CSP334 : Computer Networks
Lab Assignment No 6
Assignment on DNS

Sahil
2016UCS0008

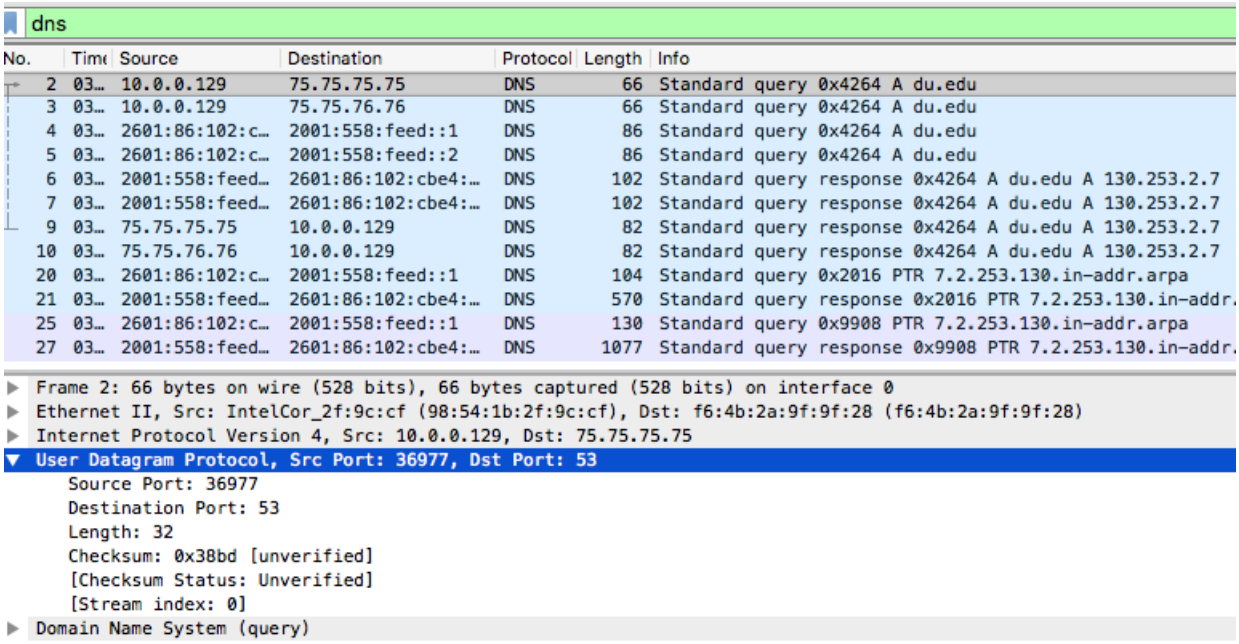
October 26, 2018

1 SET 1: The Basic DNS:

1.1 :

The transport layer protocol used for sending the DNS queries is **UDP**.
Benefits of UDP: There is no connection establishment in UDP, so there is no need to maintain connection state. Hence, it is a simple protocol.
Also, data is not retransmitted if there is any loss of data, which can be used in time sensitive applications like real-time audio or video.
Drawbacks of UDP: Data loss can occur as it does not provide reliability. Also, no timing and minimum throghput guarantees are provided.

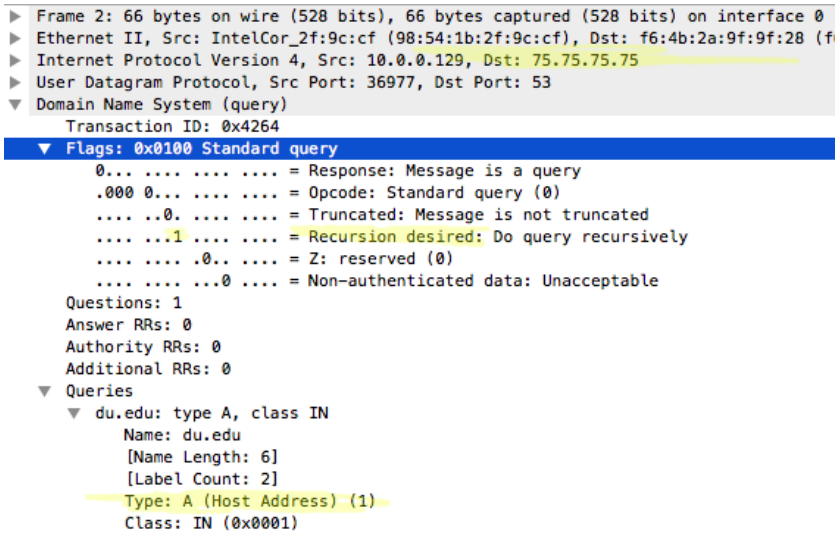
1.2 :



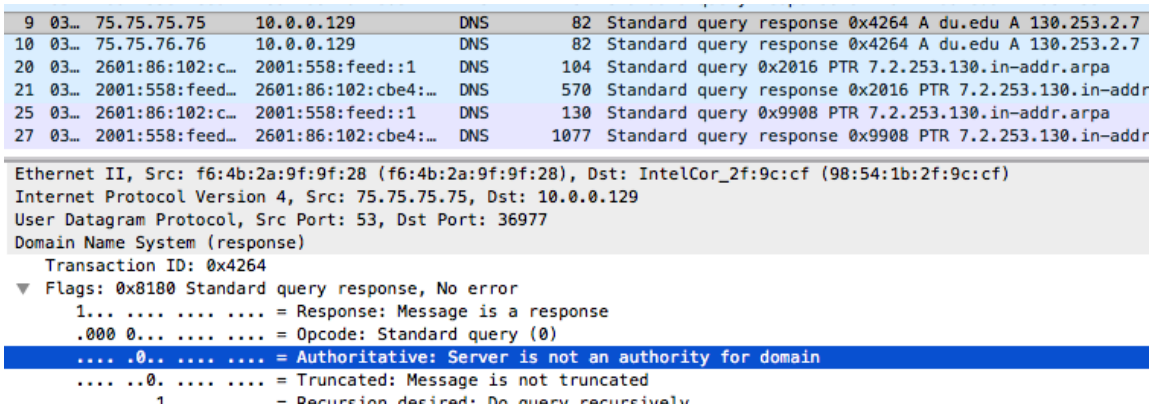
The port numbers used for sending the packet is 36977 and receiving the packet is 53.

1.3 :

- The destination of packet 2 is 75.75.75.75.
- It is a DNS query of type **A** as shown. In this, we give the hostname in the query and receive the IPA in the response.



- The only flag set in the query is **recursion desired**.
- To know the type of DNS server, we check the response to this query.



In the response, the flag **authoritative** is not set. Thus, it must be a local server having the IPA of the hostname cached.

1.4 :

No.	Time	Source	Destination	Protocol	Length	Info
2	03…	10.0.0.129	75.75.75.75	DNS	66	Standard query 0x4264 A du.edu
3	03…	10.0.0.129	75.75.76.76	DNS	66	Standard query 0x4264 A du.edu
4	03…	2601:86:102:c…	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu
5	03…	2601:86:102:c…	2001:558:feed::2	DNS	86	Standard query 0x4264 A du.edu
6	03…	2001:558:feed…	2601:86:102:cbe4:…	DNS	102	Standard query response 0x4264 A du.edu A 1…
7	03…	2001:558:feed…	2601:86:102:cbe4:…	DNS	102	Standard query response 0x4264 A du.edu A 1…
9	03…	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 1…
10	03…	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 1…

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

1.5 :

	Time	Source	Destination	Proto	Lengt	Info
2	03:40:10.1…	10.0.0.129	75.75.75.75	DNS	66	Standard query 0x4264 A du.edu
3	03:40:10.1…	10.0.0.129	75.75.76.76	DNS	66	Standard query 0x4264 A du.edu
4	03:40:10.1…	2601:86:102:cbe…	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu
5	03:40:10.1…	2601:86:102:cbe…	2001:558:feed::2	DNS	86	Standard query 0x4264 A du.edu
6	03:40:10.1…	2001:558:feed::1	2601:86:102:cbe4…	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
7	03:40:10.1…	2001:558:feed::2	2601:86:102:cbe4…	DNS	102	Standard query response 0x4264 A du.edu A 130.253.2.7
9	03:40:14.6…	75.75.75.75	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
10	03:40:14.6…	75.75.76.76	10.0.0.129	DNS	82	Standard query response 0x4264 A du.edu A 130.253.2.7
20	03:40:16.4…	2601:86:102:cbe…	2001:558:feed::1	DNS	104	Standard query 0x2016 PTR 7.2.253.130.in-addr.arpa
21	03:40:16.5…	2001:558:feed::1	2601:86:102:cbe4…	DNS	570	Standard query response 0x2016 PTR 7.2.253.130.in-addr.arpa P
25	03:40:16.5…	2601:86:102:cbe…	2001:558:feed::1	DNS	130	Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
27	03:40:16.6…	2001:558:feed::1	2601:86:102:cbe4…	DNS	1077	Standard query response 0x9908 PTR 7.2.253.130.in-addr.arpa P

Packet #9 contains the response of the query sent in packet #2 as highlighted. The flags set are response, recursion desired and recursion available.

```
▼ 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 au
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
```

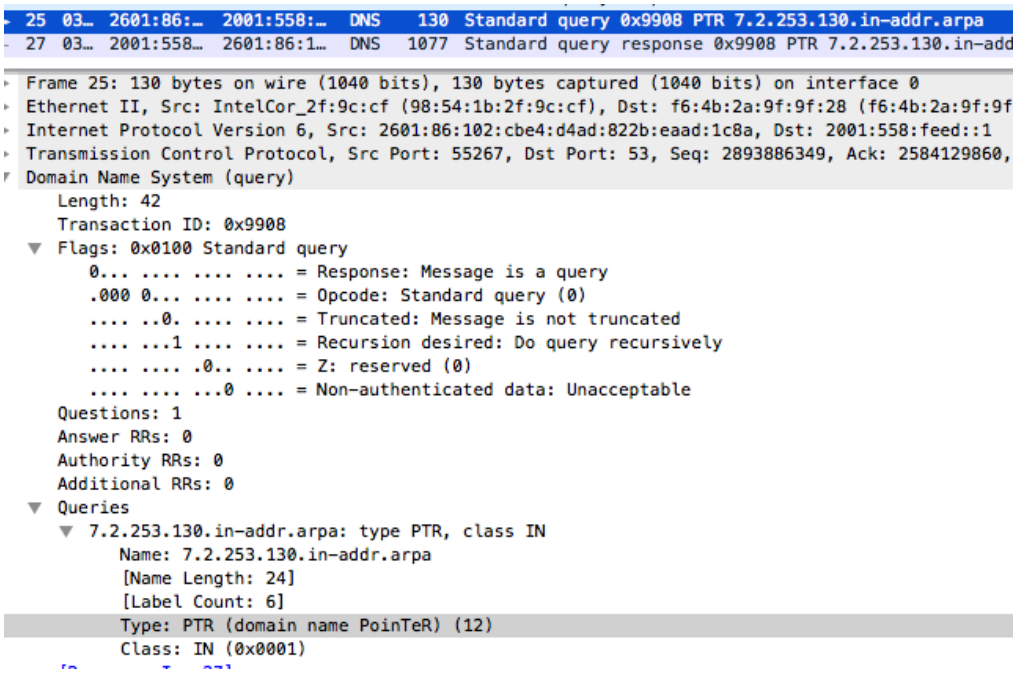
1.6 :

```
Questions: 1
Answer RRs: 1
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)
▼ Answers
  ▼ du.edu: type A, class IN, addr 130.253.2.7
      Name: du.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 600
      Data length: 4
      Address: 130.253.2.7
```

We get one answer from the server. The response is not from an authoritative server as this flag is not set.

```
    9  03:40:14.6…  75.75.75.75       10.0.0.129          DNS    82  Standard query response 0x4264 A du.edu A 130.253.2.7
   10  03:40:14.6…  75.75.76.76       10.0.0.129          DNS    82  Standard query response 0x4264 A du.edu A 130.253.2.7
   20  03:40:16.4…  2601:86:102:cbe…  2001:558:feed::1    DNS   104  Standard query 0x2016 PTR 7.2.253.130.in-addr.arpa
   21  03:40:16.5…  2001:558:feed::1  2601:86:102:cbe4…   DNS   570  Standard query response 0x2016 PTR 7.2.253.130.in-addr
   25  03:40:16.5…  2601:86:102:cbe…  2001:558:feed::1    DNS   130  Standard query 0x9908 PTR 7.2.253.130.in-addr.arpa
   27  03:40:16.6…  2001:558:feed::1  2601:86:102:cbe4…   DNS  1077  Standard query response 0x9908 PTR 7.2.253.130.in-addr
▶ 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 server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
```

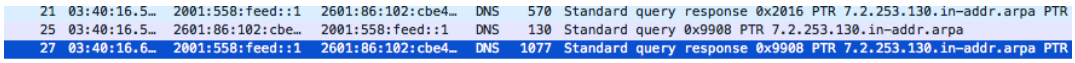
1.7 :



The query in packet #25 is of the type PTR and it is used for reverse DNS lookup, i.e. given the IPA, the hostname is provided in the response.

1.8 :

The packet #27 contains the response of the packet #25.



```
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
      Name: 7.2.253.130.in-addr.arpa
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
      Time to live: 86400
      Data length: 17
      Domain Name: notagora.du.edu
  ▼ 7.2.253.130.in-addr.arpa: type PTR, class IN, mme.du.edu
      Name: 7.2.253.130.in-addr.arpa
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
      Time to live: 86400
      Data length: 6
      Domain Name: mme.du.edu
  ▼ 7.2.253.130.in-addr.arpa: type PTR, class IN, m.du.edu
      Name: 7.2.253.130.in-addr.arpa
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
```

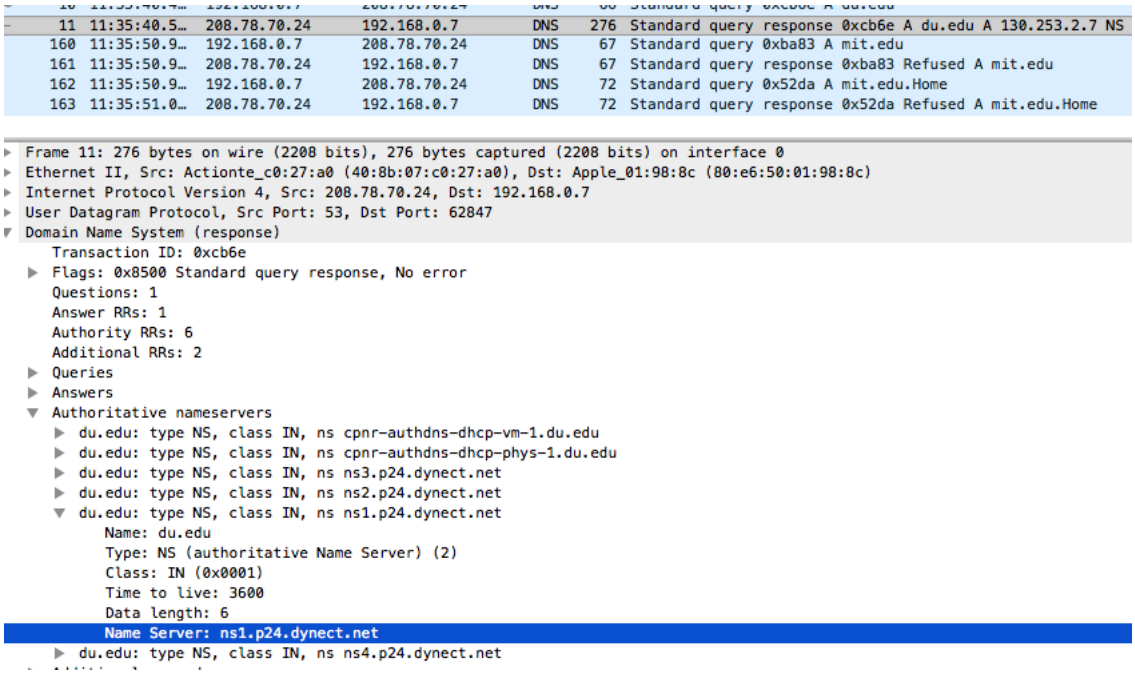
The response contains 42 resource records. All of them contain the hostname to which the queried IPA maps to.

