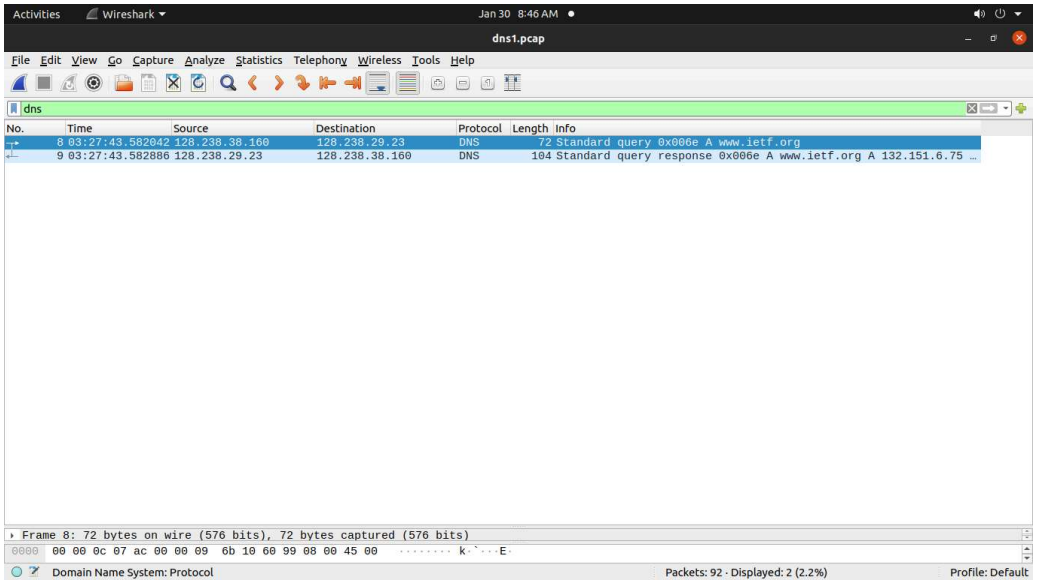
ASSIGNMENT -03

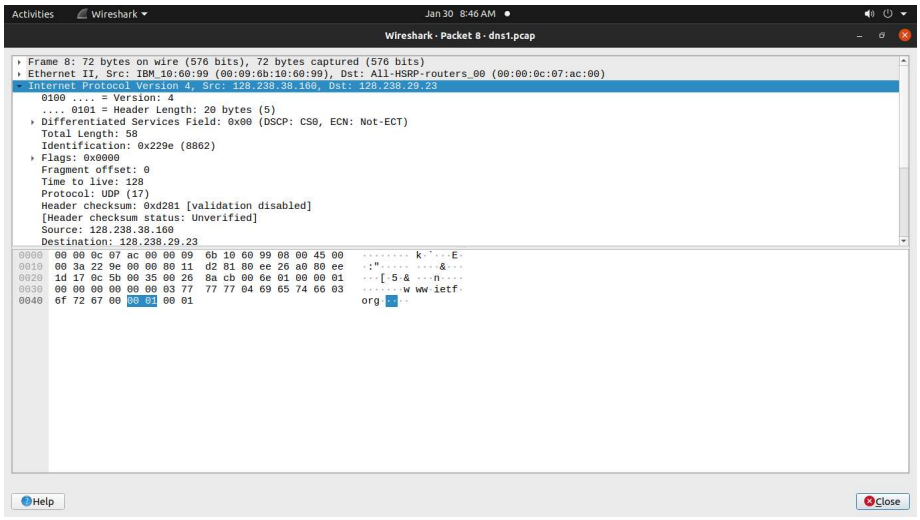
SUB CODE: CS3072

NAME: Aditee Ping

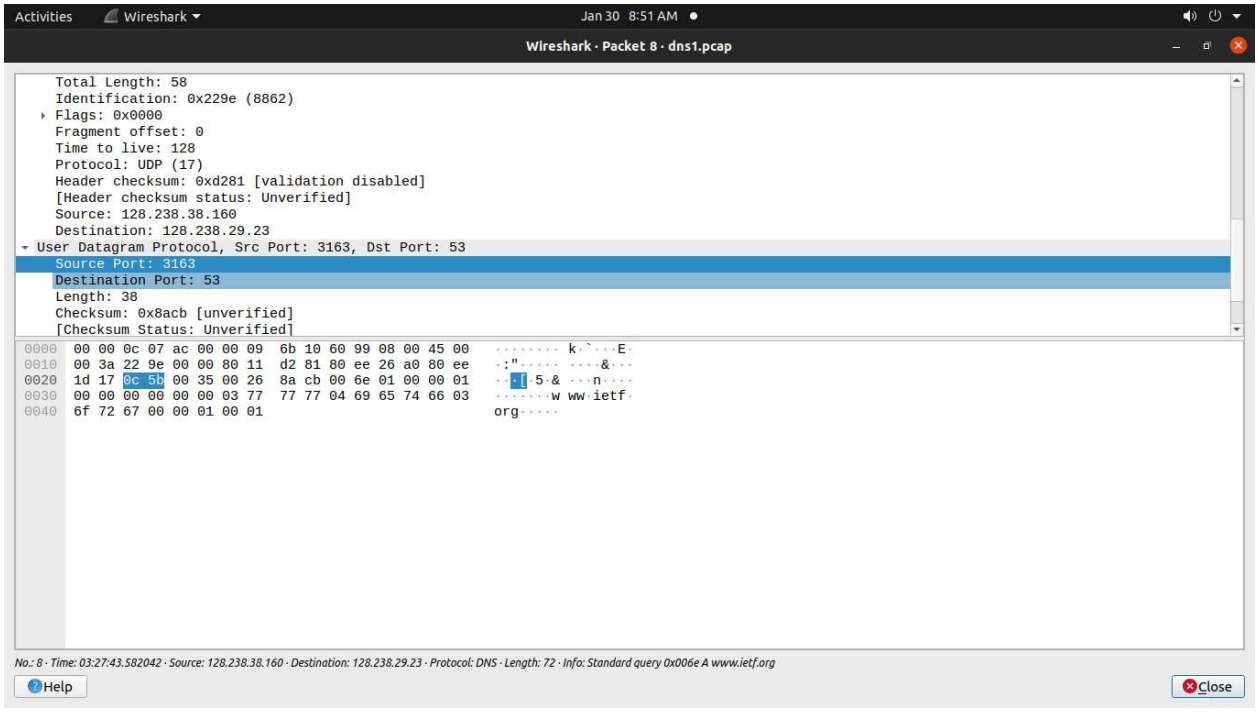
ROLL NO: 123CS0204

Q1.Locate the DNS query and response messages. Are they sent over UDP or TCP?

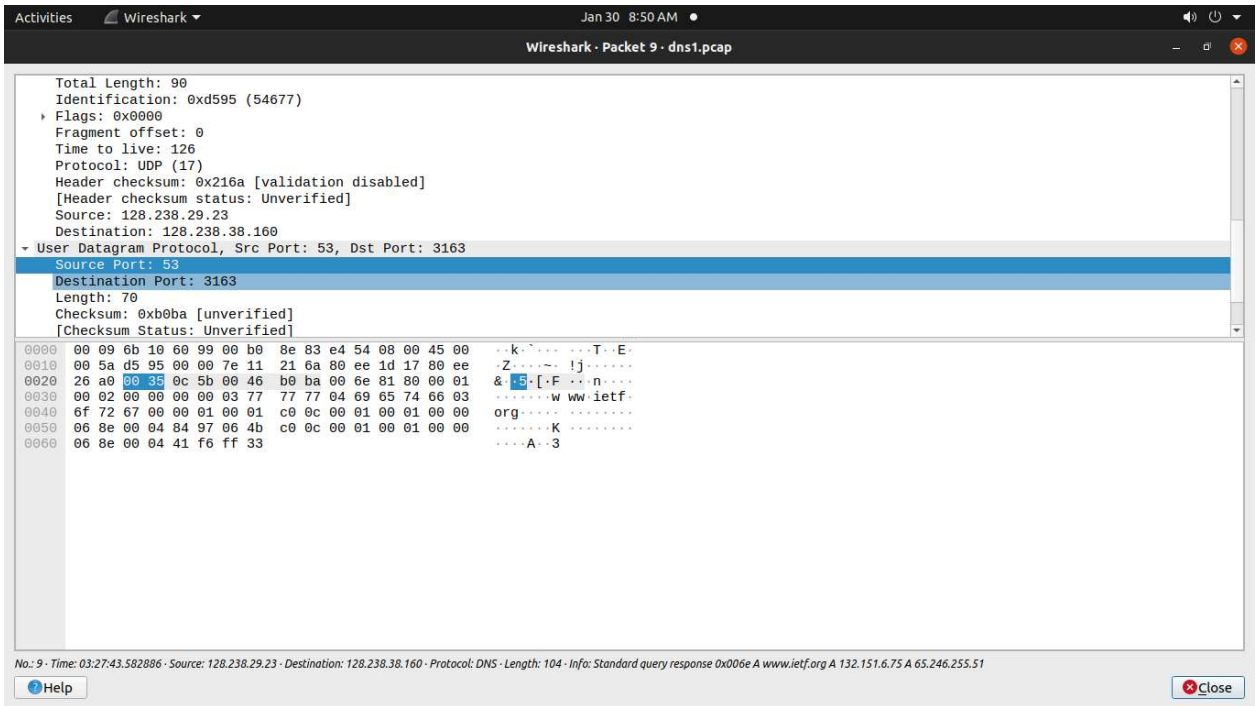




Q 2.What is the destinantion port for the DNS query message? What is the source port of the DNS response message?



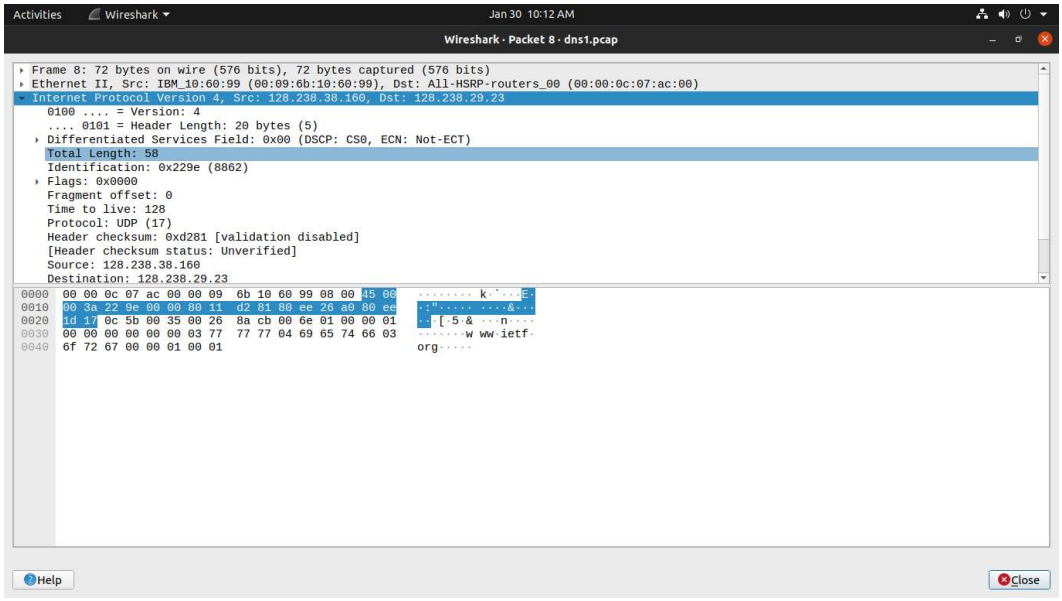
Destination port of the query message: 53

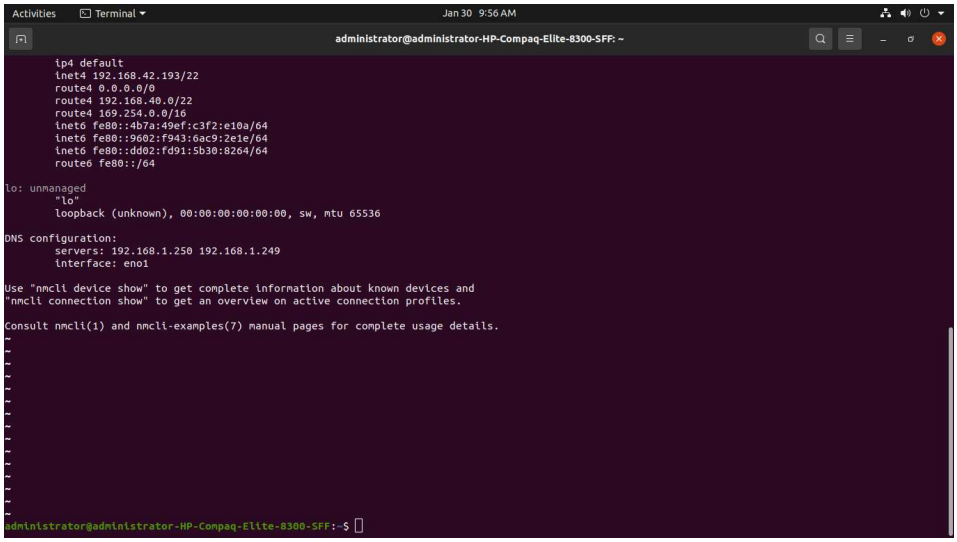


Source port of DNS response message: 53

Q3.To what IP address is the DNS query message sent? Use the nmcli command to determine the IP address of your local DNS server. Are these two IP addresses the same?

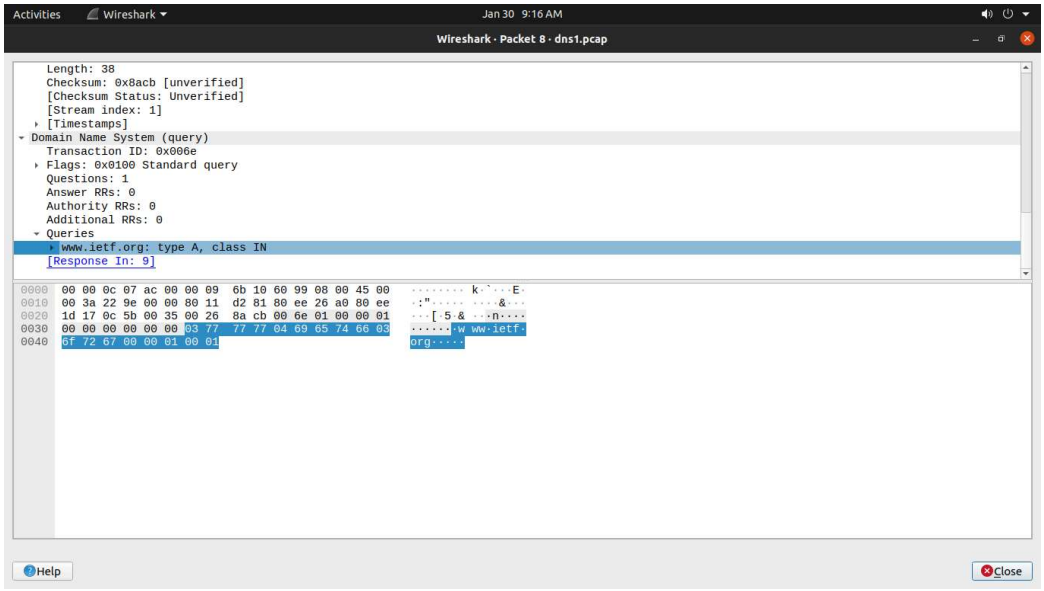
IP address to which sent: 128.238.29.23





IP address of your local DNS server -192.168.1.250 192.168.1.249

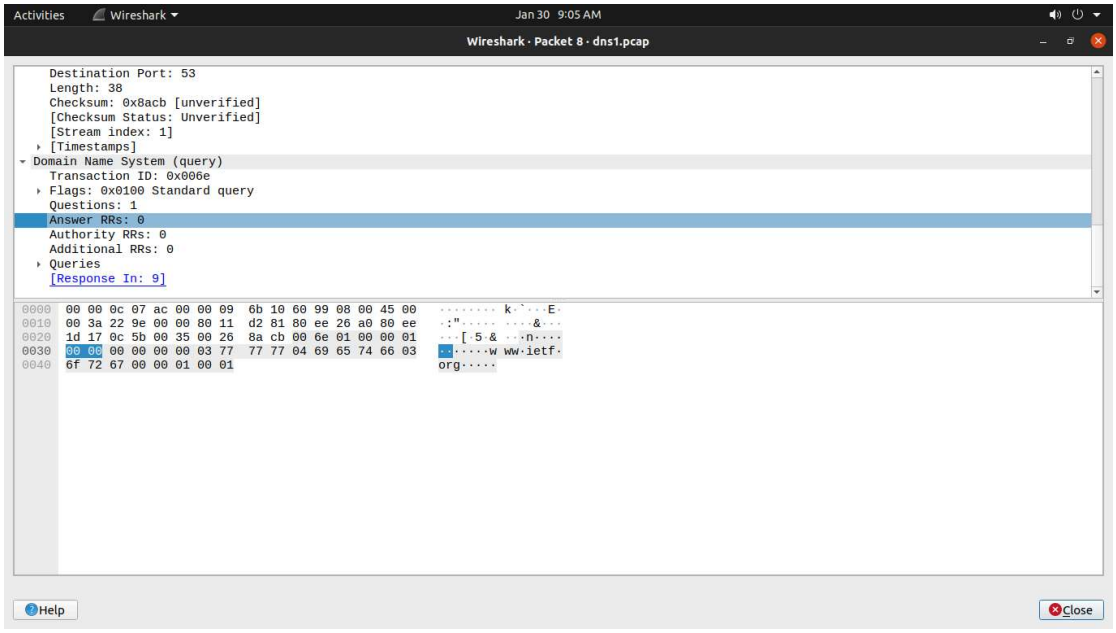
Q 4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any answers?



Type:A

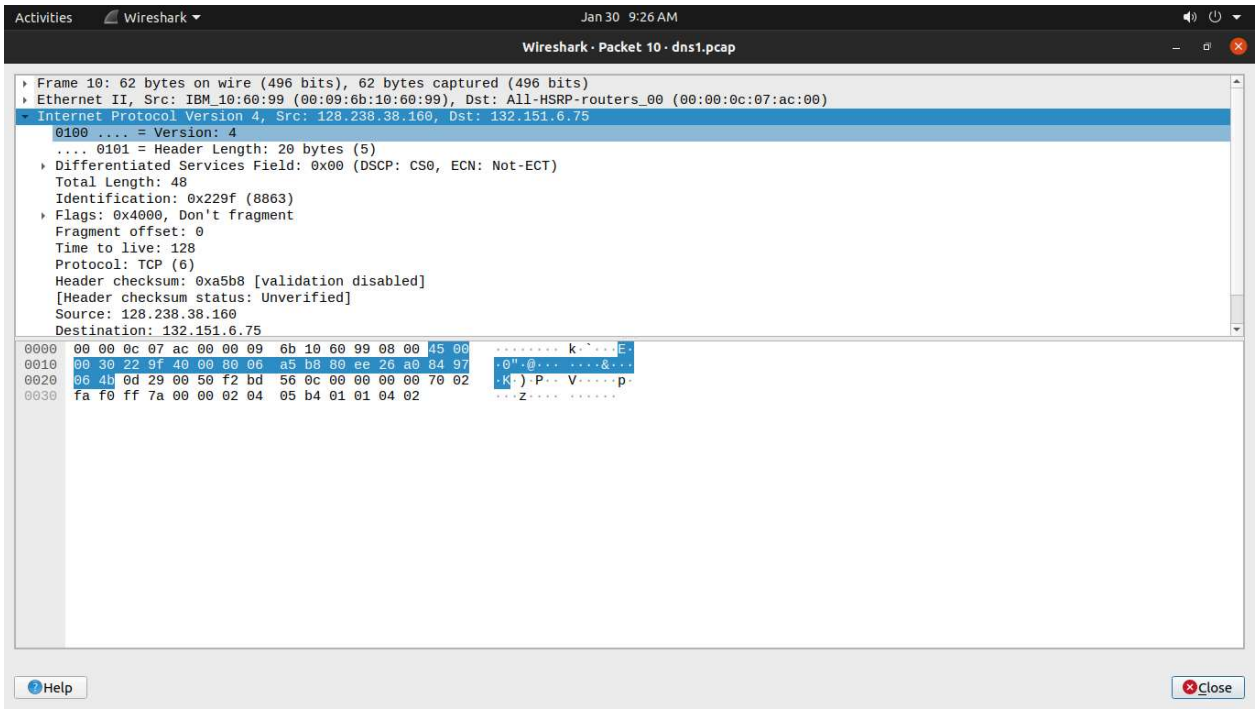
Answers : 0

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



Answers Provided = 2

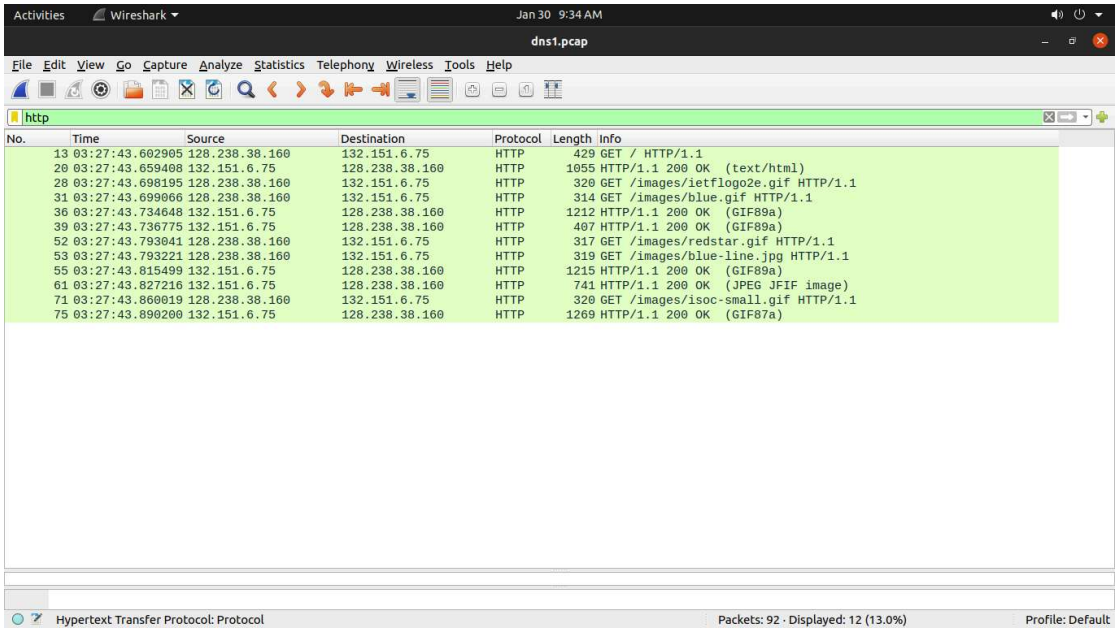
Q6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS message?



Destination IP address: 132.165.6.75
Yes it corresponds to the IP addresses provided in the DNS response message.

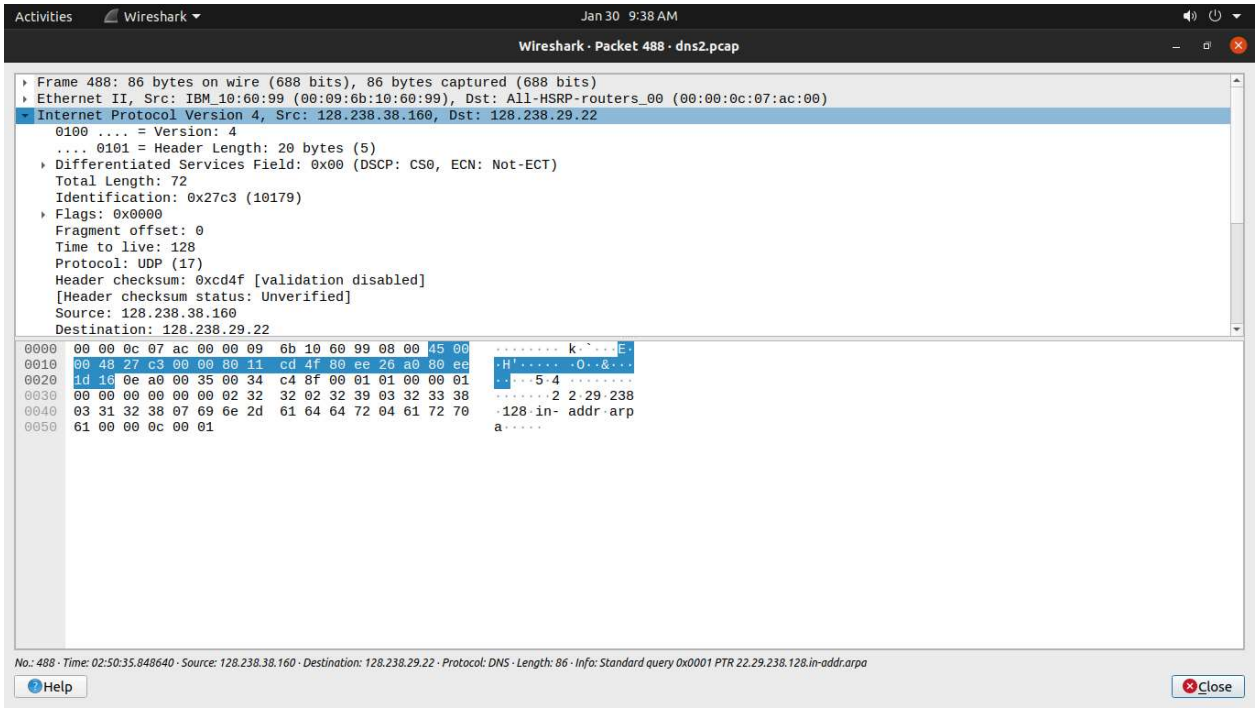
Q7.This web pages contain images. Before retrieving each image, does your host issue new DNS queries?

No new DNS query is issued by our host for any images being retrieved.



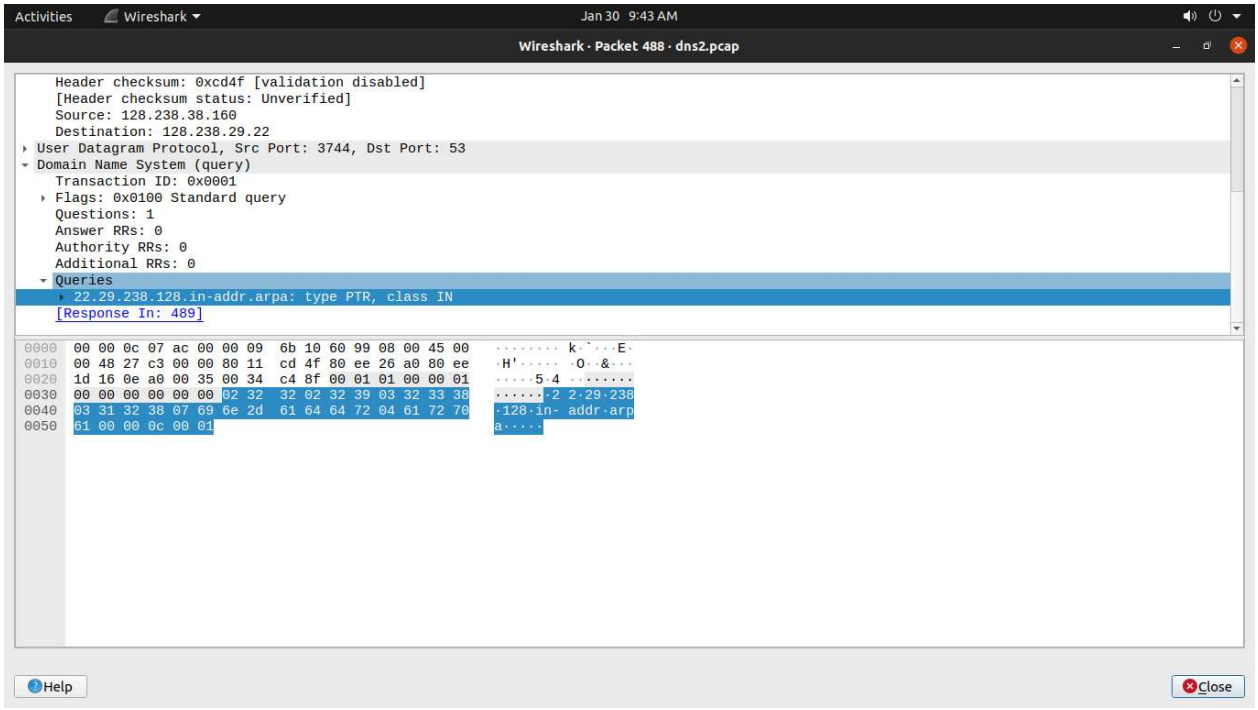
IN DNS2.PCAP:

Q8.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



Destination IP address of the DNS query message: 128.238.29.22

Q 9.Examine the DNS query message. What “type” of DNS query is it? Does the query message contain any “answers”?

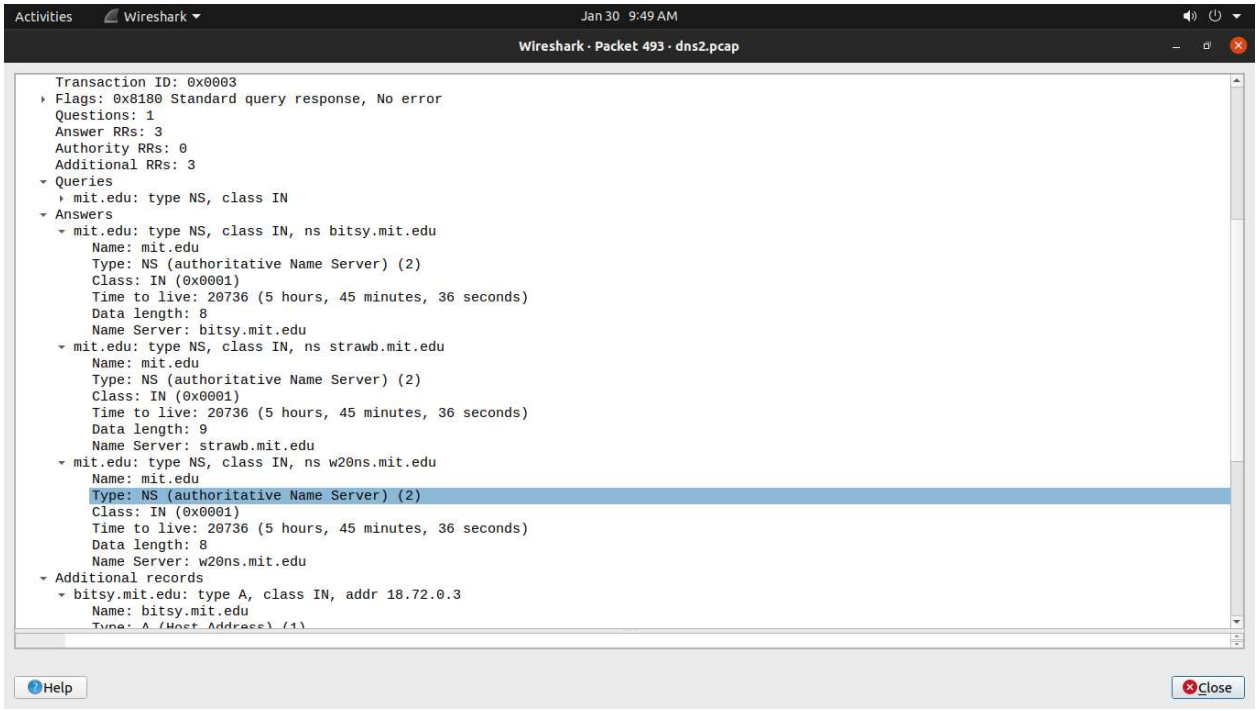


Type: PTR

It contains no answers.

10. 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 nameservers?

It provides the following nameservers:



and the IP addresses of the nameservers: