**Balwinder Singh Hayer**

**Computer Communications**

**CPSC 471-04**

**LAB – 02-B**

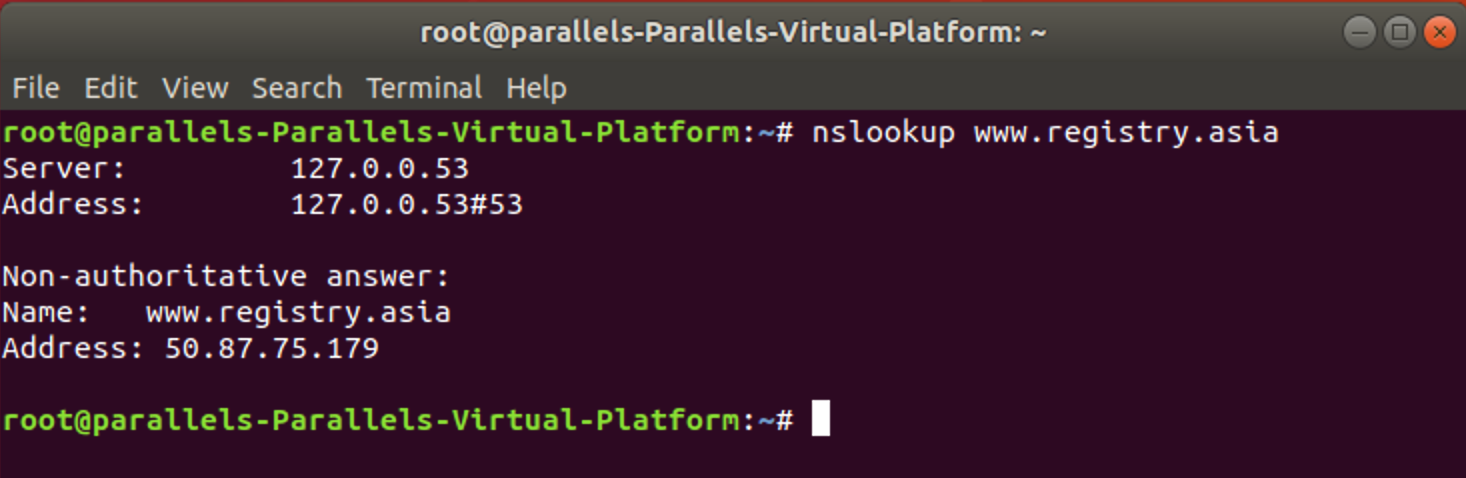
**Due – FRI 08 2019**

1. nslookup

Now that we have provided an overview of *nslookup*, it is time for you to test drive it yourself. Do the following (and write down the results):

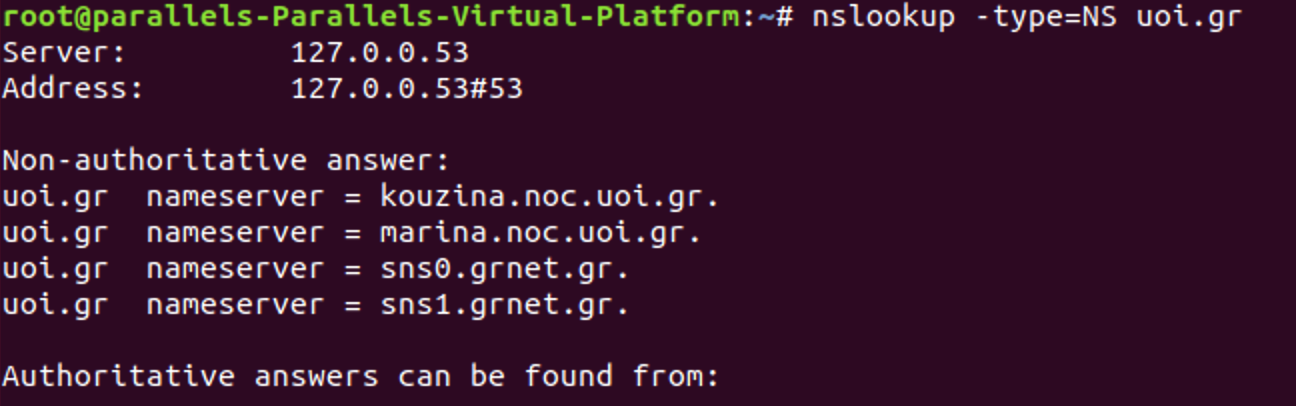
1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?

IP Address: 127.0.0.53



1. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

University in Europe: uoi.gr



1. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

The IP address of the mail server is 18.72.0.3.



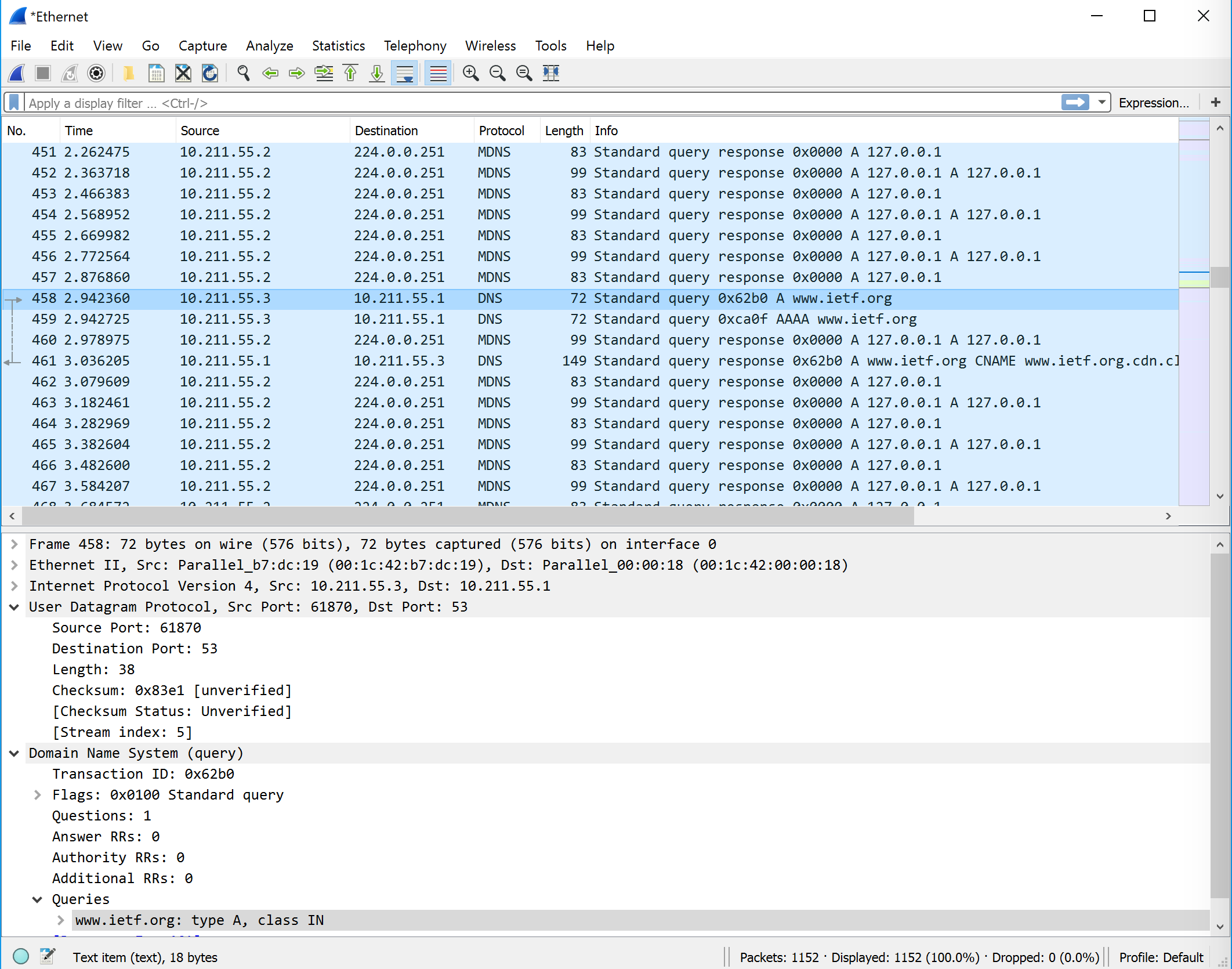
3. Tracing DNS with Wireshark

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Ans:

DNS query and response messages are sent over UDP. (User Datagram Protocol)

Queries are located at bottom.



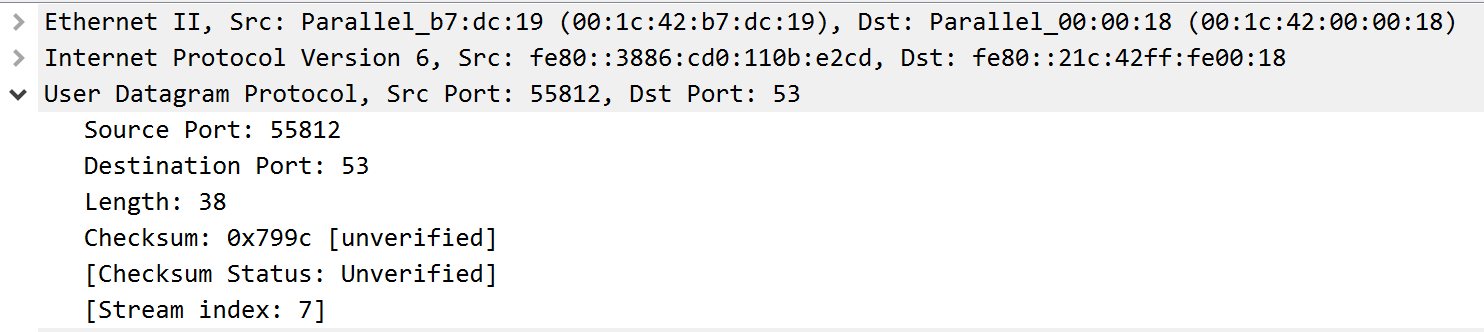
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

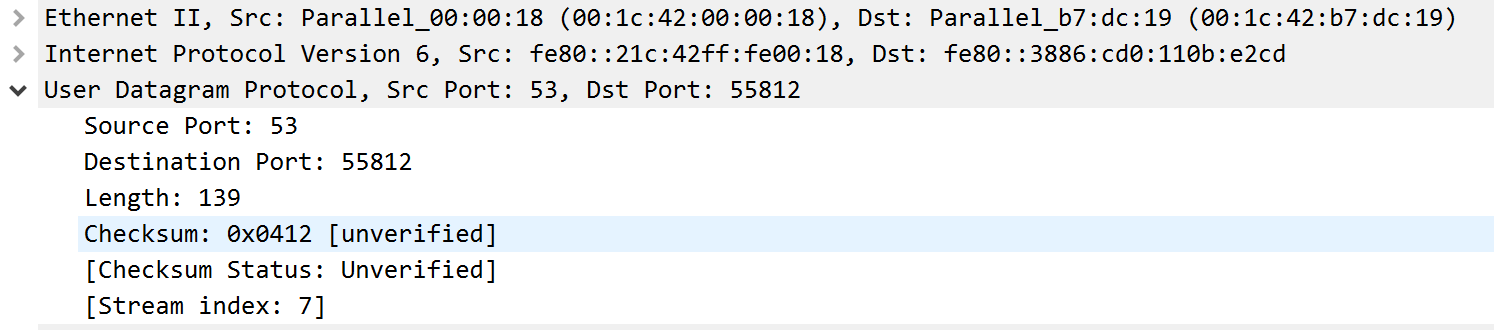
Ans:

Destination Port for the DNS query message is 53.

Source port of DNS response message is 53

[Destination port and Source port are equal in both cases.]

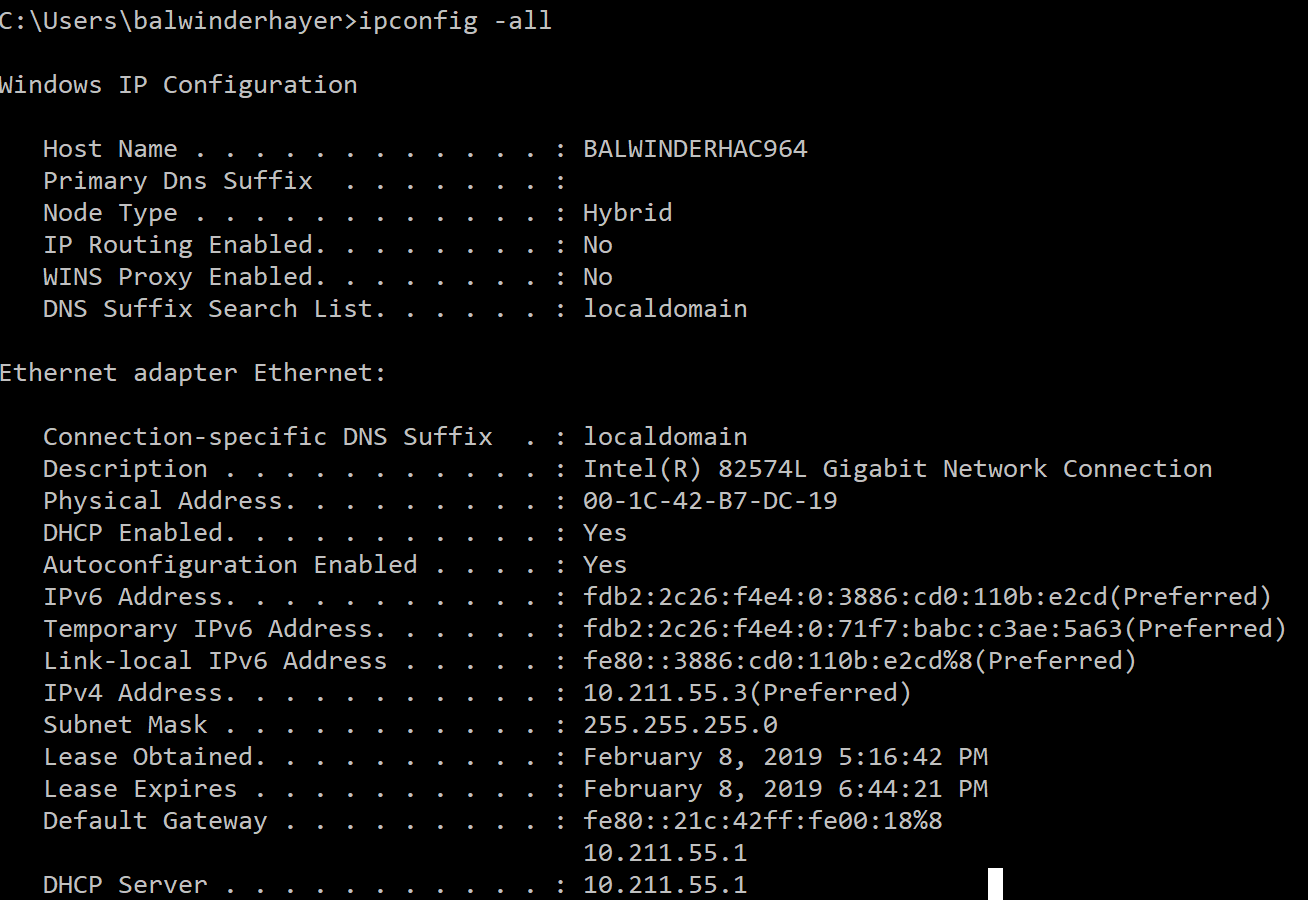




1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans:

The DNS query message was sent to 10.211.55.1 and the IP address of the local DNS server was 10.211.55.1. These two IP addresses are same.

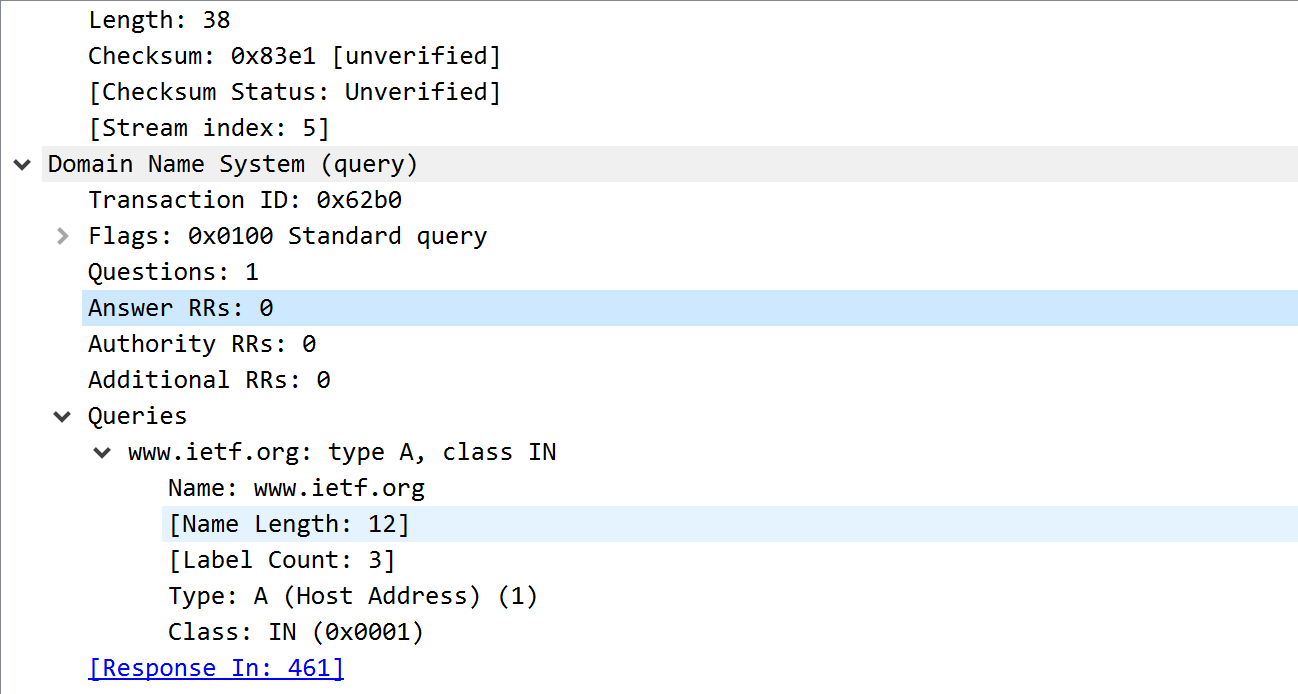


1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans:

It is a “type A” standard Query and it does not appear to contain any answers.

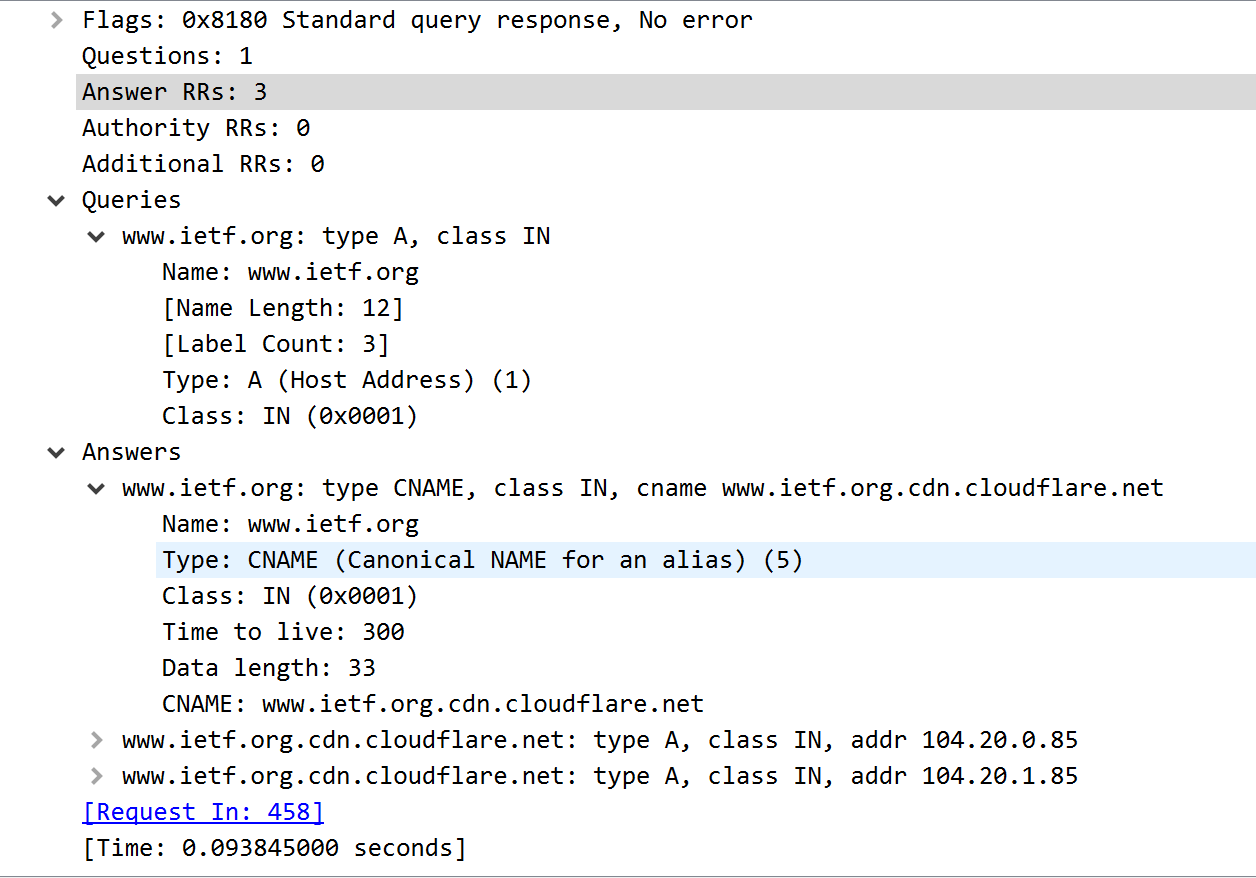
Below is the screenshot which clearly shows Type: A. and contains no answer in query.

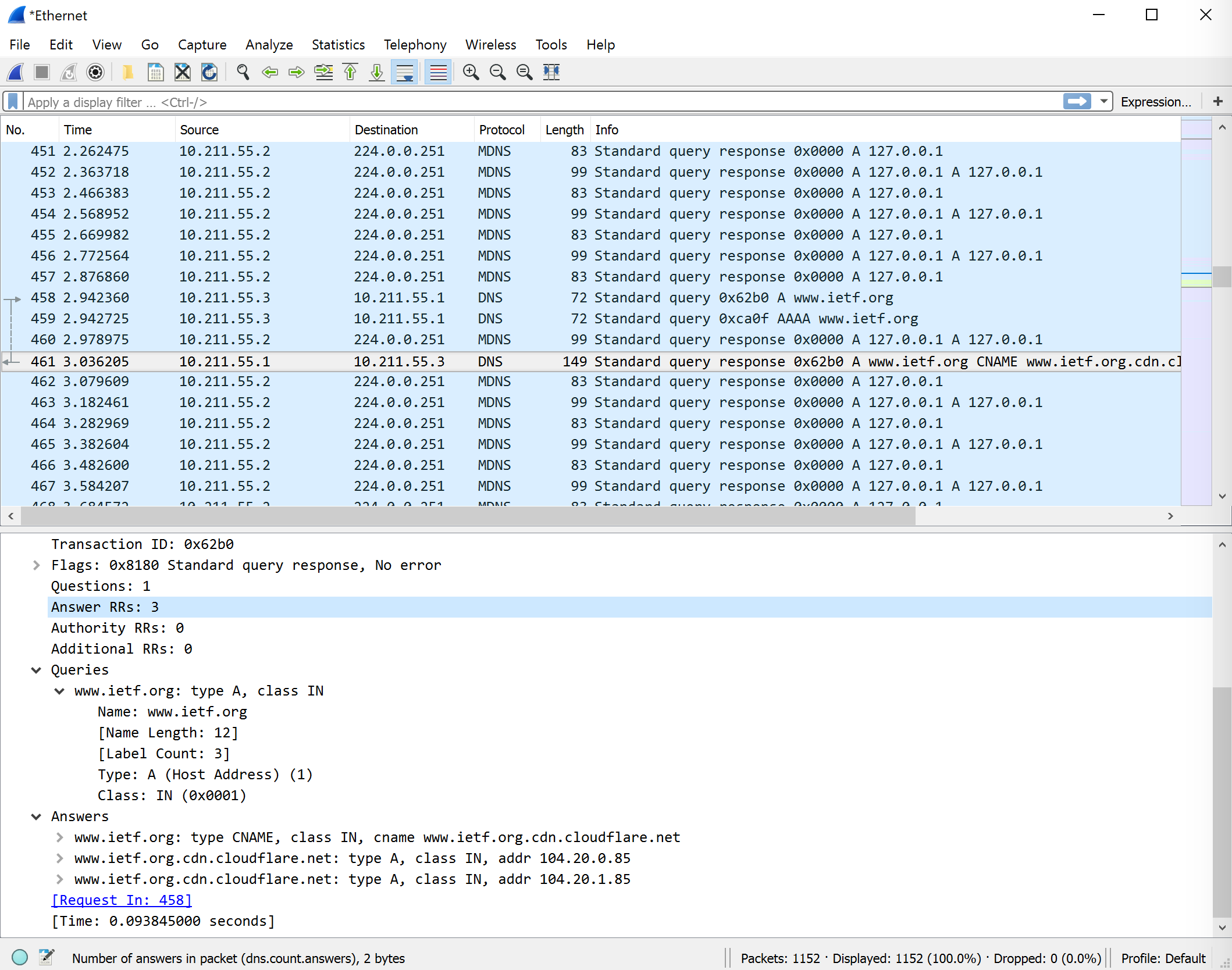


1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans:

There are total of 3 answers present in the DNS response message. Each answer represents the information about the name of the host, the type of the address, class, Time to live, data length, and cname.





1. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans: The first SYN packet was sent to 104.20.0.85 which corresponds to the first IP address provided in the DNS response message.

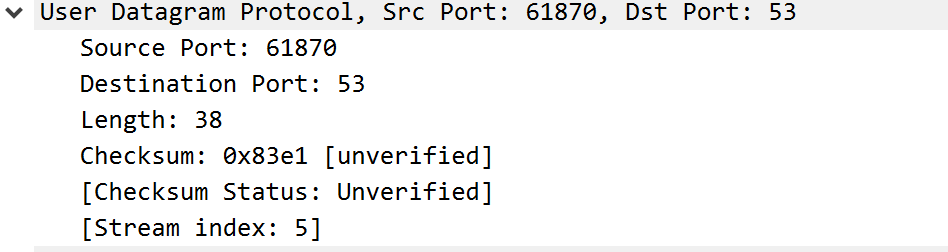
1. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

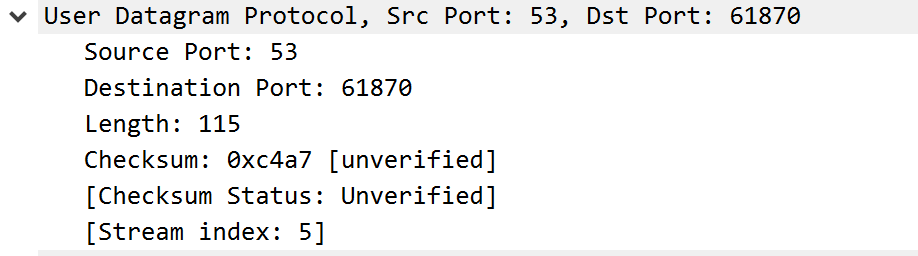
Ans: No, there is no new DNS queries before retrieving images in the web page.

1. What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans:

The destination port of the DNS query is 53 and source port of the DNS response is 53.





1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

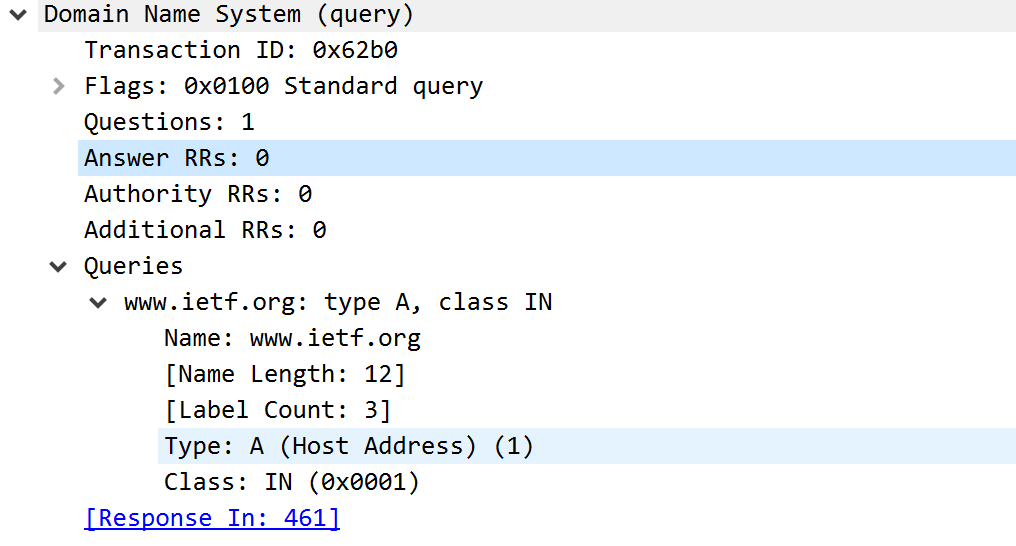
Ans: It is sent to 10.211.55.1 which as we can also see from the ipconfig -all screenshot above.

This is the IP address of my default local DNS server.

1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

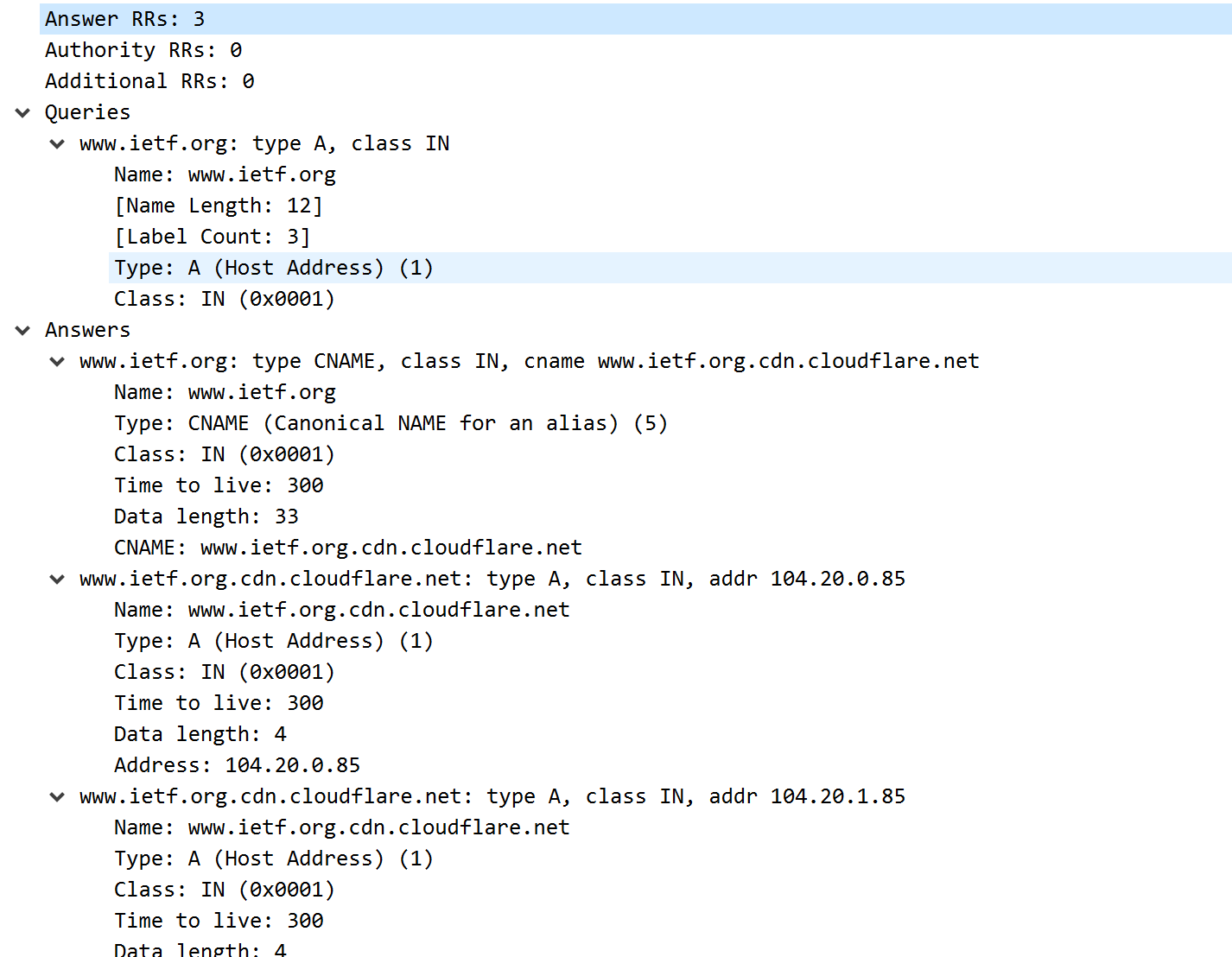
Ans: The type of DNS query is Type A. It contains no answers. It is a standard query.

Screenshot is on next page.

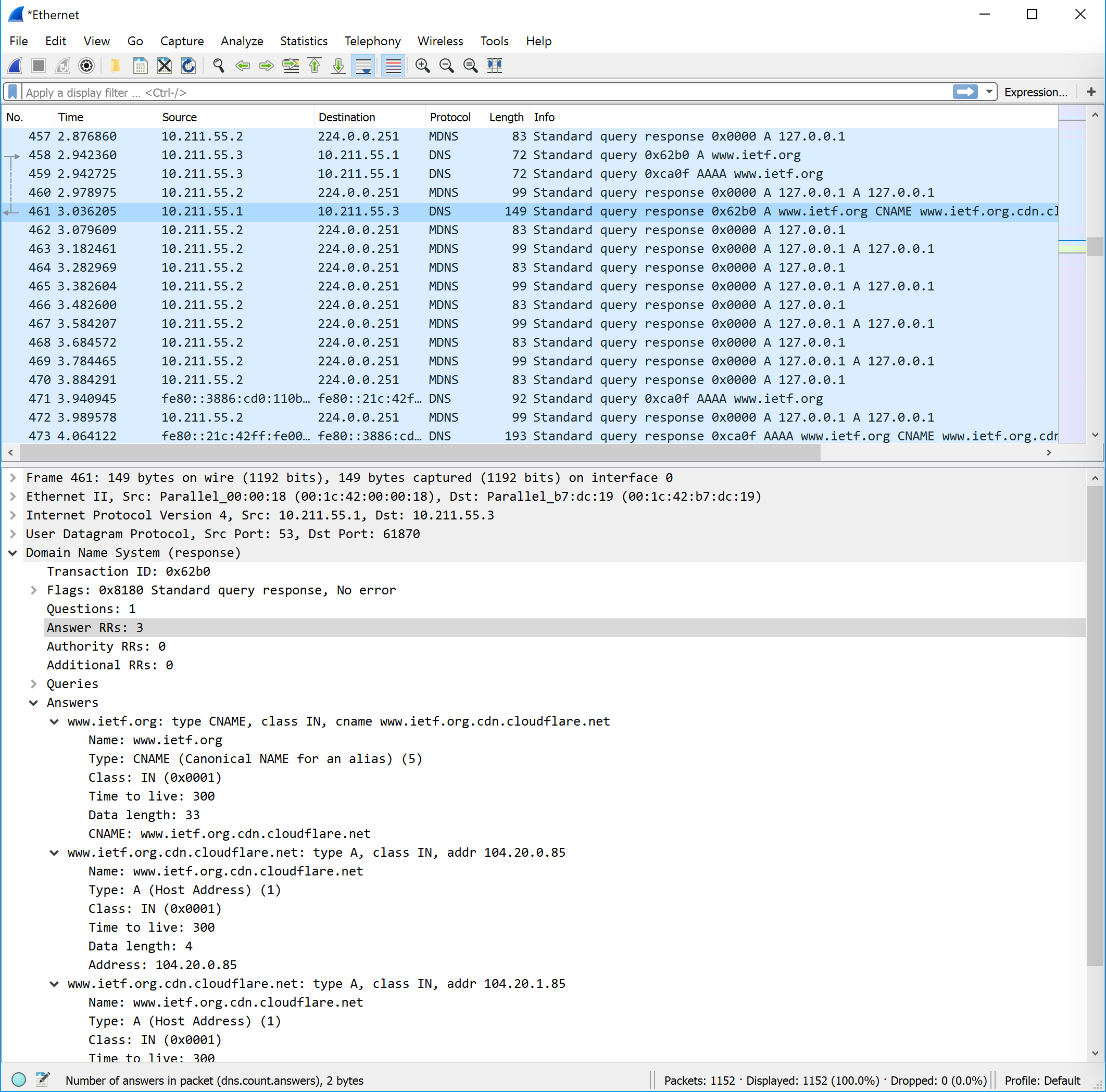


1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans: The DNS response message contains three (3) answers, each answer contains the name of the host, the type of address, the class, IP address.



1. Provide a screenshot.



Now repeat the previous experiment, but instead issue the command: nslookup –type=NS mit.edu

Answer the following questions5 :

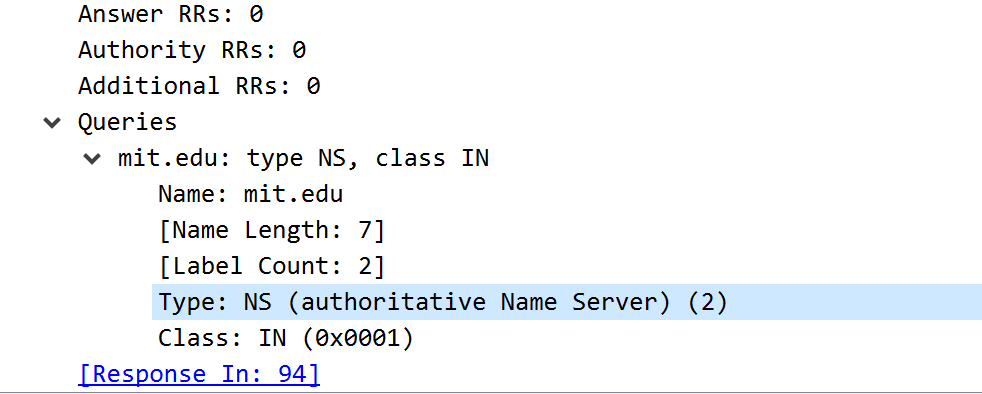
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans: It is sent to 23.217.18.195 which is my default DNS server.

(IPv6 IP address = fe80::21c:42ff:fe00:18)

1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

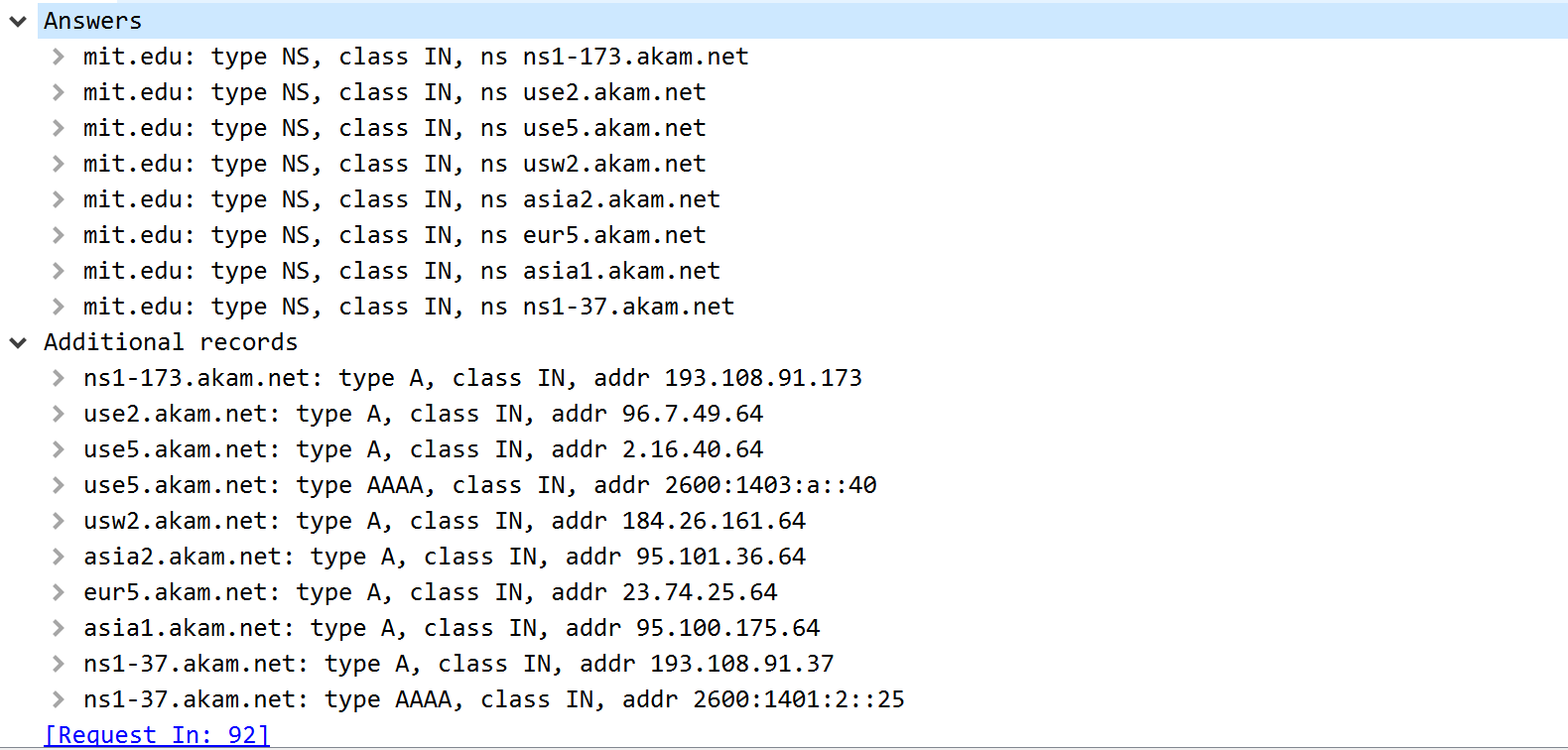
Ans: It is “Type: NS” DNS query and does not contain any answers.



1. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

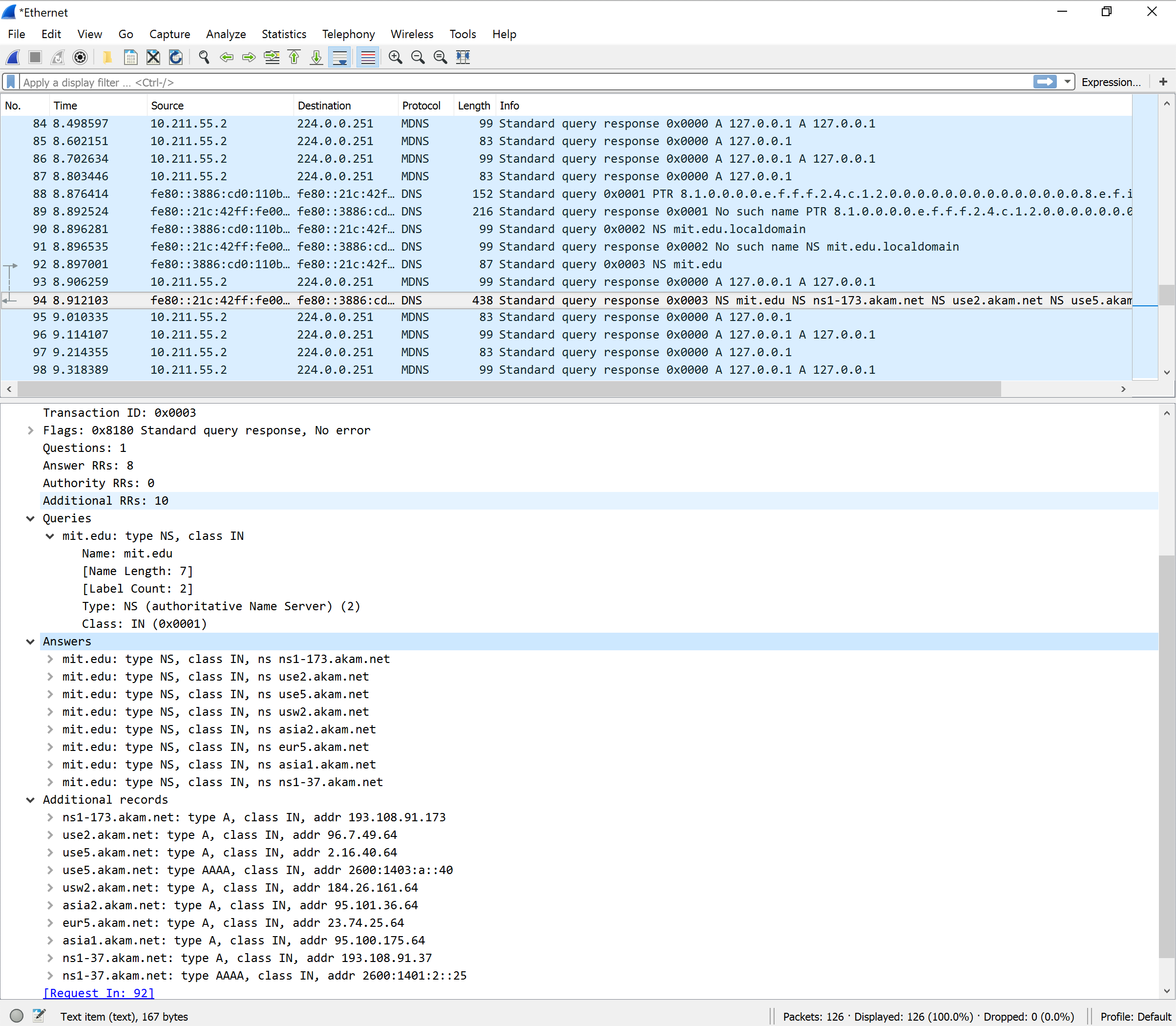
Ans:

MIT response message provides 8 MIT nameservers which includes their names and also includes their IP addresses of all MIT namesers in additional records section.



1. Provide a screenshot.

[Screenshot is on next page]



Now repeat the previous experiment, but instead issue the command: nslookup www.aiit.or.kr bitsy.mit.edu

Answer the following questions6:

1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Ans: The query is sent to 18.72.0.3 which corresponds to address “bitsy.mit.edu”

1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans: It is a “Type: A” standard query which does not contain any answers.

1. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Ans: There is only one answer in the DNS response message. It contains the address, name, type, class, address.

However, I could not completely finish the last part of the assignment due to the destination of the given query being unreachable.

1. Provide a screenshot.

[Screenshots is given below]