2 SET 2: Using the DNS_2.pcapng:

2.1 :

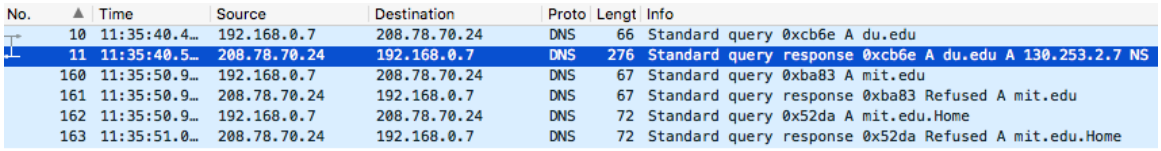
No.	Time	Source	Destination	Proto	Lengt	Info
10	11:35:40.4…	192.168.0.7	208.78.70.24	DNS	66	Standard query 0xcb6e A du.edu
11	11:35:40.5…	208.78.70.24	192.168.0.7	DNS	276	Standard query response 0xcb6e A du.edu A 130.253.2.7 N
160	11:35:50.9…	192.168.0.7	208.78.70.24	DNS	67	Standard query 0xba83 A mit.edu
161	11:35:50.9…	208.78.70.24	192.168.0.7	DNS	67	Standard query response 0xba83 Refused A mit.edu
162	11:35:50.9…	192.168.0.7	208.78.70.24	DNS	72	Standard query 0x52da A mit.edu.Home
163	11:35:51.0…	208.78.70.24	192.168.0.7	DNS	72	Standard query response 0x52da Refused A mit.edu.Home

The destination IPA of the server is 208.78.70.24.

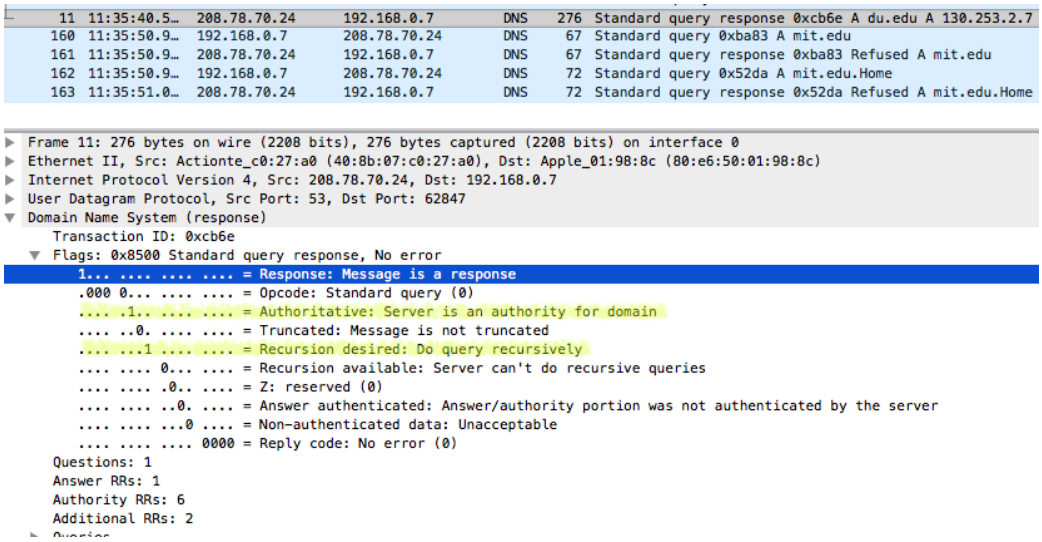


The request is being sent to the authoritative name server **ns1.p24.dynect.net** as seen in the response in the packet #11.

2.2 :

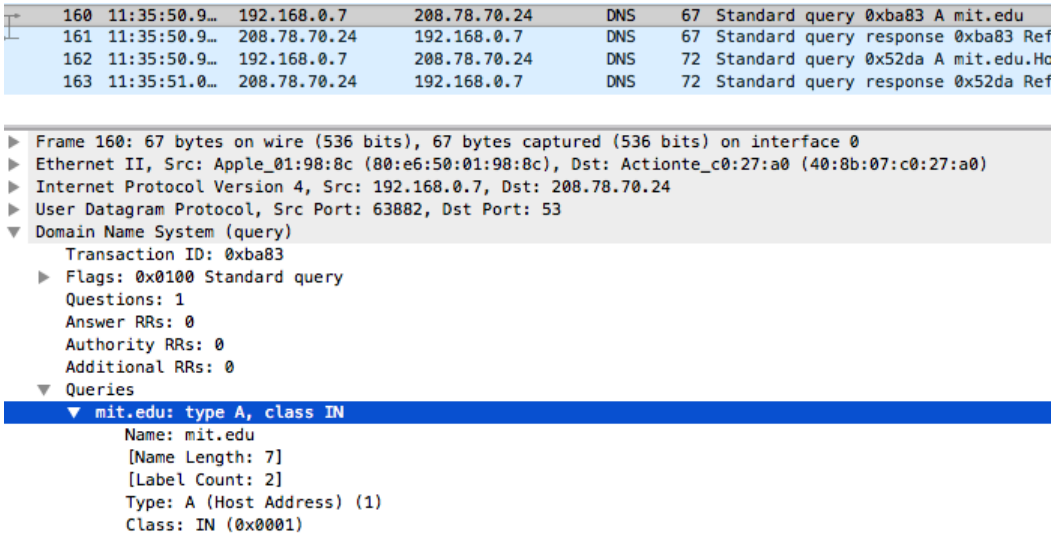


Packet #11 contains the reply of the query sent in the packet #10. Yes, the DNS server replied as we are getting a standard query response.



The response, recursion desired and authoritative flags are set in the response.

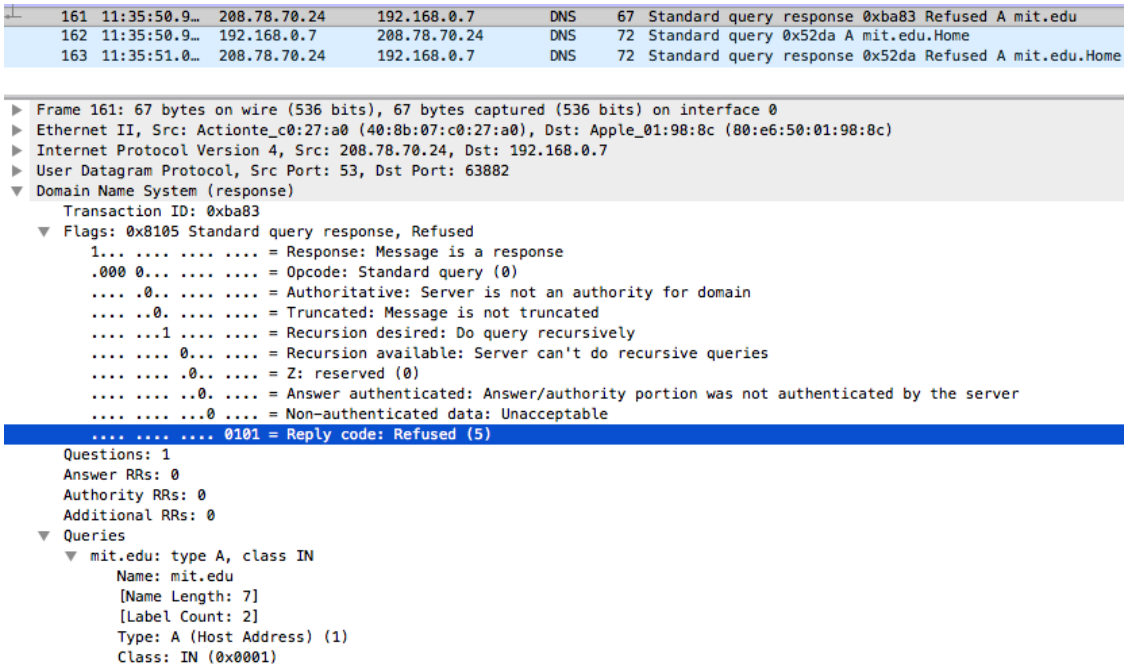
2.3 :



The DNS request in #160 is sent to **ns1.p24.dynect.net**. The DNS request asks the IPA of the hostname **mit.edu** as the type of query is **A**.

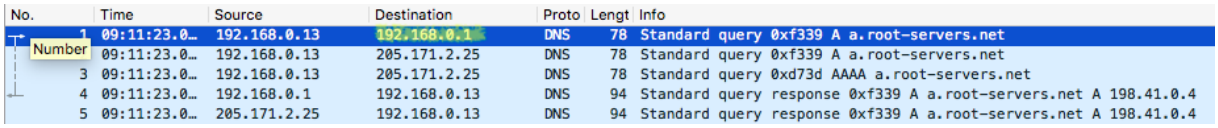
2.4 :

The response from the DNS server for the query sent in packet #160, as shown in the packet #161, contains no answer RRs. The reply code is refused. So, the server did not resolve the DNS request.



3 SET 3: Using the DNS_3.pcapng:

3.1 :



The DNS query in packet #1 is sent to the IPA 192.168.0.1. It is a local DNS server.

3.2 :

No.	Time	Source	Destination	Proto	Lengt	Info
1	09:11:23.0…	192.168.0.13	192.168.0.1	DNS	78	Standard query 0xf339 A a.root-servers.net
2	09:11:23.0…	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xf339 A a.root-servers.net
3	09:11:23.0…	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xd73d AAAA a.root-servers.net
4	09:11:23.0…	192.168.0.1	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4
5	09:11:23.0…	205.171.2.25	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4

The DNS query in packet #2 is sent to the IPA 205.171.2.25. It is a local DNS server.

3.3 :

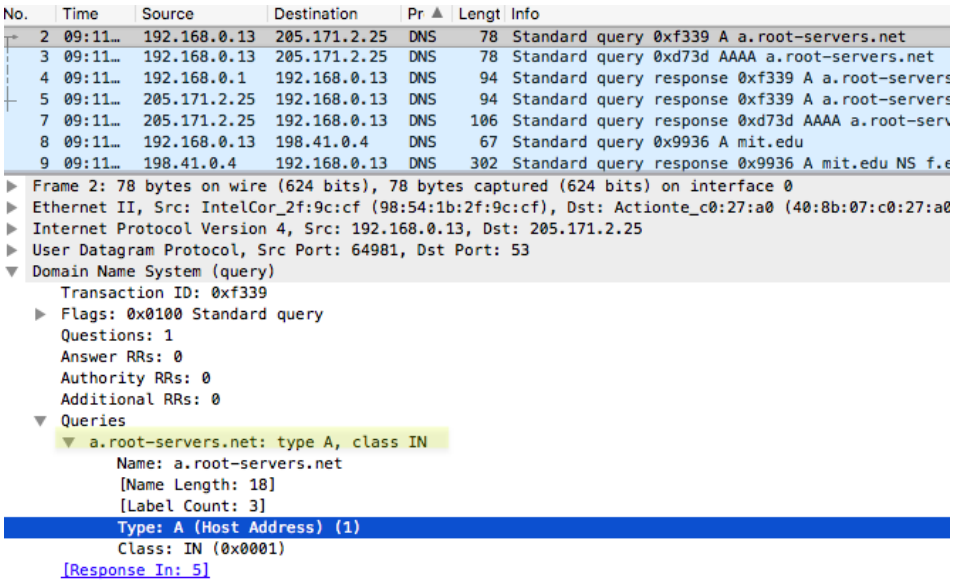
No.	Time	Source	Destination	Proto	Lengt	Info
1	09:11:23.0…	192.168.0.13	192.168.0.1	DNS	78	Standard query 0xf339 A a.root-servers.net
2	09:11:23.0…	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xf339 A a.root-servers.net
3	09:11:23.0…	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xd73d AAAA a.root-servers.net
4	09:11:23.0…	192.168.0.1	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4
5	09:11:23.0…	205.171.2.25	192.168.0.13	DNS	94	Standard query response 0xf339 A a.root-servers.net A 198.41.0.4

Packet #5 contains the response of the packet sent in the query #2.

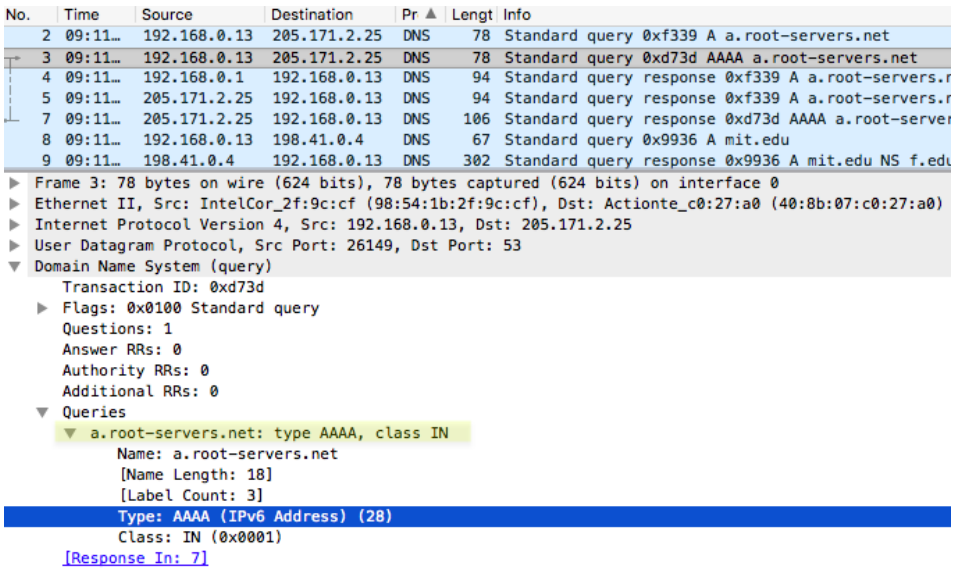
```
5 09:11:23.0…  205.171.2.25       192.168.0.13       DNS     94 Standard query response 0xf339 A a.root-servers.net A
▶ Frame 5: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
▶ Ethernet II, Src: Actionte_c0:27:a0 (40:8b:07:c0:27:a0), Dst: IntelCor_2f:9c:cf (98:54:1b:2f:9c:cf)
▶ 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
        Name: a.root-servers.net
        [Name Length: 18]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▼ 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]
```

In the response, we get the IPA of the hostname **a.root-servers.net** which was what was queried as the type of query is **A**.

