

# Assignment 6

## Computer Networks

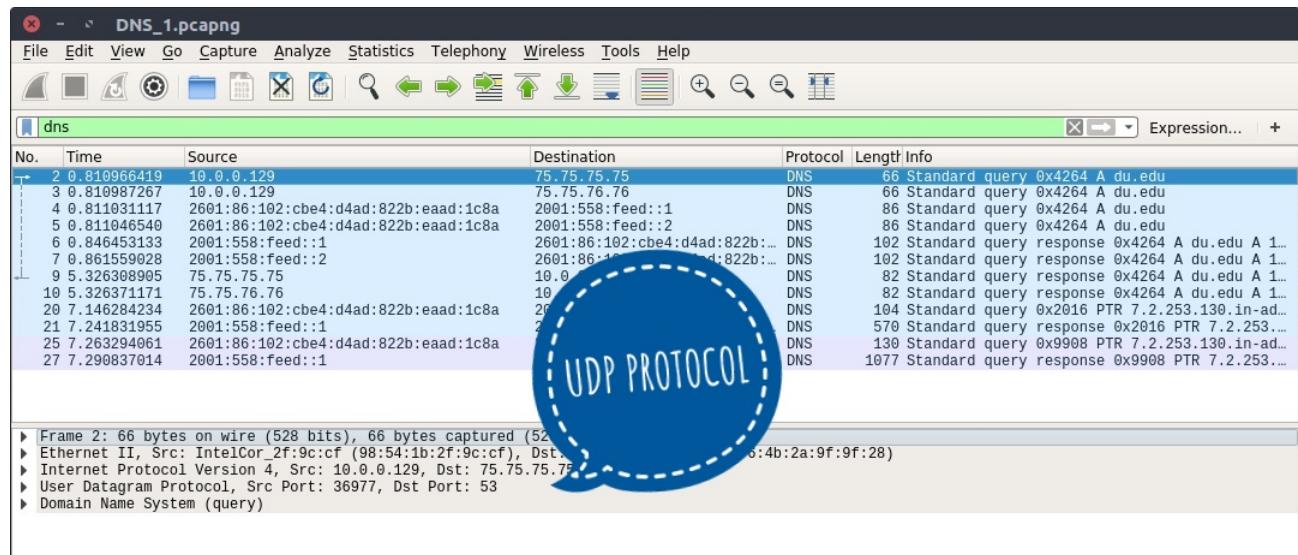
Vikas Gola : 2016UCS0023

October 26, 2018

# SET 1: The Basic DNS

**Question 1** Determine which transport layer protocol was used for sending the DNS queries? What are the benefits and drawbacks of using that protocol ?

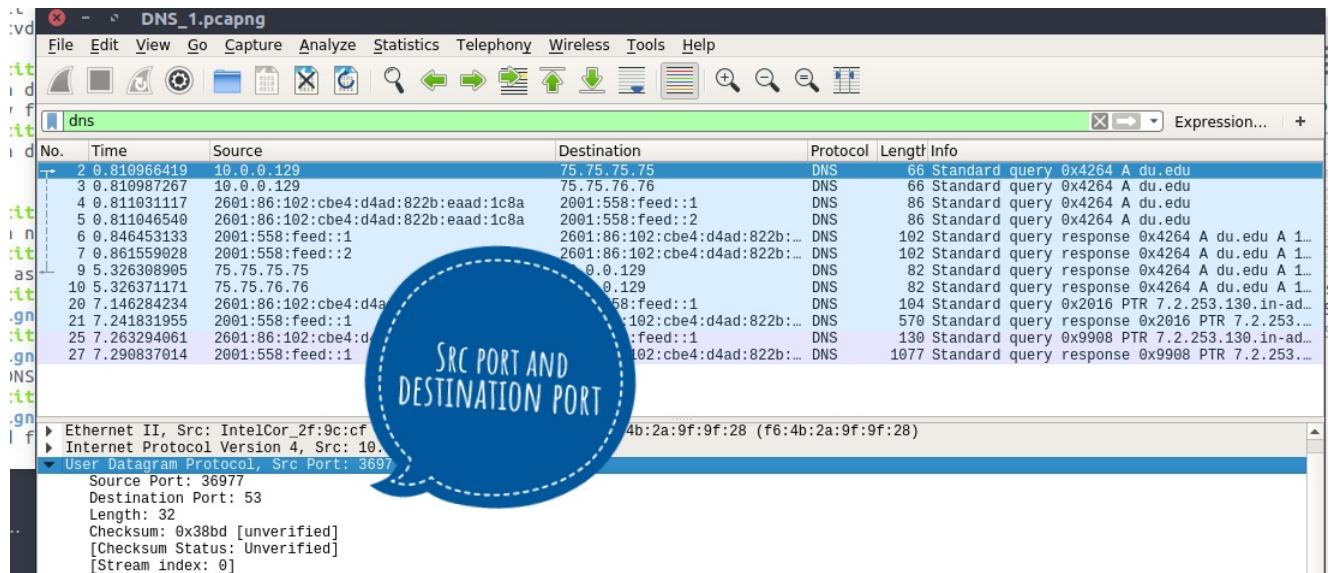
**Answer** UDP (User Datagram protocol) was used for sending the DNS queries. The benefits of using UDP is that it is fast, efficient and lightweight. The one of the big drawbacks of UDP is that it does not support error recovery. The another drawback of UDP is that it does not give guarantee that the messages or packets sent would reach at all.



**Question 2** What port numbers are used for sending and receiving the packet in packet #2 ?

**Answer** Source port: 36977

Destination port: 53



**Question 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 ?

**Answer** Destination address: 75.75.75.75

It is a Recursive Query( 0x0100 Standard Query ). The DNS server type is authoritative server.

Flags in the query are:

0.... .... .... = Response: Message is a query

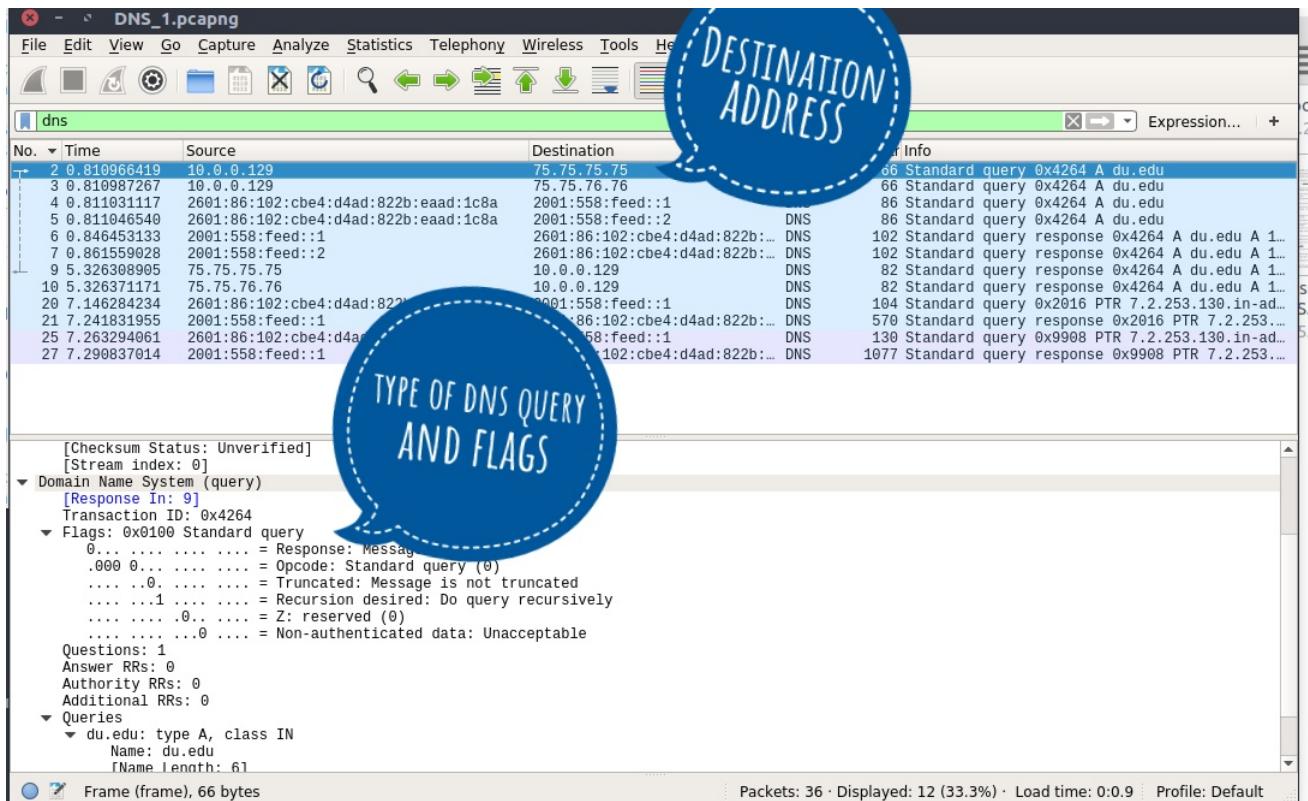
.000 0... .... .... = Opcode: Standard query (0)

.... .0. .... .... = Truncated: Message is not truncated

.... ..1 .... .... = Recursion desired: Do query recursively

.... .... .0.. .... = Z: reserved (0)

.... .... ...0 .... = Non-authenticated data: Unacceptable



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

**Answer** 1 DNS server is queried to for resolving the domain name du.edu.

**Question 5** Which packet contains the response of the query sent in packet #2 ? Which flags are set in the response?

**Answer** 9th packet contains the response of query of packet #2.

Flags in the response are:

- 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)

The screenshot shows a Wireshark capture window titled "DNS\_1.pcapng". The "dns" protocol is selected in the left pane. A specific DNS response packet (row 9) is highlighted in blue. The "Flags" field of this packet is expanded, showing the bit definitions for response, opcode, authoritative, truncated, recursion desired, recursion available, Z reserved, answer authenticated, non-authenticated data, and reply code. The reply code is listed as "0000 = Reply code: No error (0)". The "Questions" section shows one question for "du.edu" type A, class IN. The "Answers" section shows one answer for "du.edu" with name length 6 and label count 21.

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:d4ad:822b:eaad:1c8a	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu
5	0.811046540	2601:86:102:cbe4:d4ad:822b:eaad:1c8a	2001:558:feed::2	DNS	86	Standard query 0x4264 A du.edu
6	0.846453133	2001:558:feed::1	2601:86:102:cbe4:d4ad:822b:eaad:1c8a	DNS	86	Standard query 0x4264 A du.edu A 1...
7	0.861559028	2001:558:feed::2	2601:86:102:cbe4:d4ad:822b:eaad:1c8a	DNS	86	Standard query 0x4264 A du.edu A 1...
9	5.326308905	75.75.75.75	10.0.0.129	DNS	66	Standard query 0x4264 A du.edu A 1...
10	5.326371171	75.75.76.76	10.0.0.129	DNS	66	Standard query 0x4264 A du.edu A 1...
20	7.146284234	2601:86:102:cbe4:d4ad:822b:eaad:1c8a	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu A 1...
21	7.241831955	2001:558:feed::1	2601:86:102:cbe4:d4ad:822b:eaad:1c8a	DNS	86	Standard query 0x4264 A du.edu A 1...
25	7.263294061	2601:86:102:cbe4:d4ad:822b:eaad:1c8a	2001:558:feed::1	DNS	86	Standard query 0x4264 A du.edu A 1...
27	7.299837014	2001:558:feed::1	2601:86:102:cbe4:d4ad:822b:eaad:1c8a	DNS	86	Standard query 0x4264 A du.edu A 1...

