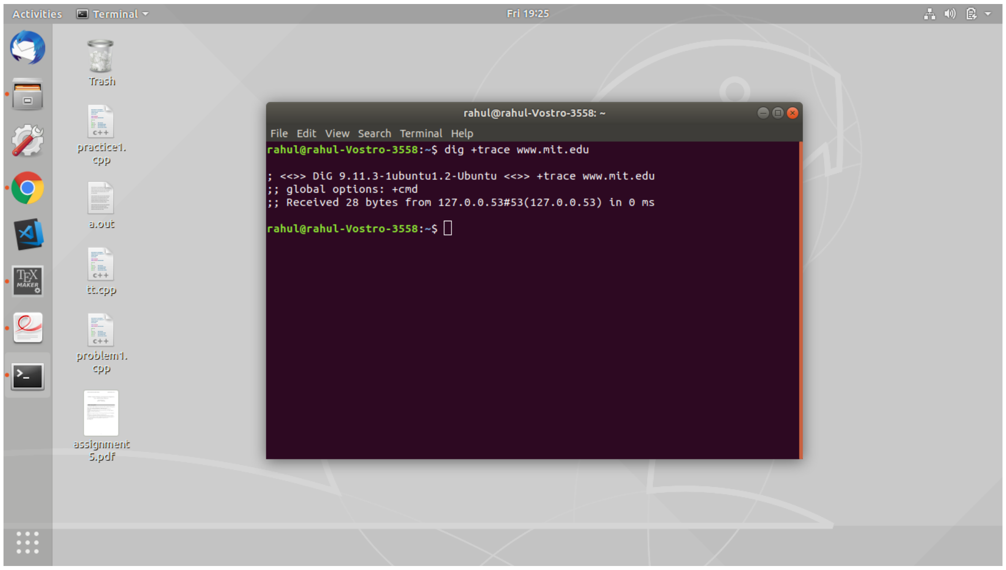


```
rahul@rahul-Vostro-3558:~$ dig +short NS du.edu ritchieschool.du.edu
ns4.p24.dynect.net.
ns1.p24.dynect.net.
ns2.p24.dynect.net.
ns3.p24.dynect.net.
ritchieschool.wpengine.com.
rahul@rahul-Vostro-3558:~$ dig +short NS du.edu
ns3.p24.dynect.net.
ns2.p24.dynect.net.
ns1.p24.dynect.net.
ns4.p24.dynect.net.
rahul@rahul-Vostro-3558:~$ dig +short NS ritchieschool.du.edu
ritchieschool.wpengine.com.
rahul@rahul-Vostro-3558:~$ 
```

Figure 24: dig command

(3) Use dig command with trace option to www.mit.edu (i.e. dig +trace www.mit.edu). What you can infer from the output?

As the link was present in the already in the application cache, the output showed us that the DNS query is answered by the local DNS server .



```
rahul@rahul-Vostro-3558:~$ dig +trace www.mit.edu

; <<>> DiG 9.11.3-1ubuntu1.2-Ubuntu <<>> +trace www.mit.edu
;; global options: +cmd
;; Received 28 bytes from 127.0.0.53#53(127.0.0.53) in 0 ms

rahul@rahul-Vostro-3558:~$ 
```

Figure 25: dig trace