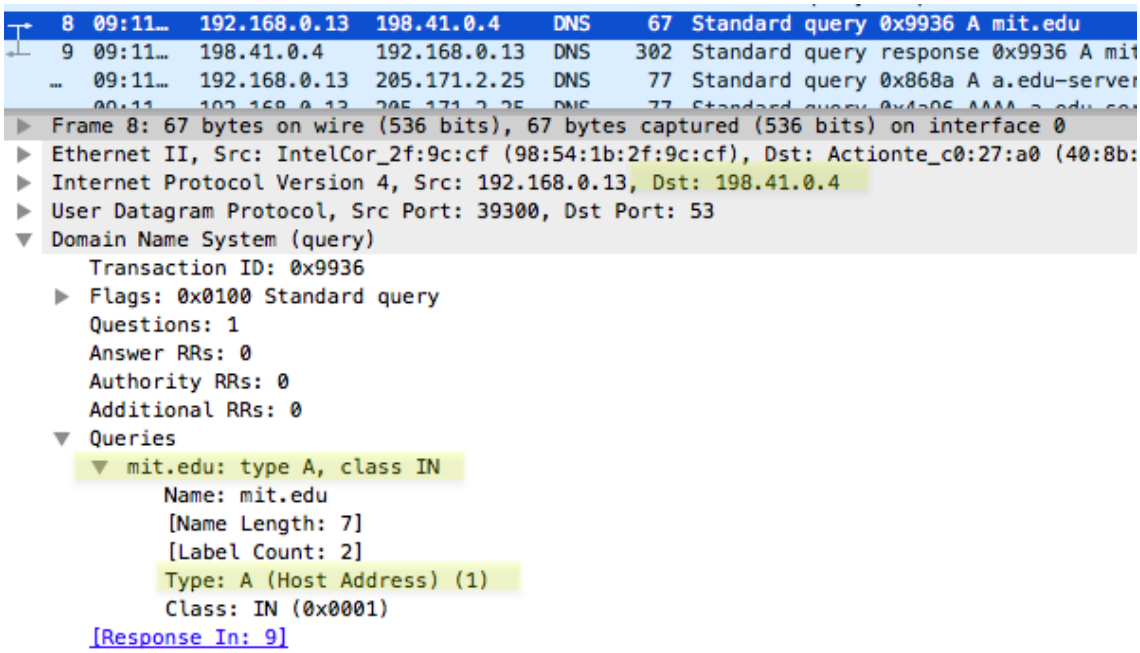
3.4 :



The difference between query in packet #2 and packet #3 is the type of the query. In #2, query has type **A** which resolves the IPA in IPv4 whereas in #3, query has type **AAAA** which resolves the IPA in IPv6.

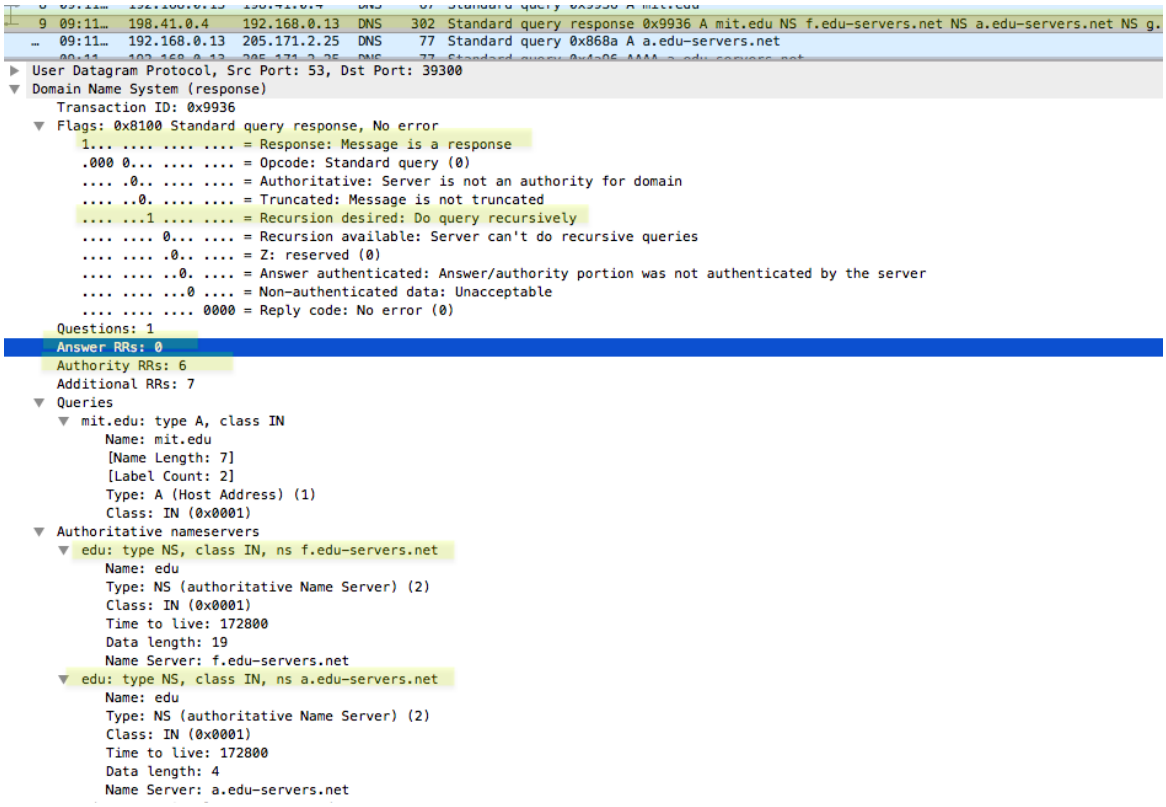


3.5 :



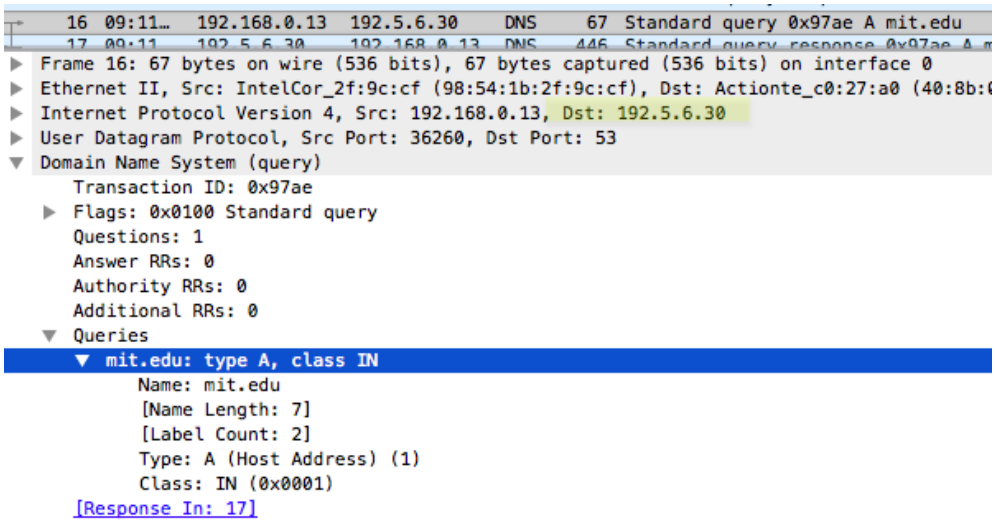
The query in packet #8 is used to get the IPA of the hostname **mit.edu** as the type of query is **A**. Since the IPA to which packet is sent is 198.41.0.4 which was earlier resolved for the hostname **a.root-servers.net**, also the response in packet #9 contains the list of .edu TLD servers, thus it is a **root server**.

3.6 :



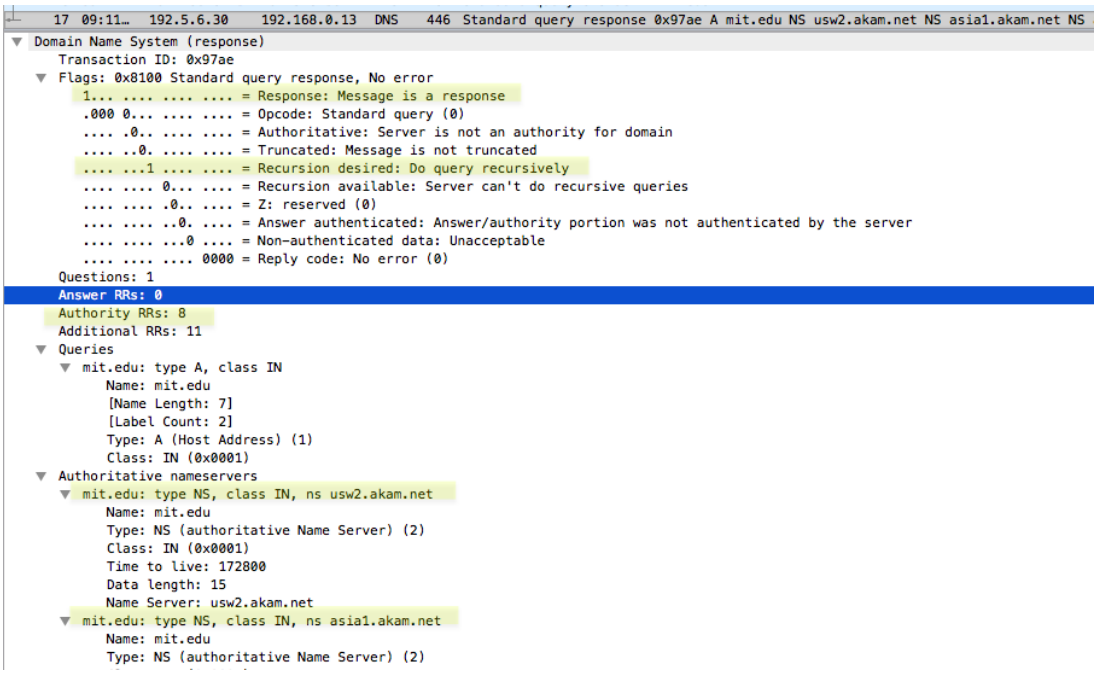
The packet #9 contains the response of the query sent in packet #8. The flags set in this are response and recursion desired. No, it does not have the answer the user wants as the no. of answer RRs = 0. It provides the list of .edu TLD servers.

3.7 :



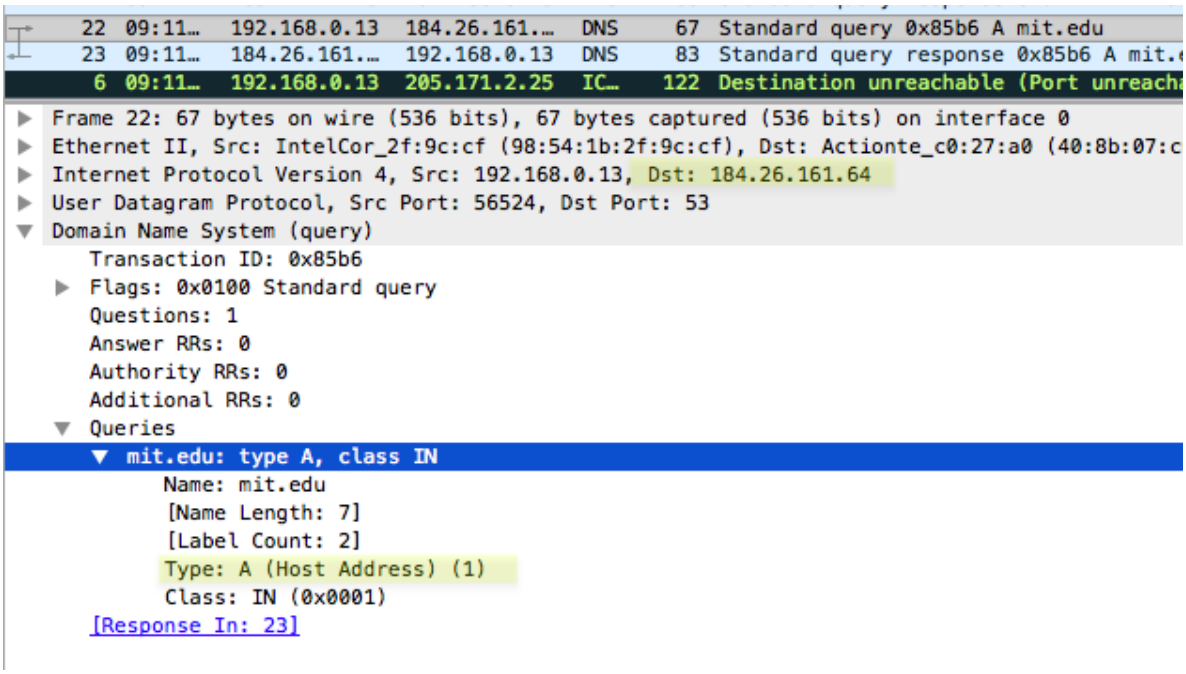
TLD server is being queried in the packet #16. It is thus not a local DNS server.

3.8 :



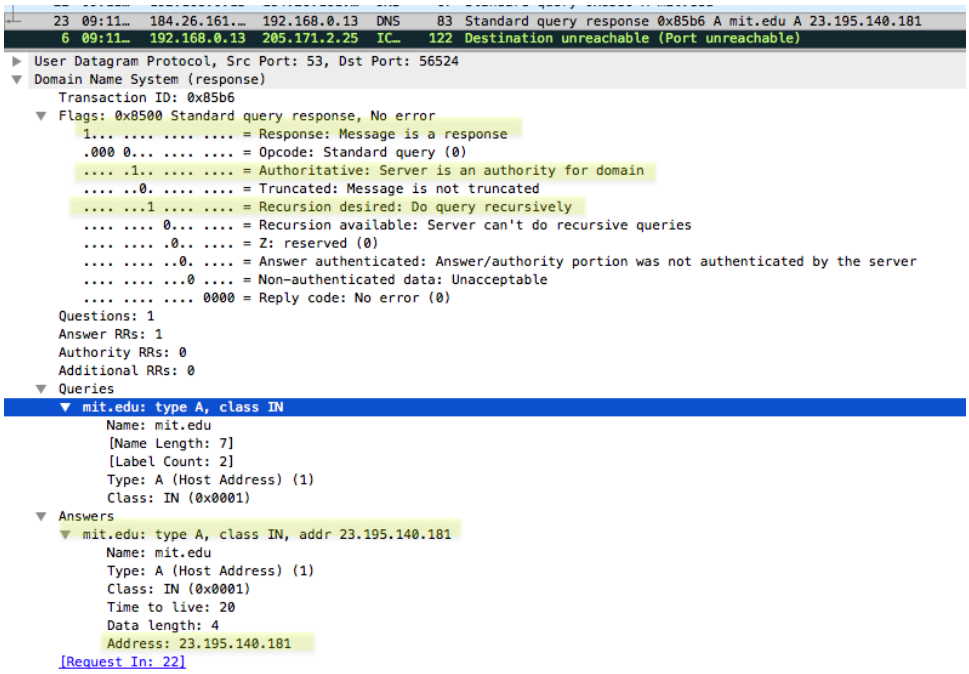
Packet #17 contains the response of the query sent in the packet #16. The flags set in this are response and recursion desired. No, it does not have the answer the user wants. It provides the information about the authoritative name servers as shown.

3.9 :



The query in packet #22 is used to get the IPA of the hostname **mit.edu** as the type of query is **A**. An authoritative name server is being queried.