[Request In: 2]  
[Time: 4.515342486 seconds]  
Transaction ID: 0x4264

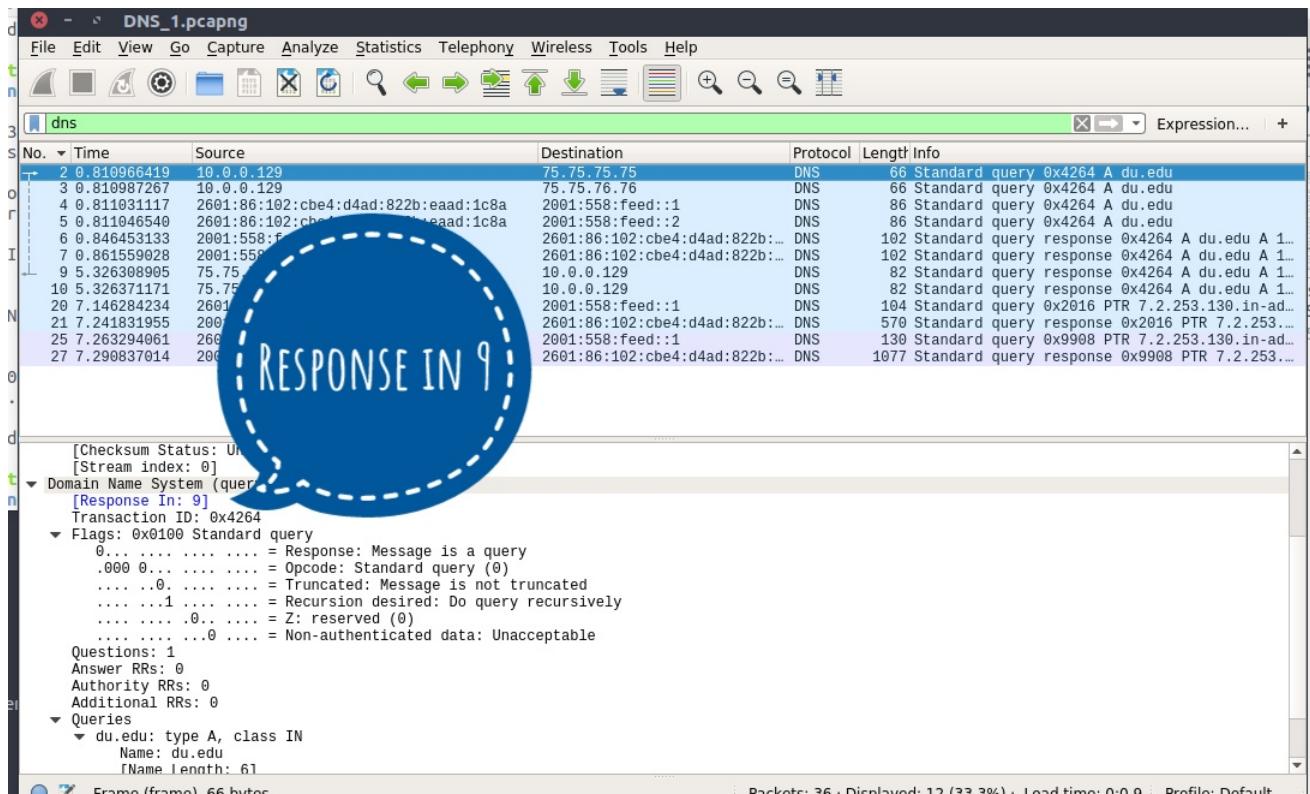
Flags: 0x8180 Standard query response, No error

- 1.... .... .... = Response: Message is a response
- .000 ... .... = 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

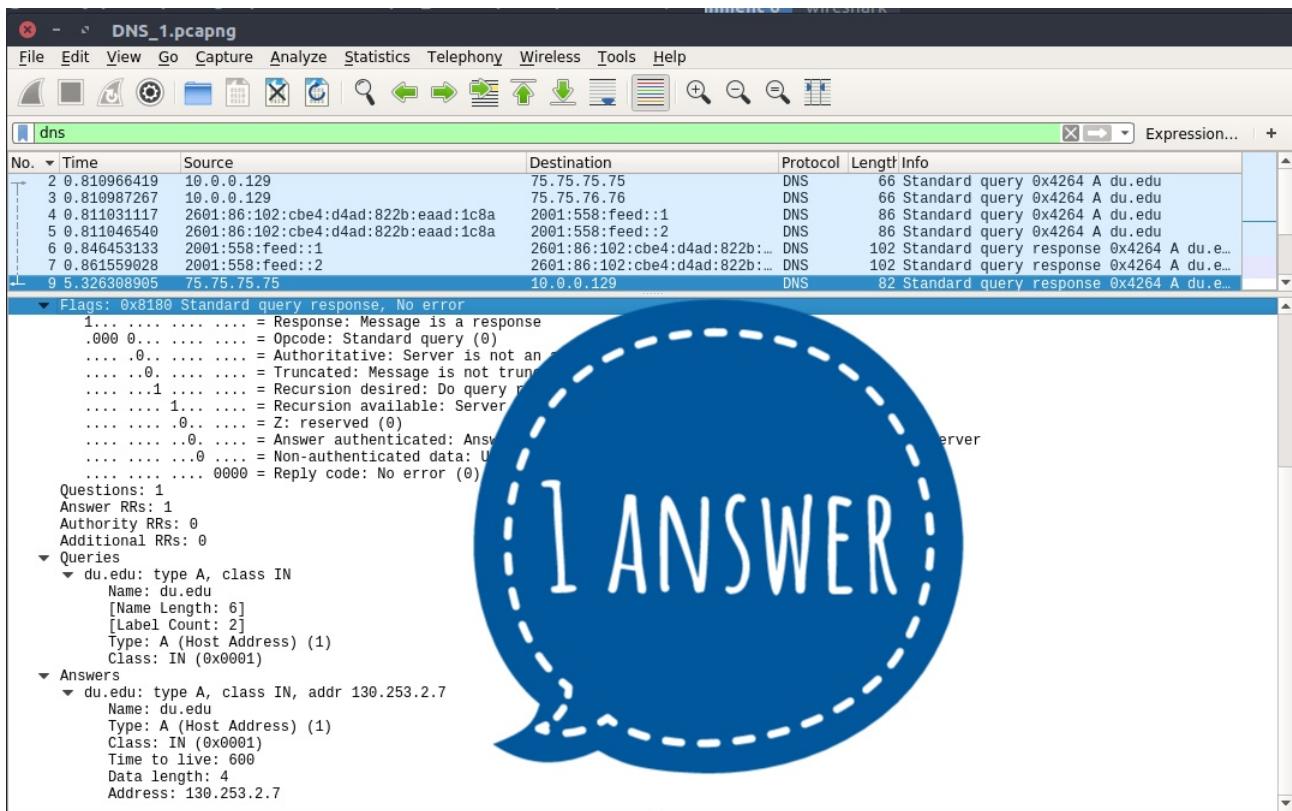
Queries

- du.edu: type A, class IN
  - Name: du.edu
  - [Name Length: 6]
  - Label Count: 21



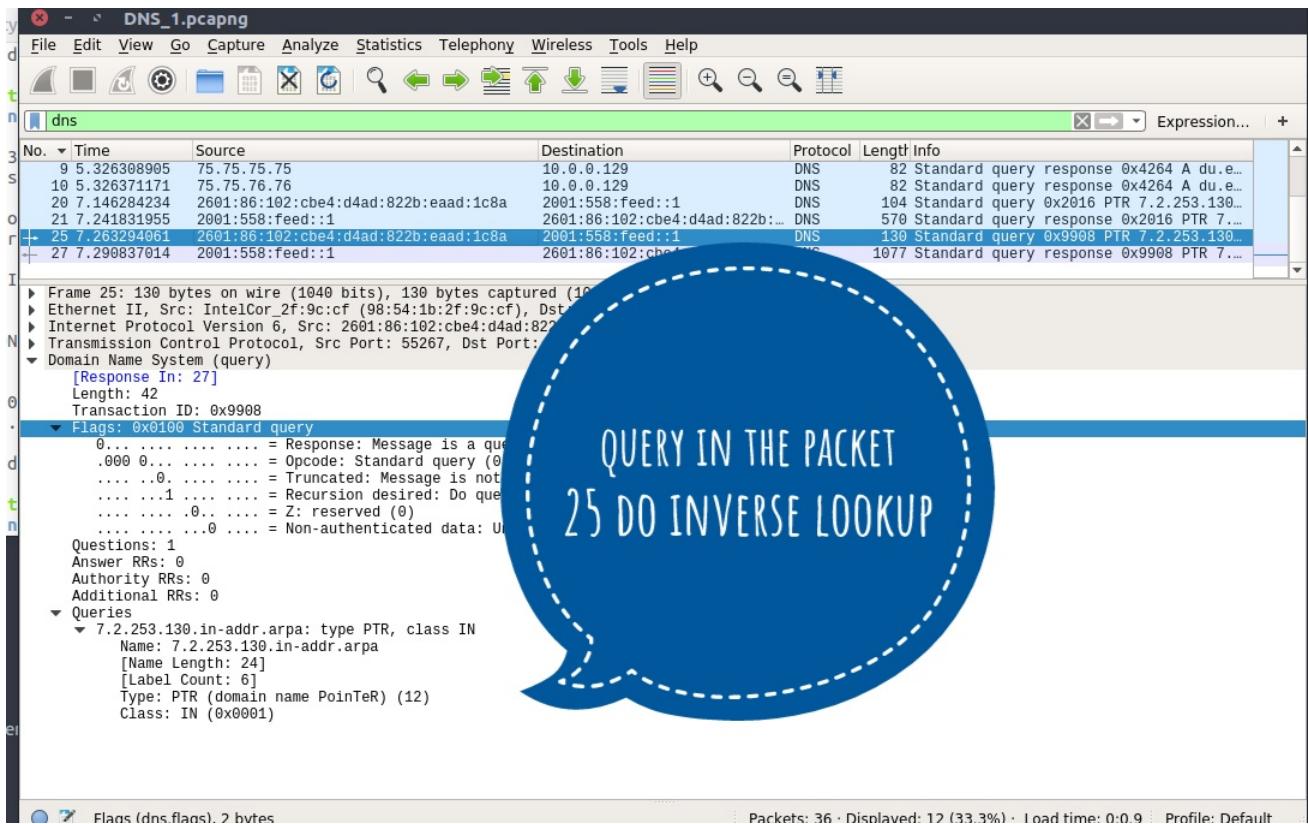
**Question 6** How many answers do you get in the response? Is the response from authoritative server ?

