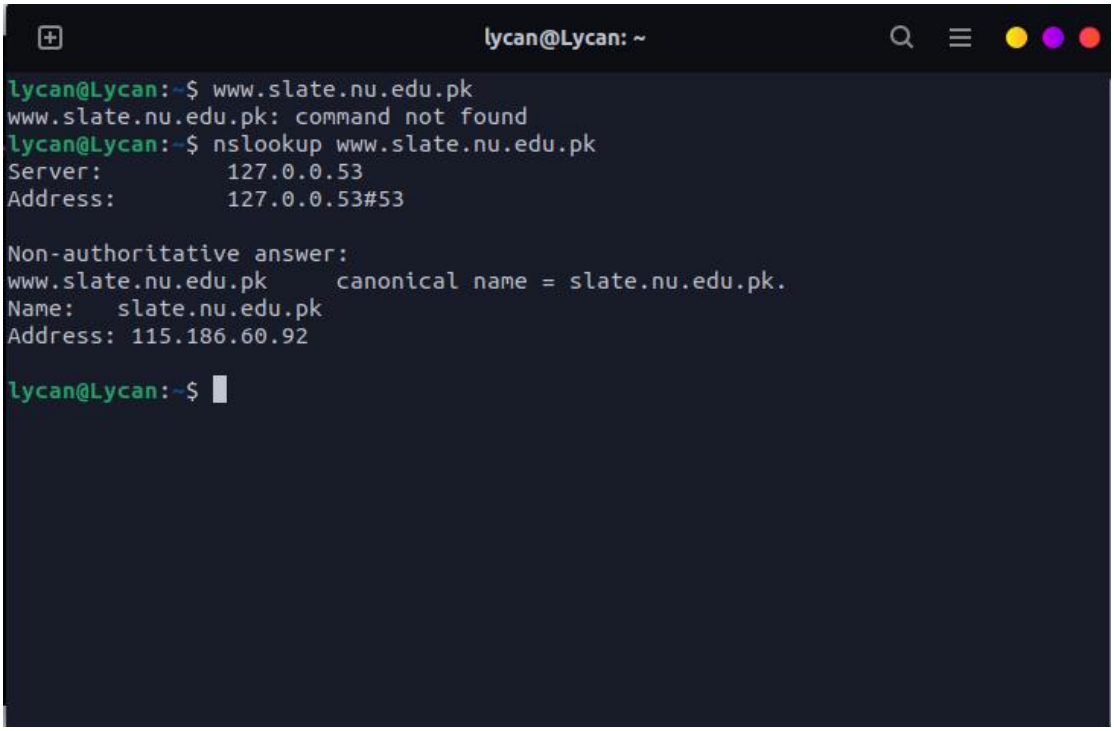
Name :Izaan Mohtashim
Roll No: P20-0613
Sec : 5A
Computer Networks

Lab Homework 2

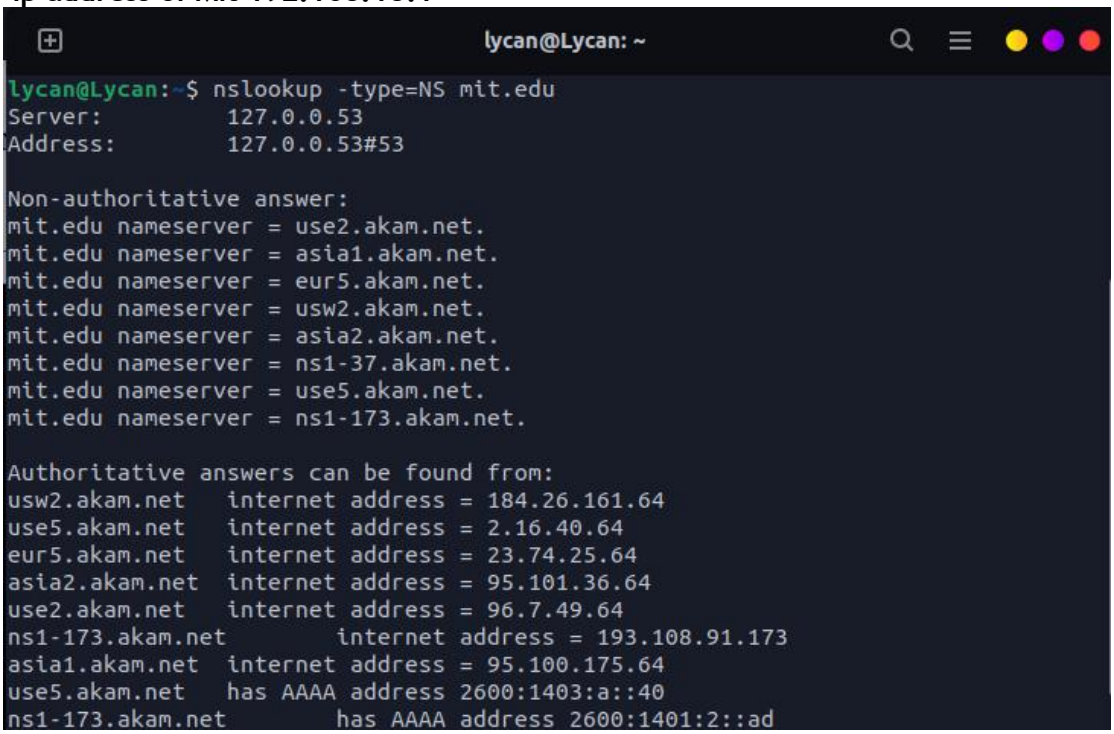
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