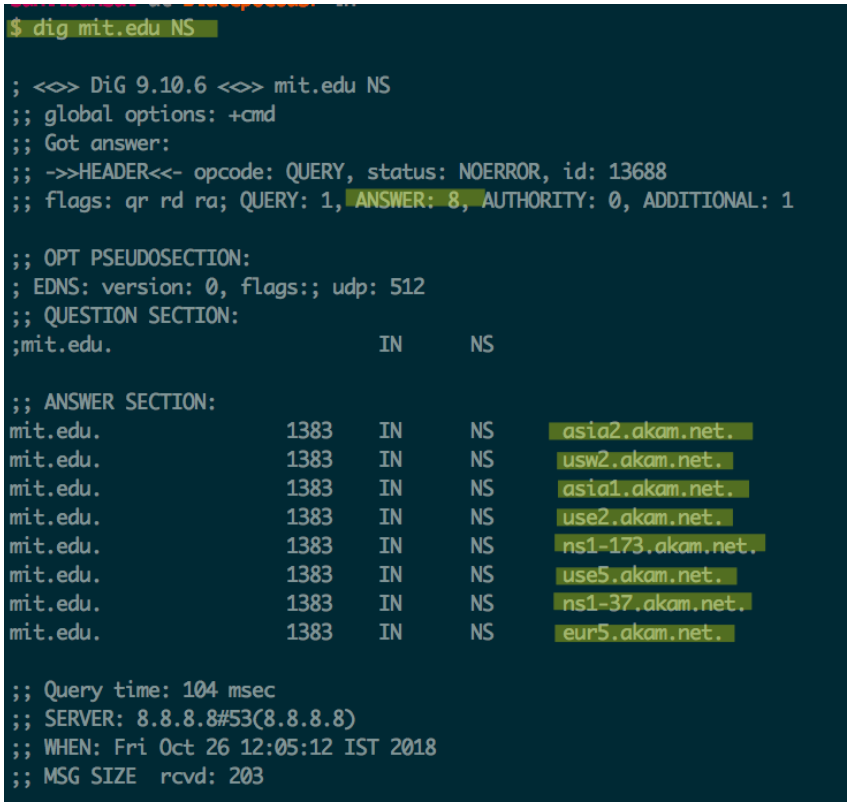
3.10 :



The packet #23 contains the response of the packet #22. The flags set in this are response, recursion desired and authoritative. Yes, it has the answer the user wants. It provides the IPA of the hostname **mit.edu**.

4 Using dig command:

4.1 :



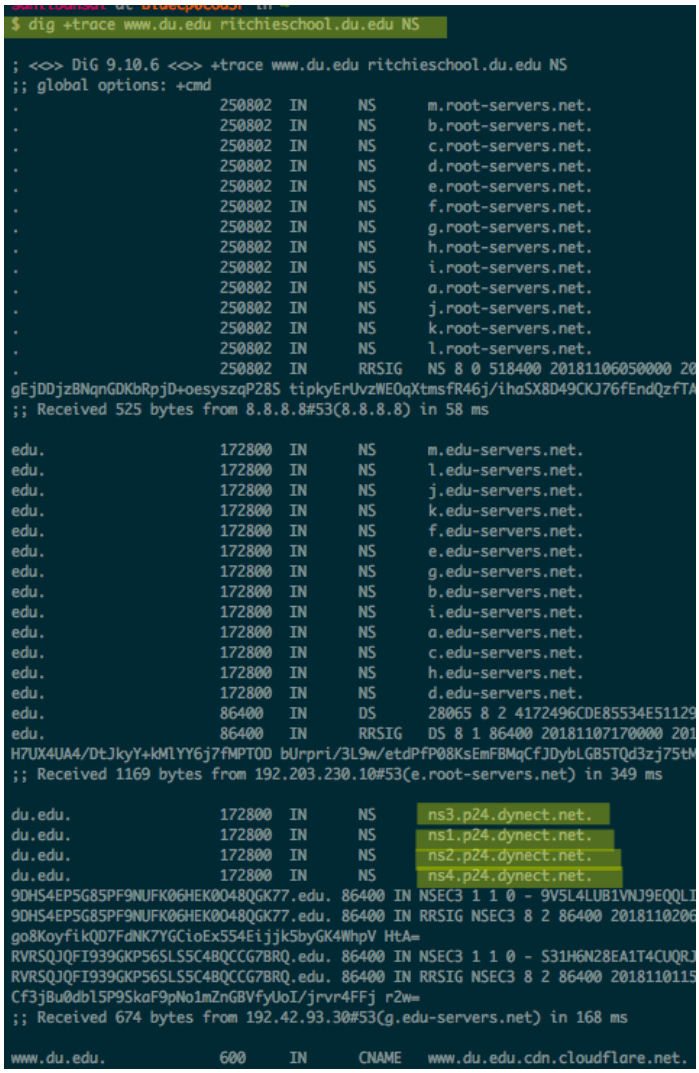
The dig command used to determine the authoritative DNS servers for *mit.edu* is: **dig mit.edu NS** as highlighted.

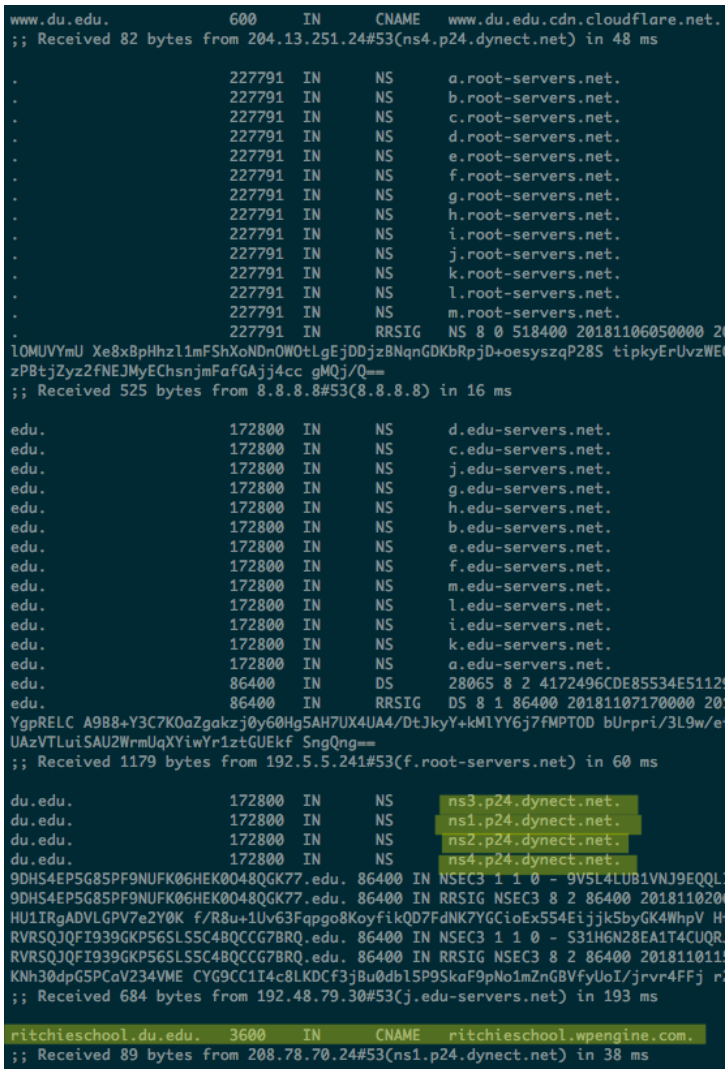
4.2 :

```
$ dig www.du.edu ritchieschool.du.edu NS

; <<>> DiG 9.10.6 <<>> www.du.edu ritchieschool.du.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61279
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.du.edu.                    IN      A

;; ANSWER SECTION:
www.du.edu.             297     IN      CNAME   www.du.edu.cdn.cloudflare.net.
www.du.edu.cdn.cloudflare.net. 137 IN   A       104.25.203.95
www.du.edu.cdn.cloudflare.net. 137 IN   A       104.25.204.95

;; Query time: 58 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 26 12:08:53 IST 2018
;; MSG SIZE  rcvd: 114

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34366
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ritchieschool.du.edu.          IN      NS

;; ANSWER SECTION:
ritchieschool.du.edu.   3599    IN      CNAME   ritchieschool.wpengine.com.

;; AUTHORITY SECTION:
wpengine.com.           1799    IN      SOA     jim.ns.cloudflare.com. dns.cloudflare.com.

;; Query time: 382 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 26 12:08:54 IST 2018
;; MSG SIZE  rcvd: 147
```

The command used to determine the authoritative DNS servers for *www.du.edu* and *ritchieschool.du.edu* in a single dig command is: **dig www.du.edu ritchieschool.du.edu NS**.