**Answer** 1 answer in the response. No, response is not from Authoritative Server.



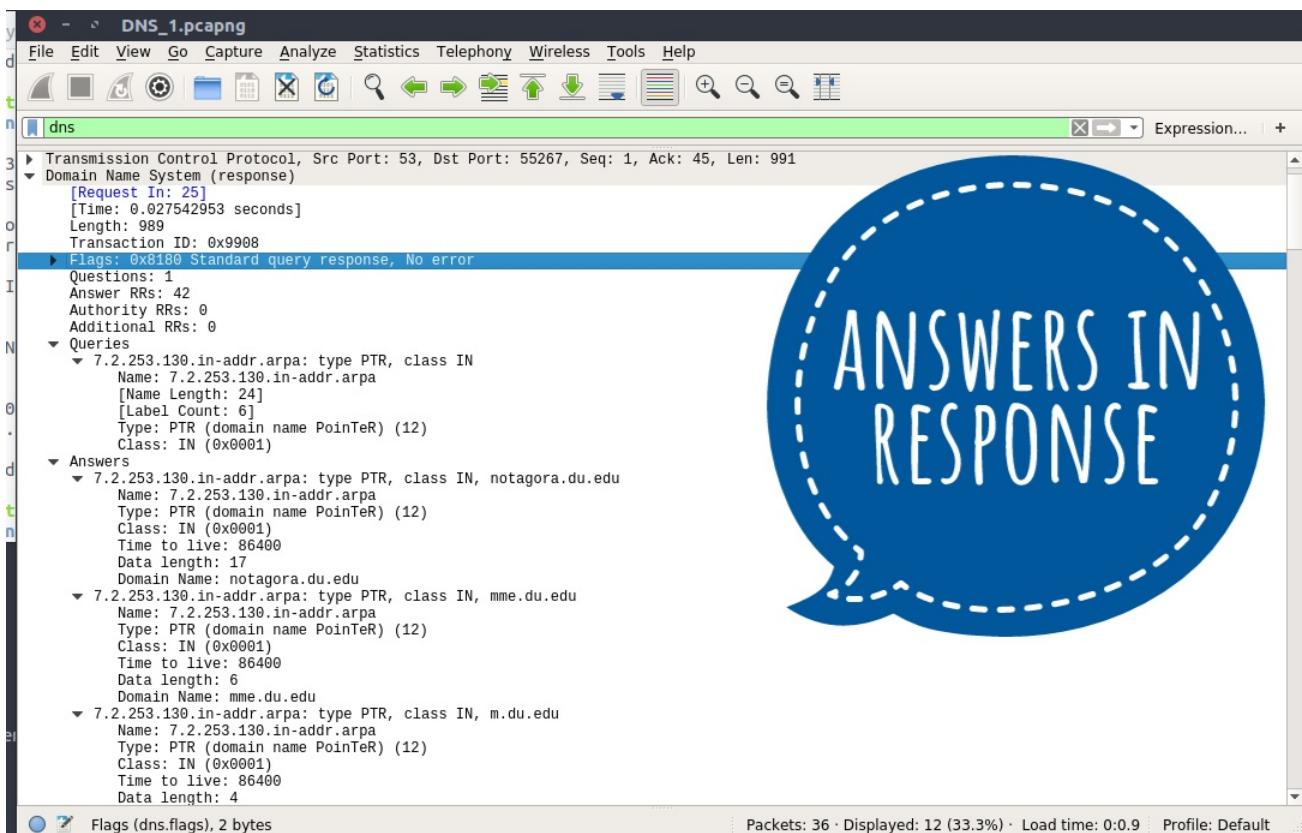
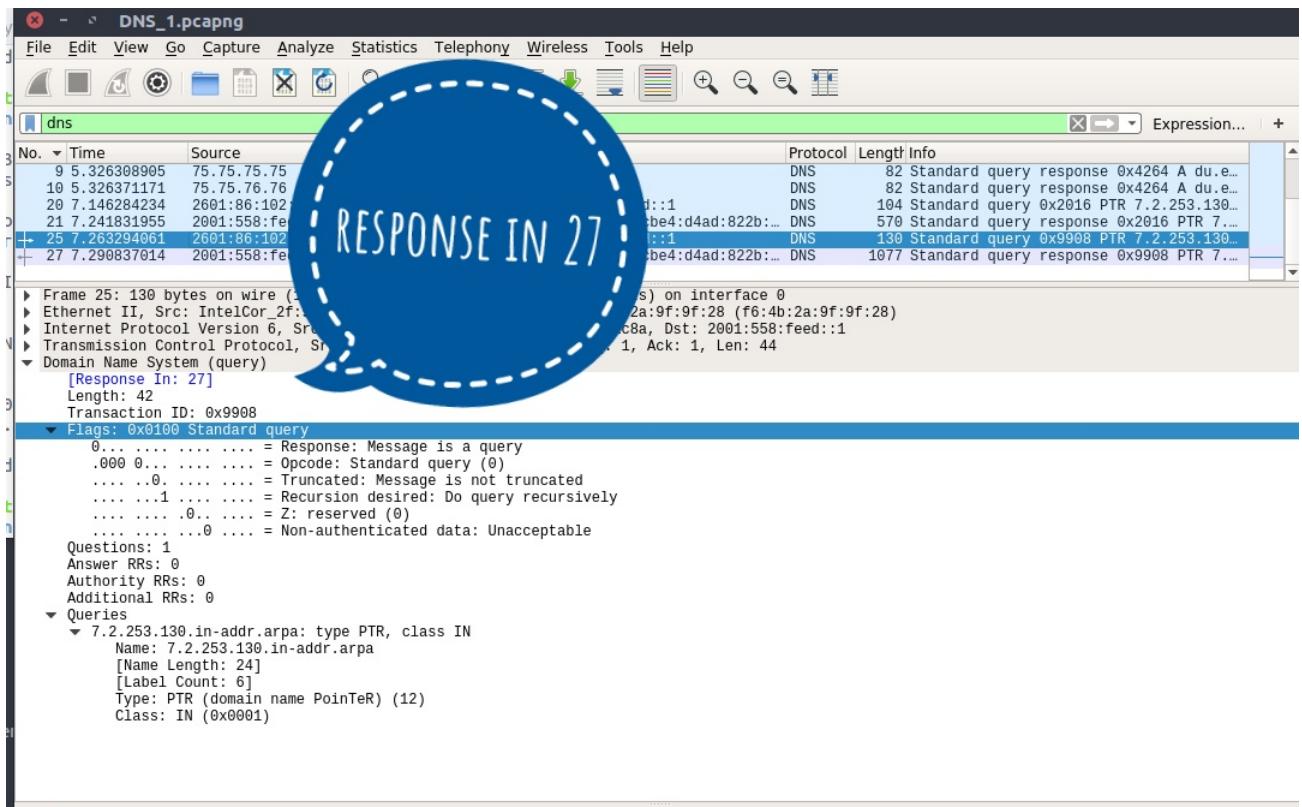
**Question 7** What does the query in the packet #25 do?

**Answer** Query in the packet #25 do inverse lookup of IP 7.2.253.130.



**Question 8** Which packet contains the response of the query sent? What is the response?

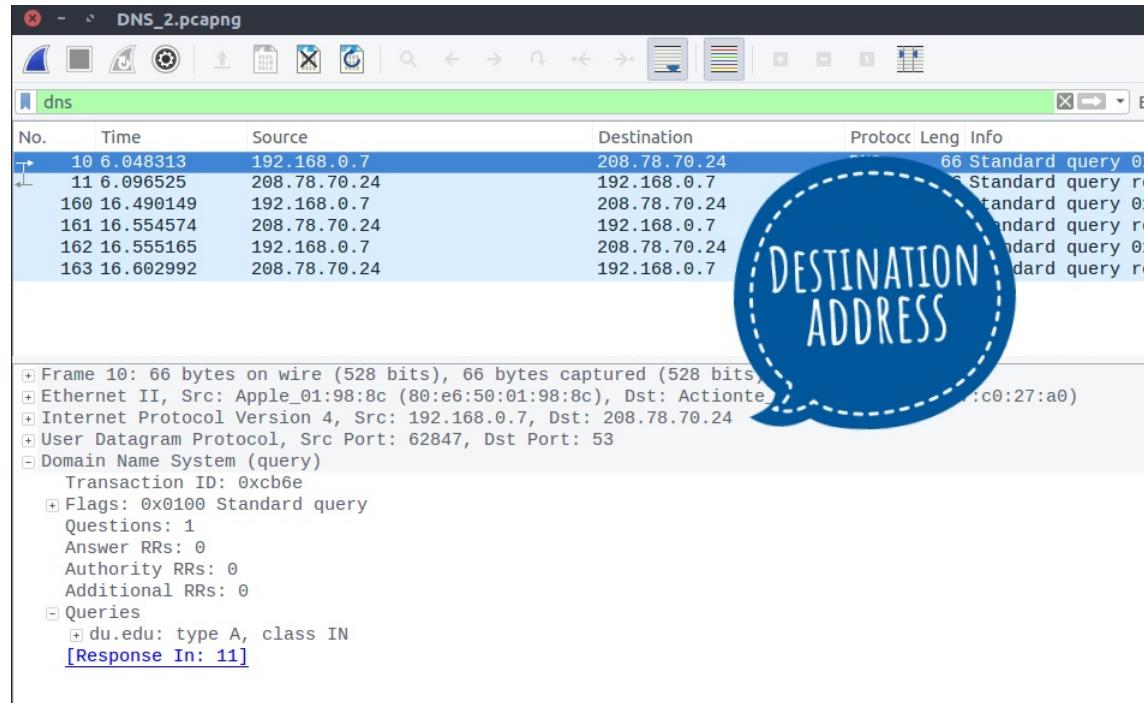
**Answer** Response of query of packet #25 contains in packet #27. The response is the answers of query in which some numbers of answers which gives Domain Name corresponding to IP address which was quired.



## SET 2: Using the DNS2.pcapng

**Question 1** In packet #10, what is the destination IP address of the server? To which DNS server request is being sent to?

**Answer** The destination IP address of the server is 208.78.70.24. The request has been sent to "cpnr-authdns-dhcp-vm-1.du.edu" DNS server



**Question 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?

**Answer** Packet #11 contains the reply of query that is sent in packet #10. Yes, DNS server reply.

Flags of the response are given below as follows which shows that request has been processed without any error:

Flags: 0x8500 Standard query response, No error

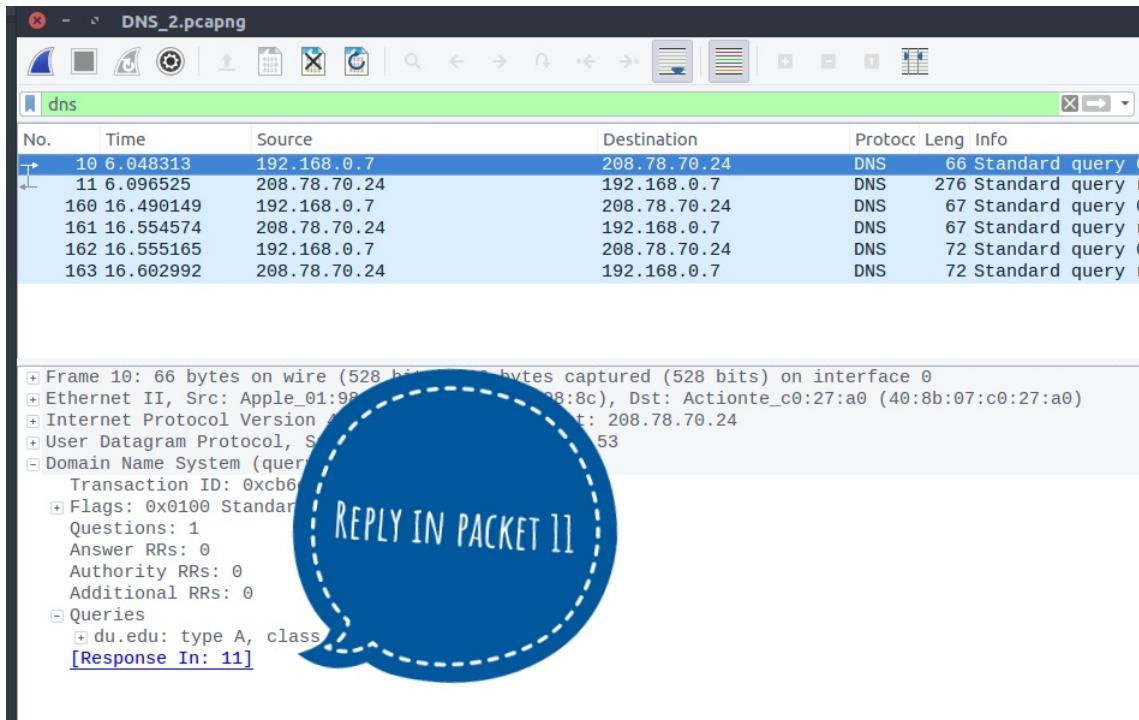
1... .... .... = Response: Message is a response

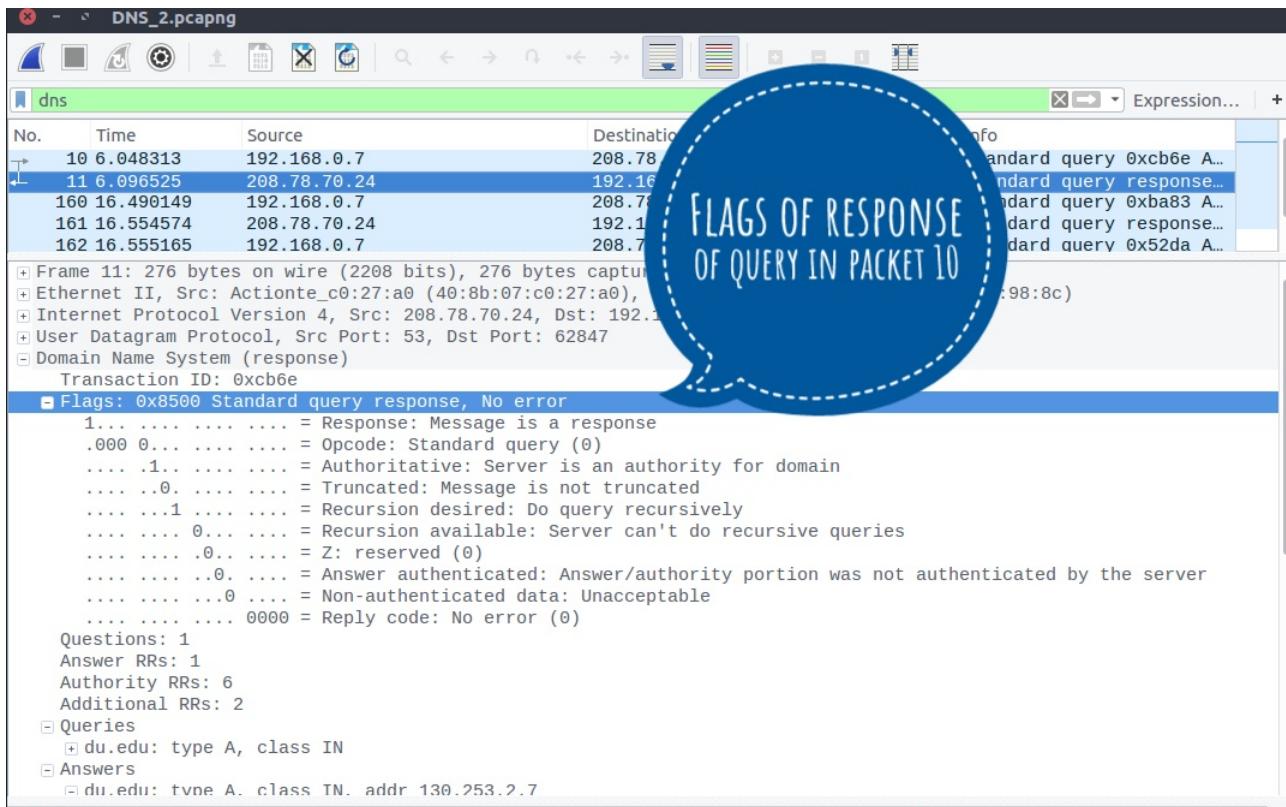
.000 0... .... .... = Opcode: Standard query (0)

.... .1.. .... .... = Authoritative: Server is an authority for domain

.... ..0. .... .... = Truncated: Message is not truncated

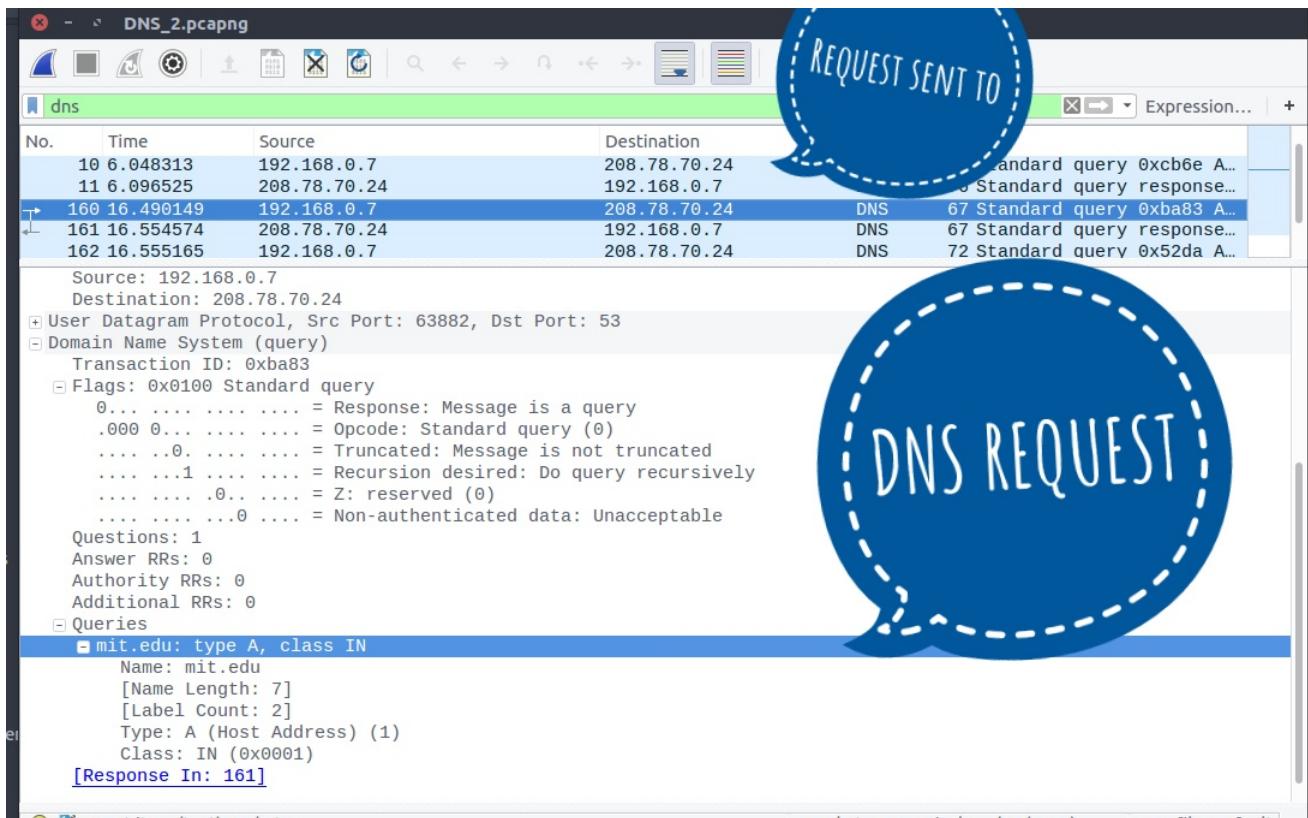
.... 1 .... = Recursion desired: Do query recursively  
 .... 0.... = Recursion available: Server can't do recursive queries  
 .... .0.. .... = Z: reserved (0)  
 .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server  
 .... ...0 .... = Non-authenticated data: Unacceptable  
 .... .... 0000 = Reply code: No error (0)





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

**Answer** The request in #160 is sent to 208.78.70.24. DNS request ask for IP address of "mit.edu".



**Question 4** What is the response from the DNS server in packet #160 ? Did the server resolve the DNS request? Explain in brief.

**Answer** The response from DNS server is in packet #160 where it refused to give answer of query. No DNS server did ot resolve the DNS request.

Here are the flags in response which clears the answer of server more precisely:

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)

Screenshot of Wireshark showing a DNS query and response. A large blue circle highlights the response packet (packet 161) with the text "RESPONSE CONTAIN IN".

The table below shows the DNS traffic:

No.	Time	Source	Destination	Protocol	Leng	Info
10	6.048313	192.168.0.7	208.78.70.24	DNS	66	Standard query 0xcb6e A...
11	6.096525	208.78.70.24	192.168.0.7	DNS	276	Standard query response...
160	16.490149	192.168.0.7	208.78.70.24	DNS	67	Standard query 0xba83 A...
161	16.554574	208.78.70.24	192.168.0.7	DNS	67	Standard query response...
162	16.555165	192.168.0.7	208.78.70.24	DNS	72	Standard query 0x52da A...

Packet details for the selected DNS response (161):

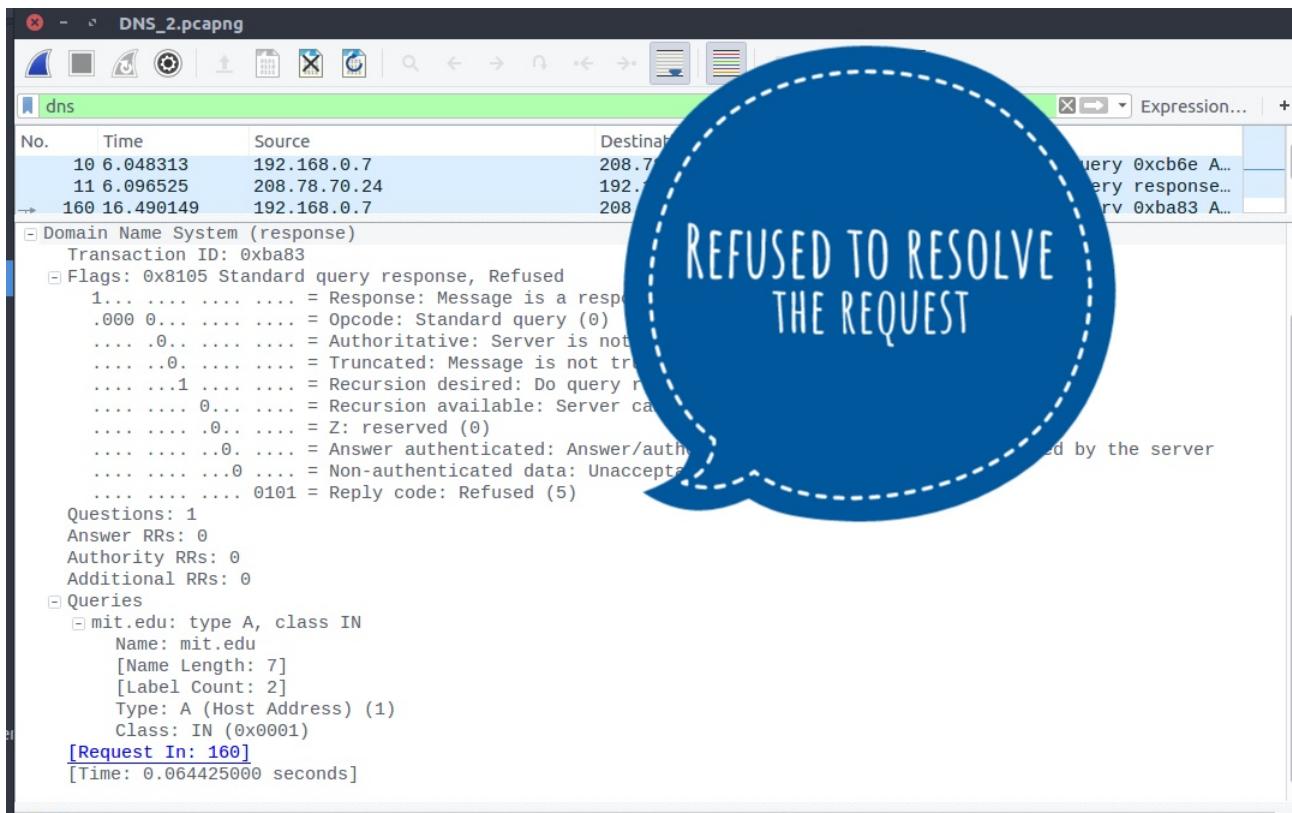
- User Datagram Protocol, Src Port: 63882, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0xba83
  - Flags: 0x0100 Standard query
    - 0... .... .... = Response: Message is a query
    - .000 0. .... .... = Opcode: Standard query (0)
    - .... .0. .... .... = Truncated: Message truncated
    - .... ..1 .... .... = Recursion Desired: Recursively
    - .... .... .0. .... = Z: reserved
    - .... .... ..0 .... = Non-authoritative Answer
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0

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

[\[Response In: 161\]](#)

Text item (text), 13 bytes

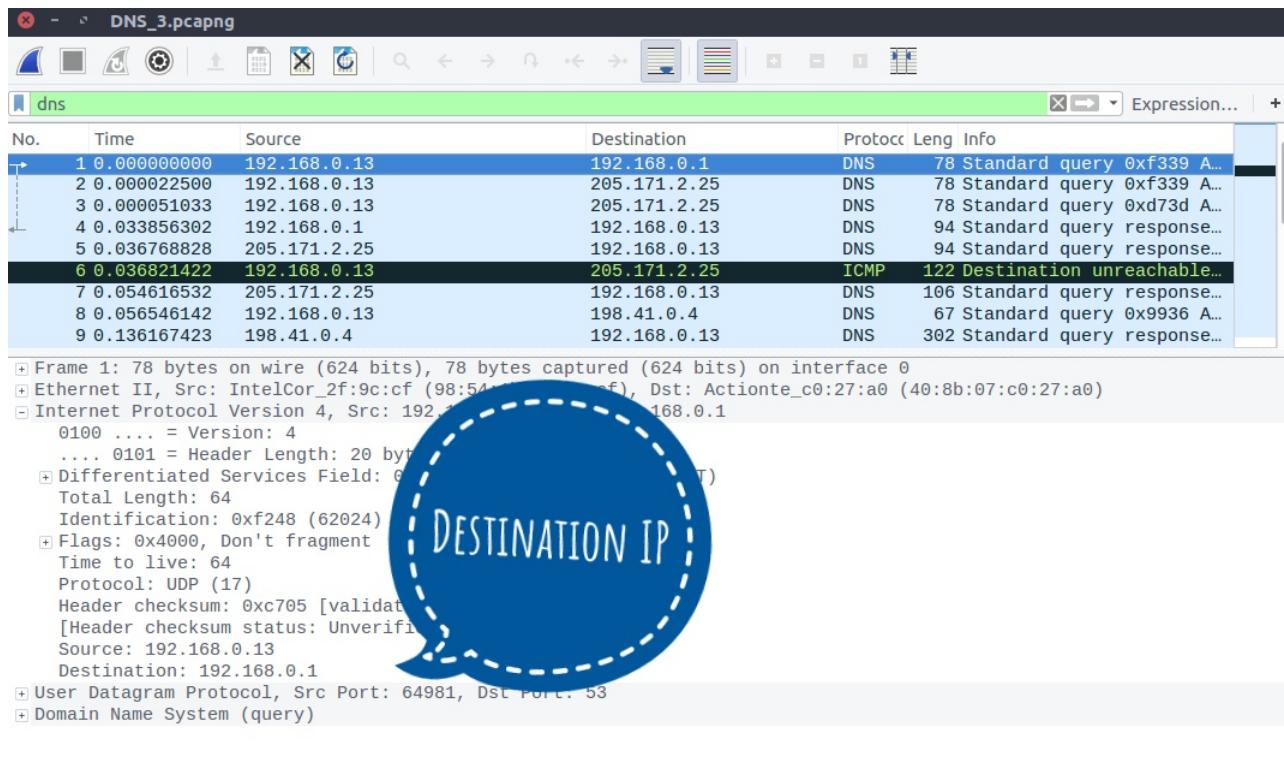
Packets: 178 · Displayed: 6 (3.4%) · Profile: Default



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

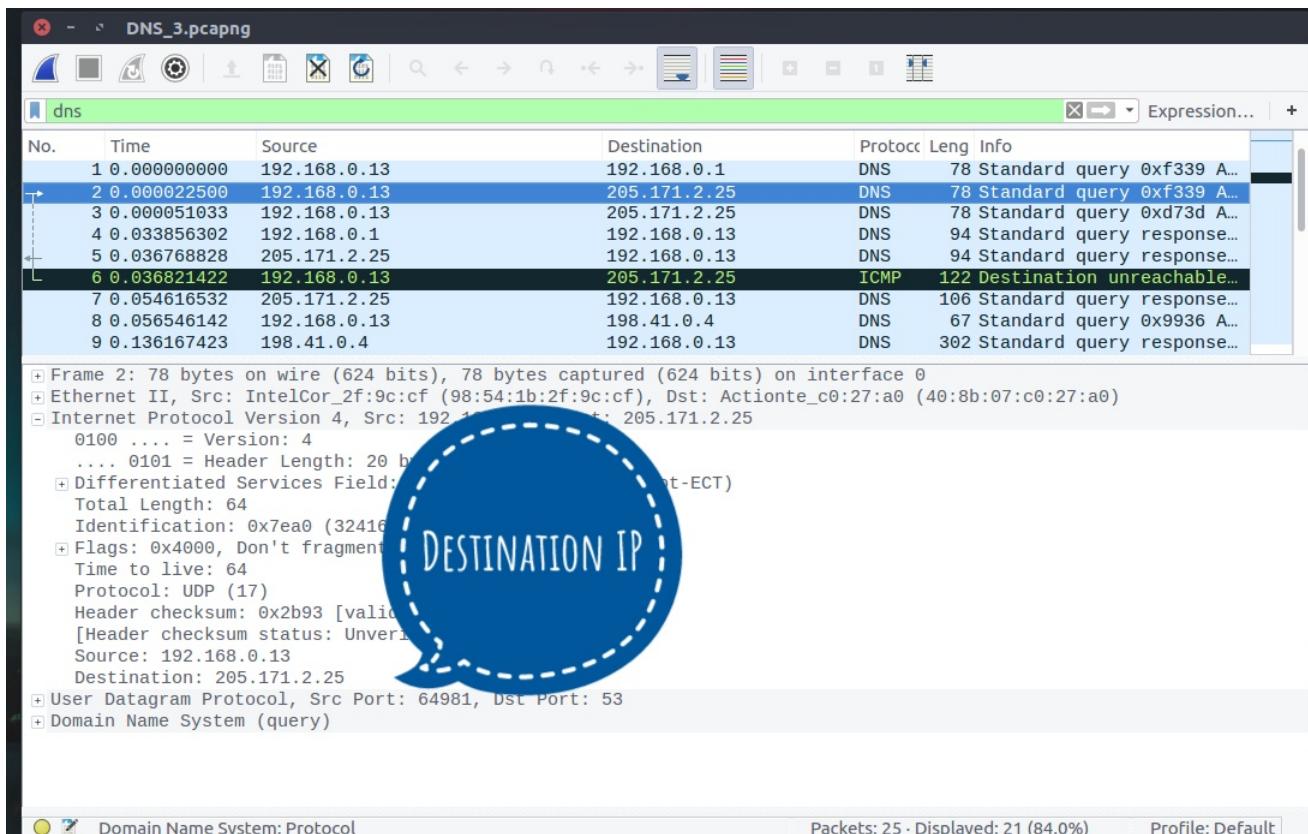
**Question 1** To what IP address, is the DNS query sent in packet #1? What "type" of DNS server is that?

**Answer** The destination IP address of the server is 192.168.0.1. The DNS server type is "Local server".



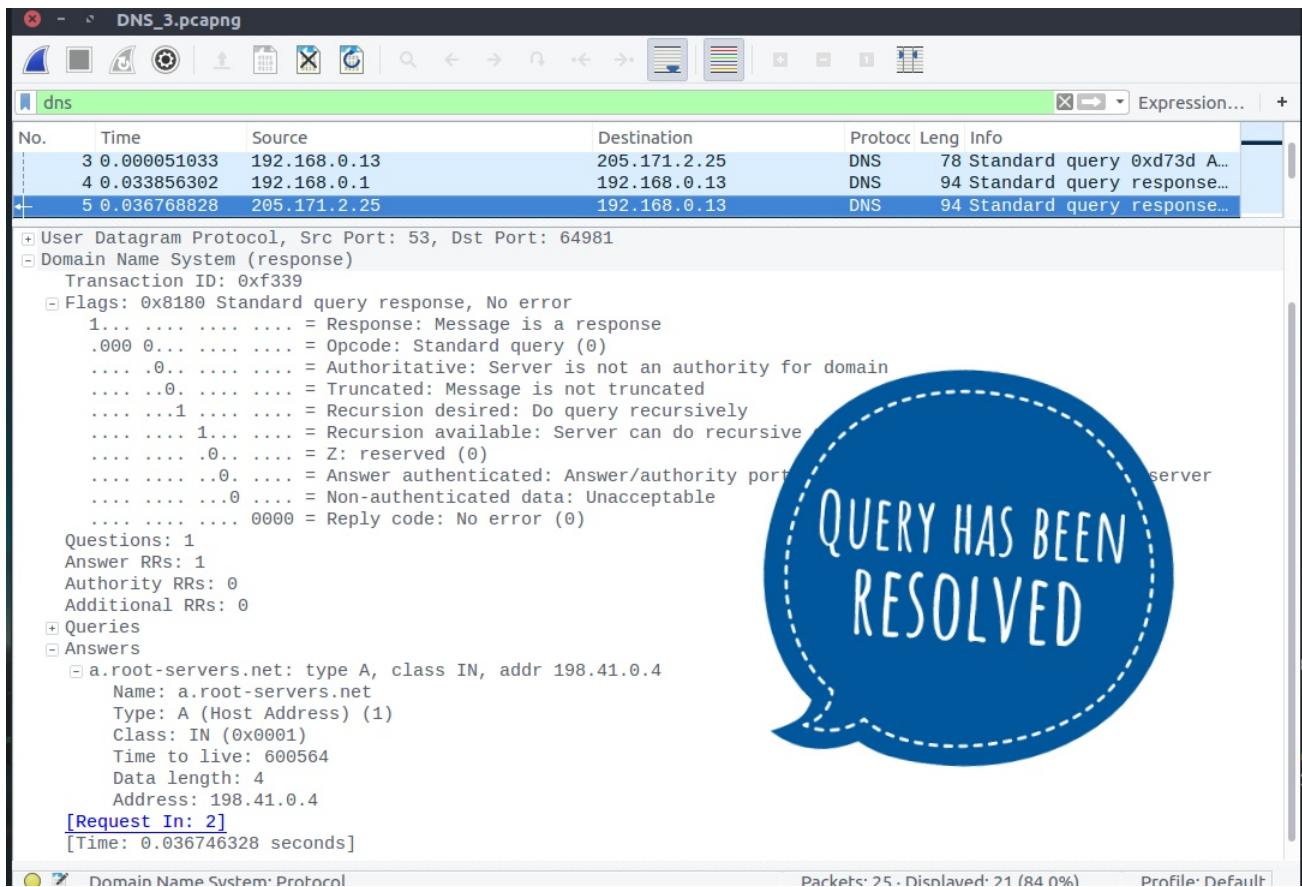
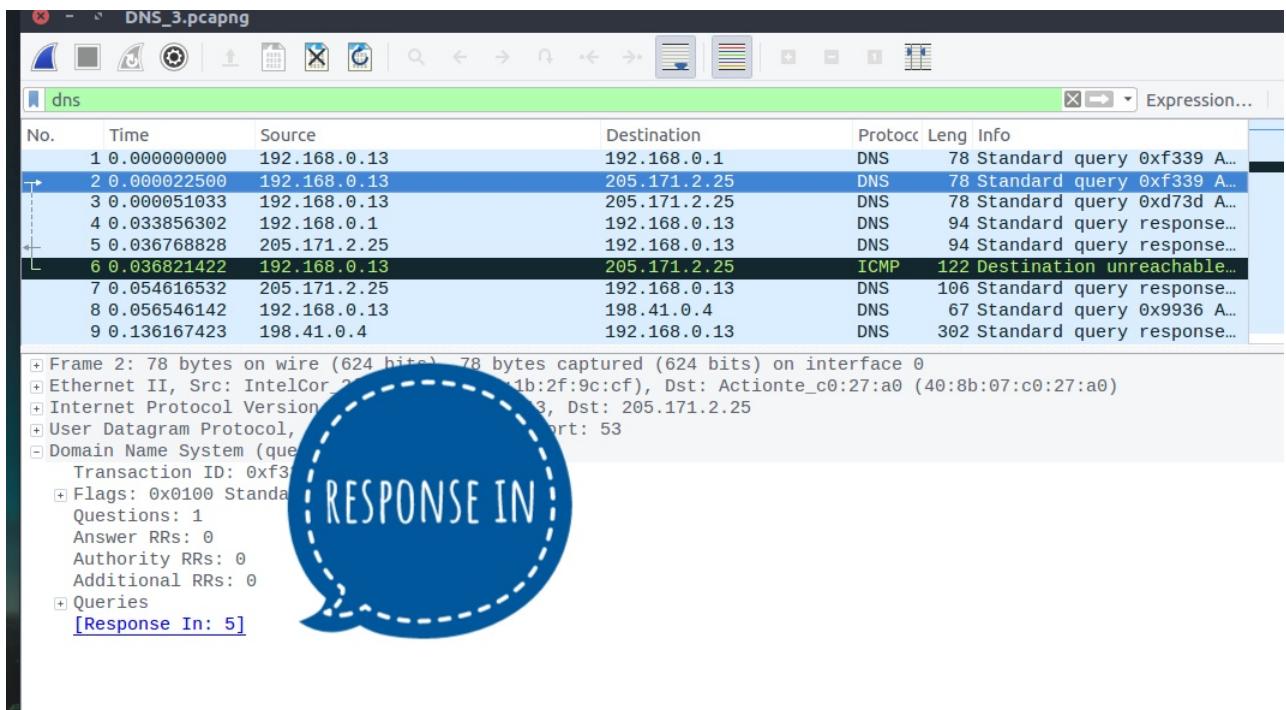
**Question 2** To what IP address, is the DNS query sent in packet #2? What "type" of DNS server is that?

**Answer** The destination IP address of the server is 205.171.2.25. The DNS server type is "Local server".



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

**Answer** The response of query in packet #2 is contained in packet number #5. The query has been resolved and answered.



**Question 4** What is the difference between query in packet #2 and that in #3 ?

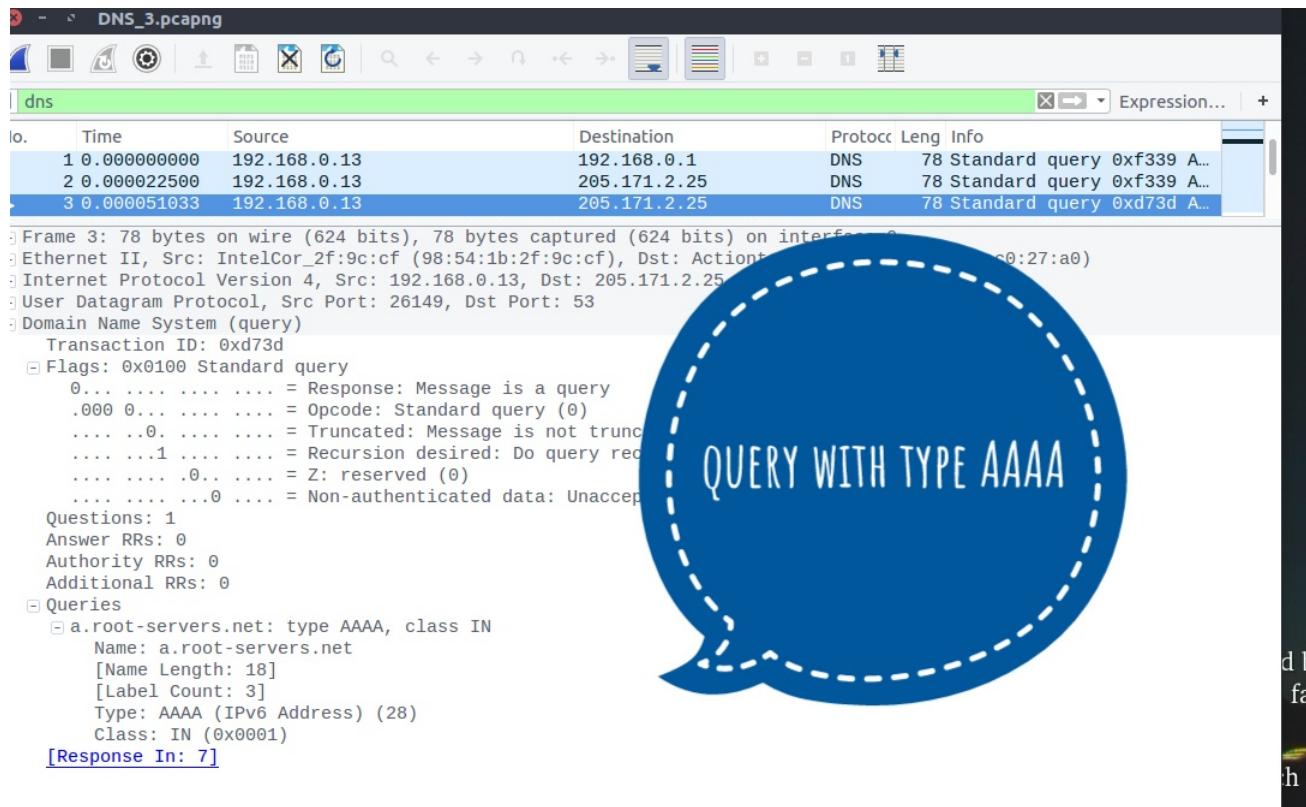
**Answer** The difference between the queries is that packet #2 have "type A" which gives IPv4 address, On the other hand, query in packet #3 have "type AAAA" which gives IPv6 address in response.

The screenshot shows a Wireshark capture of a DNS request. The packet list pane shows three DNS requests:

No.	Time	Source	Destination	Protocol	Leng	Info
1	0.0000000000	192.168.0.13	192.168.0.1	DNS	78	Standard query 0xf339 A...
2	0.000022500	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xf339 A...
3	0.000051033	192.168.0.13	205.171.2.25	DNS	78	Standard query 0xd73d A...

The details pane shows the second DNS request (Frame 2) in expanded view. The Flags field is set to 0x0100 (Standard query). The Questions section lists a single query for 'a.root-servers.net' of type A (Host Address). A blue callout bubble with the text 'QUERY WITH TYPE A' points to this section.

Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 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: 205.171.2.25  
User Datagram Protocol, Src Port: 64981, Dst Port: 53  
Domain Name System (query)  
Transaction ID: 0xf339  
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  
.... .0.... .... = Z: reserved (0)  
.... .0.... .... = Non-authenticated data: Unknown  
Questions: 1  
Answer RRs: 0  
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)  
[Response In: 5]



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

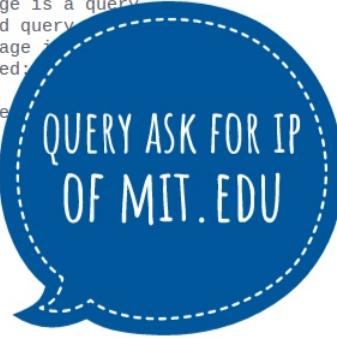
**Answer** Query in packet #8 ask for IP address of "mit.edu". The server that has been queried is a.root-servers.net which is a root server.

DNS\_3.pcapng

dns

No.	Time	Source	Destination	Protocol	Leng	Info
6	0.036821422	192.168.0.13	205.171.2.25	ICMP	122	Destination unreachable...
7	0.054616532	205.171.2.25	192.168.0.13	DNS	106	Standard query response...
8	0.056546142	192.168.0.13	198.41.0.4	DNS	67	Standard query 0x9936 A...

+ Frame 8: 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: 198.41.0.4  
+ User Datagram Protocol, Src Port: 39300, Dst Port: 53  
+ Domain Name System (query)  
  Transaction ID: 0x9936  
  Flags: 0x0100 Standard query  
    0... .... .... = Response: Message is a query  
    .000 0... .... .... = Opcode: Standard query  
    .... .0. .... .... = Truncated: Message is not truncated  
    .... .1 .... .... = Recursion desired  
    .... .... .0. .... = Z: reserved (0)  
    .... .... ..0 .... = Non-authenticated data  
  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)  
[\[Response In: 9\]](#)



**Question 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?

**Answer** The response of query sent in packet #8 is in packet #9.

The flags in the response are:

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

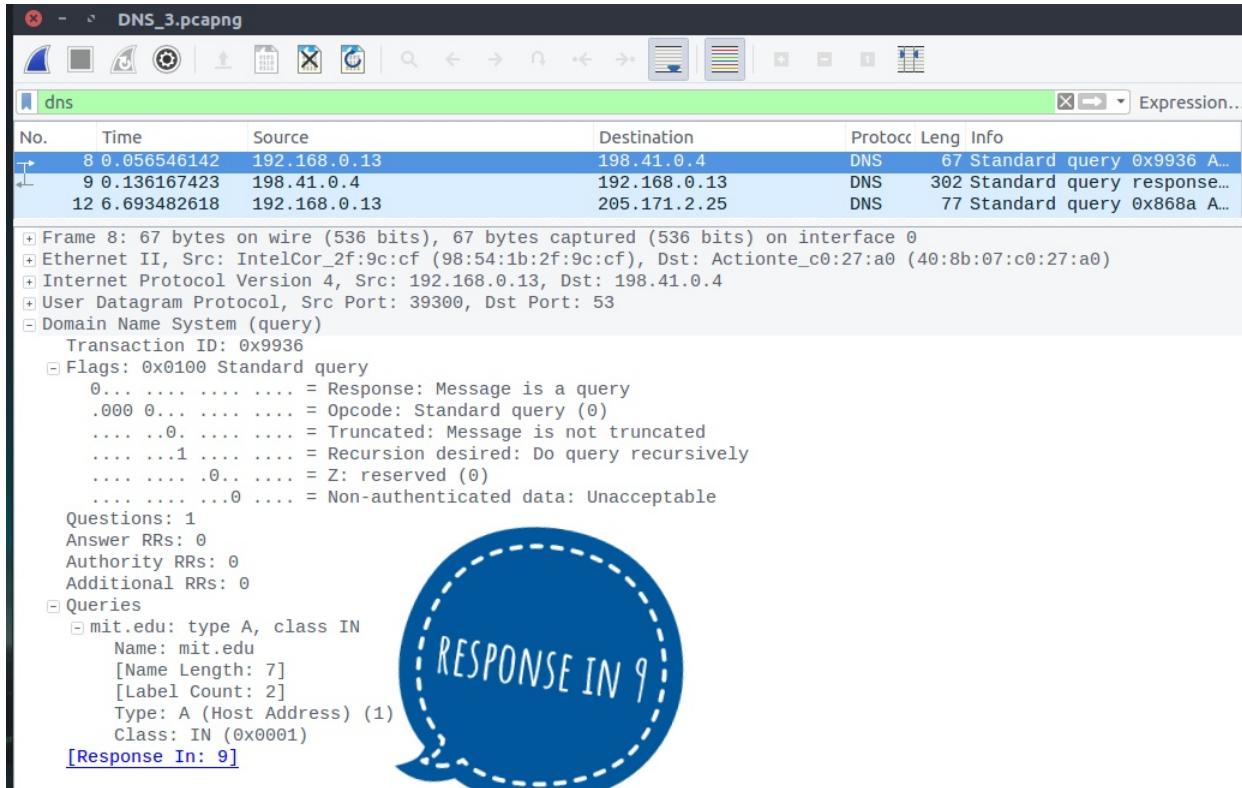
.... .... .0. .... = Z: reserved (0)

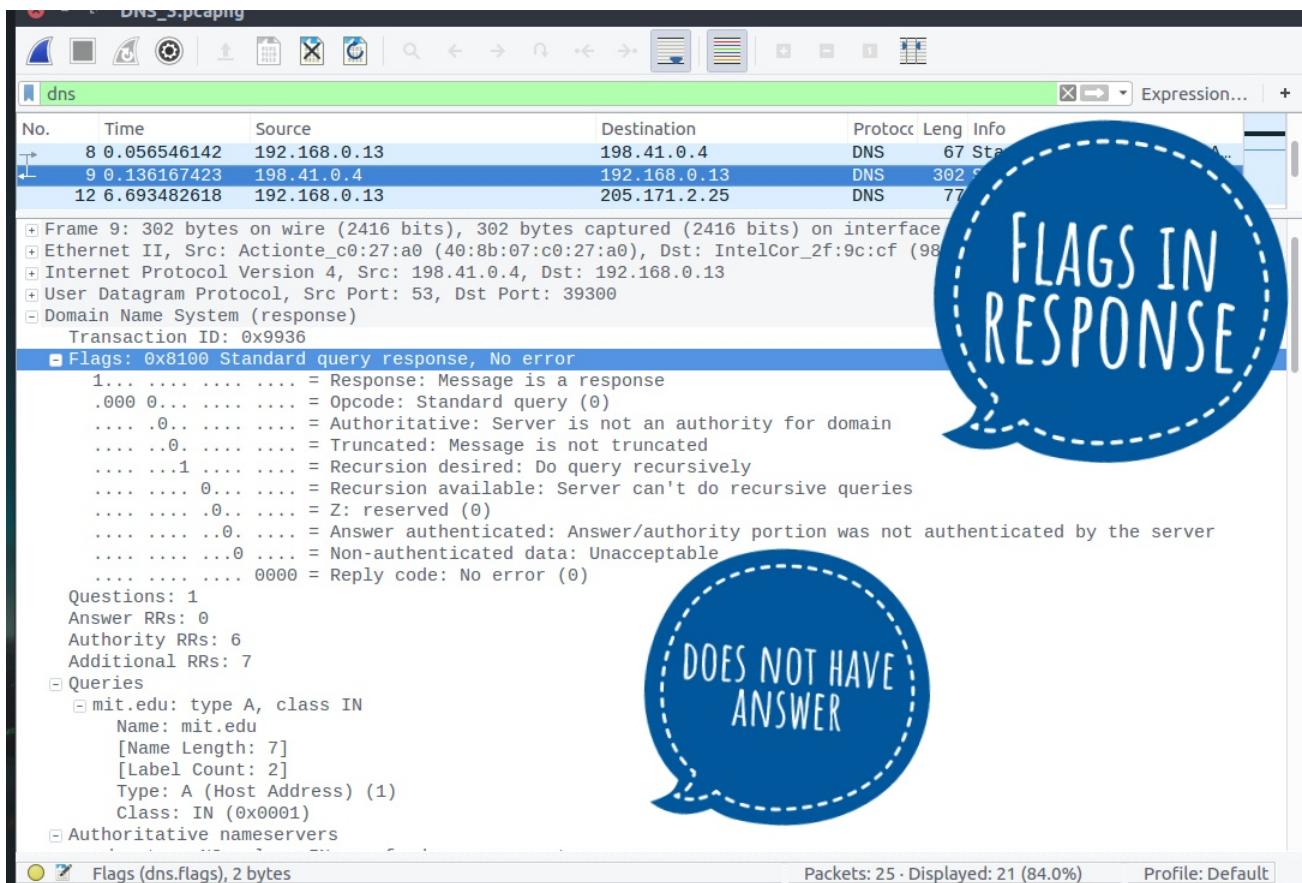
.... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server

.... .... ..0 .... = Non-authenticated data: Unacceptable

.... .... .... 0000 = Reply code: No error (0)

No it does not have answer which user wants. It provide information about which DNS servers have been tried to get answer of query.





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

**Answer** The server which has been queried is a.gtld-servers.net. No, it is not local server.

```
vikasgola@identity:/media/vikasgola/Tutorials&Files/IIT_JAMMU/sem 5/CS334-ComputerNetworks$ nslookup 192.5.6.30
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
30.6.5.192.in-addr.arpa name = a.gtld-servers.net.

Authoritative answers can be found from:

vikasgola@identity:/media/vikasgola/Tutorials&Files/IIT_JAMMU/sem 5/CS334-ComputerNetworks$
```

**Question 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?

**Answer** The response of query of the packet #16 is contains in packet #17.

The flags in the response is as follows:

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

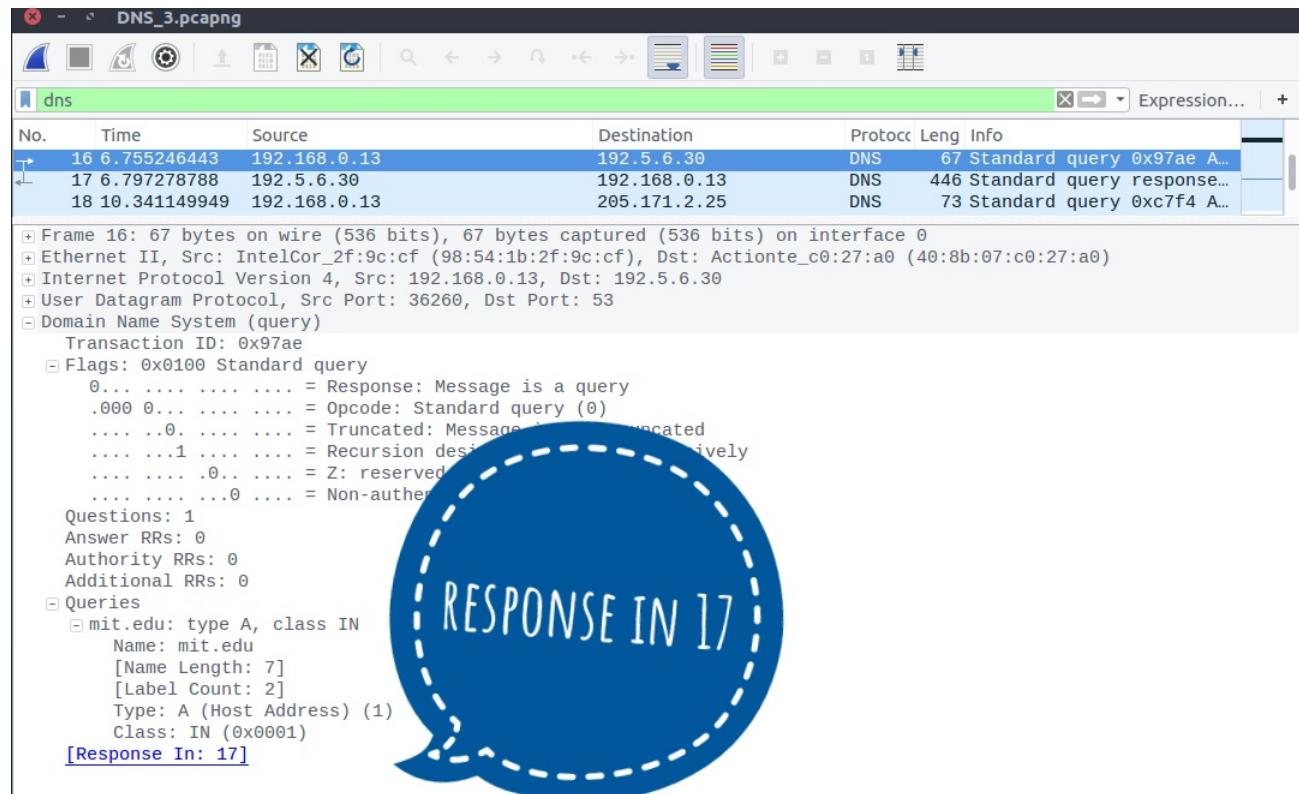
.... .... .0.. .... .... = Z: reserved (0)

.... .... ..0. .... .... = Answer authenticated: Answer/authority portion was not authenticated by the server

.... .... ...0 .... .... = Non-authenticated data: Unacceptable

.... .... .... 0000 = Reply code: No error (0)

No, it does not have the answer which user wants. It provide information about which DNS servers have been tried to get answer of query.



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

**Answer** Query in packet #22 ask for IP address of "mit.edu". The server which has been queried is a14-64.akam.net.

The screenshot shows the Wireshark interface with the file 'DNS\_3.pcapng' open. The 'dns' filter is applied. The packet list shows three DNS packets:

- Packet 21: Standard query response from 192.168.0.13 to 192.168.0.25.
- Packet 22: Standard query from 192.168.0.13 to 184.26.161.64.
- Packet 23: Standard query response from 192.168.0.13 to 184.26.161.64.

Details for packet 22:

- Frame 22: 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: 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 not recurse
    - .... .... .0 .... = Z: reserved (0)
    - .... .... ..0 .... = Non-authenticated
  - 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)

**ASK FOR IP OF MIT.EDU**

```
vikasgola@identity:/media/vikasgola/Tutorials&Files/IIT_JAMMU/sem 5/CS334-ComputerNetworks$ nslookup 184.26.161.64
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
64.161.26.184.in-addr.arpa name = a14-64.akam.net.

Authoritative answers can be found from:
vikasgola@identity:/media/vikasgola/Tutorials&Files/IIT_JAMMU/sem 5/CS334-ComputerNetworks$
```

**Question 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?

**Answer** The response of query of the packet #22 is contains in packet #23.

The flags in the response is as follows:

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

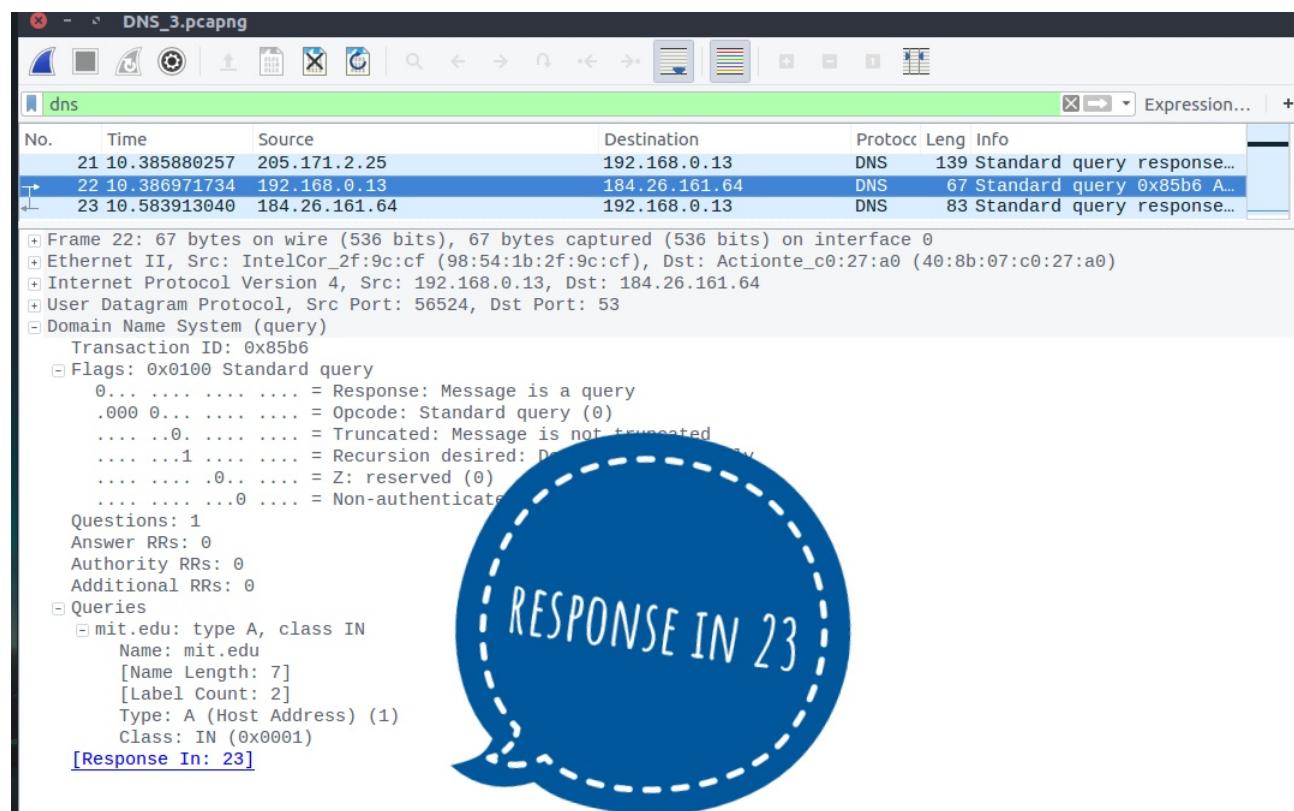
.... .... .0.. .... = Z: reserved (0)

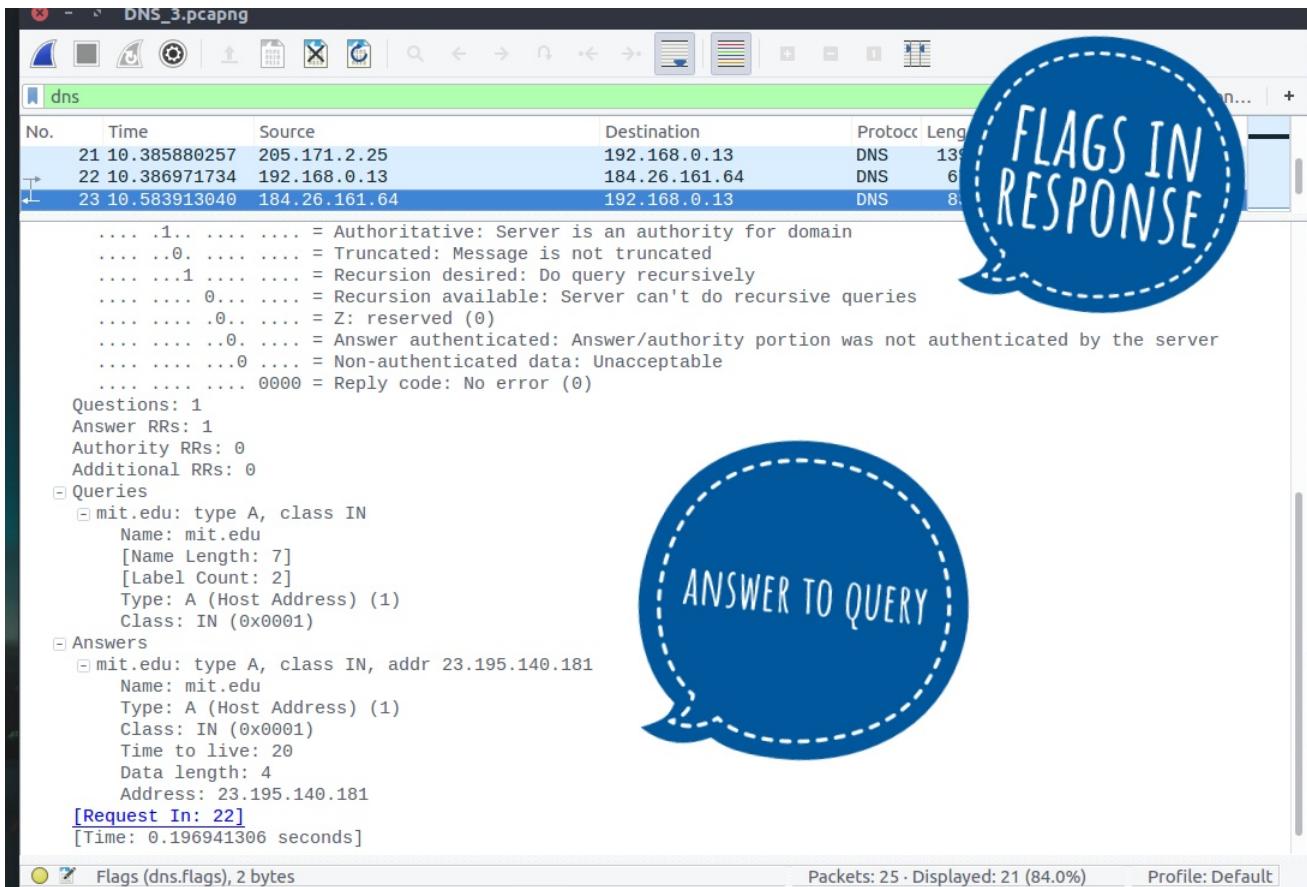
.... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server

.... .... ...0 .... = Non-authenticated data: Unacceptable

.... .... .... 0000 = Reply code: No error (0)

Yes, it does have the answer which user wants. It provide information about IP address of "mit.edu".





## SET 4 - Using dig command

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

**Answer** The dig command used to determine the authoritative DNS servers for www.mit.edu is `dig mit.edu -t NS`.

```

vikasgola@identity:~$ dig mit.edu -t NS

; <>> DiG 9.10.3-P4-Ubuntu <>> mit.edu -t NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61604
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
mit.edu.        34      IN      NS      use5.akam.net.
mit.edu.        34      IN      NS      use2.akam.net.
mit.edu.        34      IN      NS      ns1-173.akam.net.
mit.edu.        34      IN      NS      ns1-37.akam.net.
mit.edu.        34      IN      NS      asia2.akam.net.
mit.edu.        34      IN      NS      usw2.akam.net.
mit.edu.        34      IN      NS      eur5.akam.net.
mit.edu.        34      IN      NS      asia1.akam.net.

;; Query time: 113 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Oct 26 21:46:15 IST 2018
;; MSG SIZE  rcvd: 203

```

**Question 2** Using dig command determine the authoritative DNS servers for www.du.edu and www.rittieschool.du.edu in a single dig command? Are DNS servers for both different?

**Answer** The dig command used to determine the authoritative DNS servers for www.du.edu and www.rittieschool.du.edu is `dig du.edu -t NS rittieschool.du.edu -t NS`. Yes, both have different DNS servers.

```

vikasgola@identity: ~
; <>> DIG 9.10.3-P4-Ubuntu <>> du.edu -t NS ritchieschool.du.edu -t NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15820
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
du.edu.            3562    IN      NS      ns3.p24.dynect.net.
du.edu.            3562    IN      NS      ns1.p24.dynect.net.
du.edu.            3562    IN      NS      ns4.p24.dynect.net.
du.edu.            3562    IN      NS      ns2.p24.dynect.net.

;; Query time: 21 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Oct 26 21:52:08 IST 2018
;; MSG SIZE  rcvd: 121

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63020
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
rittieschool.du.edu.  3417    IN      CNAME   rittieschool.wpengine.com.

;; AUTHORITY SECTION:
wpengine.com.       1617    IN      SOA     jim.ns.cloudflare.com. dns.cloudflare.com. 2029223729 10000 2400 604800 3600

;; Query time: 18 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Oct 26 21:52:08 IST 2018

```

**Question 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?

**Answer**

```

vikasgola@identity:~$ dig +trace mit.edu

; <>> DiG 9.10.3-P4-Ubuntu <>> +trace mit.edu
;; global options: +cmd
.          194495  IN      NS      m.root-servers.net.
.          194495  IN      NS      b.root-servers.net.
.          194495  IN      NS      c.root-servers.net.
.          194495  IN      NS      d.root-servers.net.
.          194495  IN      NS      e.root-servers.net.
.          194495  IN      NS      f.root-servers.net.
.          194495  IN      NS      g.root-servers.net.
.          194495  IN      NS      h.root-servers.net.
.          194495  IN      NS      i.root-servers.net.
.          194495  IN      NS      a.root-servers.net.
.          194495  IN      NS      j.root-servers.net.
.          194495  IN      NS      k.root-servers.net.
.          194495  IN      NS      l.root-servers.net.
.          194495  IN      RRSIG   NS 8 0 518400 20181106050
000 20181024040000 2134 . U+MGSYDgKo+5jyYLe+S79ElGmlL47I9evDL4rBfqHQMFtnj
5ygh9xzK+ 6IQMTIppGB5oB7w7LAQ2bpu5Fzkc23jXh8icWyFDFJv4UjEFLOMUVYmU Xe8xBp
Hhzl1mFShXoNDnOW0tLgEjDDjzBNqnGDKbRpjD+oesyszqP28S tipkyErUvzWE0qXtmsfR46
j/ihaSX8D49CKJ76fEndQzfTAVForOrcgW yYxUZhboSetZKTESpamdqsOGMREN7XEB1n3Vxb
lzs0H9aC/L/VburAzU vGk8/RWLZZwm/hQMjbsLIu3JzPBtjZyz2fNEJMyEChsnjmFafGAjj4
cc gMQj/Q==

;; Received 525 bytes from 127.0.1.1#53(127.0.1.1) in 17 ms

edu.          172800  IN      NS      i.edu-servers.net.
edu.          172800  IN      NS      m.edu-servers.net.
edu.          172800  IN      NS      h.edu-servers.net.
edu.          172800  IN      NS      d.edu-servers.net.
edu.          172800  IN      NS      c.edu-servers.net.
edu.          172800  IN      NS      l.edu-servers.net.
edu.          172800  IN      NS      a.edu-servers.net.
edu.          172800  IN      NS      f.edu-servers.net.
edu.          172800  IN      NS      g.edu-servers.net.
edu.          172800  IN      NS      k.edu-servers.net.
edu.          172800  IN      NS      j.edu-servers.net.
edu.          172800  IN      NS      b.edu-servers.net.
edu.          172800  IN      NS      e.edu-servers.net.
edu.          86400   IN      DS      28065 8 2 4172496CDE85534

```

```

vargasgola@identity: ~
edu.          172800  IN      NS      j.edu-servers.net.
edu.          172800  IN      NS      b.edu-servers.net.
edu.          172800  IN      NS      e.edu-servers.net.
edu.          86400   IN      DS      28065 8 2 4172496CDE85534
E51129040355BD04B1FCFEBAE996DFDDE652006F6 F8B2CE76
edu.          86400   IN      RRSIG   DS 8 1 86400 201811080500
00 20181026040000 2134 . gvacVm0KydeW1i70CoSvdbScKn0ugTeVlqJLkzTK0yUB0789
J3nof6Z9 1M4R0eVd8gLUmkBcpBlWXNrTteDHkefiNcZidlEdNKrvZhj0Z9BJmwo 3nVL5bZ
JmGTjHdm63pqkDexwD1tsIQkhSuVDOHZeQZUXOL/40zxDxnMx sqDnEwgfizSF6bLViRieXiL
g6zfA6ygoauzJU/4tVxb2PdeA5b7NjaIG MdpIgByTBRpatbr3hUEw9g0od4NRplRYntzjVDC
AhOG+gHCMwQMaMlPV BOInp3hGTDJh7QMghPWSok2dvl9LIp3hDYtCJYbejoqKblqtoTzVsLZ
0 gXQe9A==
;; Received 1166 bytes from 192.36.148.17#53(i.root-servers.net) in 182 ms

mit.edu.       172800  IN      NS      usw2.akam.net.
mit.edu.       172800  IN      NS      asia1.akam.net.
mit.edu.       172800  IN      NS      asia2.akam.net.
mit.edu.       172800  IN      NS      use2.akam.net.
mit.edu.       172800  IN      NS      ns1-37.akam.net.
mit.edu.       172800  IN      NS      ns1-173.akam.net.
mit.edu.       172800  IN      NS      eur5.akam.net.
mit.edu.       172800  IN      NS      use5.akam.net.
9DHS4EP5G85PF9NUFK06HEK0048QGK77.edu. 86400 IN NSEC3 1 1 0 - 9V5L4LUB1VNJ
9EQQLIHEQCBREACL2500 NS SOA RRSIG DNSKEY NSEC3PARAM
9DHS4EP5G85PF9NUFK06HEK0048QGK77.edu. 86400 IN RRSIG NSEC3 8 2 86400 2018
1102140824 20181026125824 37217 edu. RRahqaffME8QvJUUUmBsJLBTwoX0Tfa8x0RP
u0Rrnqx+IjI2QK9xnPJq Fk/X/iTq24D245MbeBuCPAw1Q000ukTslEg9mY/tT/BczJjn83XAi
RWHC g9TlAwm/5HIPnYY9uJZ1EGiPWJR6HzNxq22YFQetIBWT0AG/3pQ2mddH +Zk=
H1SPUQIV7KAEG07MNVFS0014TGESK44N.edu. 86400 IN NSEC3 1 1 0 - I4667HA7DROB
ISP0J03FLRA51T795C7K NS DS RRSIG
H1SPUQIV7KAEG07MNVFS0014TGESK44N.edu. 86400 IN RRSIG NSEC3 8 2 86400 2018
1102155104 20181026144104 37217 edu. BWhFQp6Wh1LxG7znM4IE2bfP7GeymU5Lv/a
x+bpZdTbWIO3861vcZtA B8lSpHRNROYuIMuGIJ1mYYQ7Ux7PMx2y/ft/+TYtjNL0mWsa6LFN
qvzT 2xkj8ju7fof1QFLs3ncg+HyW20RMkTdw7UiYna3H5dHcsLmvT/HvMoMc gIw=
;; Received 900 bytes from 192.31.80.30#53(d.edu-servers.net) in 171 ms

mit.edu.       20      IN      A      184.26.196.231
;; Received 52 bytes from 95.100.175.64#53(asia1.akam.net) in 86 ms

vargasgola@identity:~$ 

```

From the output we can see that this command is tracing how mit.edu domain is resolved from DNS servers.