Assignment 6
Computer Networks

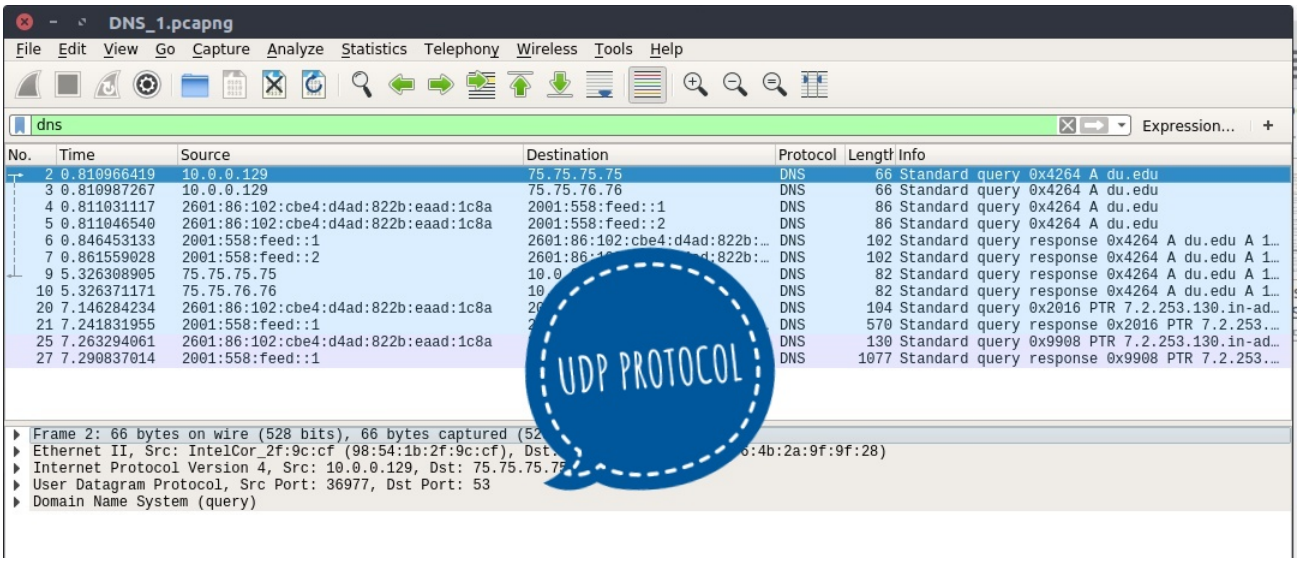
Vikas Gola : 2016UCS0023

October 26, 2018

SET 1: The Basic DNS

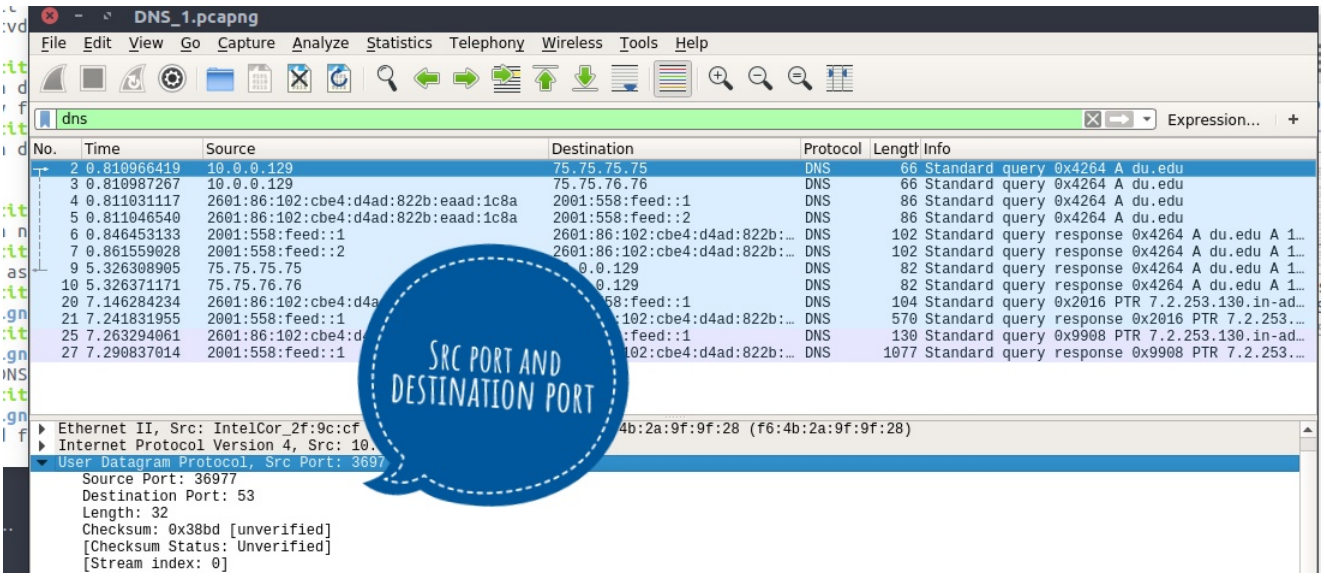
Question 1 Determine which transport layer protocol was used for sending the DNS queries? What are the benefits and drawbacks of using that protocol ?

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.



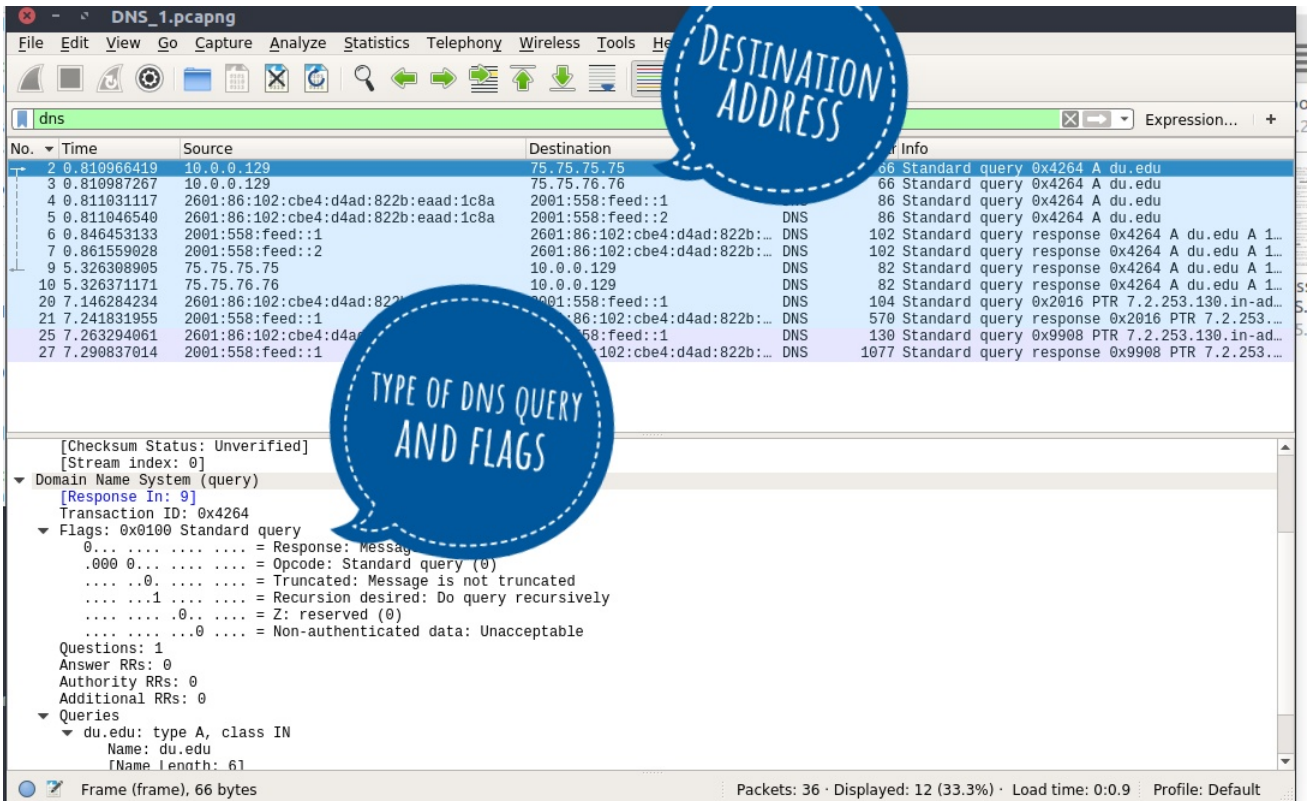
Question 2 What port numbers are used for sending and receiving the packet in packet #2 ?

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



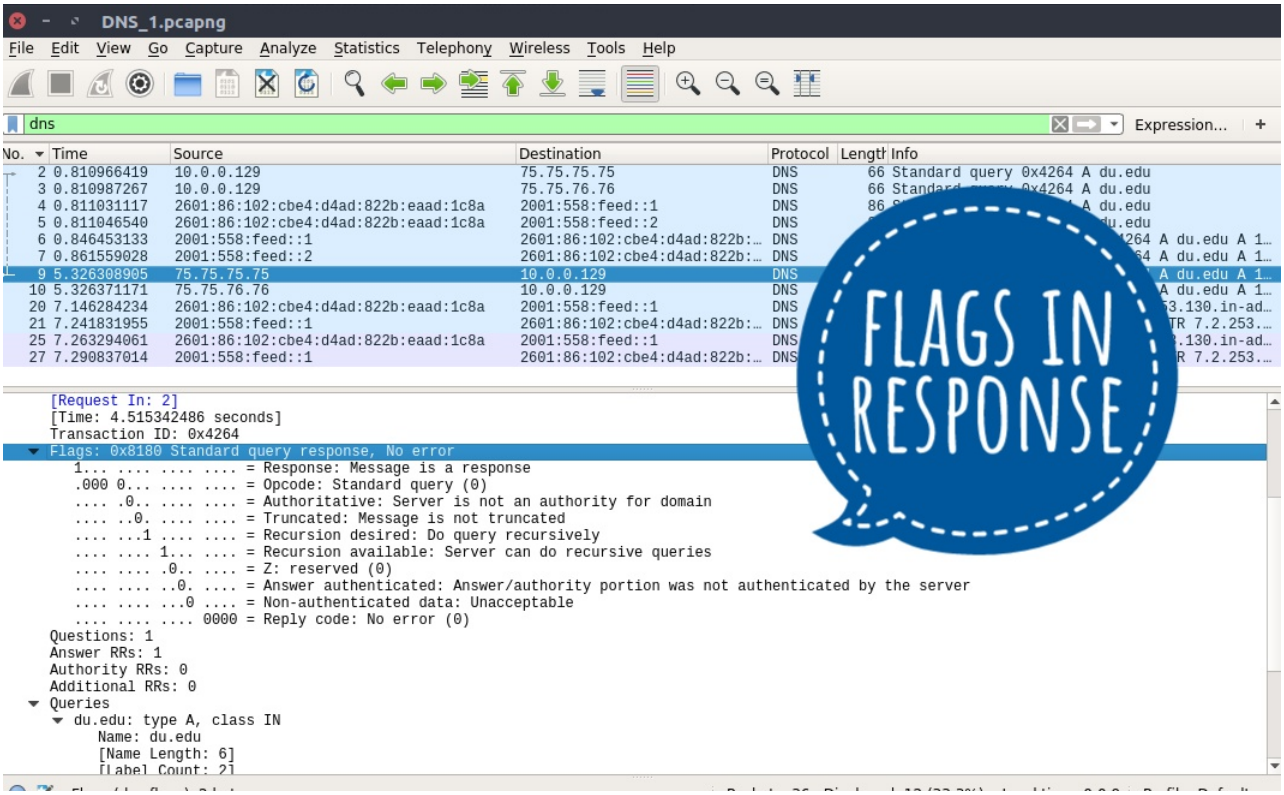
Question 4 How many DNS servers are queried to for resolving the domain name du.edu.?

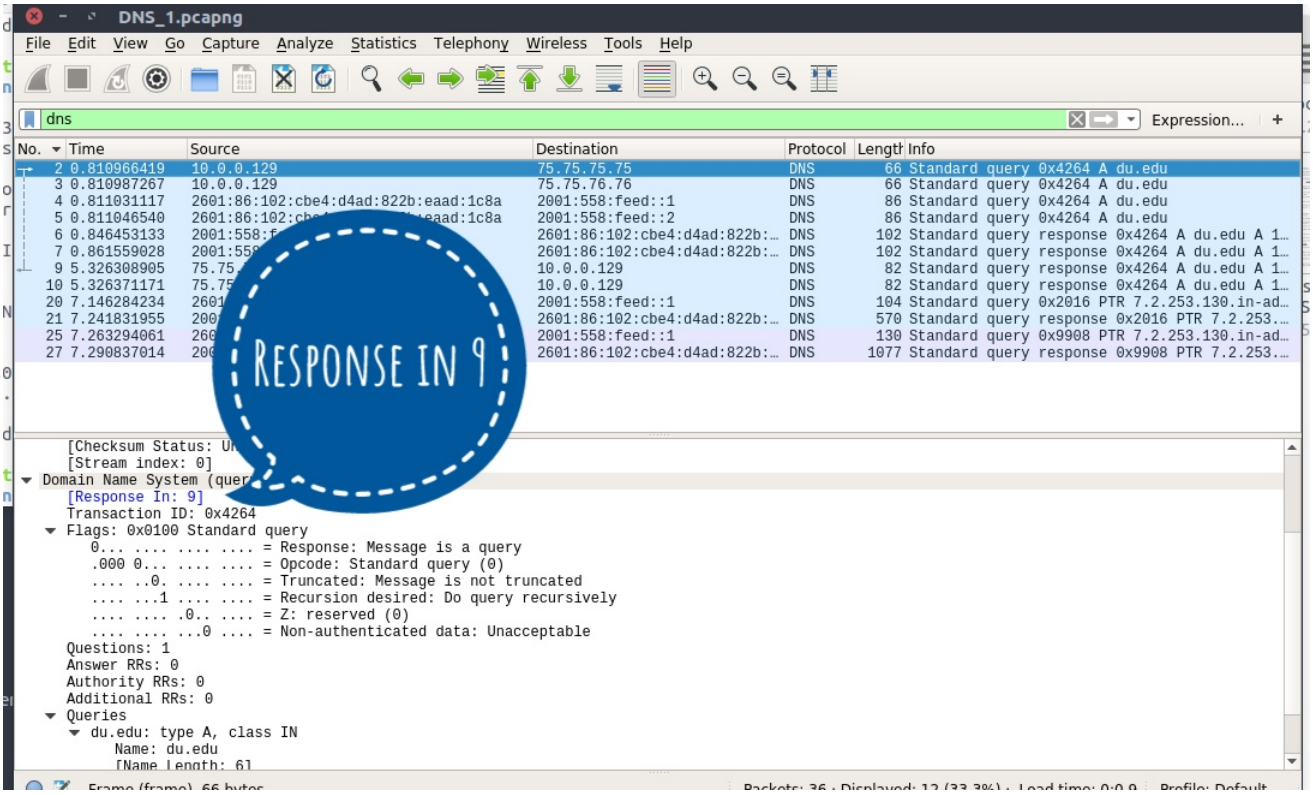
Answer 1 DNS server is queried to for resolving the domain name du.edu.

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

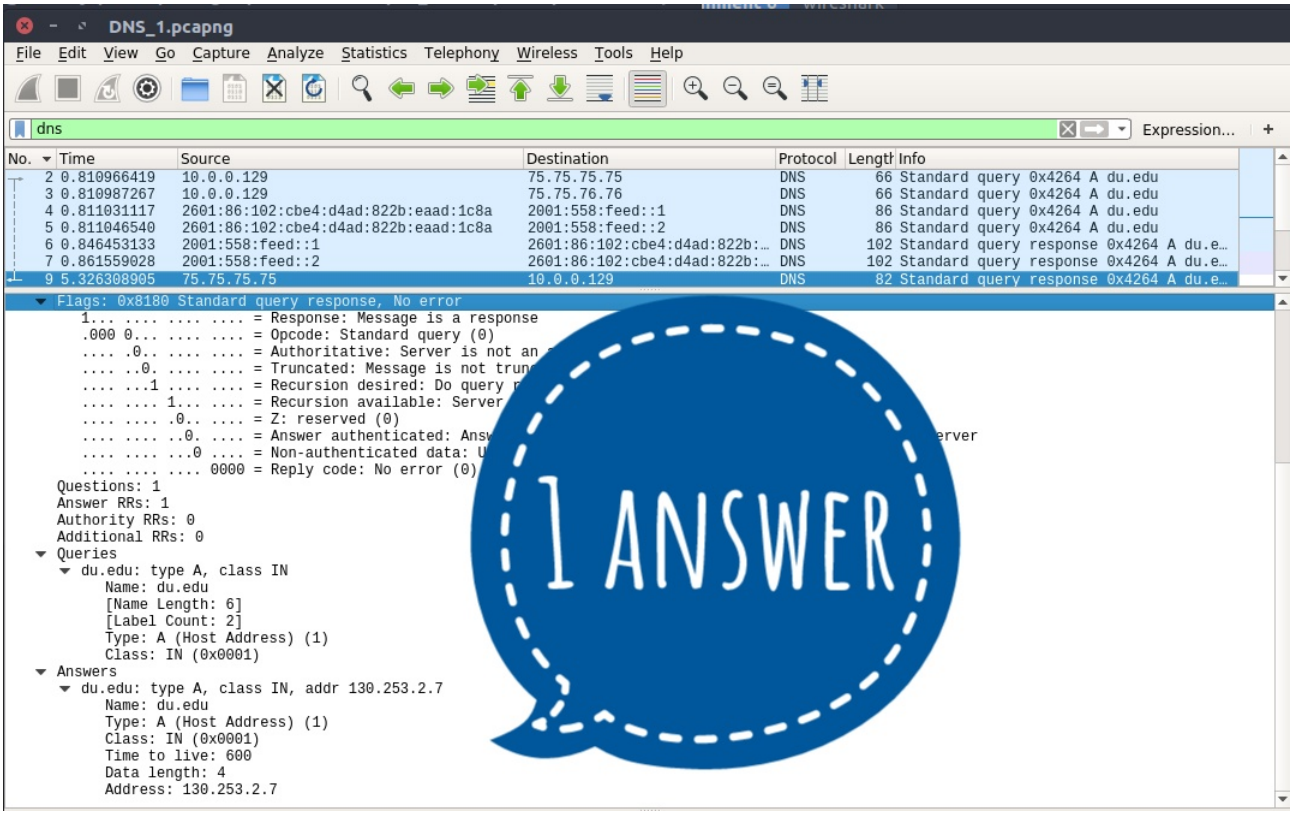
authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)





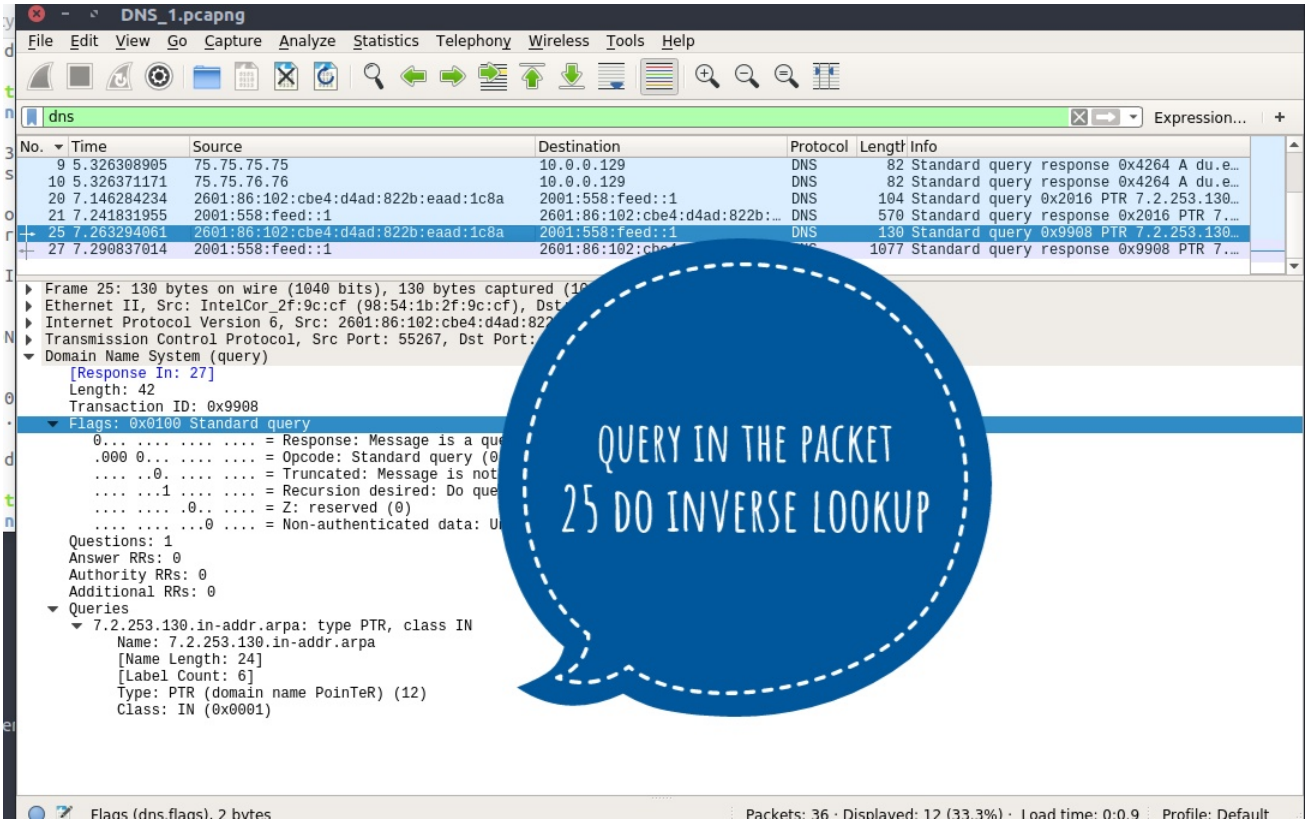
Question 6 How many answers do you get in the response? Is the response from authoritative server ?

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



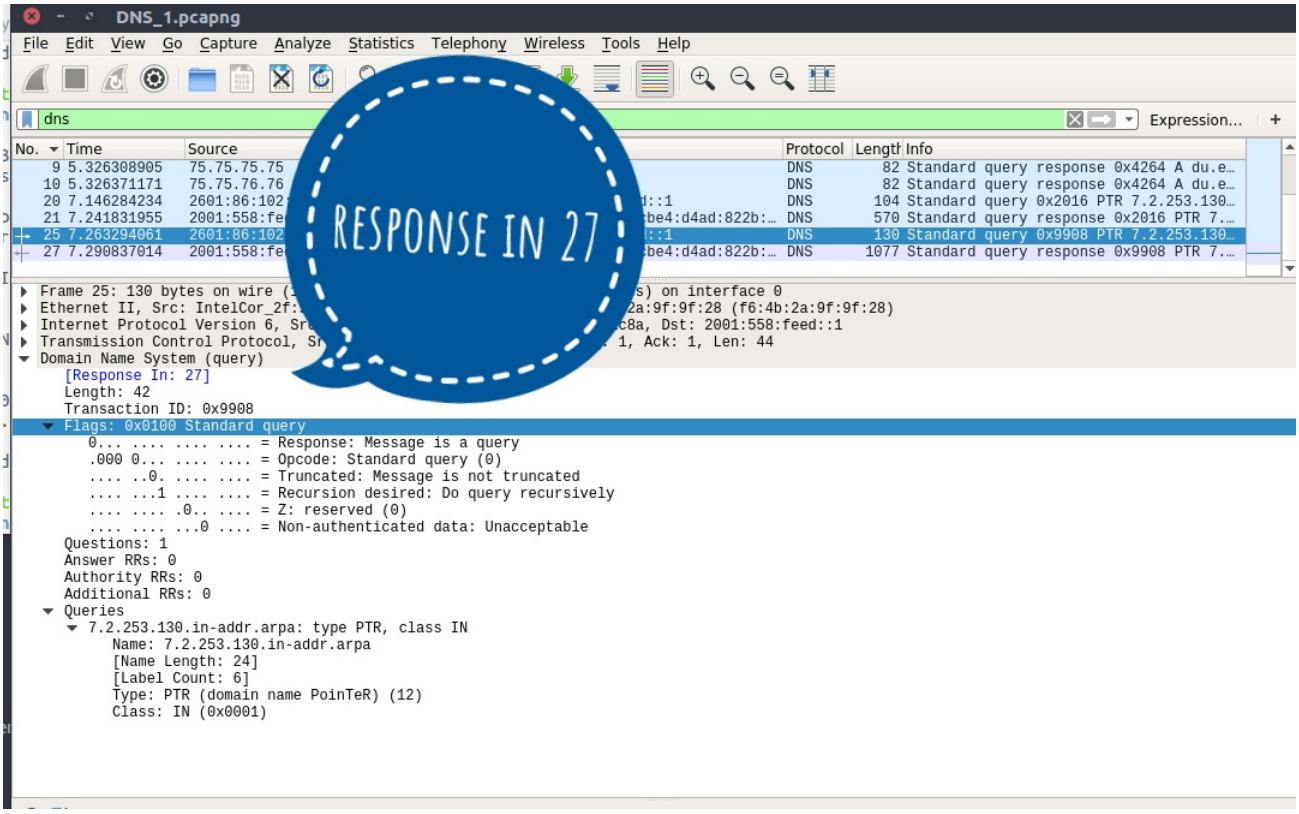
Question 7 What does the query in the packet #25 do?

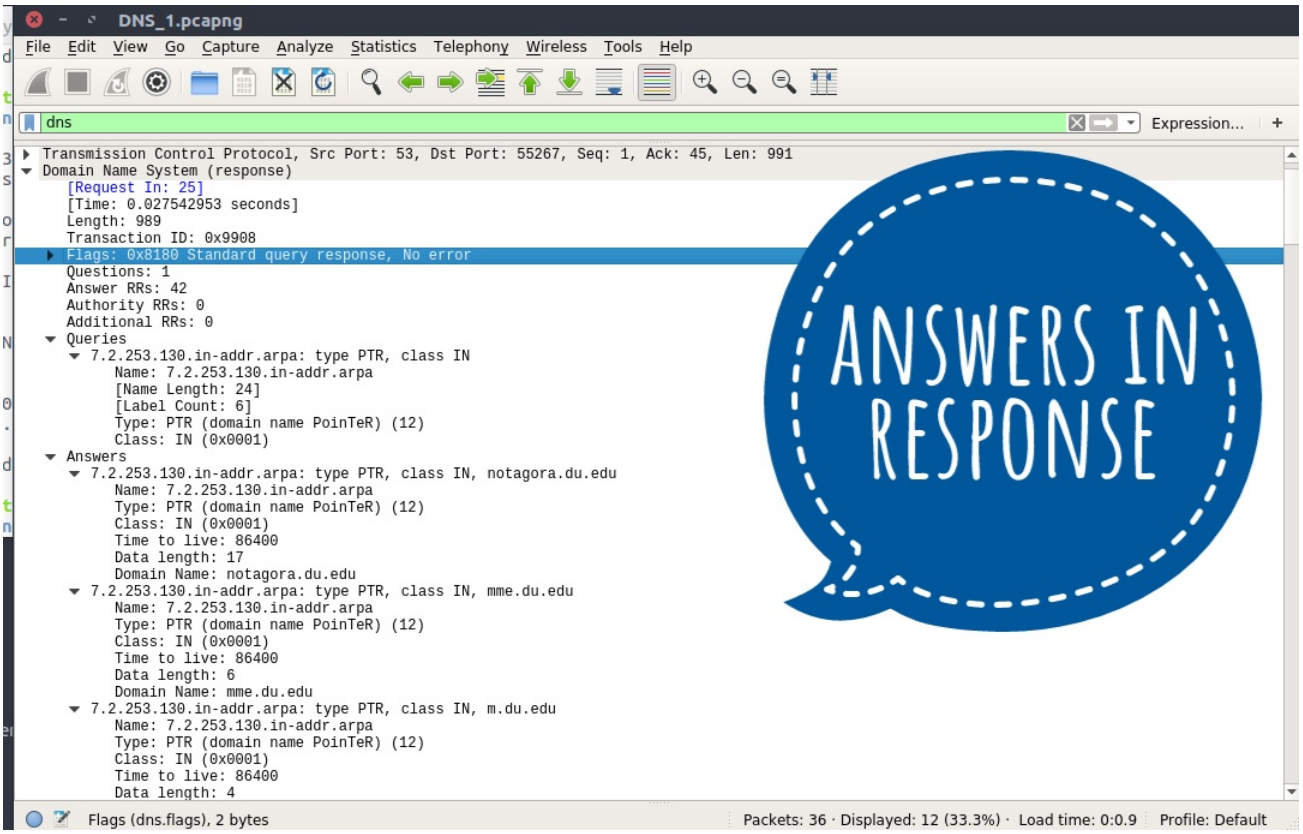
Answer Query in the packet #25 do inverse lookup of IP 7.2.253.130.



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.

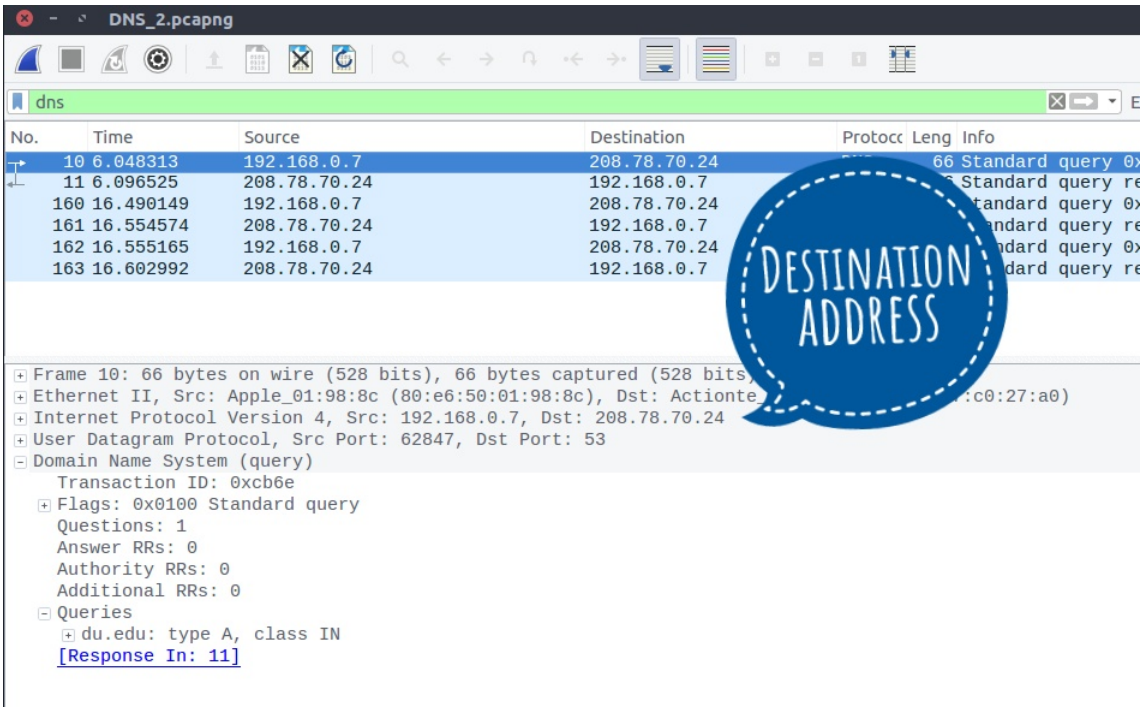

DNS_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
No. Time Source Protocol Length Info
9 5.326308905 75.75.75.75 DNS 82 Standard query response 0x4264 A du.e…
10 5.326371171 75.75.76.76 DNS 82 Standard query response 0x4264 A du.e…
20 7.146284234 2601:86:102 ::1 DNS 104 Standard query 0x2016 PTR 7.2.253.130…
21 7.241831955 2001:558:fe be4:d4ad:822b:… DNS 570 Standard query response 0x2016 PTR 7.…
25 7.263294061 2601:86:102 ::1 DNS 130 Standard query 0x9908 PTR 7.2.253.130…
27 7.290837014 2001:558:fe be4:d4ad:822b:… DNS 1077 Standard query response 0x9908 PTR 7.…
RESPONSE IN 27
Frame 25: 130 bytes on wire (
Ethernet II, Src: IntelCor_2f:
Internet Protocol Version 6, Sr
Transmission Control Protocol, Sr
Domain Name System (query)
[Response In: 27]
Length: 42
Transaction ID: 0x9908
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
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)


DNS_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
Transmission Control Protocol, Src Port: 53, Dst Port: 55267, Seq: 1, Ack: 45, Len: 991
Domain Name System (response)
[Request In: 25]
[Time: 0.027542953 seconds]
Length: 989
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
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)
Time to live: 86400
Data length: 4
ANSWERS IN RESPONSE
Flags (dns.flags), 2 bytes
Packets: 36 · Displayed: 12 (33.3%) · Load time: 0:0.9
Profile: Default

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?

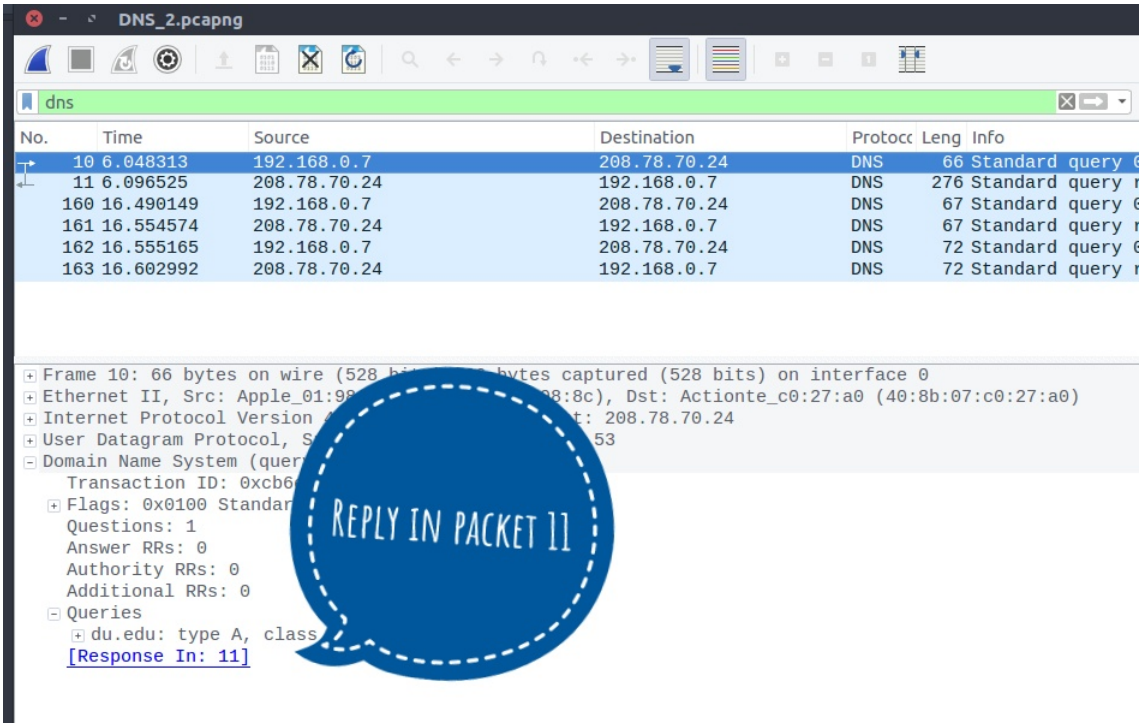
Answer The destination IP address of the server is 208.78.70.24. The request has been sent to "cpnr-authdns-dhcp-vm-1.du.edu" DNS server

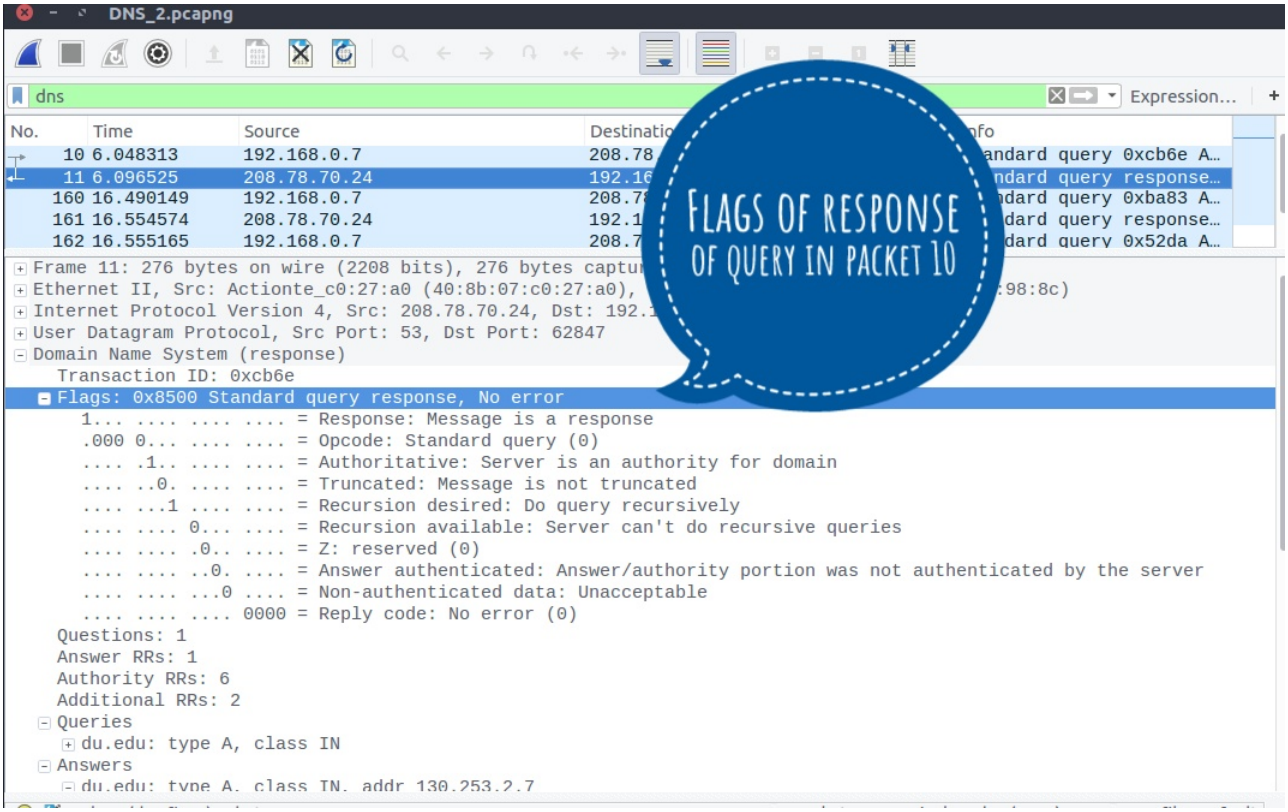


Question 2 Which packet contains the reply of the query that is sent in packet #10? Did DNS server reply ? Examine the flags of the response and what you infer from the flags?

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 which 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

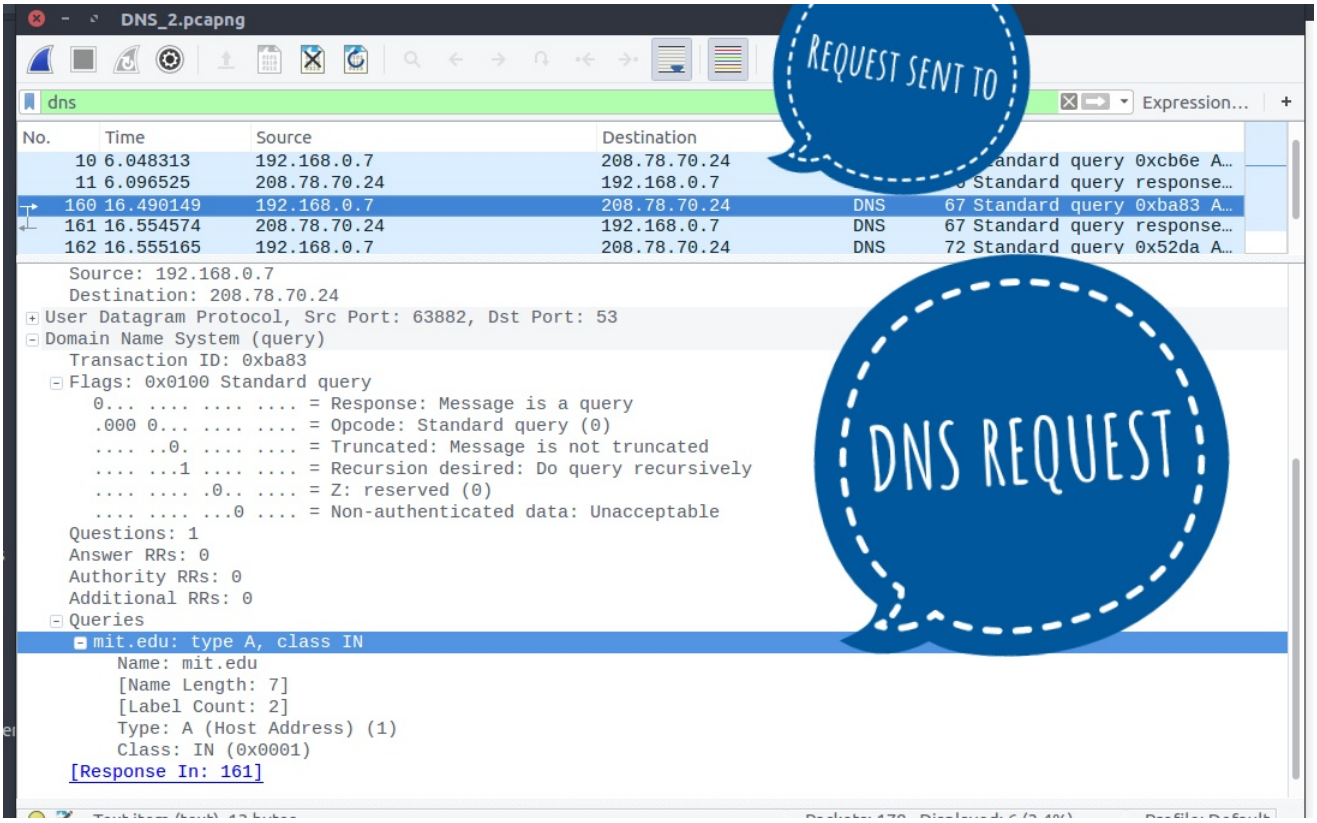
....1 .... = Recursion desired: Do query recursively
.... 0... .... = Recursion available: Server can't do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 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?

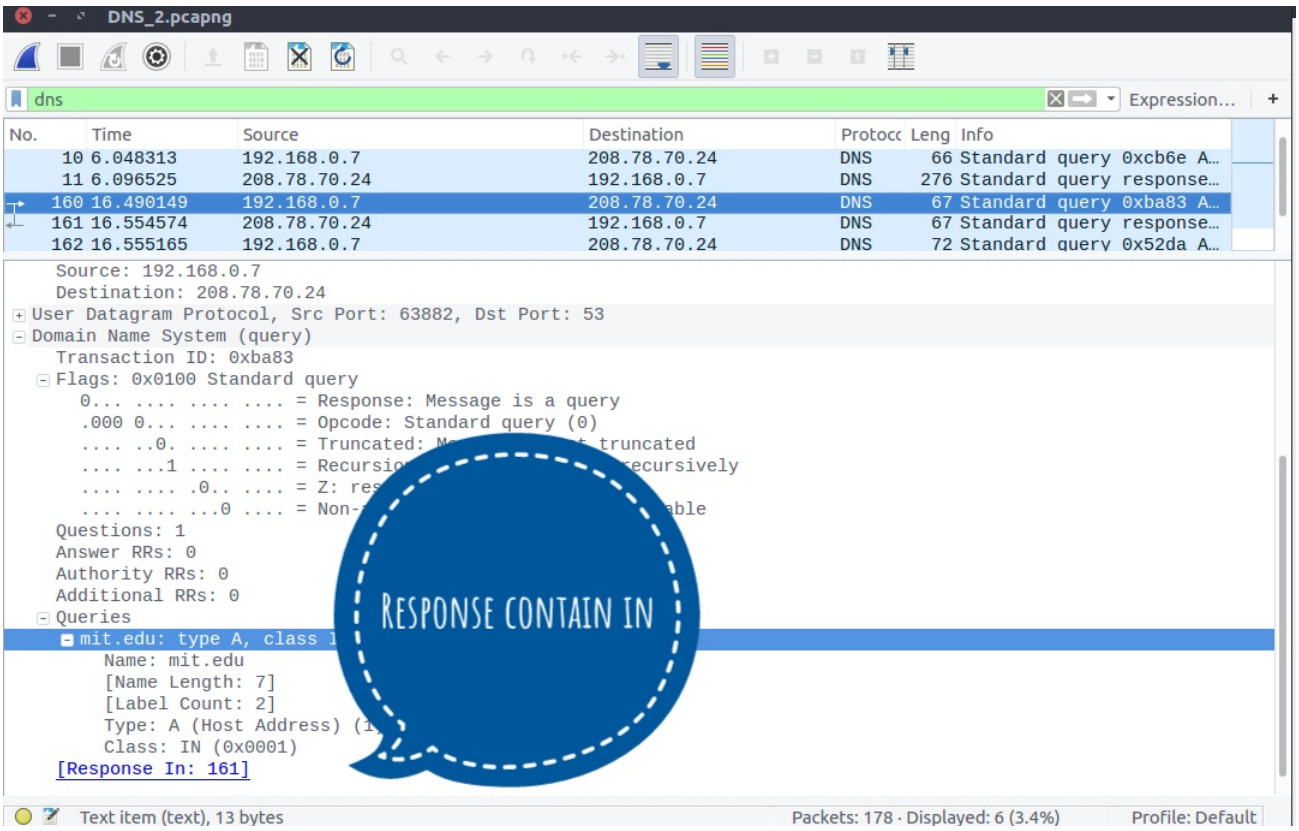
Answer The request in #160 is sent to 208.78.70.24. DNS request ask for IP address of "mit.edu".

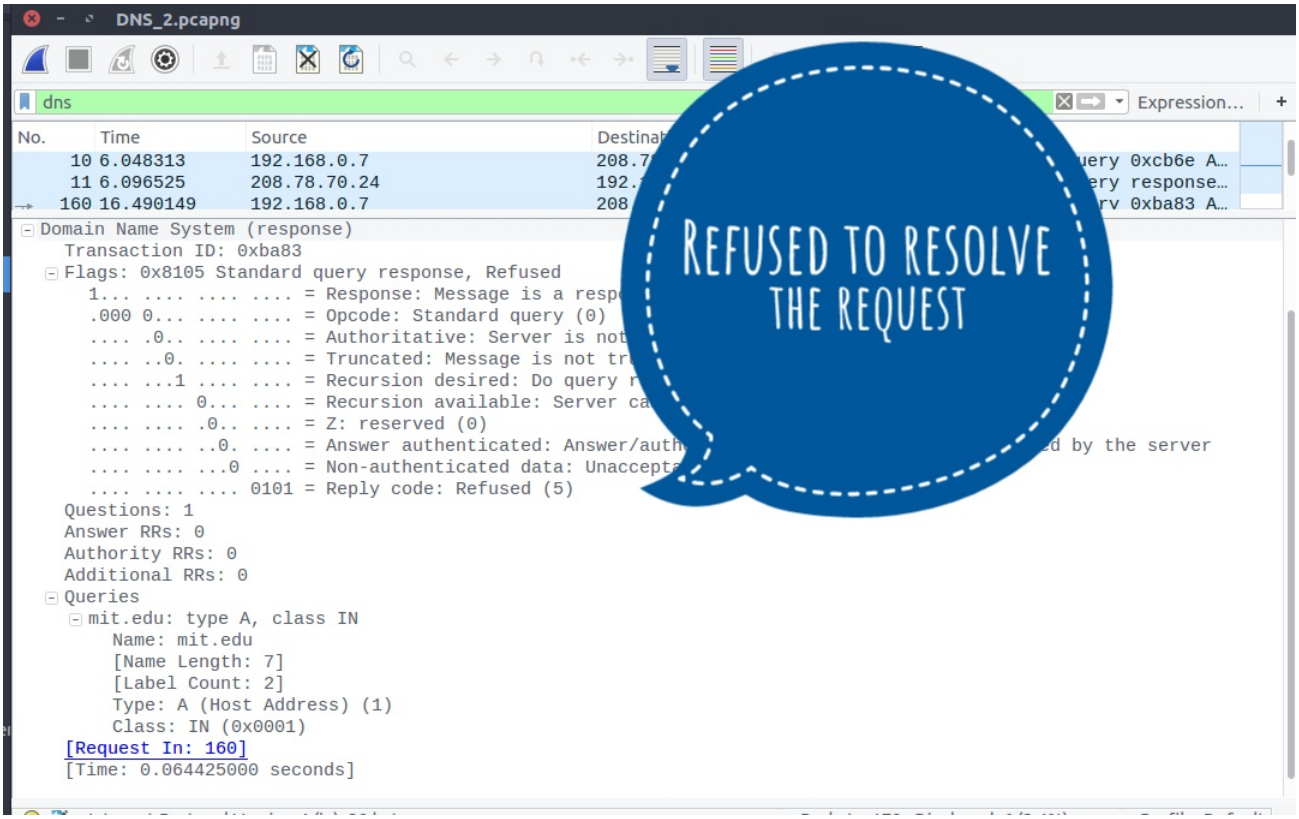


Question 4 What is the response from the DNS server in packet #160 ? Did the server resolve the DNS request? Explain in brief.

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)

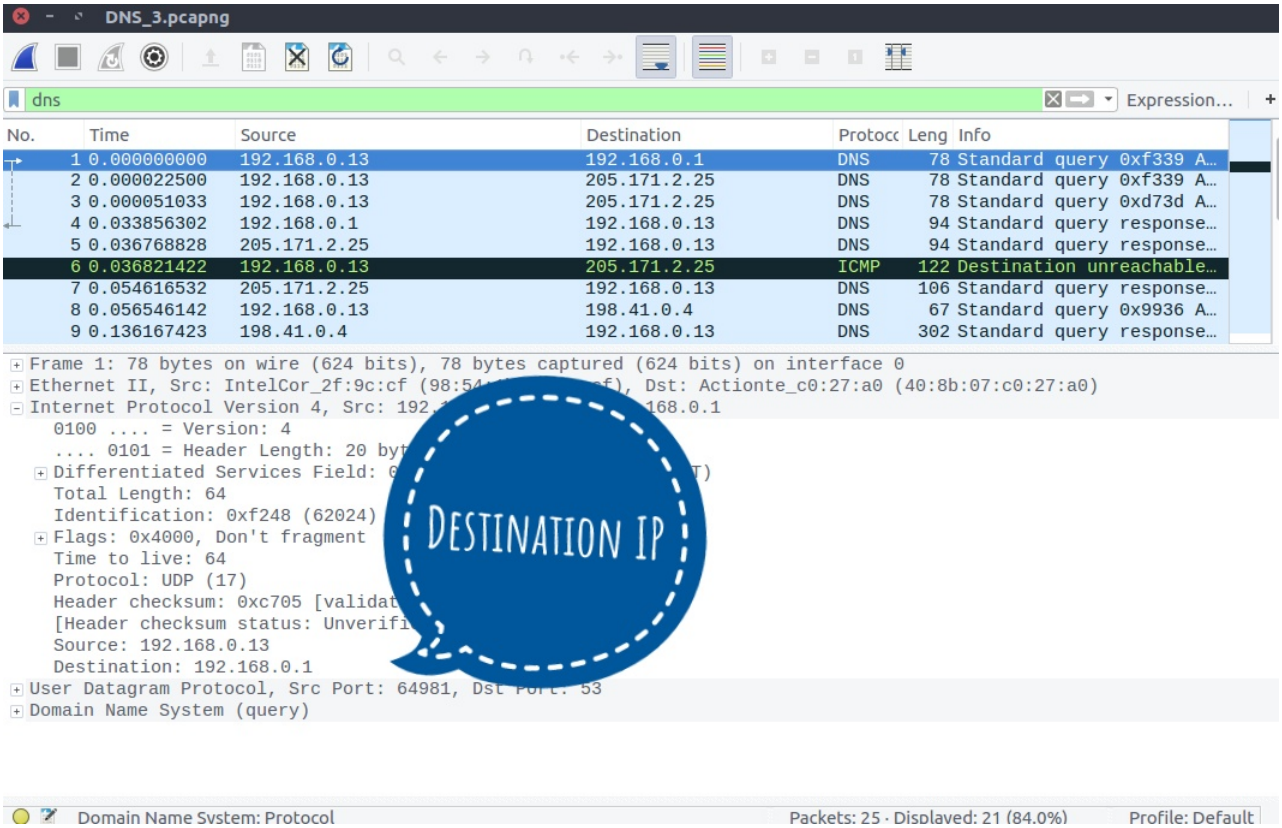




SET 3: Working with the DNS 3.pcapng

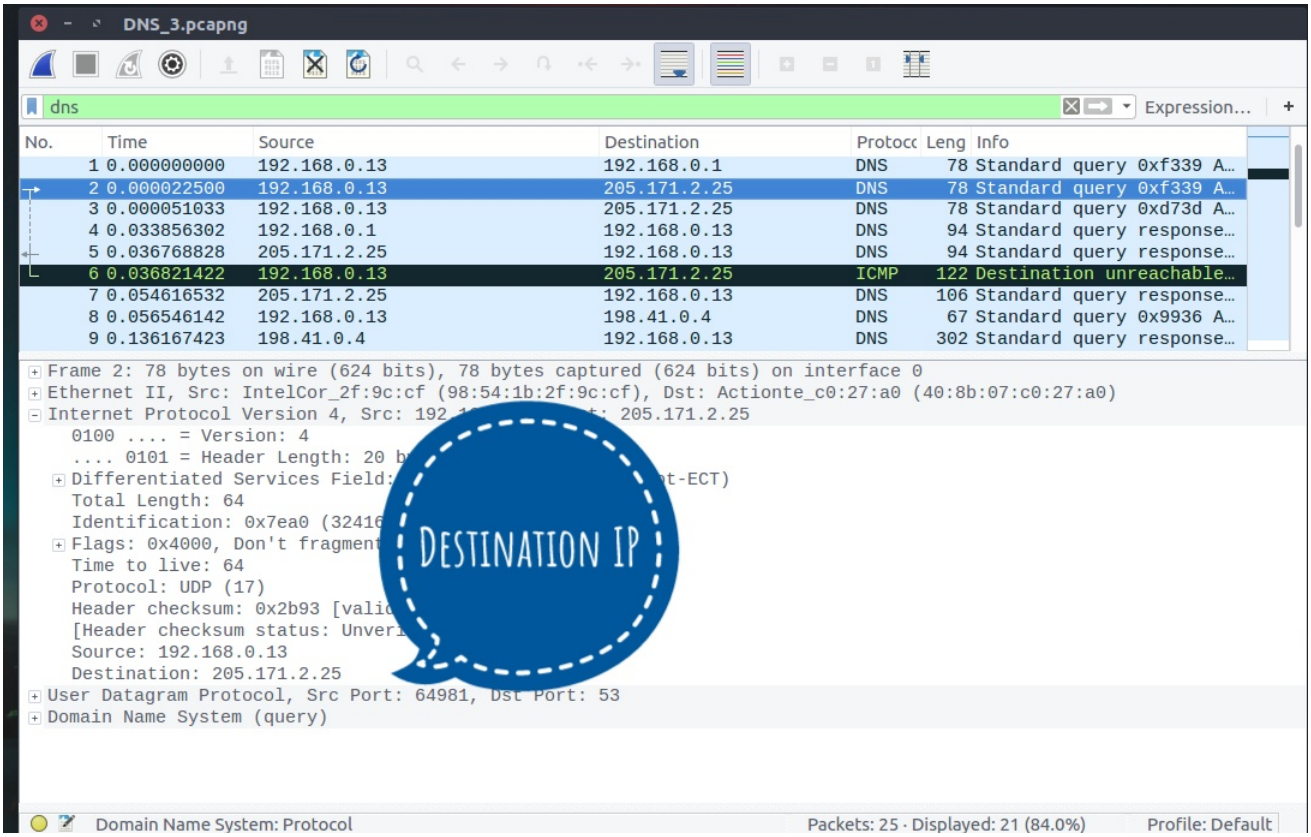
Question 1 To what IP address, is the DNS query sent in packet #1? What "type" of DNS server is that?

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



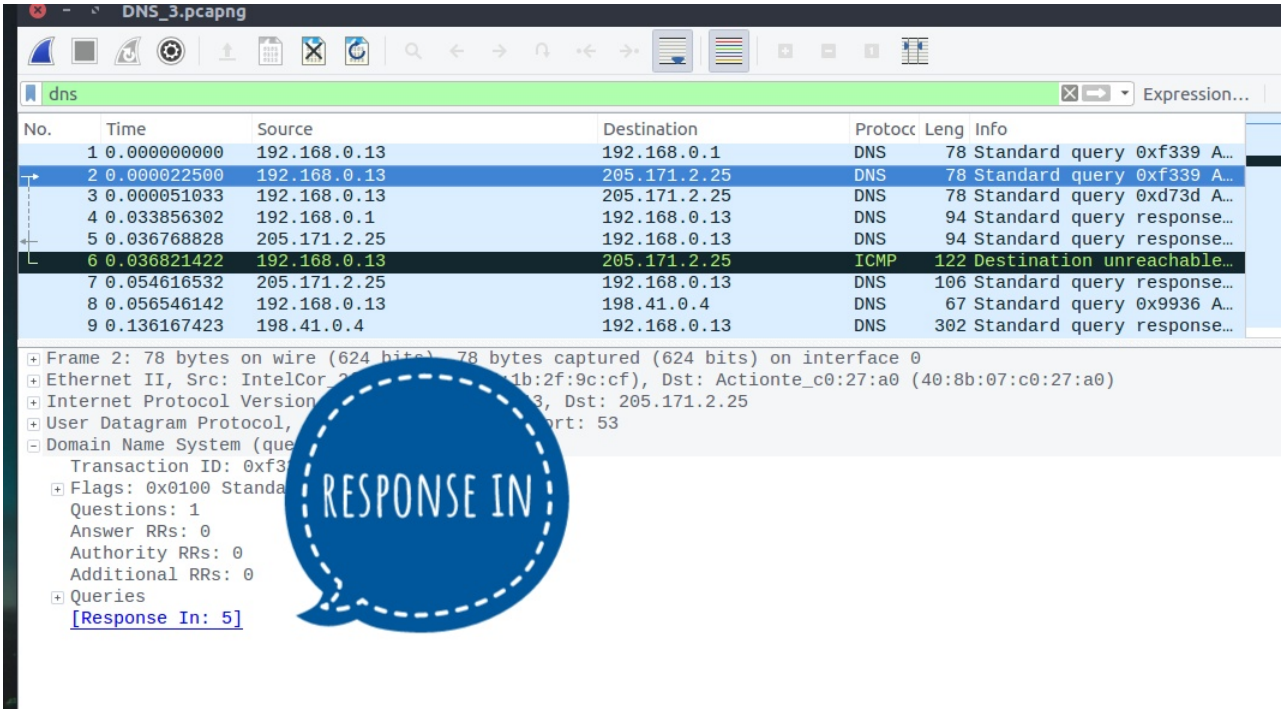
Question 2 To what IP address, is the DNS query sent in packet #2? What "type" of DNS server is that?

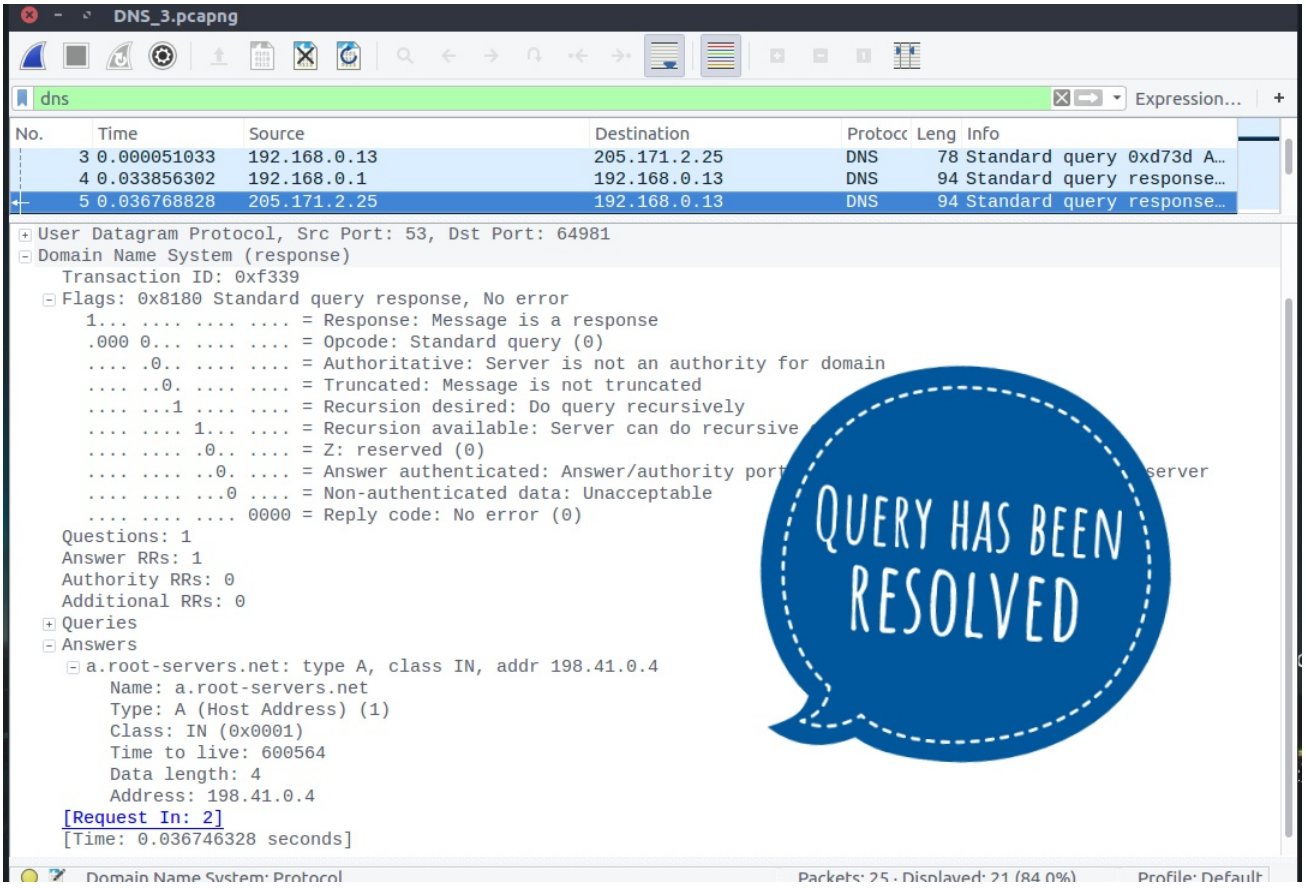
Answer The destination IP address of the server is 205.171.2.25. The DNS server type is "Local server".



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

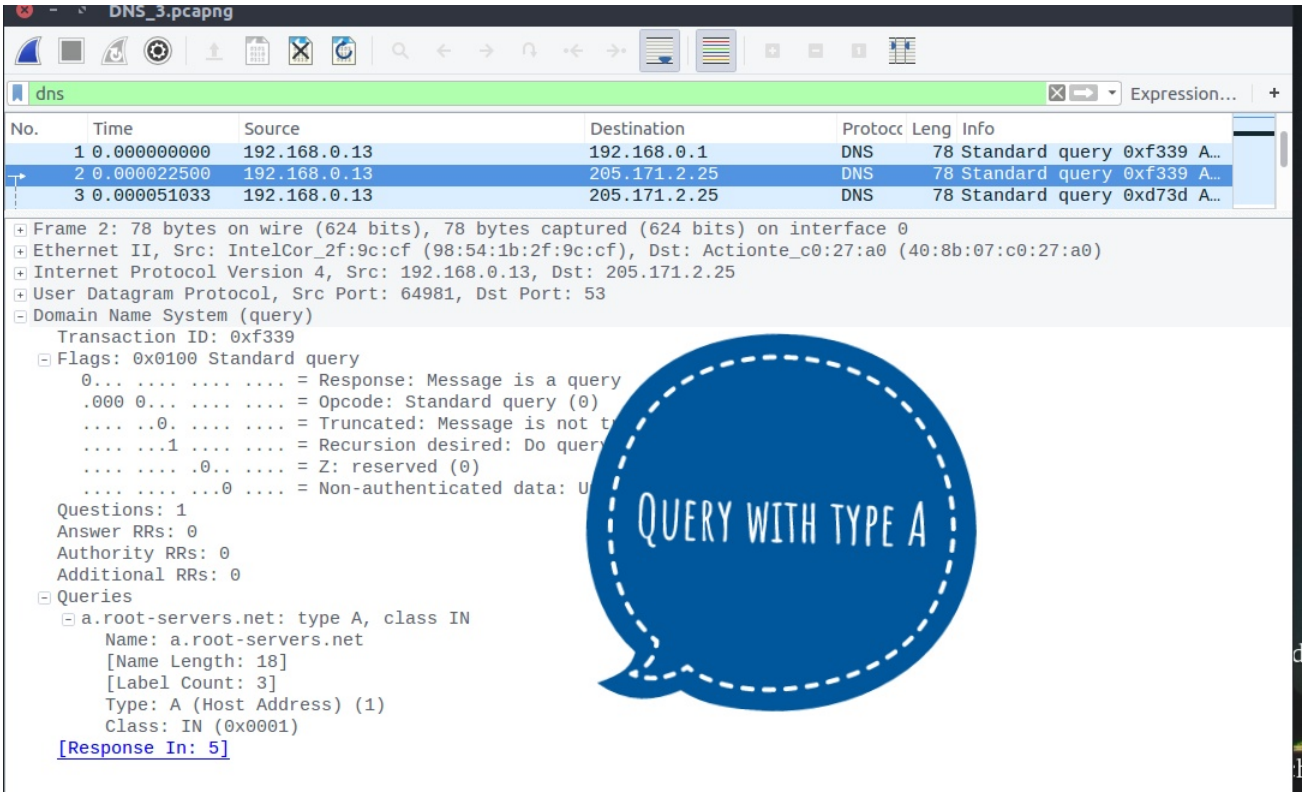
Answer The response of query in packet #2 is contains in packet number #5. The query has been resolved and answered.

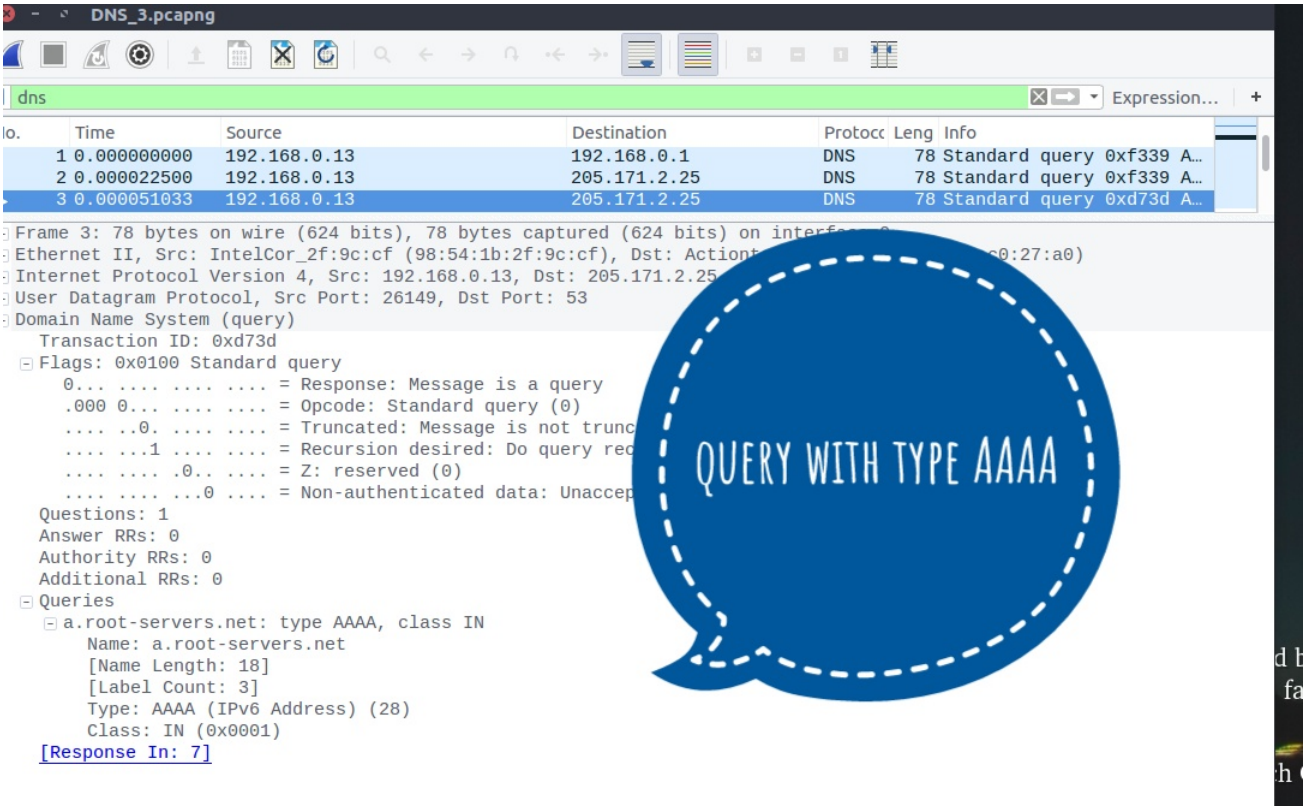

DNS_3.pcapng
dns
Expression…
No. Time Source Destination Protocc Leng Info
1 0.000000000 192.168.0.13 192.168.0.1 DNS 78 Standard query 0xf339 A…
2 0.000022500 192.168.0.13 205.171.2.25 DNS 78 Standard query 0xf339 A…
3 0.000051033 192.168.0.13 205.171.2.25 DNS 78 Standard query 0xd73d A…
4 0.033856302 192.168.0.1 192.168.0.13 DNS 94 Standard query response…
5 0.036768828 205.171.2.25 192.168.0.13 DNS 94 Standard query response…
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…
9 0.136167423 198.41.0.4 192.168.0.13 DNS 302 Standard query response…
Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: IntelCor
1b:2f:9c:cf), Dst: Actionte_c0:27:a0 (40:8b:07:c0:27:a0)
Internet Protocol Version
3, Dst: 205.171.2.25
User Datagram Protocol,
rt: 53
Domain Name System (que
Transaction ID: 0xf3
Flags: 0x0100 Standa
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 5]
RESPONSE IN


DNS_3.pcapng
dns
Expression…
No. Time Source Destination Protocc Leng Info
3 0.000051033 192.168.0.13 205.171.2.25 DNS 78 Standard query 0xd73d A…
4 0.033856302 192.168.0.1 192.168.0.13 DNS 94 Standard query response…
5 0.036768828 205.171.2.25 192.168.0.13 DNS 94 Standard query response…
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
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority port
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
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]
[Time: 0.036746328 seconds]
QUERY HAS BEEN RESOLVED

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

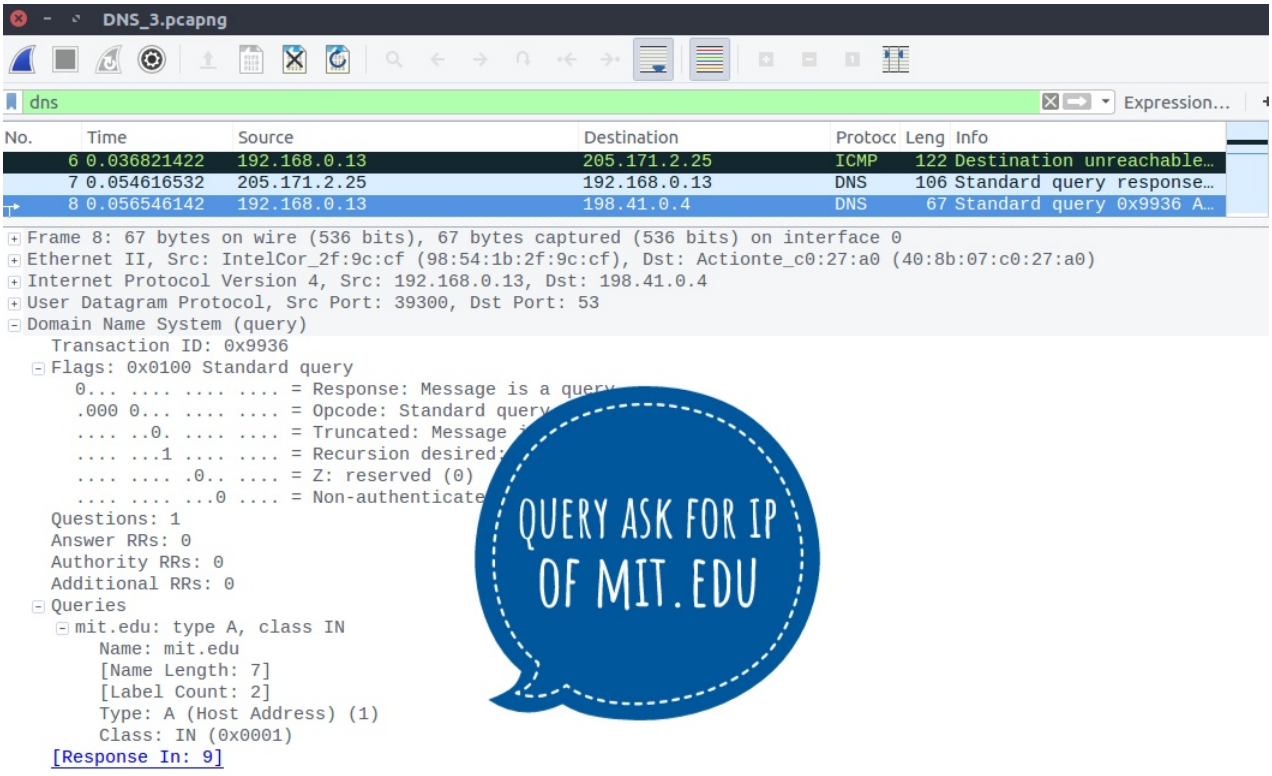
Answer The difference between the queries is that packet #2 have "type A" which gives IPv4 address, On the other hand, query in packet #3 have "type AAAA" which gives IPv6 address in response.





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.

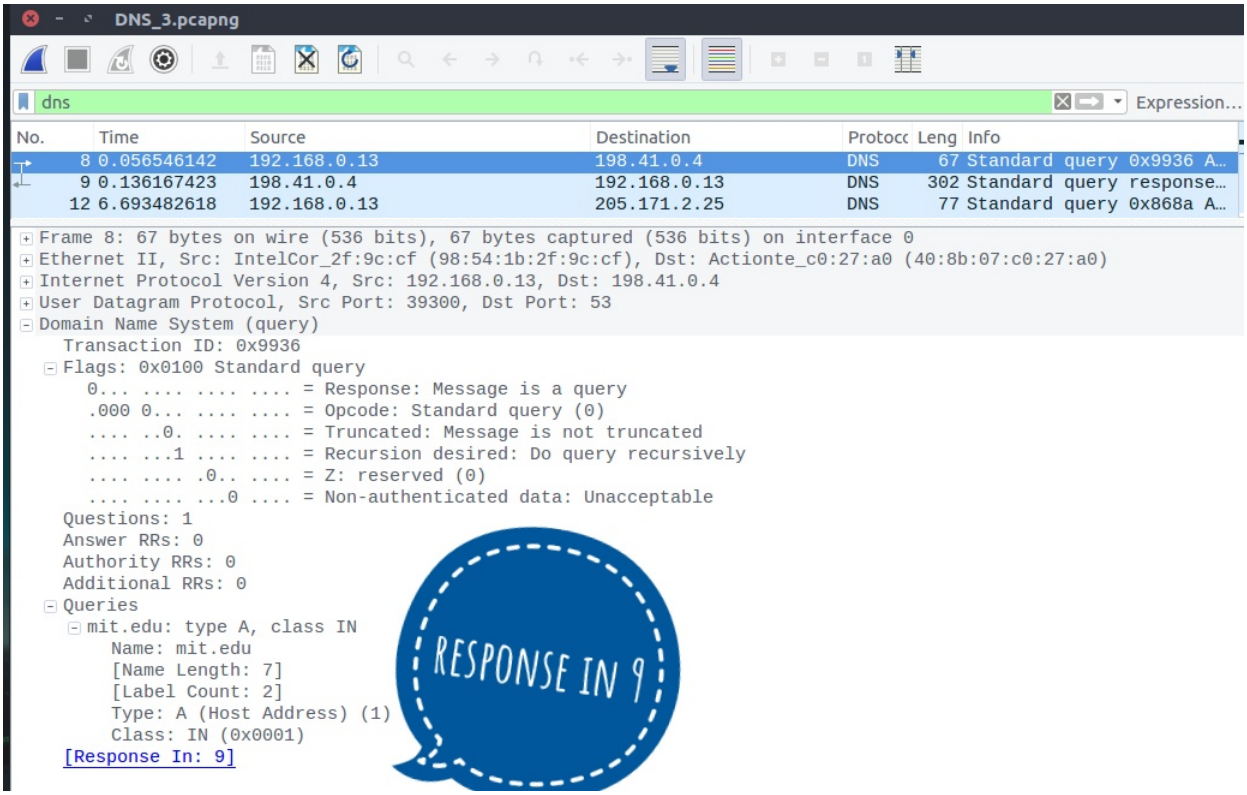


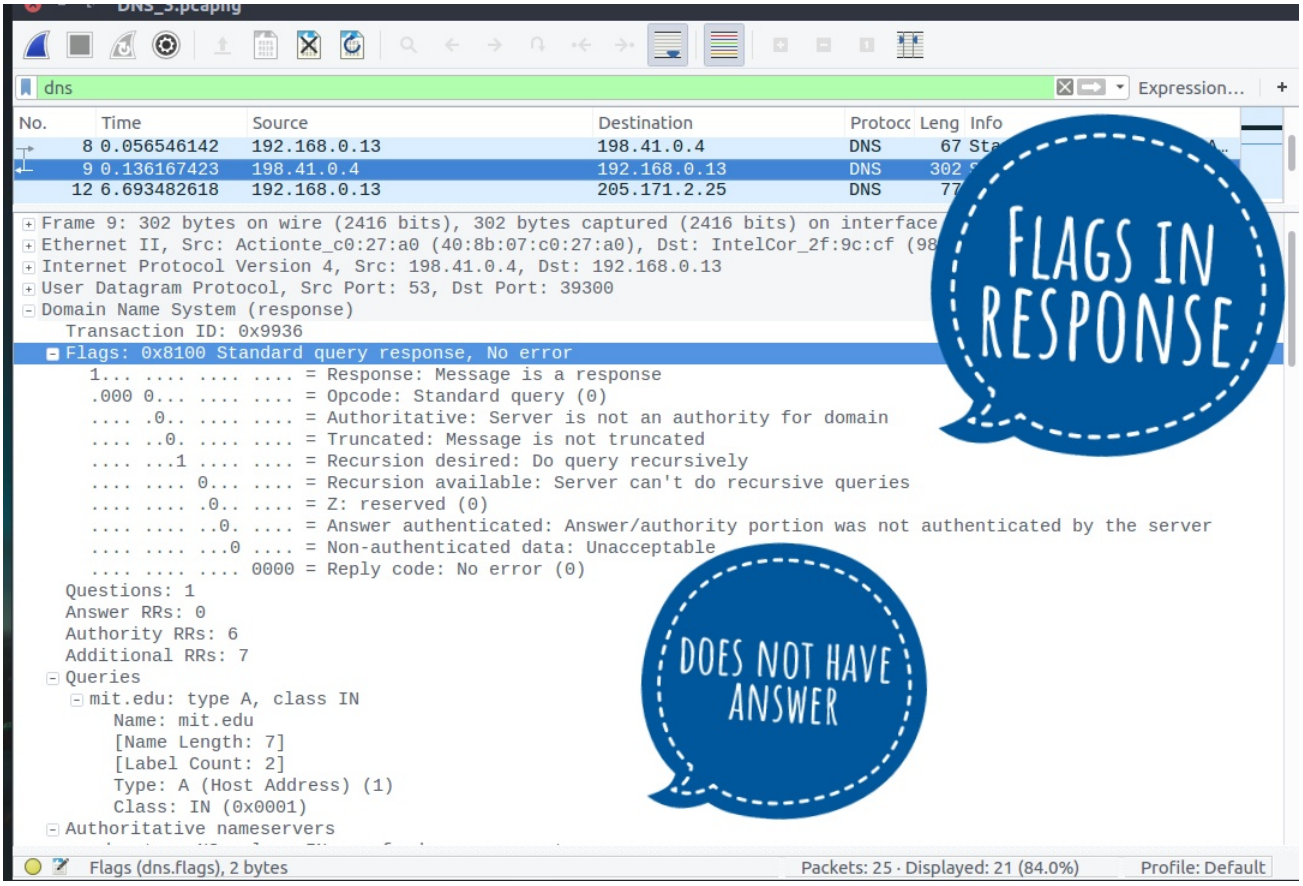
Question 6 Which packet contains the response of the query sent in packet #8? What flags are set in this response? Does it have the answer user wants? What information does it provide?

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 ?

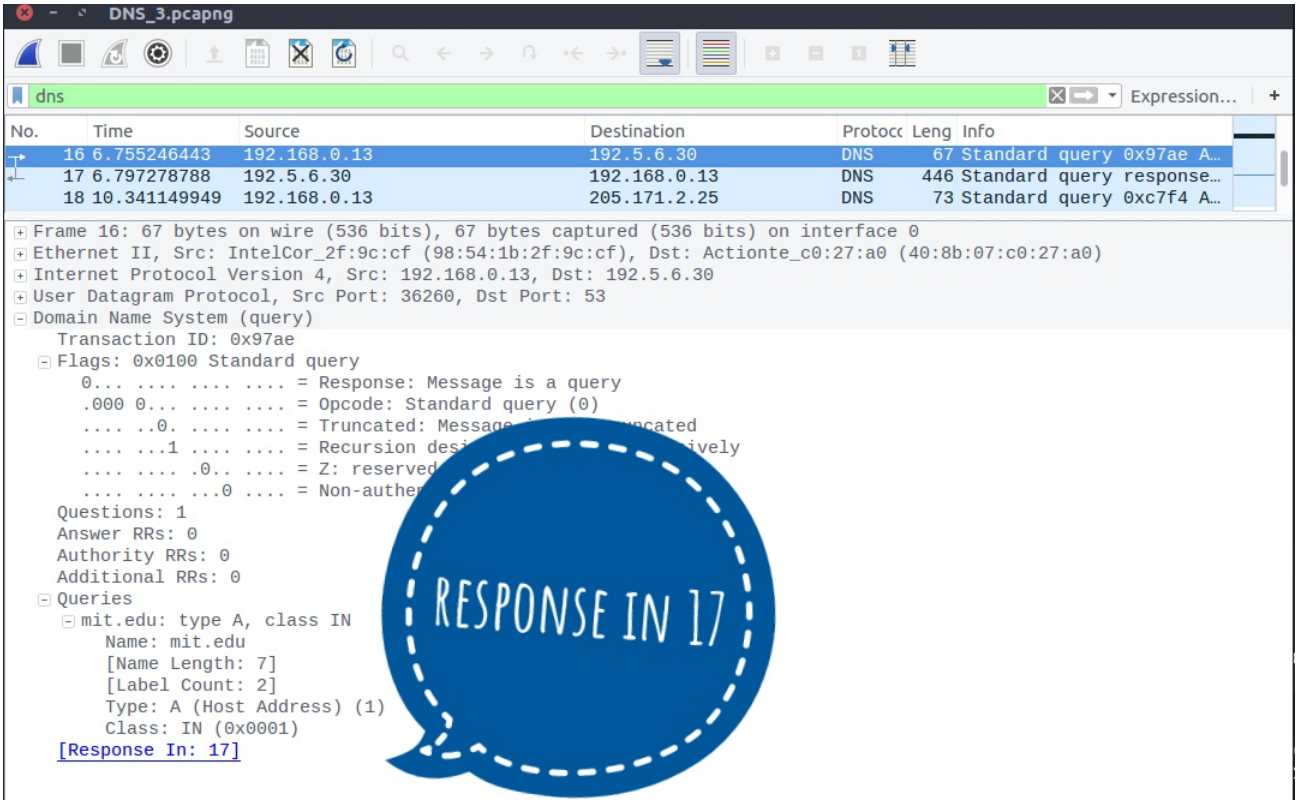
Answer The server which has been quired is a.gtld-servers.net. No, it is not local server.

```
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?

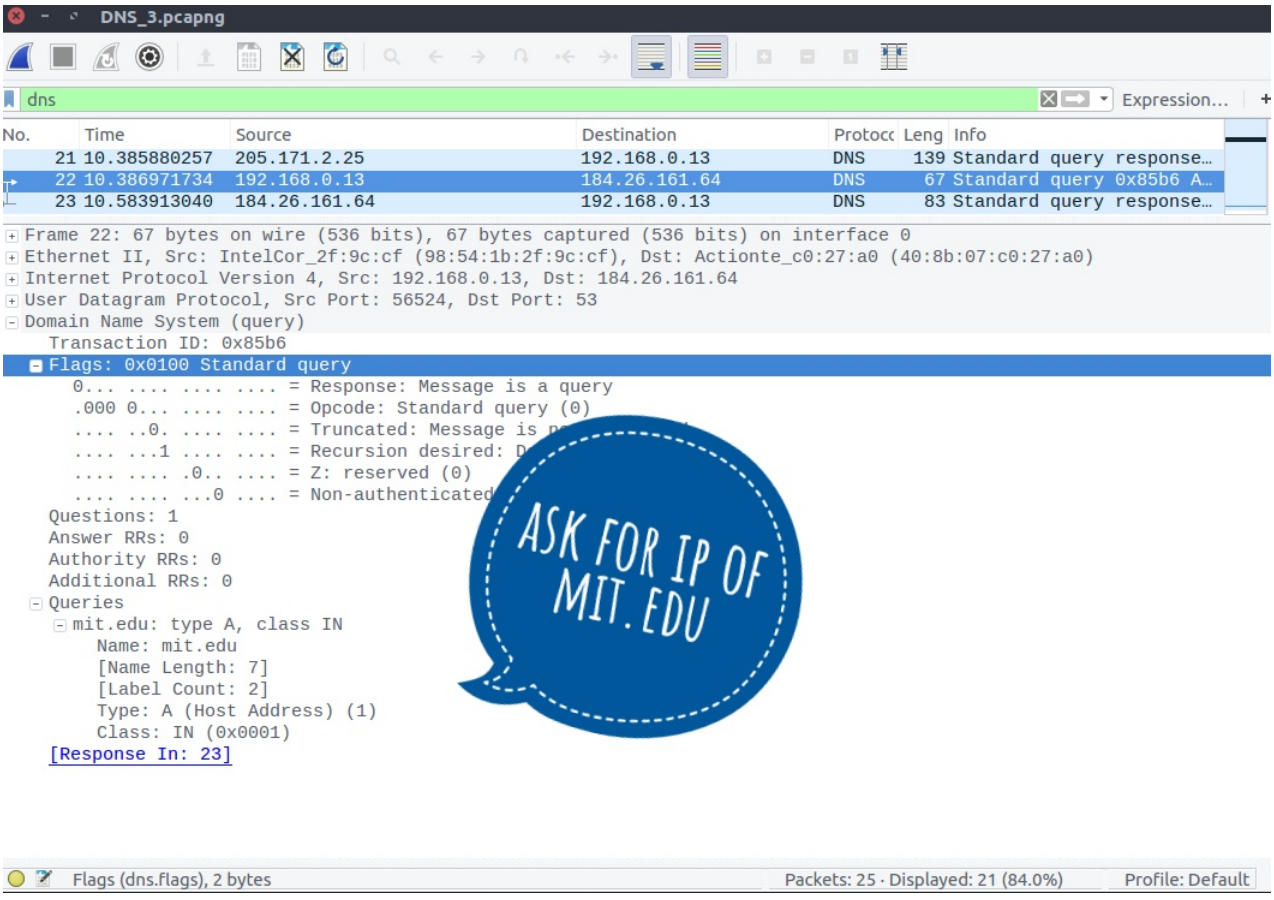
What information does it provide?

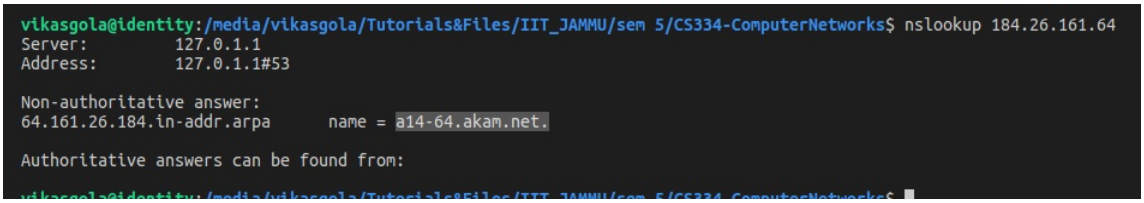
Answer The response of query of the packet #16 is contains in packet #17. The flags in the response is as follows:
Flags: 0x8100 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority 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 quired is a14-64.akam.net.

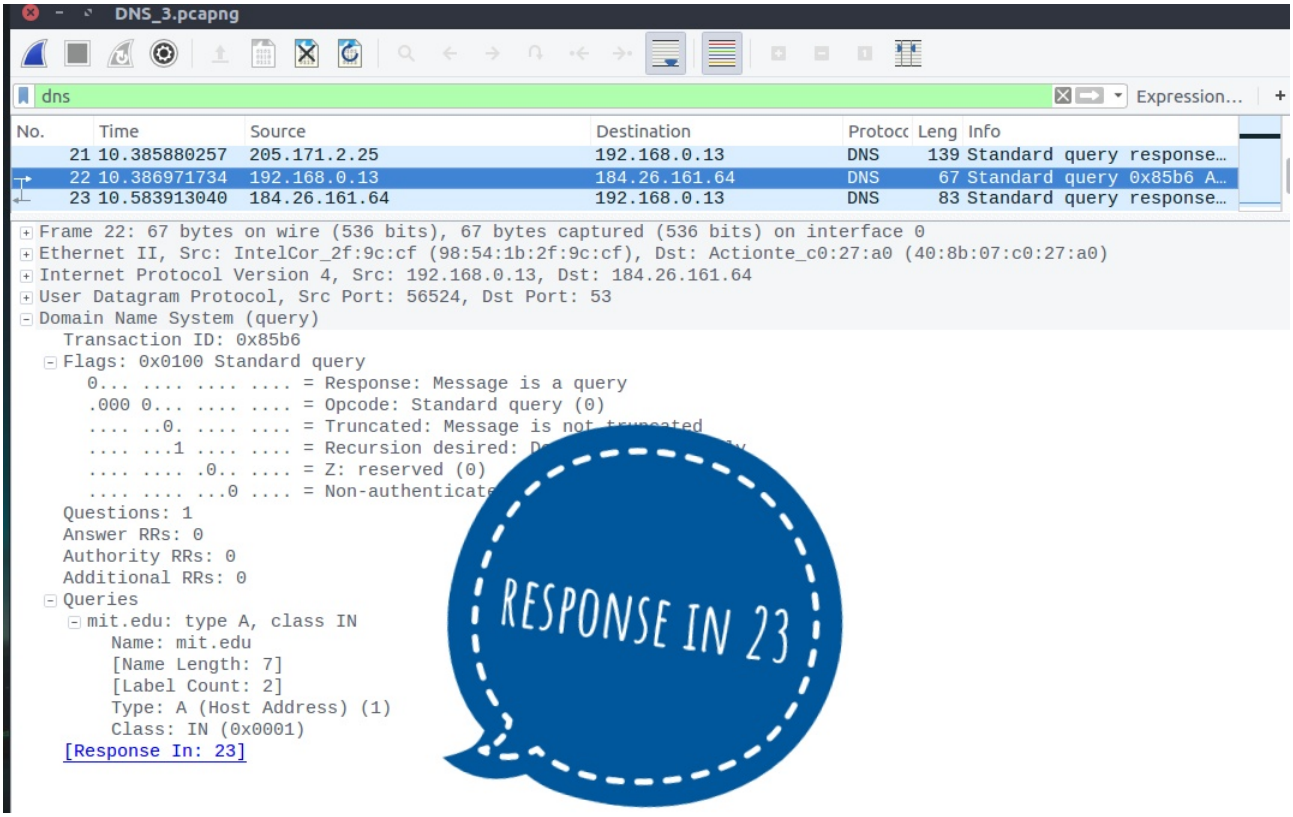


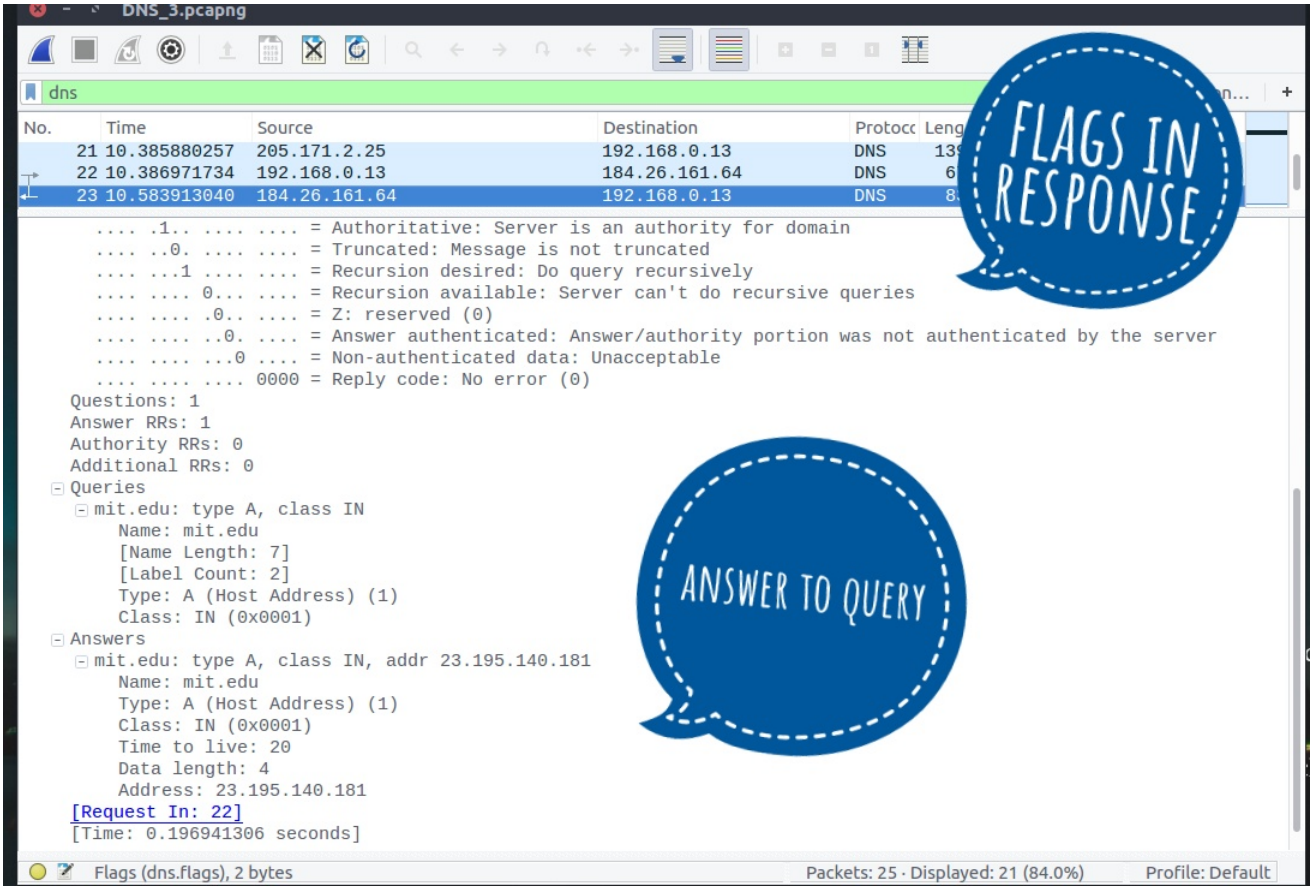


Question 10 Which packet contains the response to the query sent in packet #22? What flags are set in this response? Does it have the answer user wants? What information does it provide?

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".

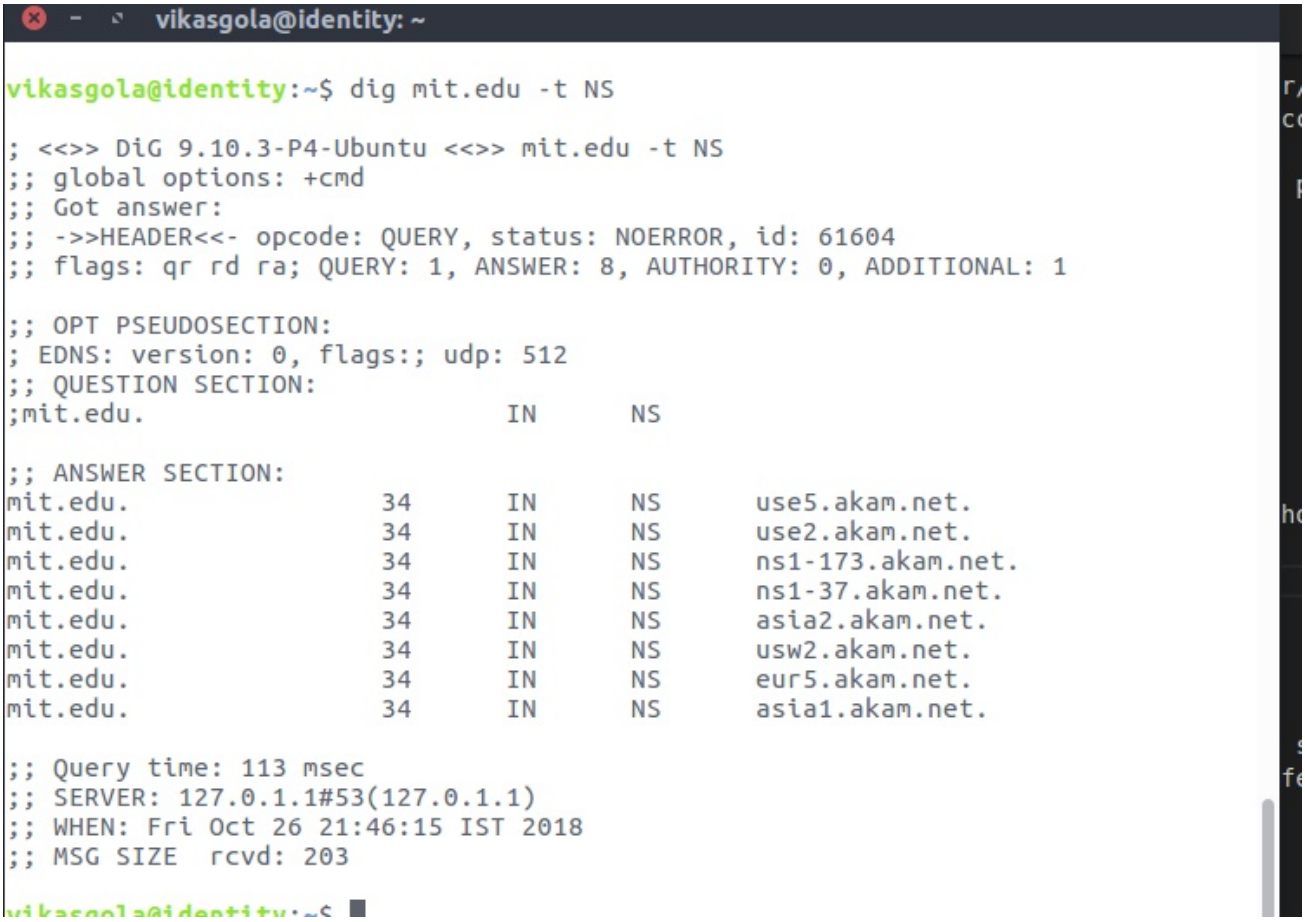




SET 4 - Using dig command

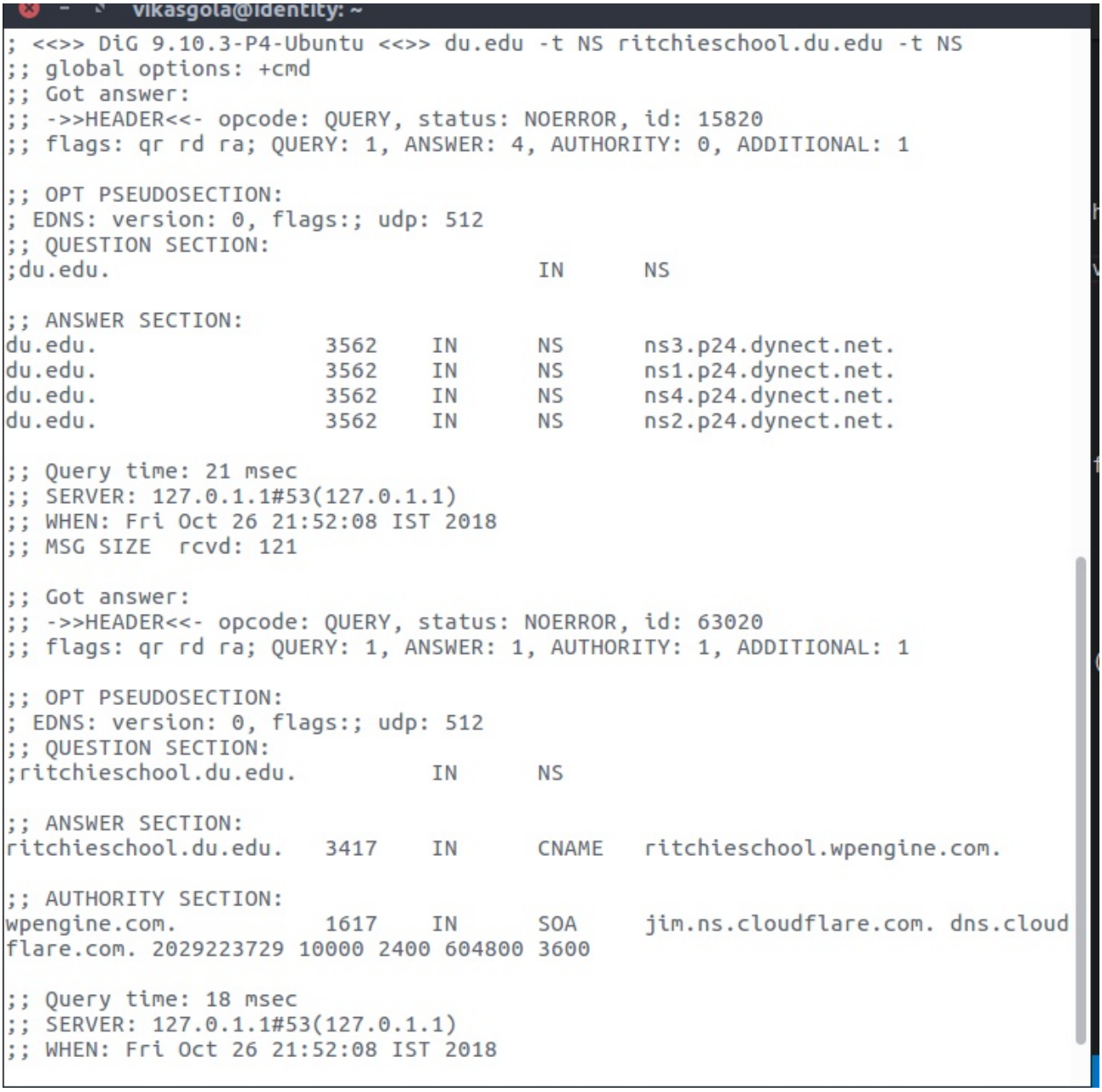
Question 1 What is the dig command used to determine the authoritative DNS servers for www.mit.edu?

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



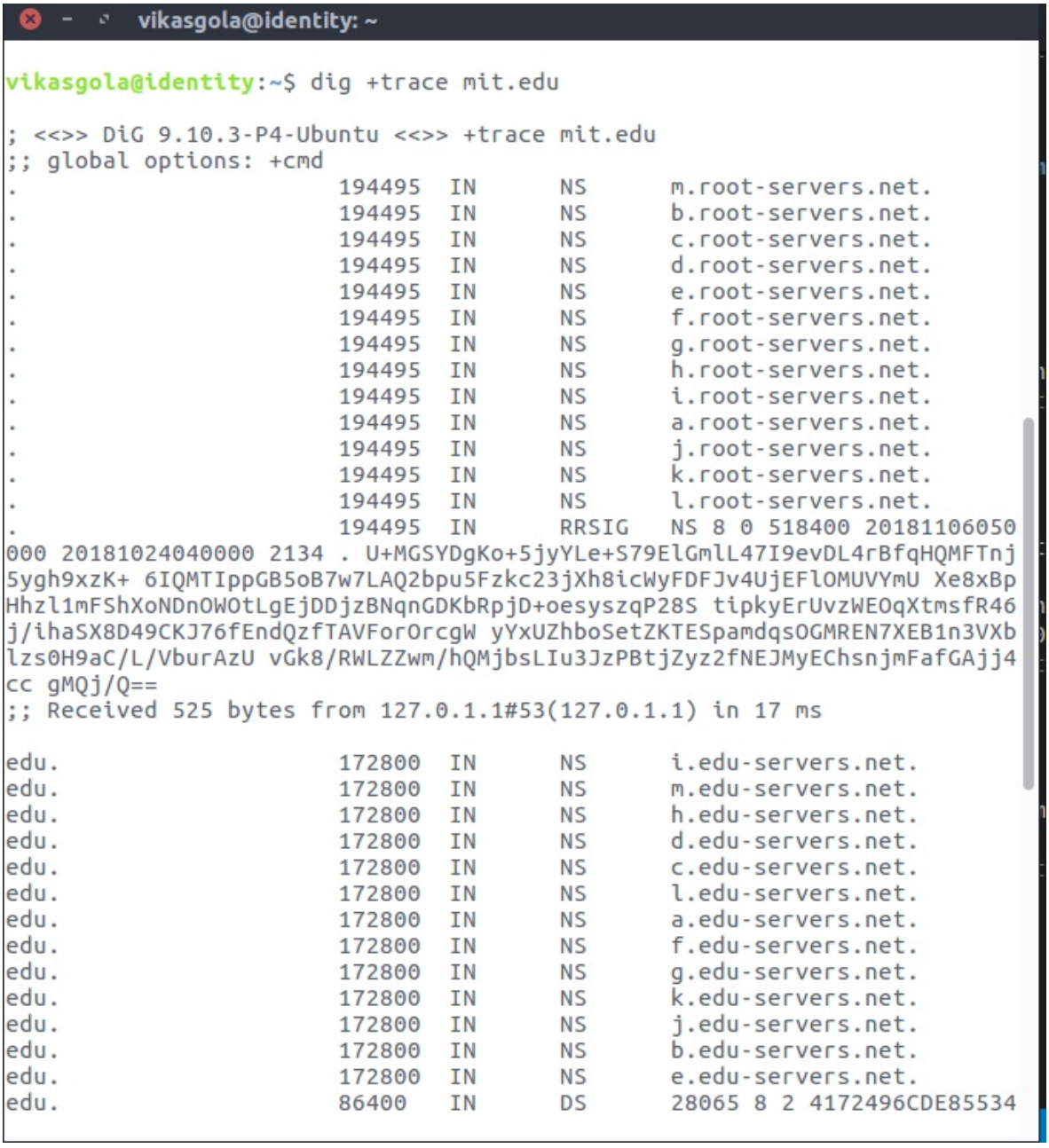
Question 2 Using dig command determine the authoritative DNS servers for www.du.edu and www.ritchieschool.du.edu in a single dig command? Are DNS servers for both different?

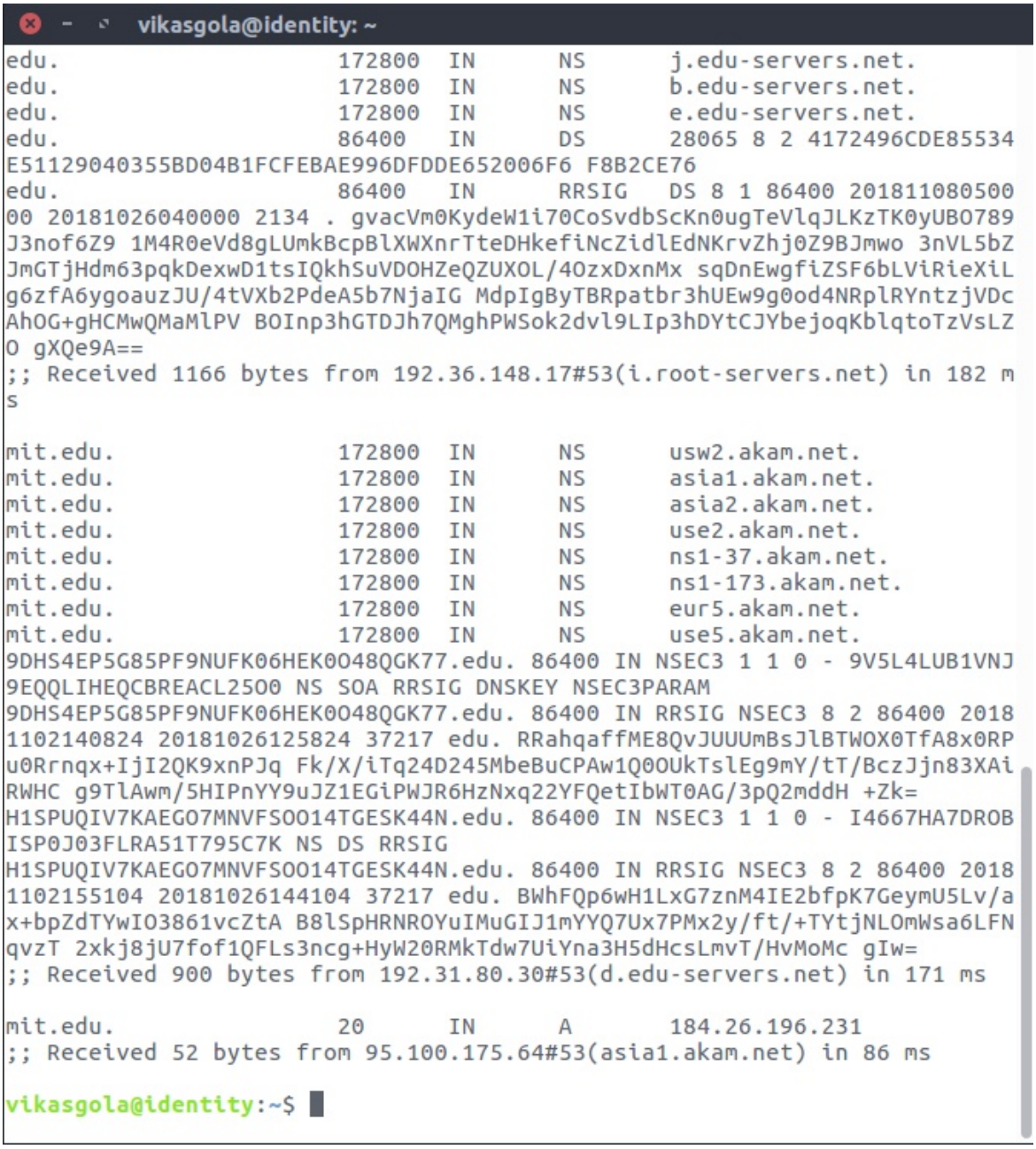
Answer The dig command used to determine the authoritative DNS servers for www.du.edu and www.ritchieschool.du.edu is dig du.edu -t NS ritchieschool.du.edu -t NS. Yes, both have different DNS servers.



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: ~
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
Hhzl1mFShXoNDnOWOtLgEjDDjzBNqnGDKbRpjD+oesyszqP28S tipkyErUvzWEOqXtmsfR46
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



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