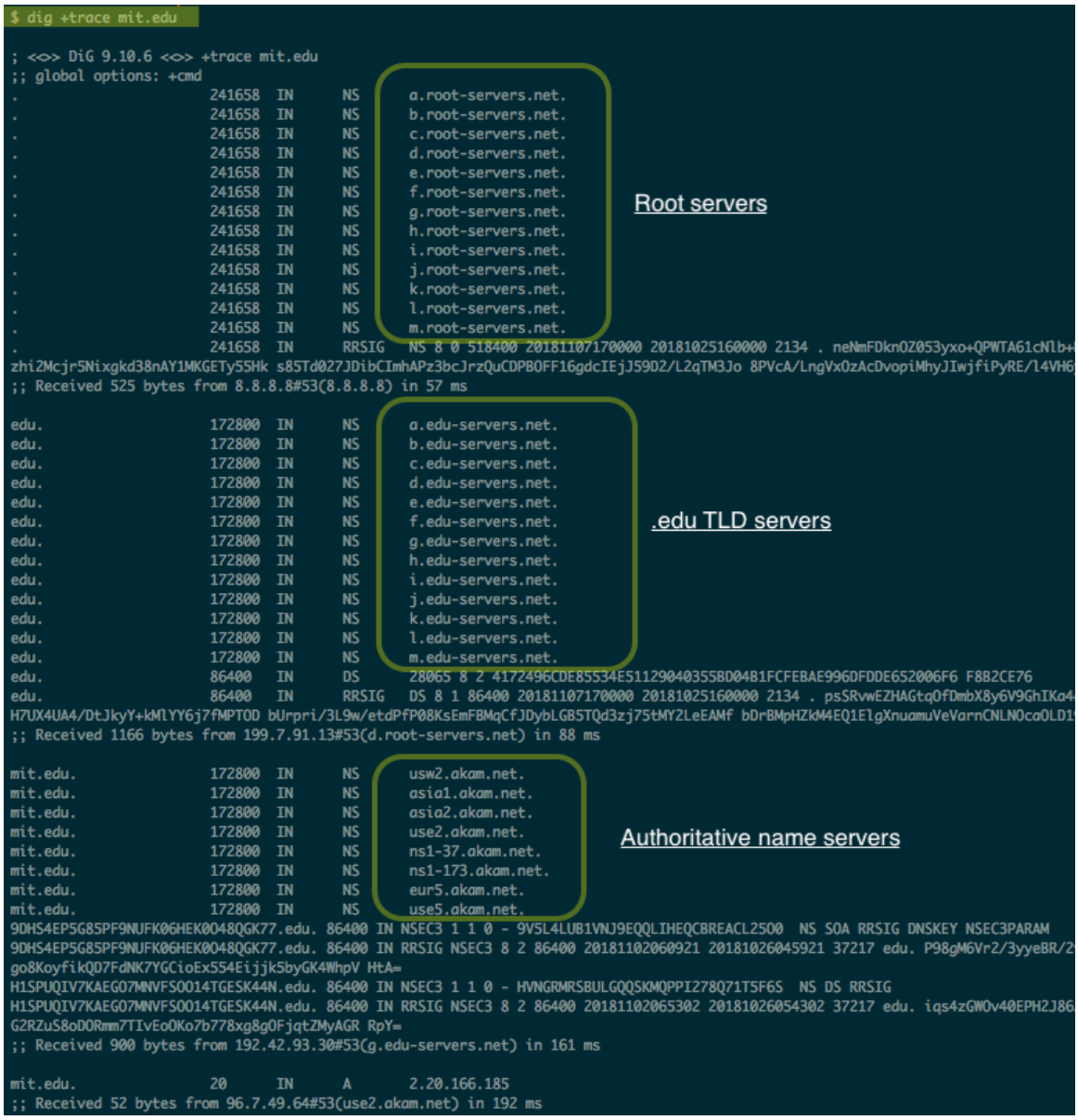
Since it does not provide any answer resource record of type NS, we run the command **dig +trace www.du.edu ritchieschool.du.edu** to see the complete execution of the DNS request.


$ dig +trace www.du.edu ritchieschool.du.edu NS
; <<>> DiG 9.10.6 <<>> +trace www.du.edu ritchieschool.du.edu NS
;; global options: +cmd
. 250802 IN NS m.root-servers.net.
. 250802 IN NS b.root-servers.net.
. 250802 IN NS c.root-servers.net.
. 250802 IN NS d.root-servers.net.
. 250802 IN NS e.root-servers.net.
. 250802 IN NS f.root-servers.net.
. 250802 IN NS g.root-servers.net.
. 250802 IN NS h.root-servers.net.
. 250802 IN NS i.root-servers.net.
. 250802 IN NS a.root-servers.net.
. 250802 IN NS j.root-servers.net.
. 250802 IN NS k.root-servers.net.
. 250802 IN NS l.root-servers.net.
. 250802 IN RRSIG NS 8 0 518400 20181106050000 20
gEjDDjzBNqnGDKbRpjD+oesyszqP28S tipkyErUvzWEOqXtmsfR46j/ihaSX8D49CKJ76fEndQzfTA
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 58 ms
edu. 172800 IN NS m.edu-servers.net.
edu. 172800 IN NS l.edu-servers.net.
edu. 172800 IN NS j.edu-servers.net.
edu. 172800 IN NS k.edu-servers.net.
edu. 172800 IN NS f.edu-servers.net.
edu. 172800 IN NS e.edu-servers.net.
edu. 172800 IN NS g.edu-servers.net.
edu. 172800 IN NS b.edu-servers.net.
edu. 172800 IN NS i.edu-servers.net.
edu. 172800 IN NS a.edu-servers.net.
edu. 172800 IN NS c.edu-servers.net.
edu. 172800 IN NS h.edu-servers.net.
edu. 172800 IN NS d.edu-servers.net.
edu. 86400 IN DS 28065 8 2 4172496CDE85534E51129
edu. 86400 IN RRSIG DS 8 1 86400 20181107170000 201
H7UX4UA4/DtJkyY+kMlYY6j7fMPTOD bUrpri/3L9w/etdPfP08KsEmFBMqCfJDybLGB5TQd3zj75tM
;; Received 1169 bytes from 192.203.230.10#53(e.root-servers.net) in 349 ms
du.edu. 172800 IN NS ns3.p24.dynect.net.
du.edu. 172800 IN NS ns1.p24.dynect.net.
du.edu. 172800 IN NS ns2.p24.dynect.net.
du.edu. 172800 IN NS ns4.p24.dynect.net.
9DHS4EP5G85PF9NUFK06HEK0O48QGK77.edu. 86400 IN NSEC3 1 1 0 - 9V5L4LUB1VNJ9EQQLI
9DHS4EP5G85PF9NUFK06HEK0O48QGK77.edu. 86400 IN RRSIG NSEC3 8 2 86400 201811020G
go8KoyfikQD7FdNK7YGCioEx554Eijjk5byGK4WhpV HtA=
RVRSQJQFI939GKP56SLS5C4BQCCG7BRQ.edu. 86400 IN NSEC3 1 1 0 - S31H6N28EA1T4CUQRJ
RVRSQJQFI939GKP56SLS5C4BQCCG7BRQ.edu. 86400 IN RRSIG NSEC3 8 2 86400 2018110115
Cf3jBu0dbl5P9SkaF9pNo1mZnGBVfyUoI/jrvr4FFj r2w=
;; Received 674 bytes from 192.42.93.30#53(g.edu-servers.net) in 168 ms
www.du.edu. 600 IN CNAME www.du.edu.cdn.cloudflare.net.



As we can see from this, the DNS servers are the same for both.

4.3 :



We can infer from this output that the DNS request first goes to the root servers, then it goes to the .edu TLD servers and then finally the authoritative name servers for mit.edu.