

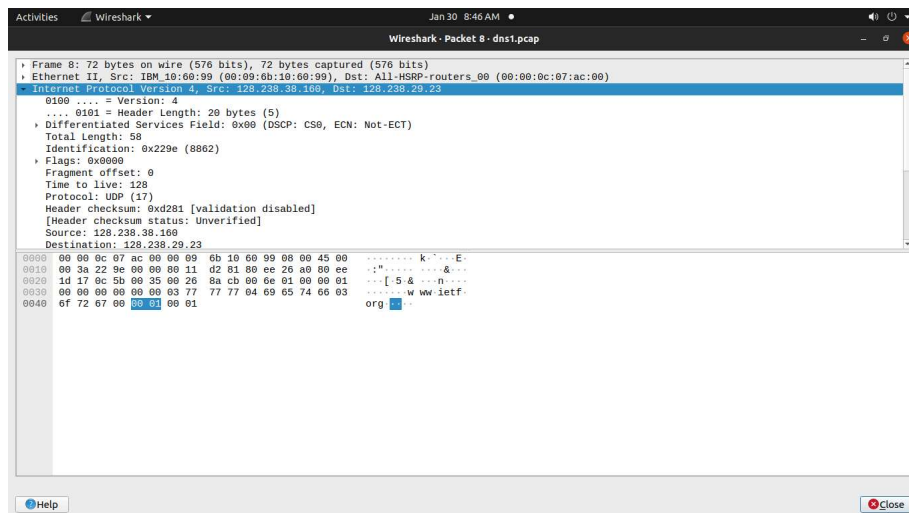
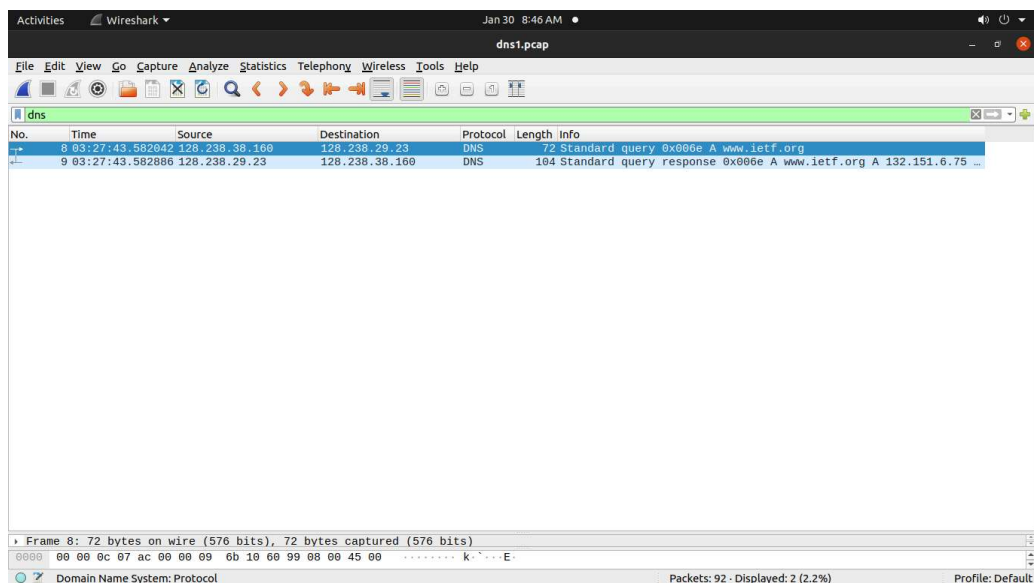
ASSIGNMENT -03

SUB CODE: CS3072

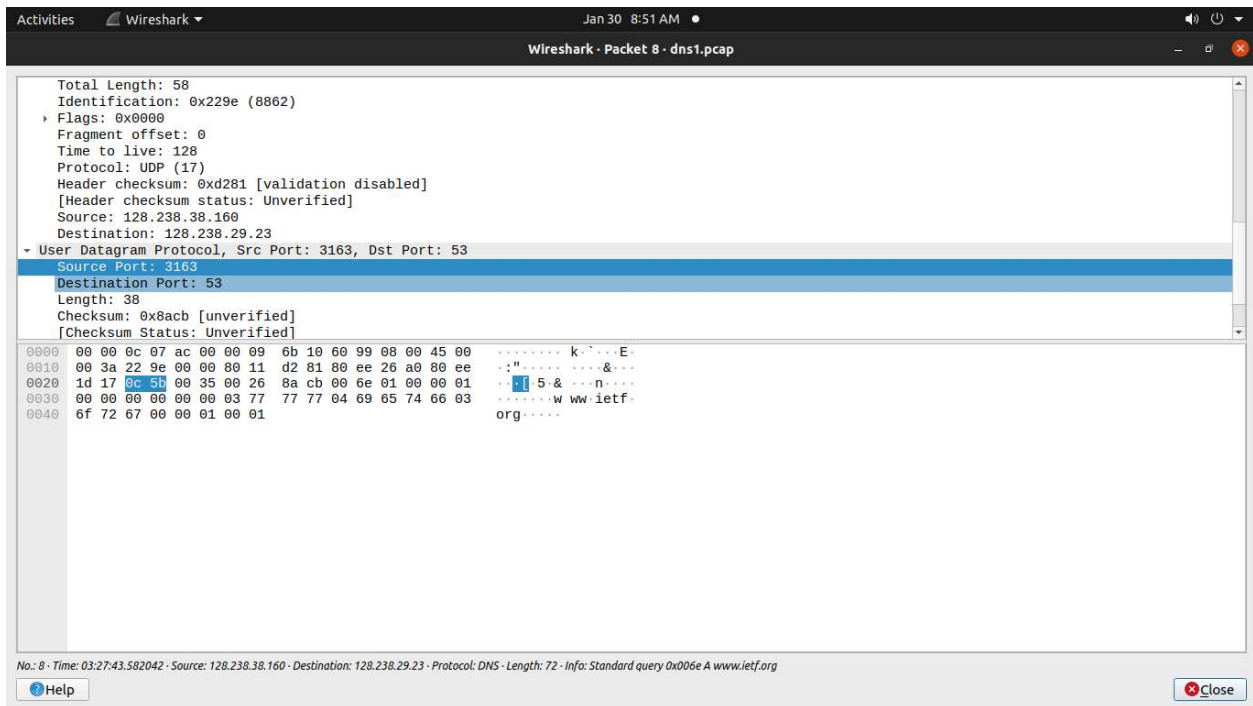
NAME: Aditee Ping

ROLL NO: 123CS0204

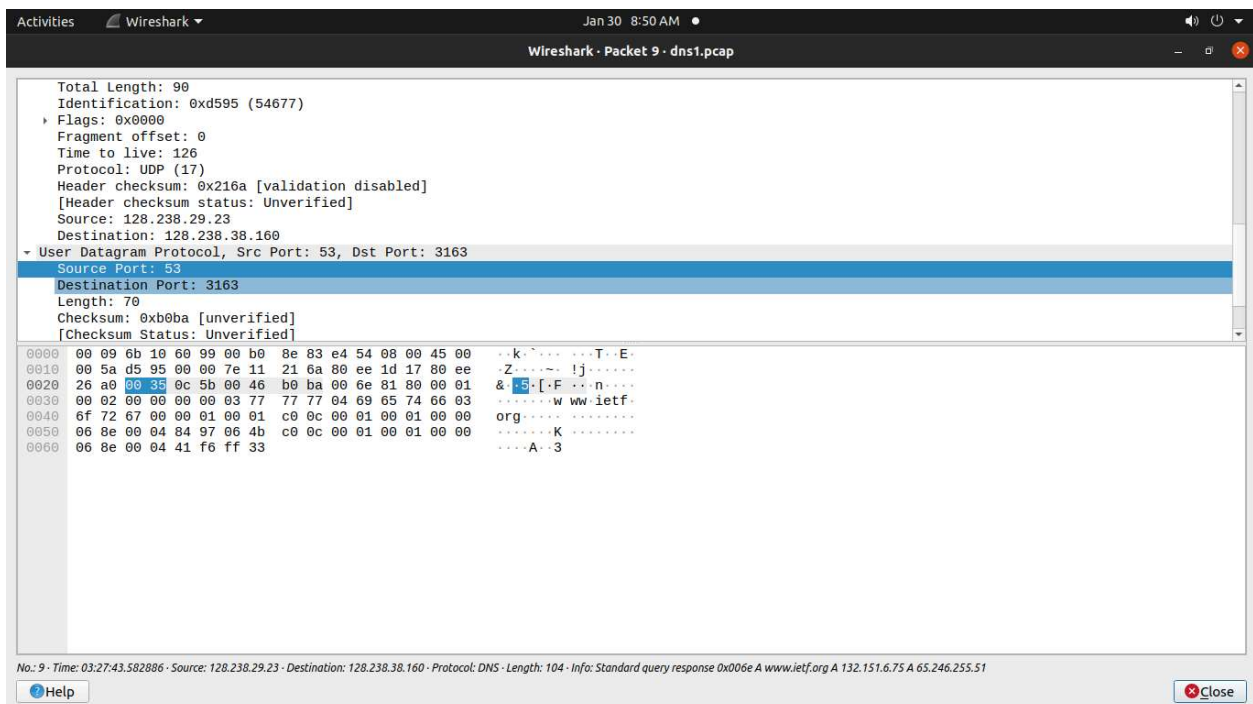
Q1. Locate the DNS query and response messages. Are they sent over UDP or TCP?



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



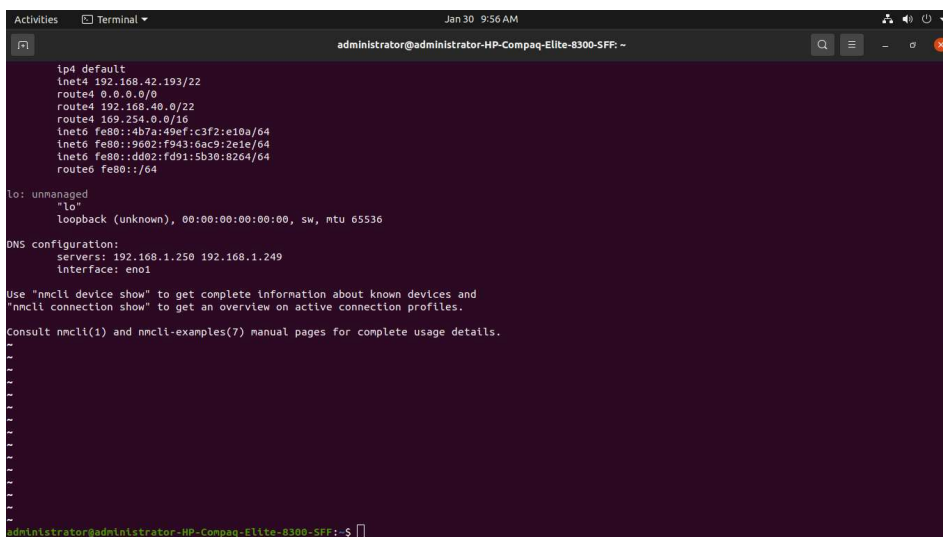
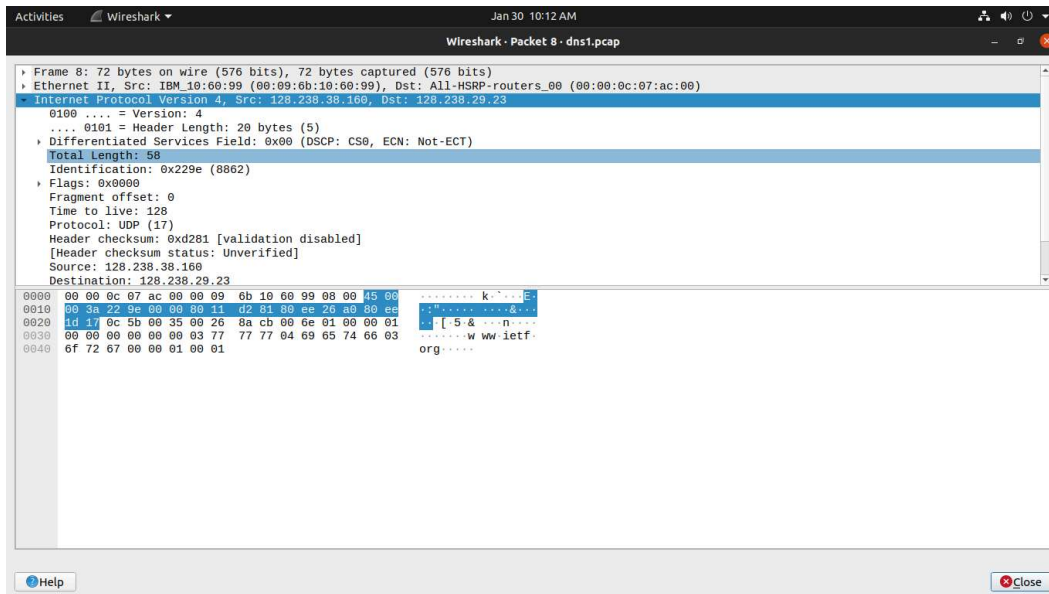
Destination port of the query message: 53



Source port of DNS response message: 53

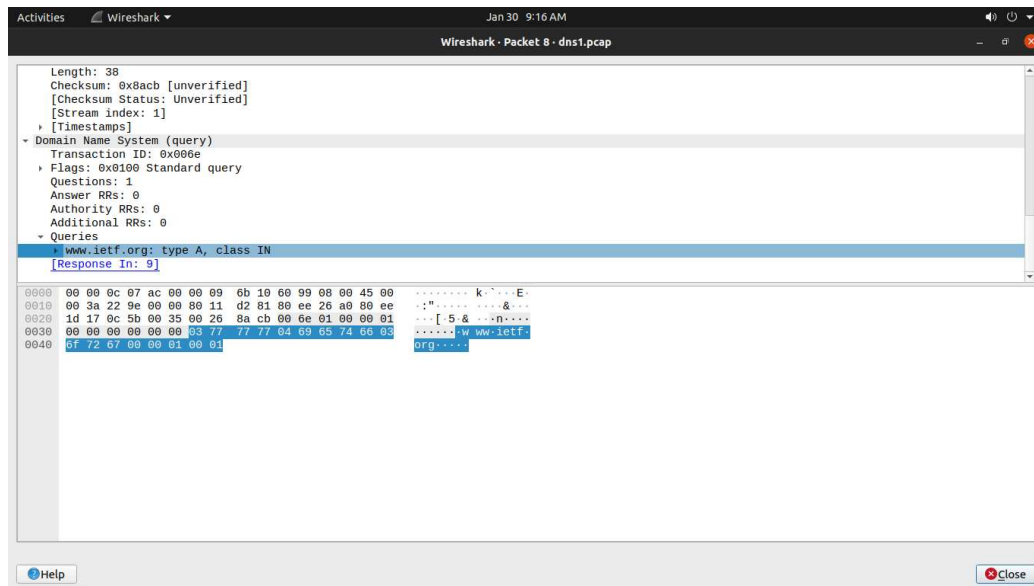
Q3.To what IP address is the DNS query message sent? Use the nmcli command to determine the IP address of your local DNS server. Are these two IP addresses the same?

IP address to which sent: 128.238.29.23



IP address of your local DNS server -192.168.1.250 192.168.1.249

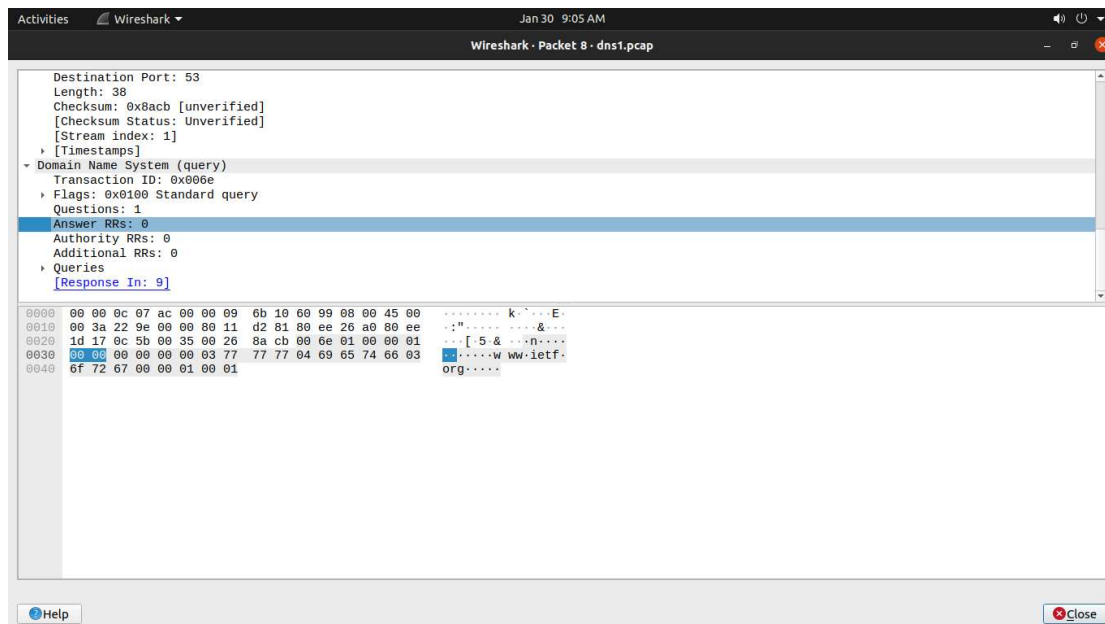
Q 4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any answers?



Type:A

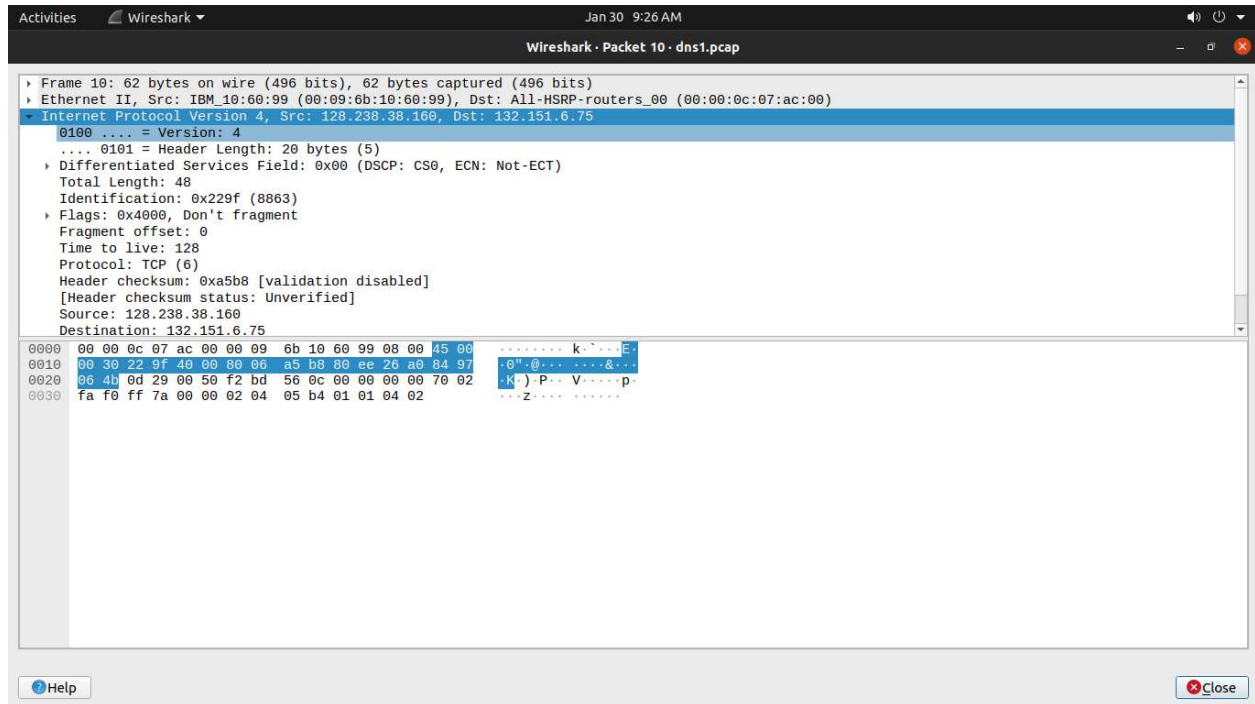
Answers : 0

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?

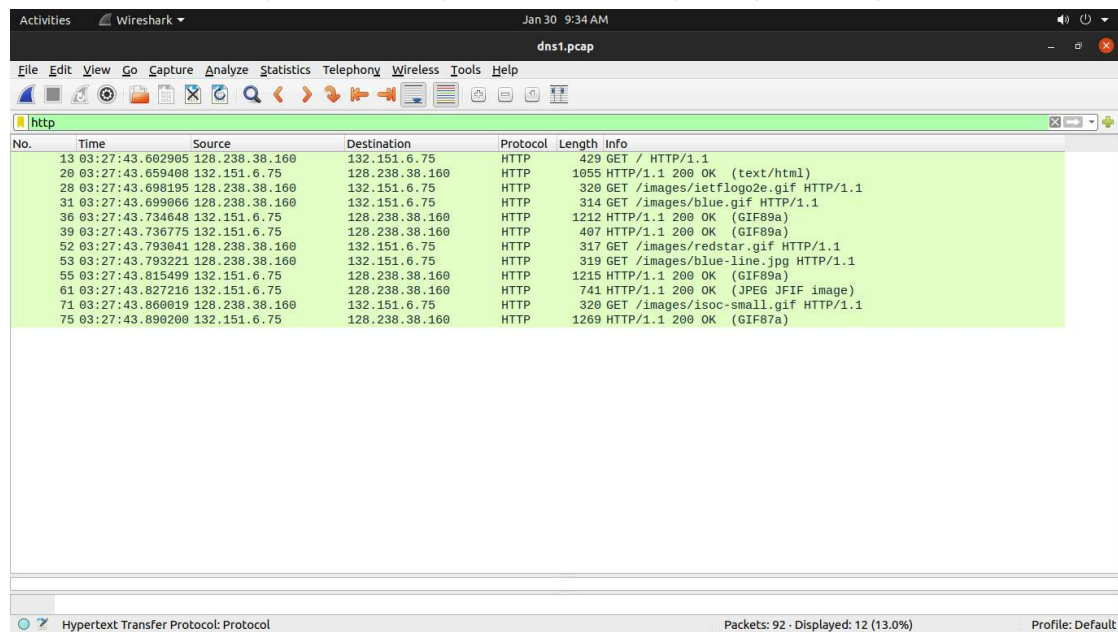


Destination IP address: 132.165.6.75

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.



Activities Wireshark Jan 30 9:34 AM dns1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

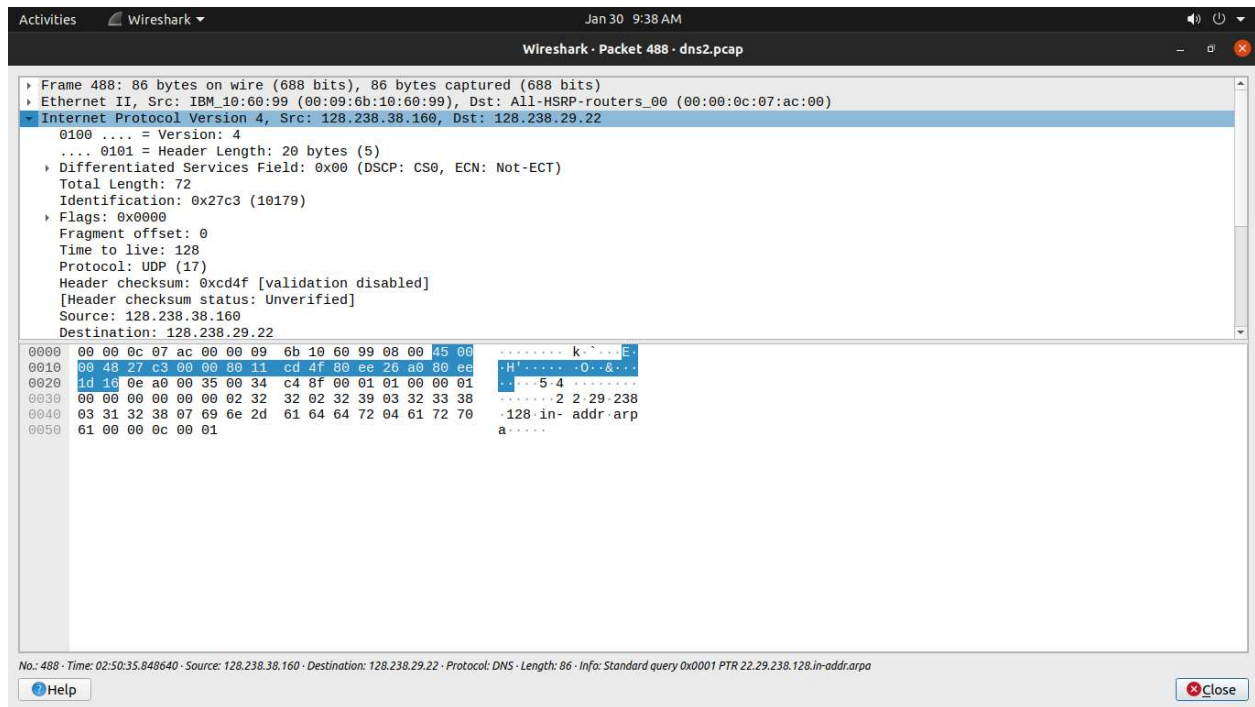
http

No.	Time	Source	Destination	Protocol	Length	Info
13	03:27:43.602905	128.238.38.160	132.151.6.75	HTTP	429	GET / HTTP/1.1
20	03:27:43.659408	132.151.6.75	128.238.38.160	HTTP	1055	HTTP/1.1 200 OK (text/html)
28	03:27:43.698195	128.238.38.160	132.151.6.75	HTTP	320	GET /images/ietflogo2e.gif HTTP/1.1
31	03:27:43.699066	128.238.38.160	132.151.6.75	HTTP	314	GET /images/blue.gif HTTP/1.1
36	03:27:43.734648	132.151.6.75	128.238.38.160	HTTP	1212	HTTP/1.1 200 OK (GIF89a)
39	03:27:43.736775	132.151.6.75	128.238.38.160	HTTP	407	HTTP/1.1 200 OK (GIF89a)
52	03:27:43.793041	128.238.38.160	132.151.6.75	HTTP	317	GET /images/redstar.gif HTTP/1.1
53	03:27:43.793221	128.238.38.160	132.151.6.75	HTTP	319	GET /images/blue-line.jpg HTTP/1.1
55	03:27:43.815499	132.151.6.75	128.238.38.160	HTTP	1215	HTTP/1.1 200 OK (GIF89a)
61	03:27:43.827216	132.151.6.75	128.238.38.160	HTTP	741	HTTP/1.1 200 OK (JPEG JFIF image)
71	03:27:43.860019	128.238.38.160	132.151.6.75	HTTP	320	GET /images/isoc-small.gif HTTP/1.1
75	03:27:43.890200	132.151.6.75	128.238.38.160	HTTP	1269	HTTP/1.1 200 OK (GIF87a)

Hypertext Transfer Protocol: Protocol Packets: 92 - Displayed: 12 (13.0%) Profile: Default

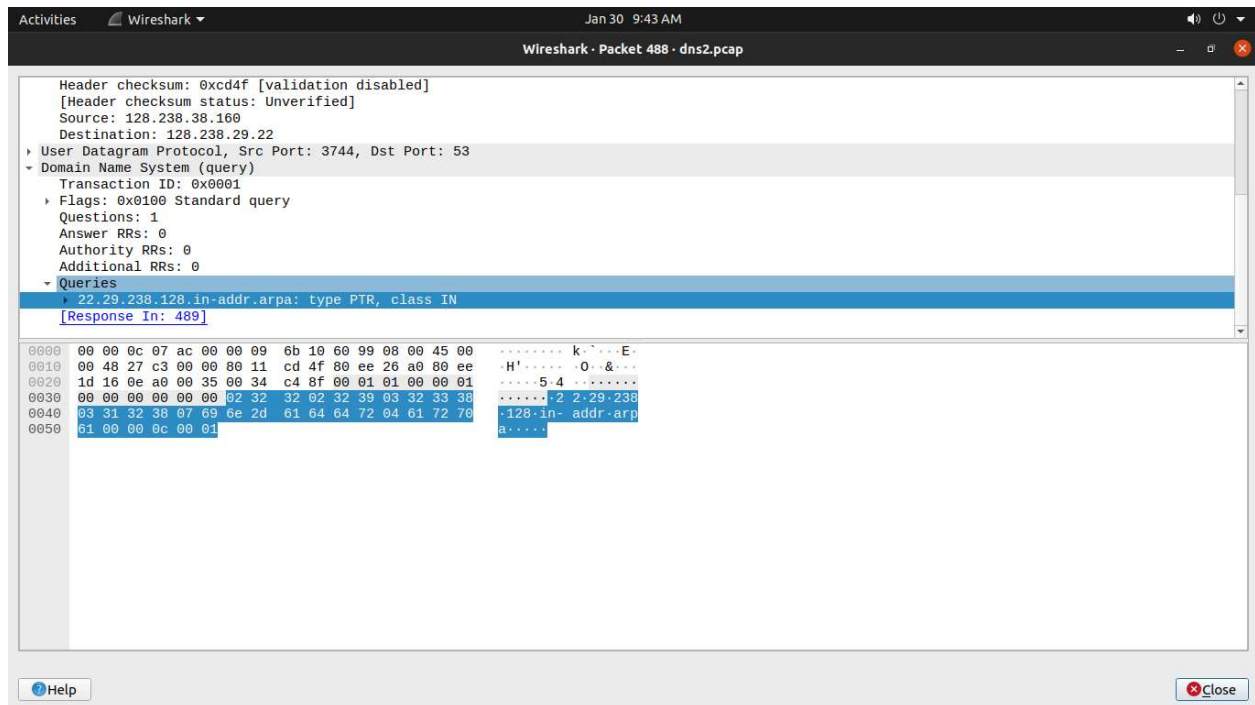
IN DNS2.PCAP:

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”?

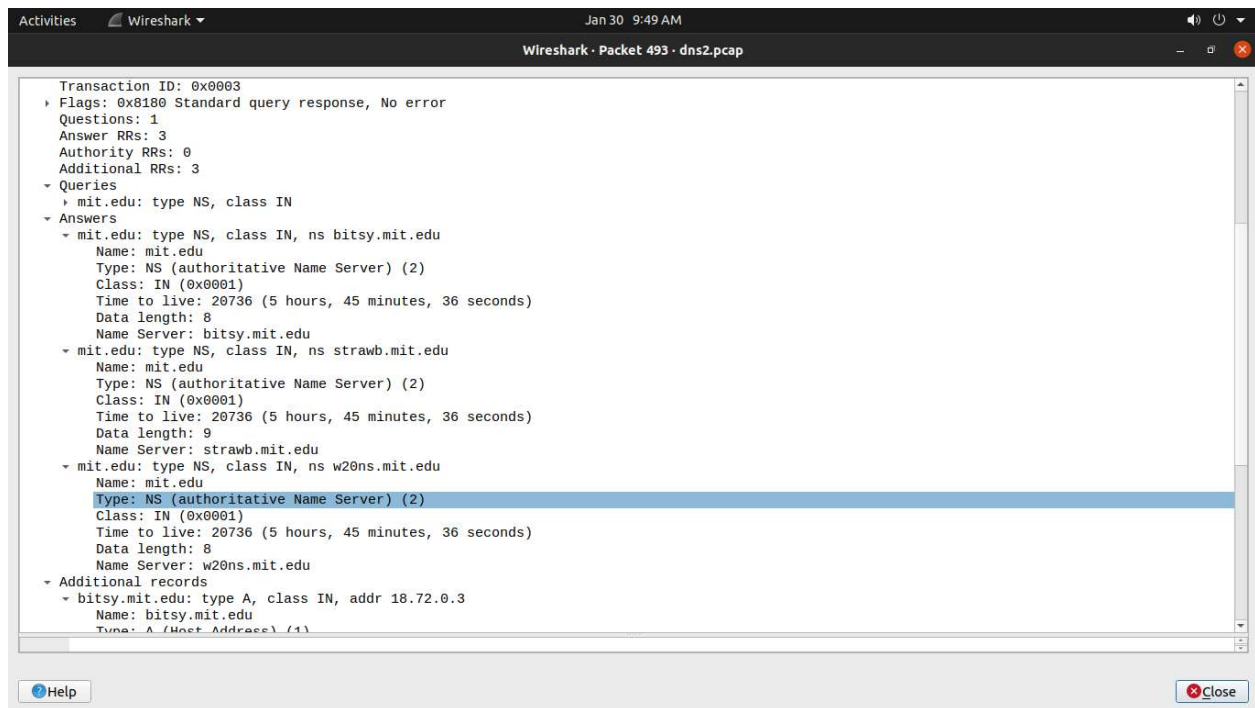


Type: PTR

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:

