

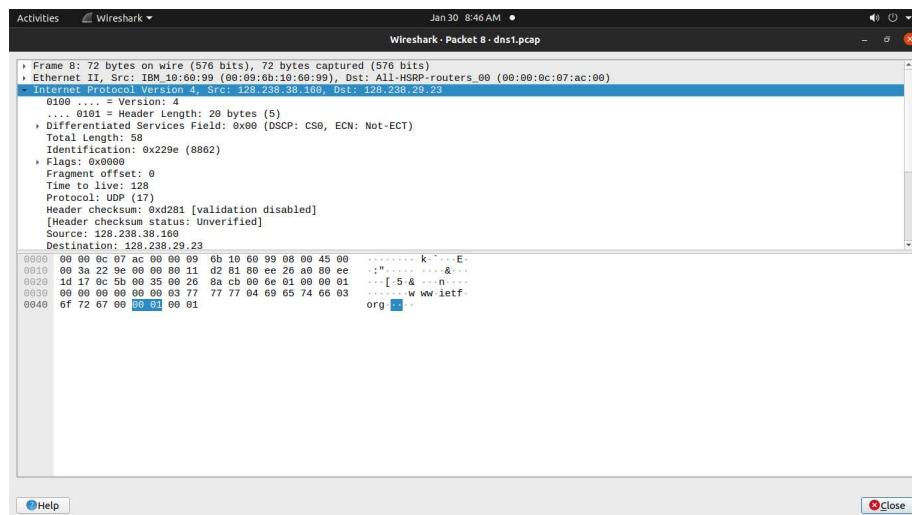
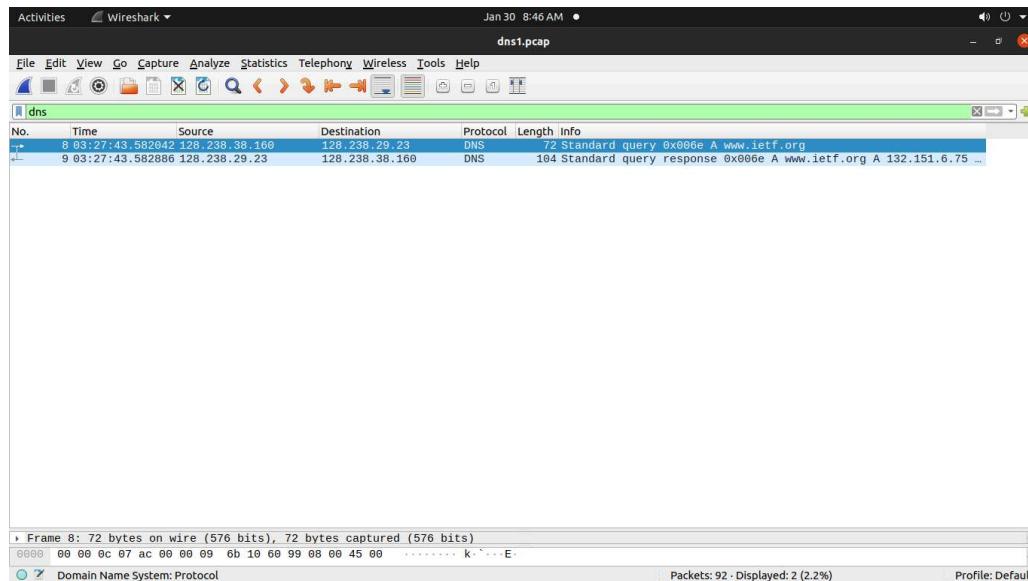
ASSIGNMENT -03

SUB CODE: CS3072

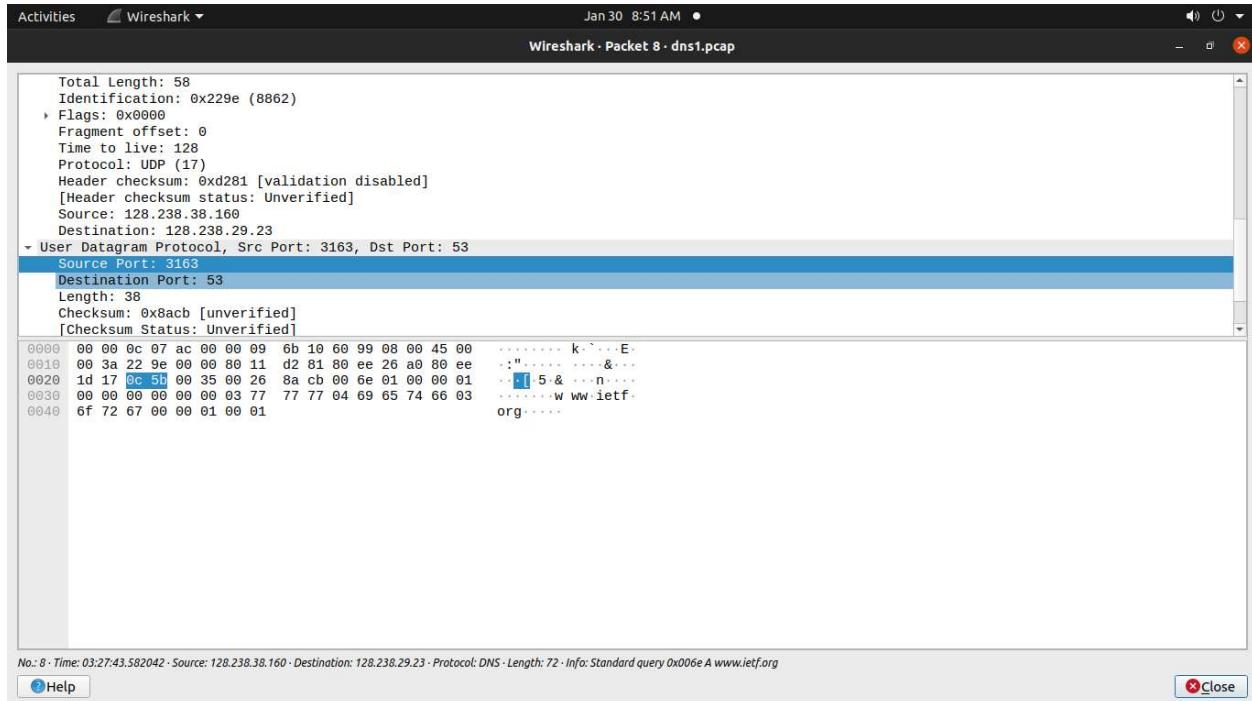
NAME: Aditee Ping

ROLL NO: 123CS0204

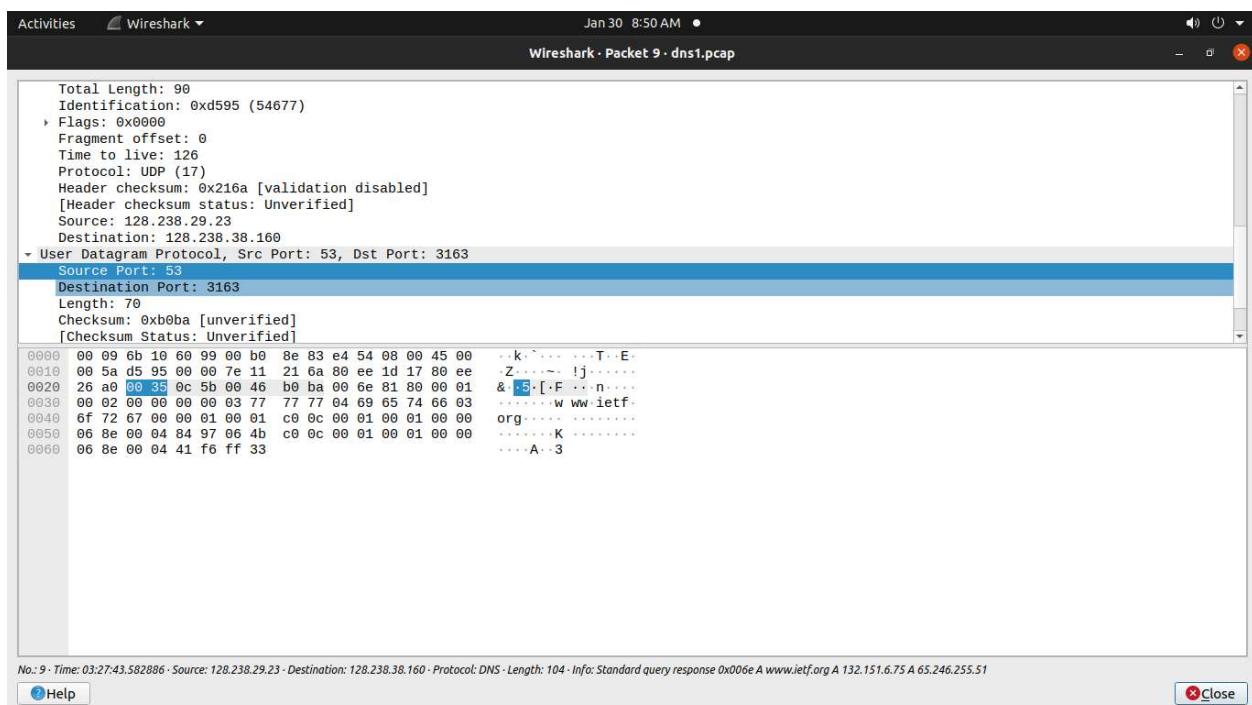
Q1. Locate the DNS query and response messages. Are they sent over UDP or TCP?