lp address of slate 115.186.60.92



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

ip address of Mit 192.168.18.1

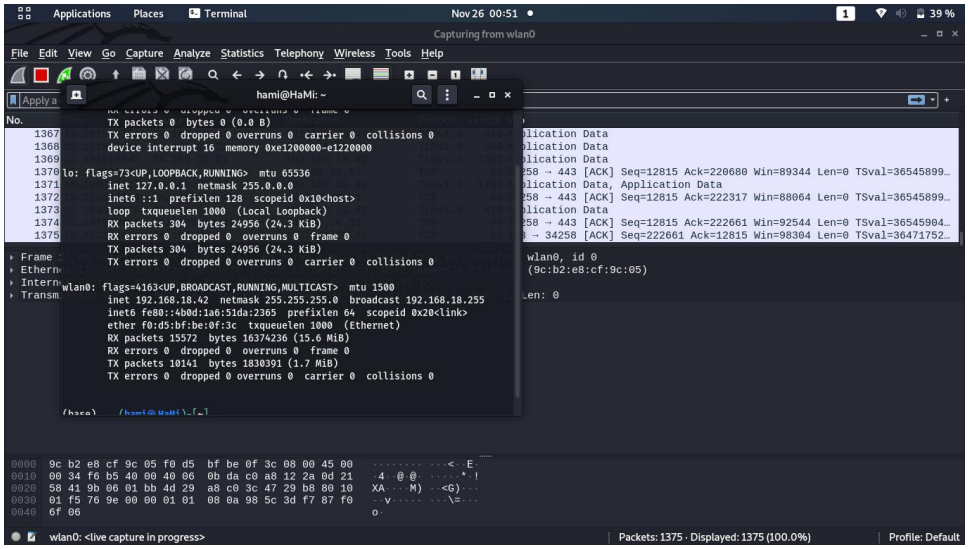


3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Ip address of yahoo is 87.248.119.252

Tracing DNS with Wireshark

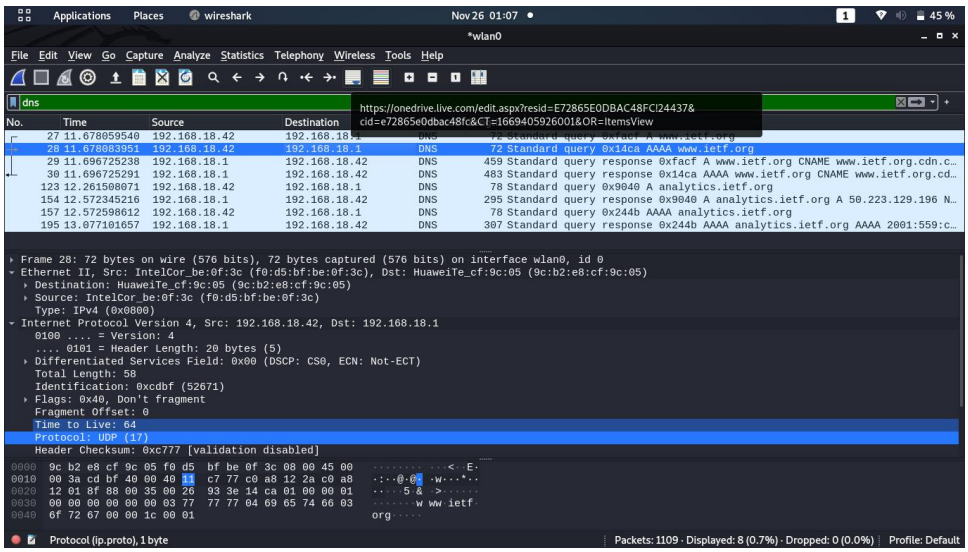
Ip address of my device -> 192.168.18.42

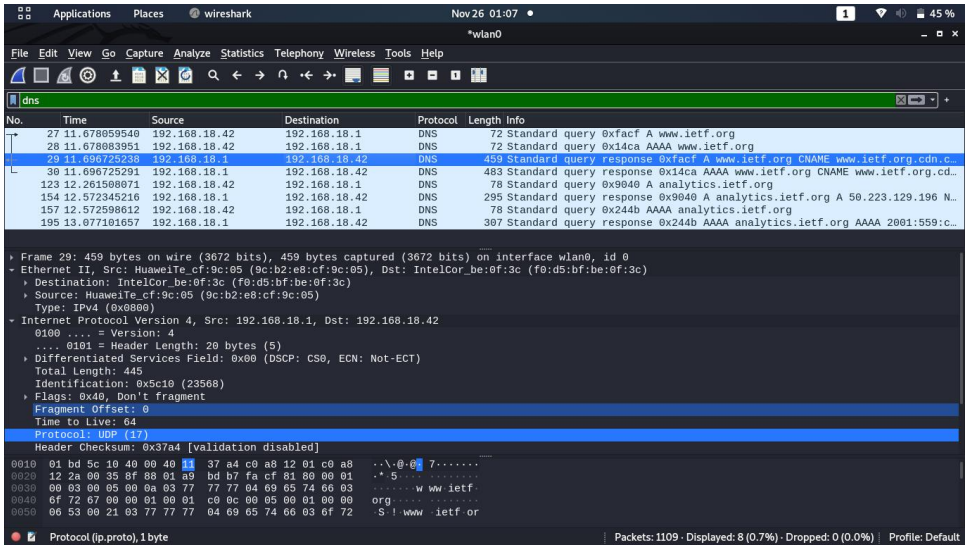


1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

The DNS query and response messages are sent over UDP.

Using UDP

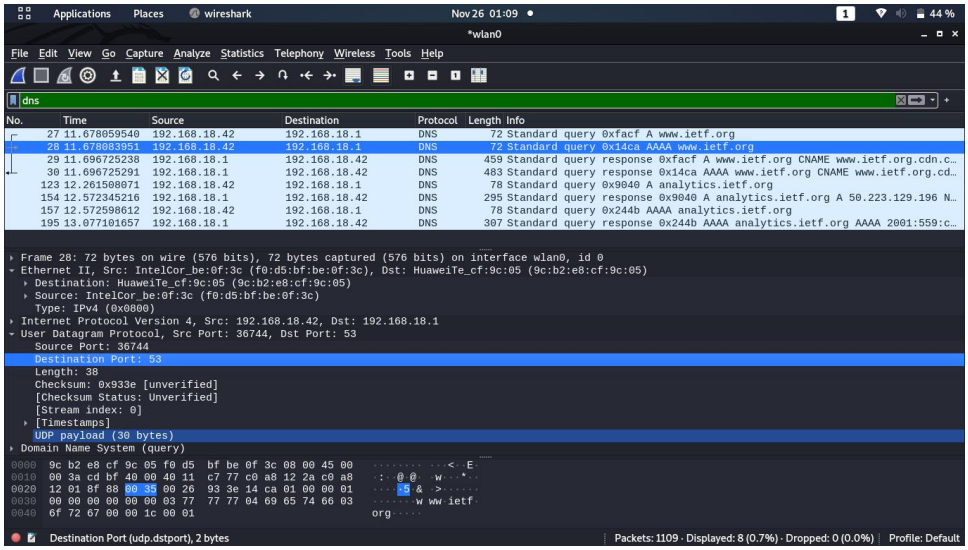




2. What is the destination port for the DNS query message? What is the source port of DNS response message?

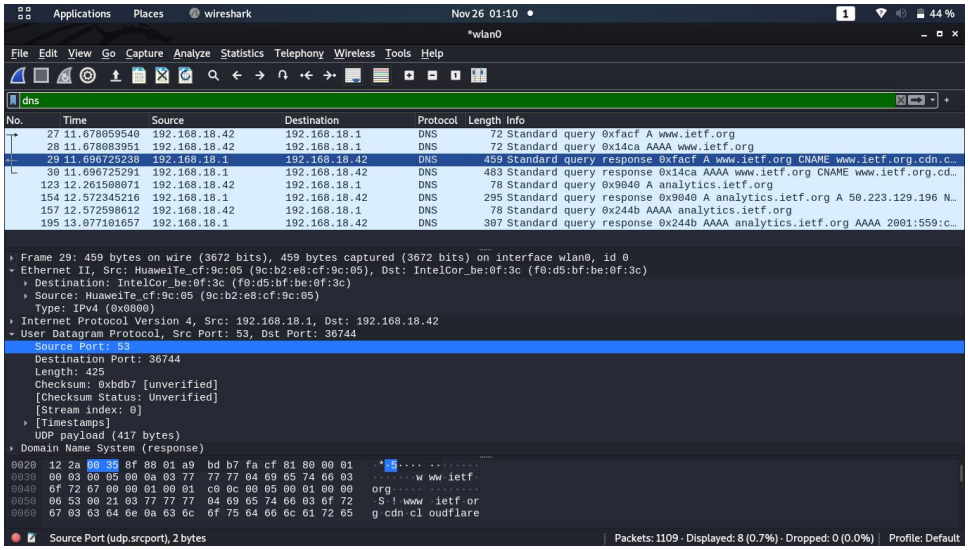
Dns query

Port 53



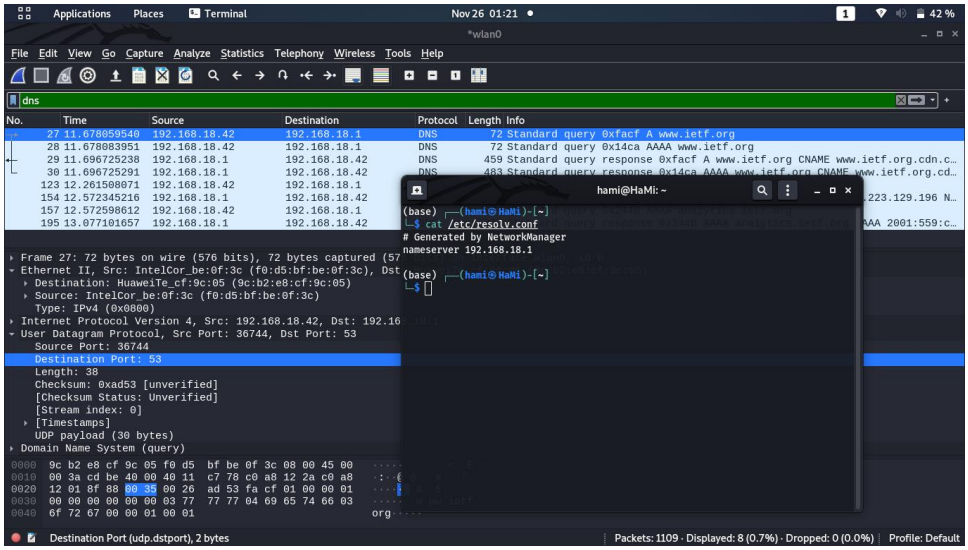
Dns response

Port 53



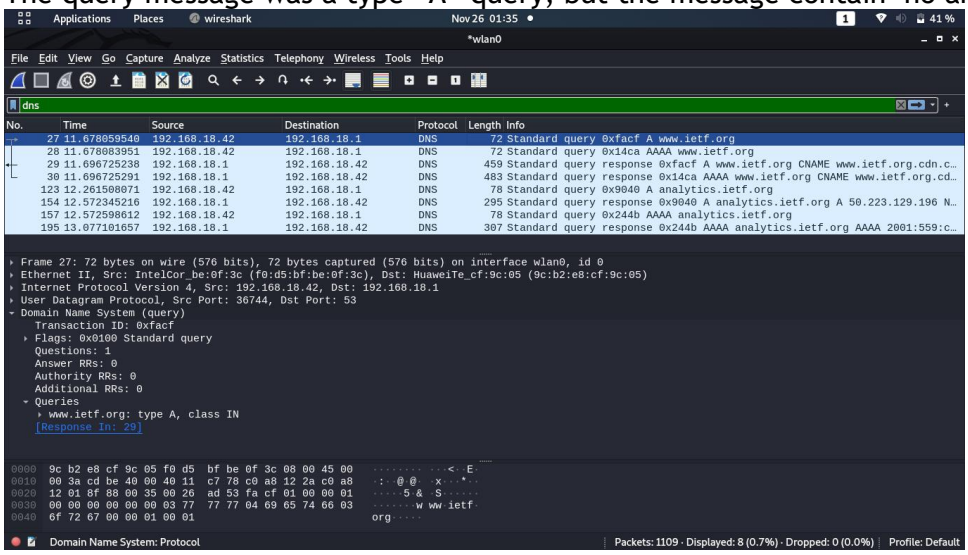
3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Both are same



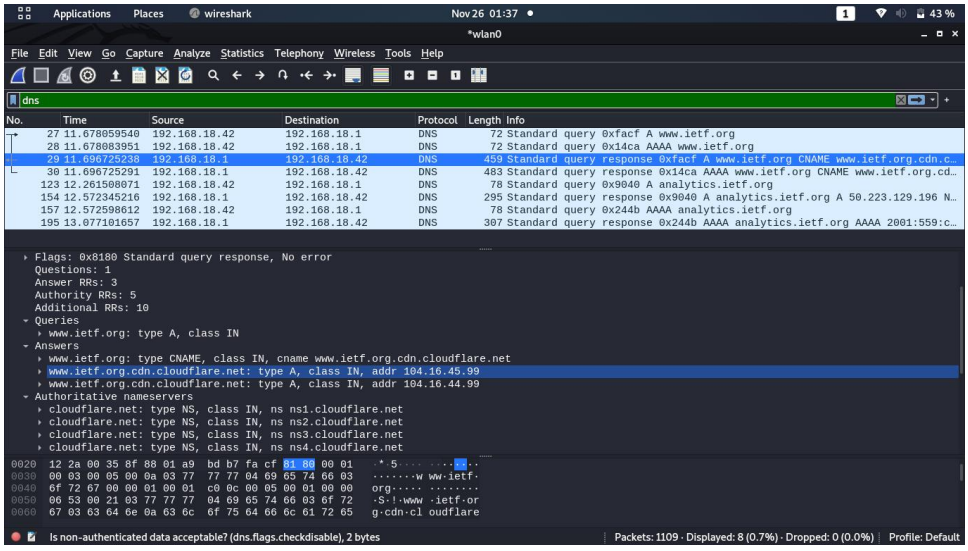
4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The query message was a type "A" query, but the message contain no answers



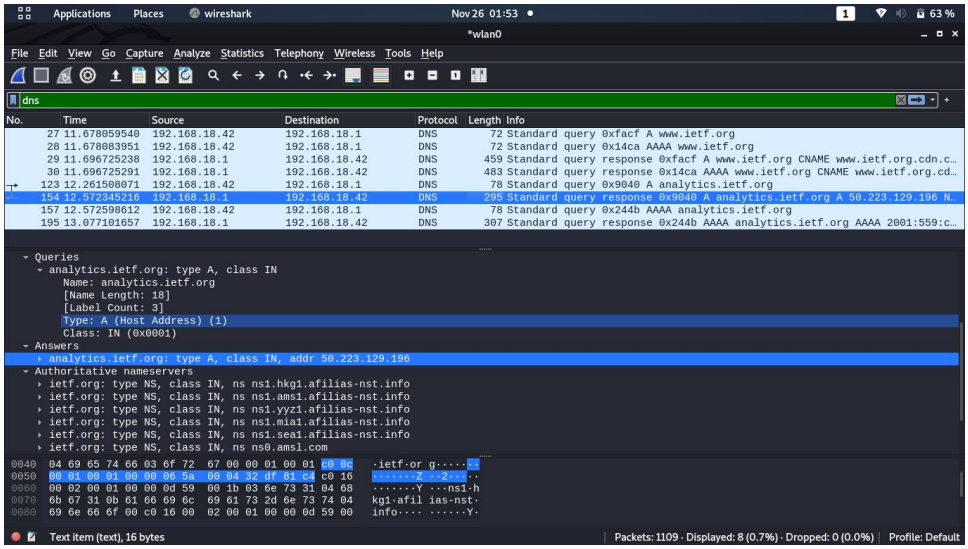
5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

3 Ans
Authority servenames : 5
Additional inforamtion : 10



6. 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?

The destination of the SYN packet is 50.223.129.196 , the same address that was provided in the DNS response message as the type "A" address of the webpage.



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

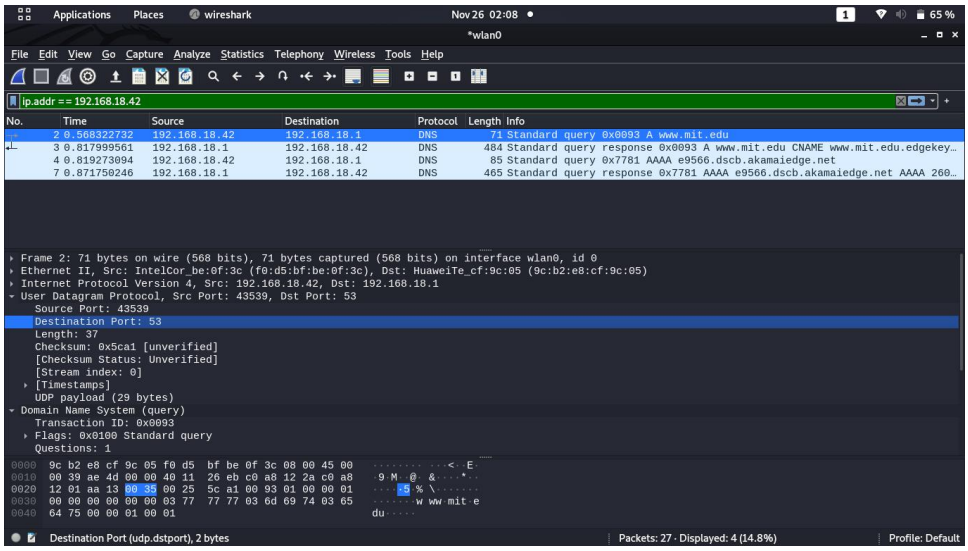
Now let's play with nslookup4.

- **Start packet capture.**
- **Do an nslookup on www.mit.edu**
- **Stop packet capture.**

Yes, my host did issue new DNS queries before the images were retrieved. For example, one such query was for an image from open-stand.org. The image corresponding to the page was not returned until this query was made

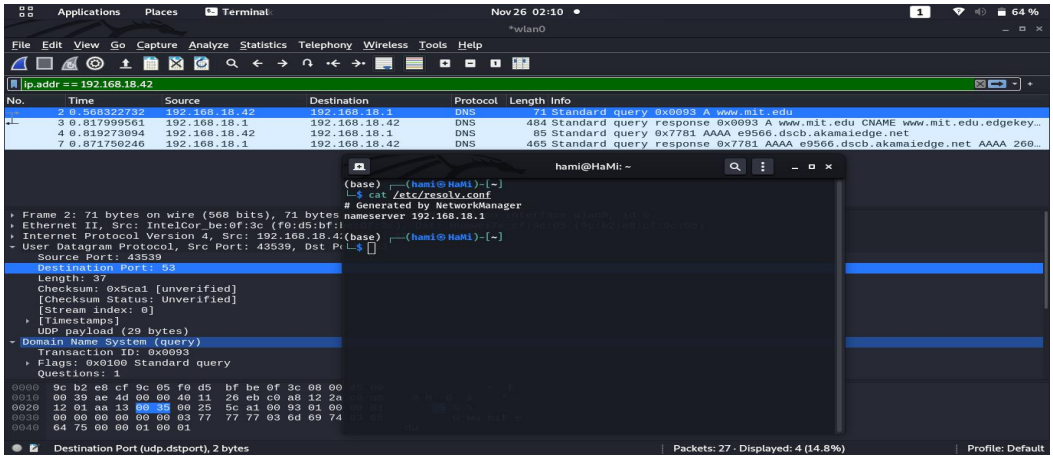
8. What is the destination port for the DNS query message? What is the source port of DNS response message?

Destination Port: 53



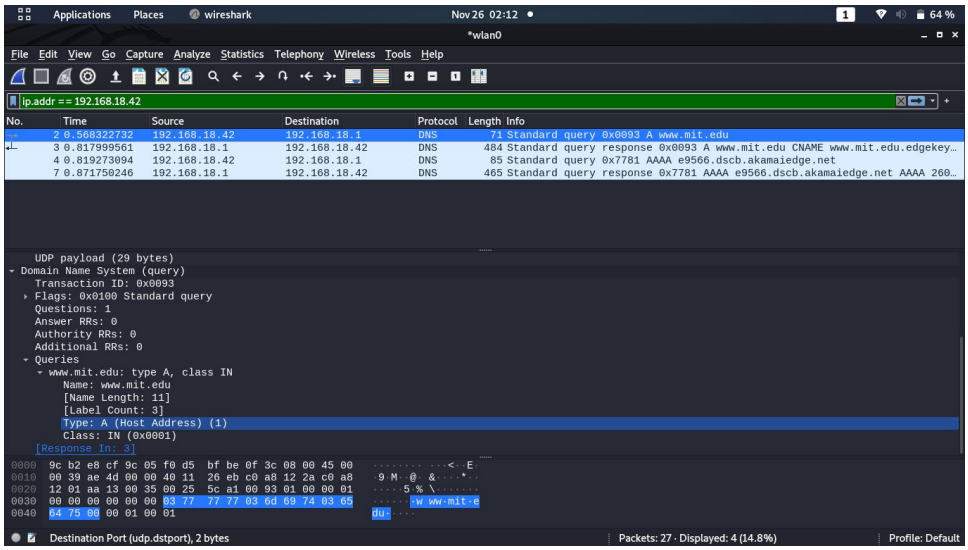
9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Both are same



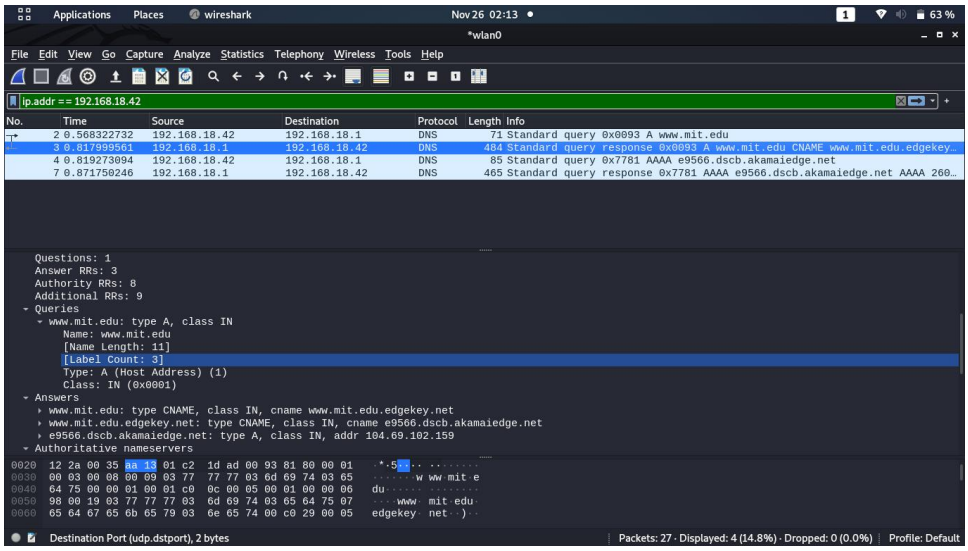
10. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The DNS query message is a type "A" query, containing only one question and not containing any answers.



11. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Answer RRs: 3
Authority RRs: 8
Additional RRs: 9



12. Provide a screenshot.