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



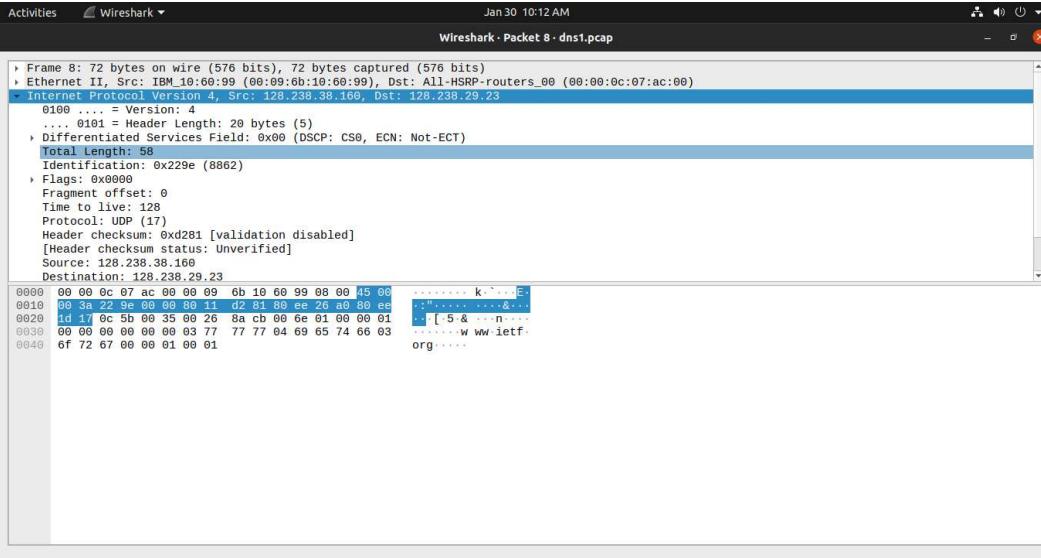
Destination port of the query message: 53



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

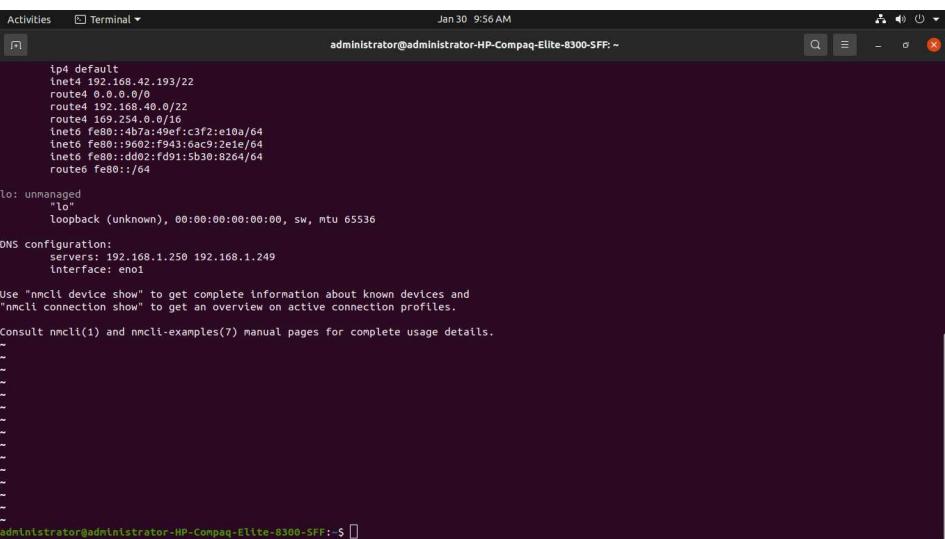


The Wireshark screenshot shows a single DNS query packet (Frame 8) captured on Jan 30 at 10:12 AM. The packet details show the following:

- Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
- Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
- Internet Protocol Version 4, Src: 128.238.38.166, Dst: 128.238.29.23
- Total Length: 56
- Identification: 0x229e (8862)
- Flags: 0x0000
- Fragment offset: 0
- Time to live: 128
- Protocol: UDP (17)
- Header checksum: 0xd281 [validation disabled]
- [Header checksum status: Unverified]
- Source: 128.238.38.166
- Destination: 128.238.29.23

The hex dump shows the DNS query message:

```
0000  00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 46 00 K .E.
0010  00 00 22 06 00 00 11 d2 01 00 00 26 a9 00 ad
0020  1d 17 0c 5b 00 35 00 26 8a cb 00 6e 01 00 00 01 1 5 & n .
0030  00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 1 5 & n .
0040  6f 72 67 00 00 01 00 01 org .....
```

```
Activities Terminal Jan 30 9:56 AM
administrator@administrator-HP-Compaq-Elite-8300-SFF: ~

ip4 default
inet4 192.168.42.193/22
routed 0.0.0.0/0
route4 192.168.40.0/22
route4 169.254.0.0/16
inet6 fe80::4b7a:49ef:c3f2:e10a/64
inet6 fe80::9602:f943:0a95:ce1e/64
inet6 fe80::dd62:fd91:5b38:8264/64
routed fe80::/64

lo: unmanaged
    "lo"
    loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

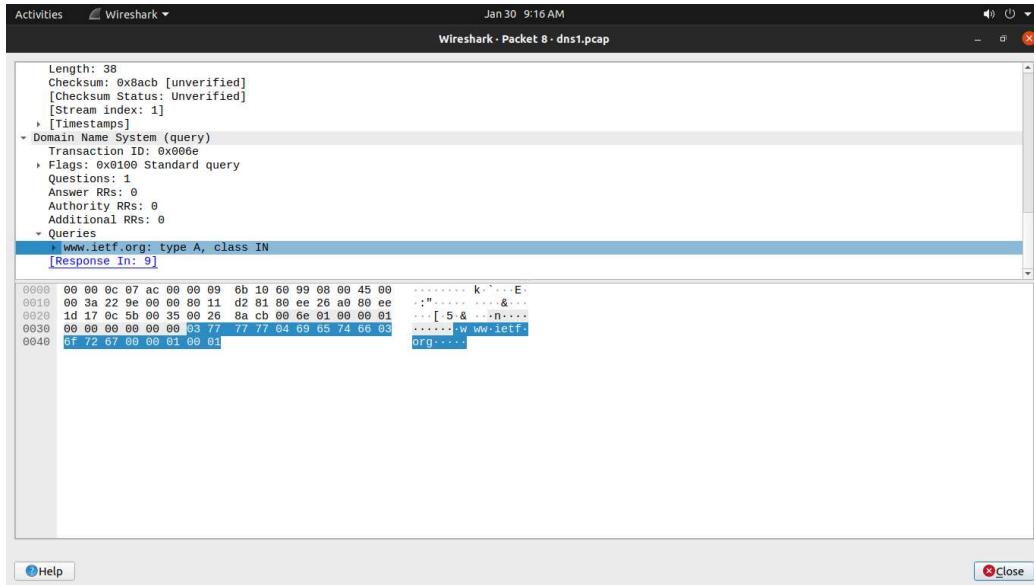
DNS configuration:
  servers: 192.168.1.250 192.168.1.249
  interface: en0

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(7) manual pages for complete usage details.
~
```

IP address of your local DNS server -192.168.1.250 192.168.1.249

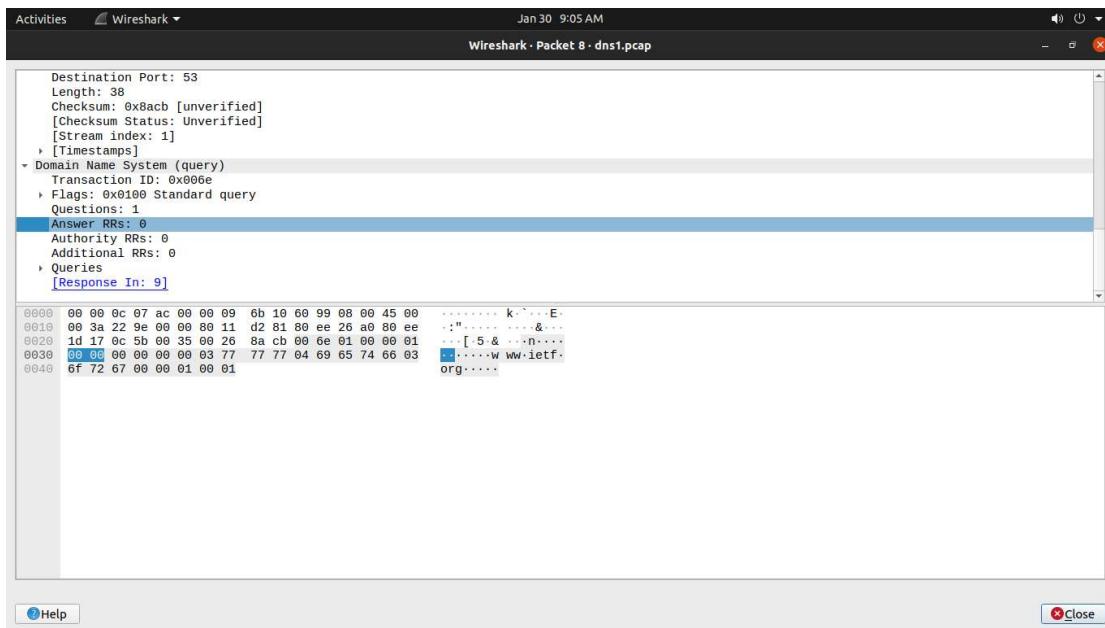
Q 4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any answers?



Type:A

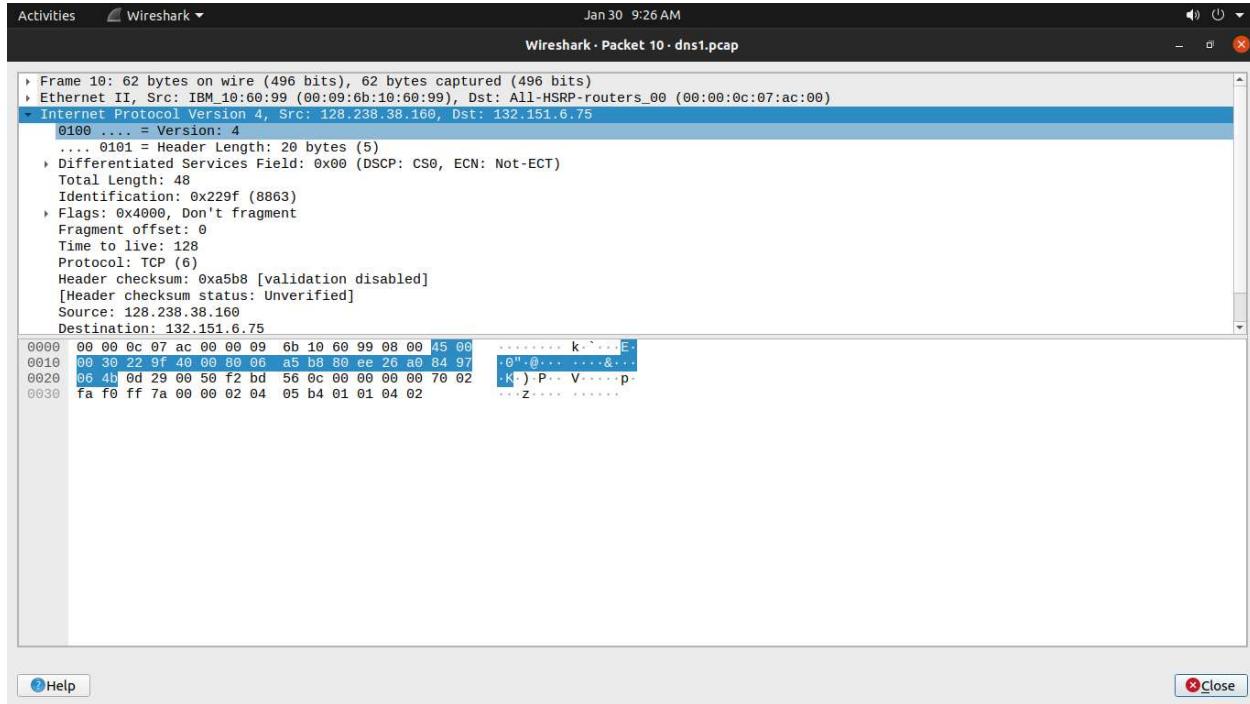
Answers : 0

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?

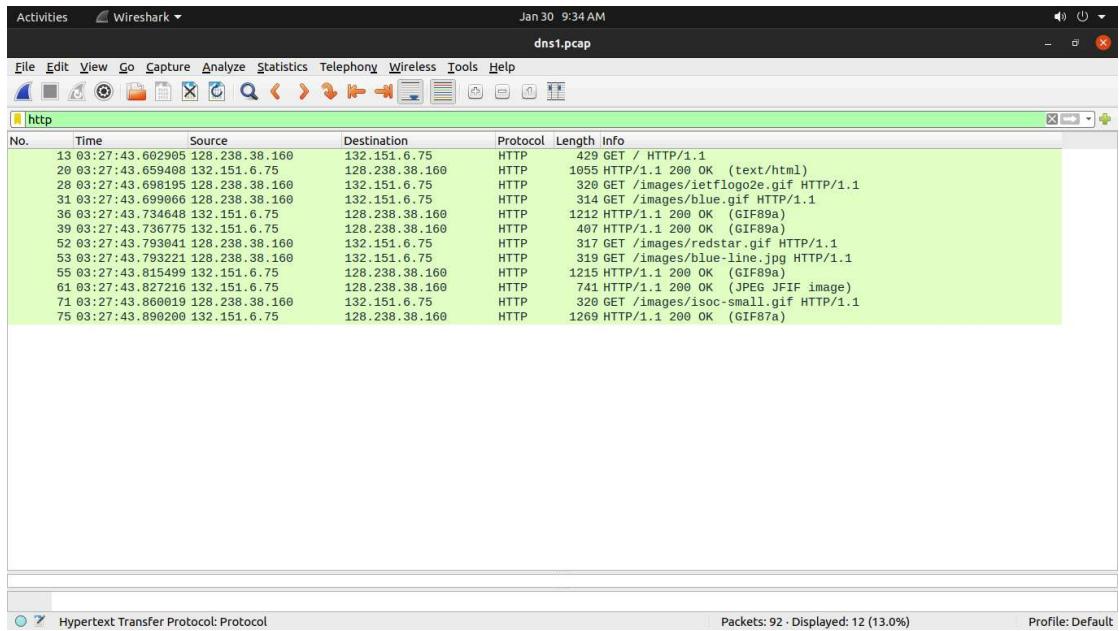


Destination IP address: 132.165.6.75

Yes it corresponds to the IP addresses provided in the DNS response message.

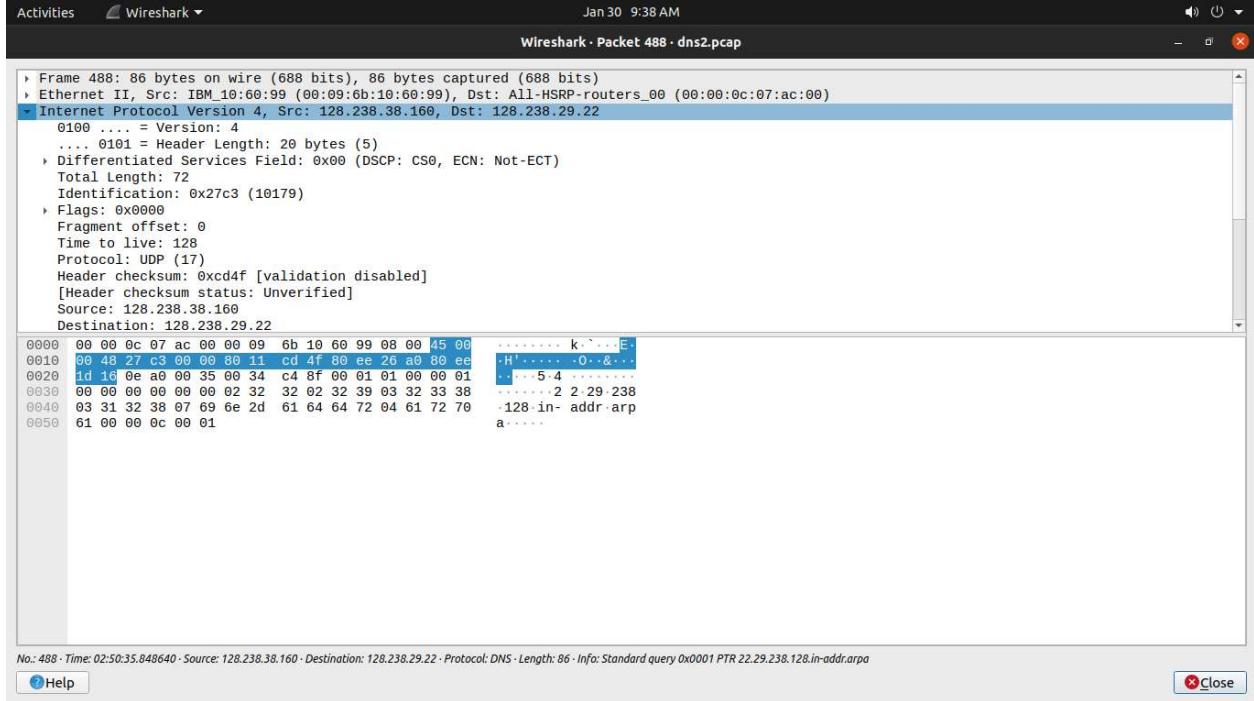
Q7. This web pages contain images. Before retrieving each image, does your host issue new DNS queries?

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



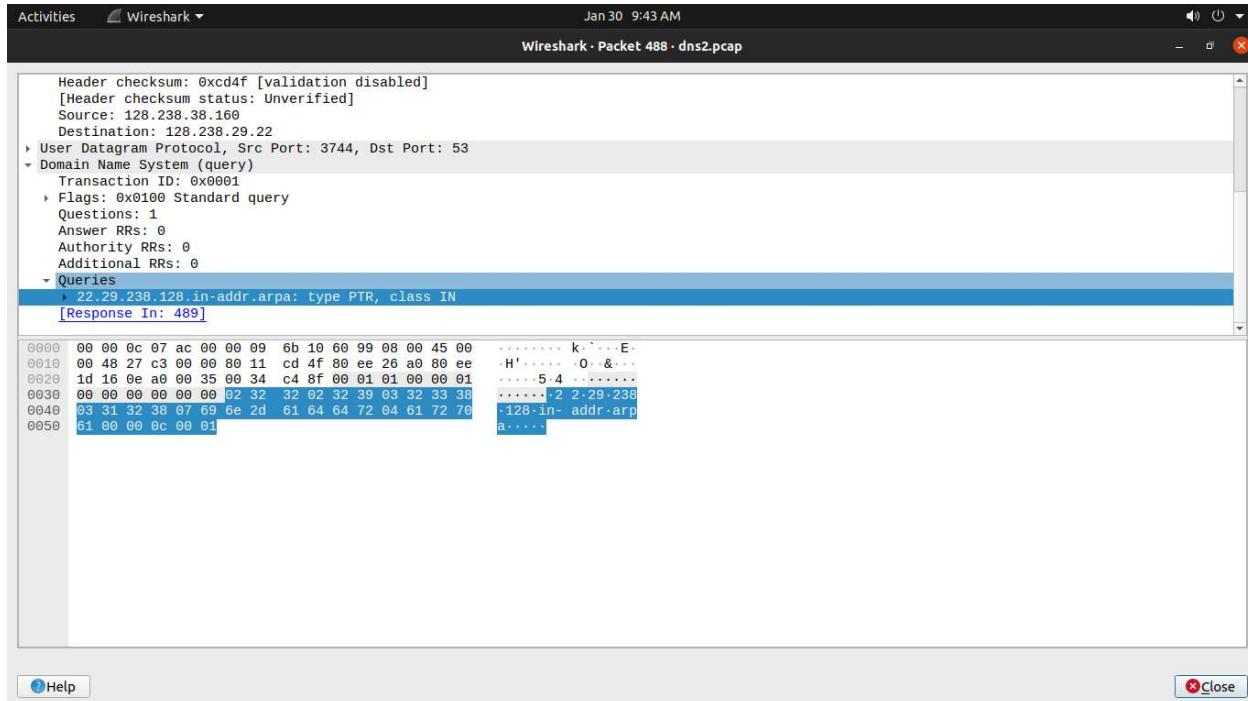
IN DNS2.PCAP:

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”?

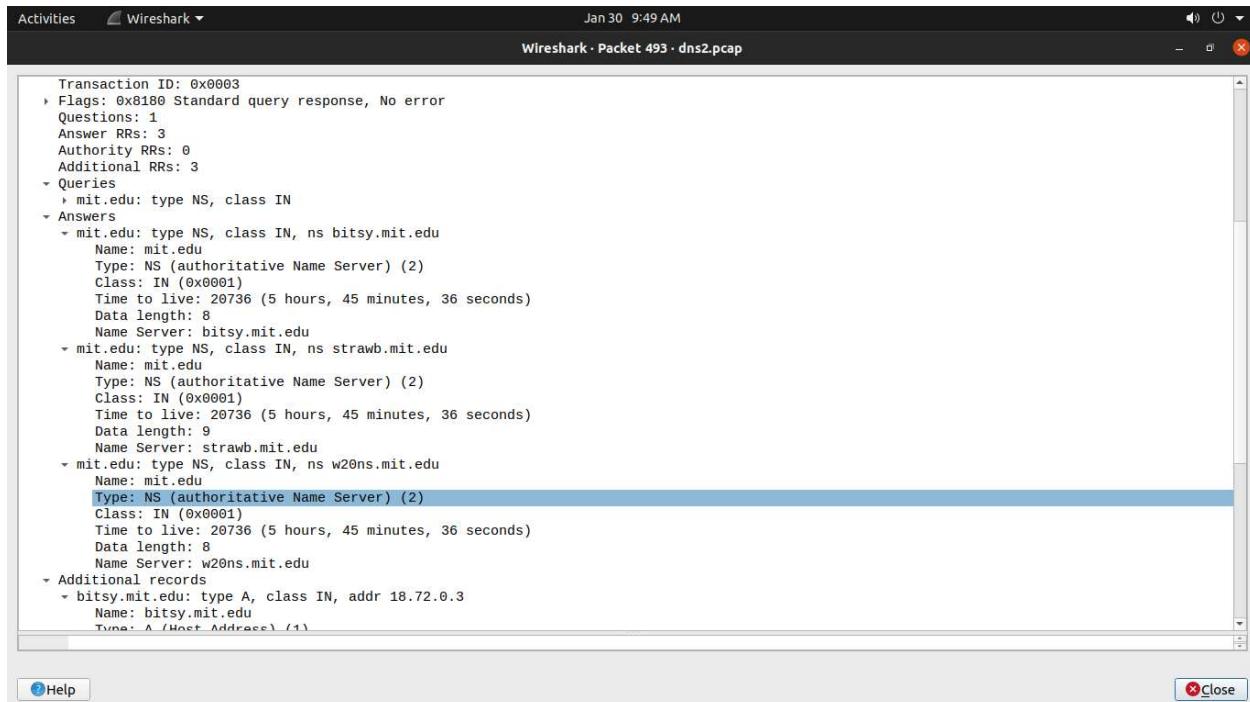


Type: PTR

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:

