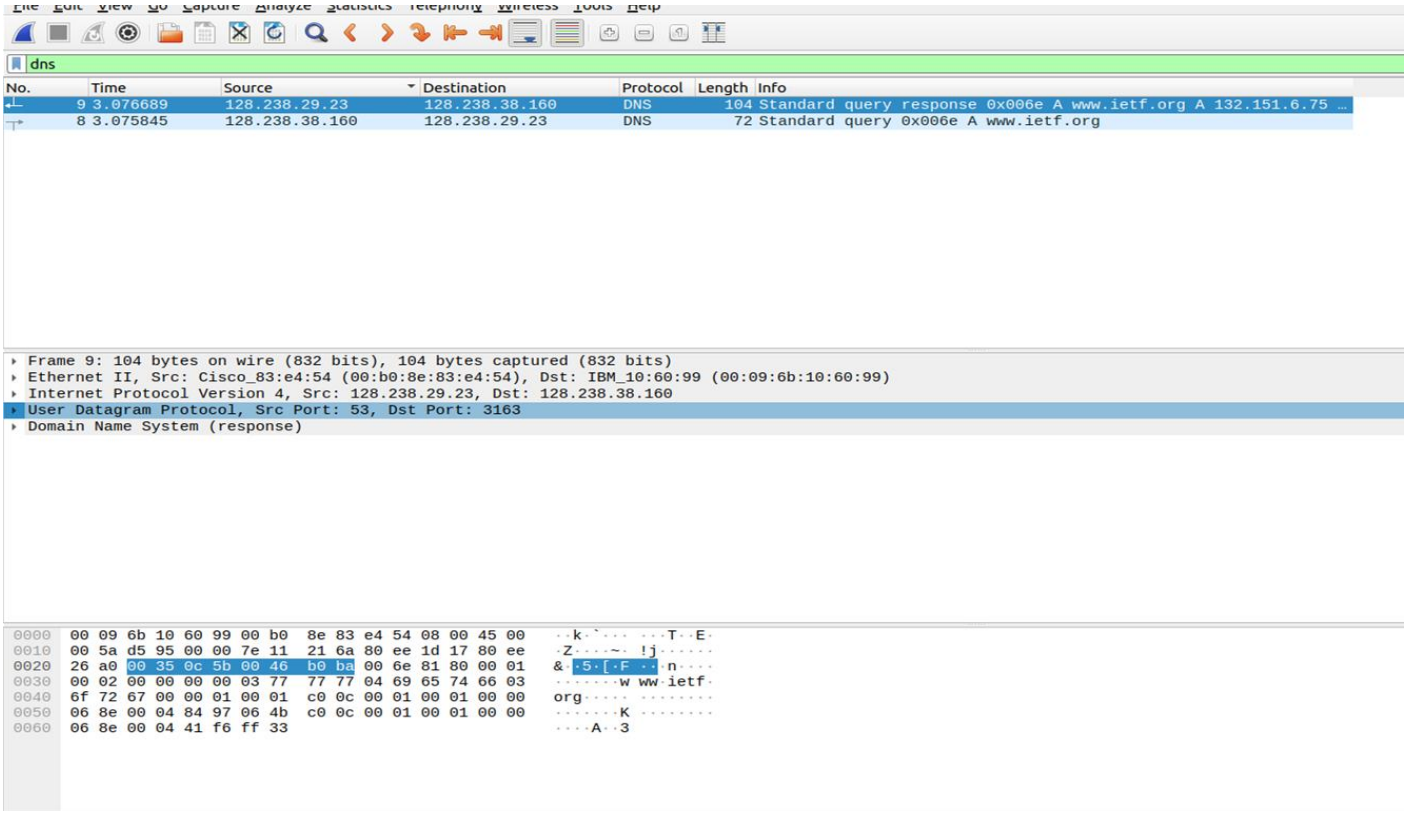
DCCN LAB -03

NAME: ATISH KUMAR
ROLL NO: 120CS0173
DATE: 19 JAN, 2023

Q1: Answer the following questions for captured file dns1.pcap (DNS Protocol)

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

Soln:



User Datagram Protocol(UDP) sent.

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

Soln:

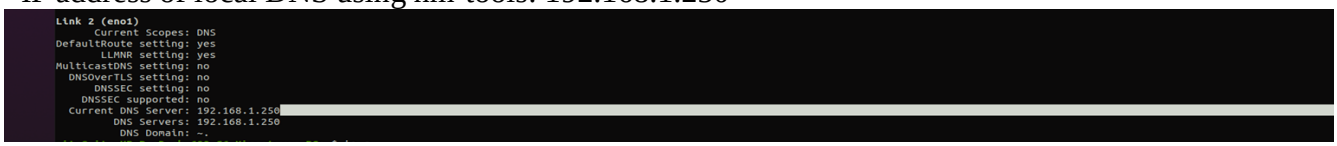
Destination port for the DNS query message : 128.238.29.23
Source port of DNS response message: 128.238.29.23

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

Soln:

IP address: 128.238.29.23

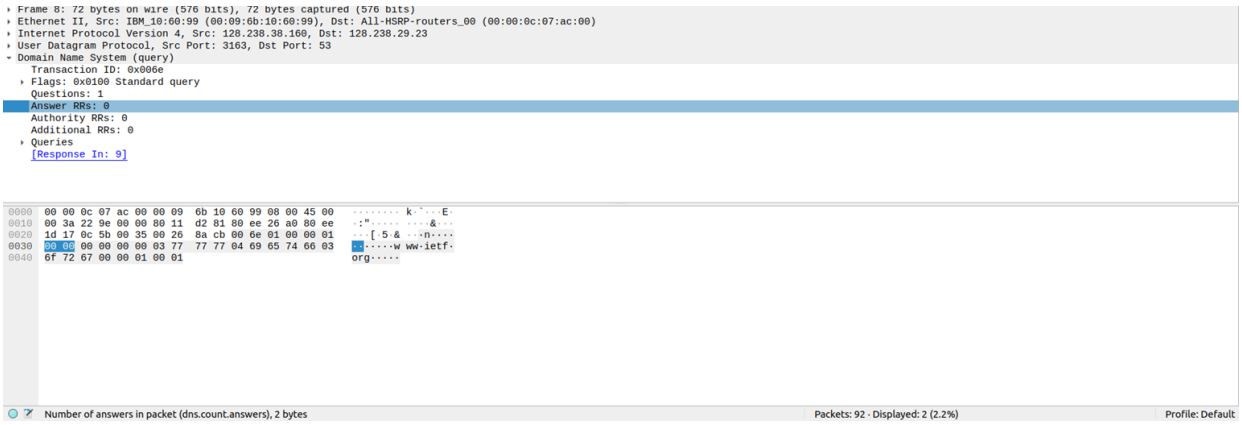
IP address of local DNS using nm-tools: 192.168.1.250



these two IP addresses are not the same.

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

Soln:

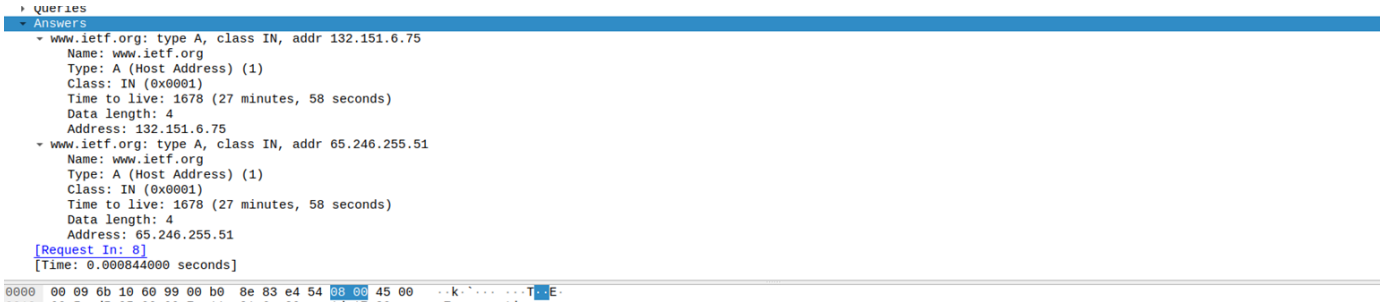


It's type a standard query and it doesnt contain any answers.

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

Soln:

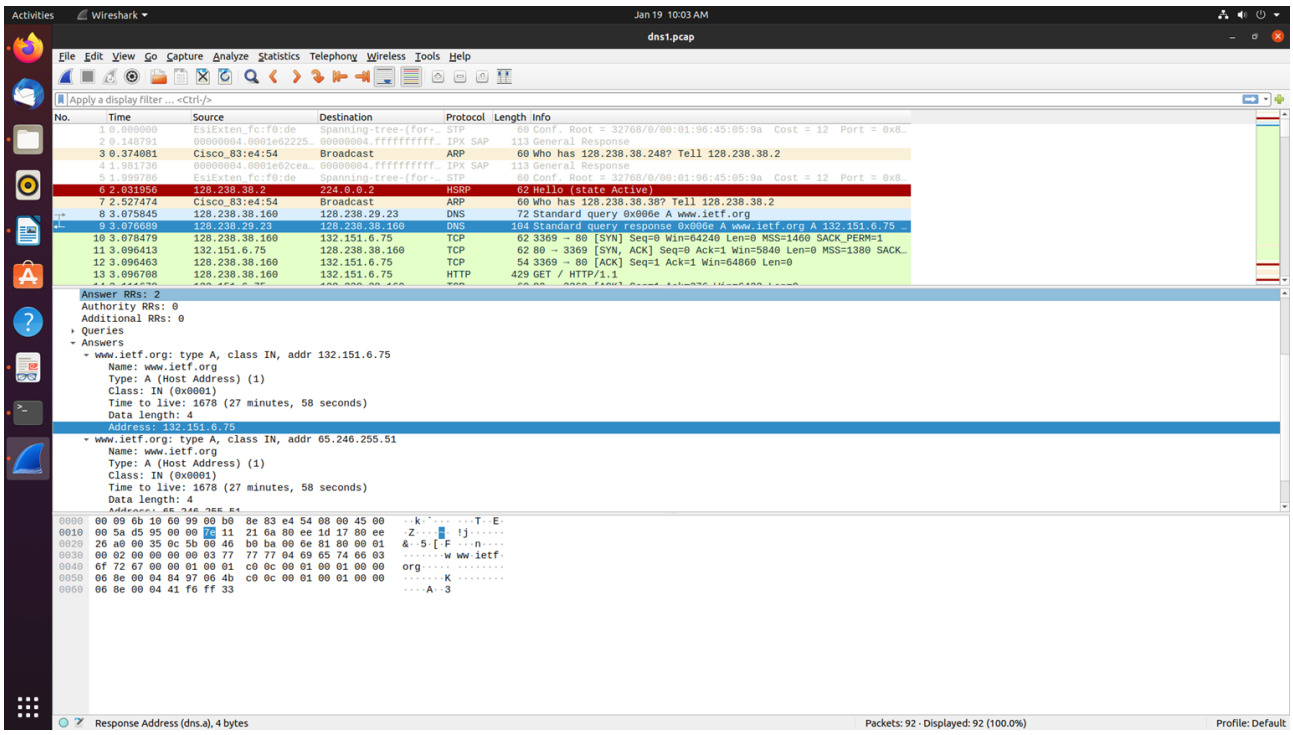
Two answer found..



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?

Soln:

Yes, the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message.



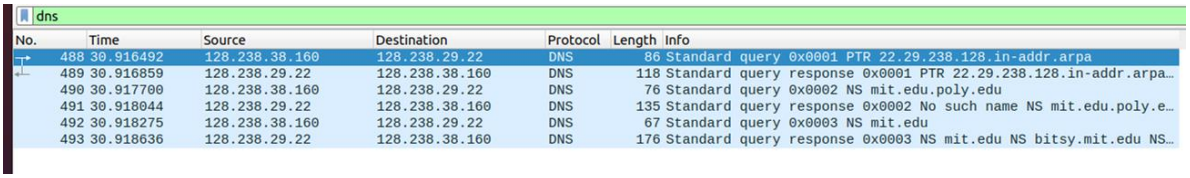
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Use the command: nslookup –type=NS mit.edu (Use dns2.pcap file)

Soln: No,the images are all loaded from www.ietf.org, so no additional DNS queries are necessary.

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

Soln: IP Address: 128.238.29.22

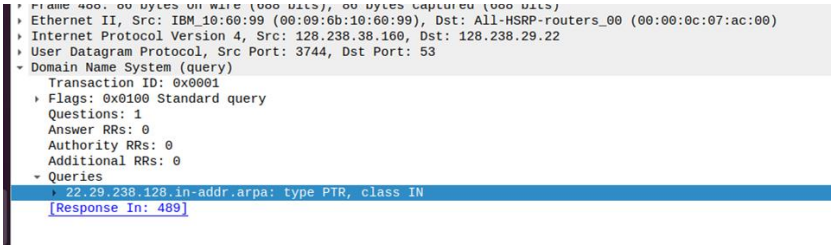


No.	Time	Source	Destination	Protocol	Length	Info
488	30.916492	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489	30.916859	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa…
490	30.917700	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.poly.edu
491	30.918044	128.238.29.22	128.238.38.160	DNS	135	Standard query response 0x0002 No such name NS mit.edu.poly.e…
492	30.918275	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
493	30.918636	128.238.29.22	128.238.38.160	DNS	176	Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS…

This is not the IP address of default local DNS server.

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

Soln:



```
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: 128.238.38.160, Dst: 128.238.29.22
User Datagram Protocol, Src Port: 3744, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0001
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        22.29.238.128.in-addr.arpa: type PTR, class IN
    [Response In: 489]
```

It is PTR type of DNS query.
Zero query message contrains any 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?

Soln:

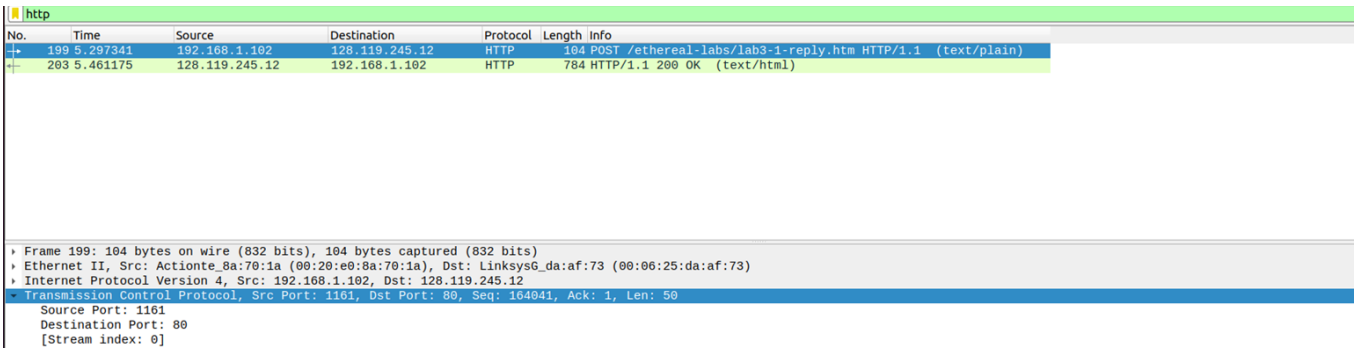
Answer contains name of domain,type,class,time to live,data length,address.
Yes it also provide nameserver IP-22.29.238.128

Q2: Answer the following questions for captured file tcp.pcap (TCP Protocol)

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows.

Soln:

IP address: 192.168.1.102
tcp Source port no: 1161



2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Soln: IP address = 128.119.245.12
Port number = 80

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

Soln:
IP address = 192.168.1.102
TCP port number = 1161

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Soln:
Sequence number = 0 (relative), 232129012 (raw)
The segment has its SYN flag set to 1.
From this information, we can classify the segment as SYN.

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Soln: Sequence number = 0 (relative), 883061785 (raw)
Value of Acknowledgement field = 1 (relative), 232129013 (raw)

6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Soln:
Sequence No: 164041

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What is the length of each of the first six TCP segments?

Soln:

source port-4
destination port-4
sequence no-8
acknoledgement no-8
the first 6
segment size-1460 Bytes

8. What is the EstimatedRTT value (see Section 3.5.3, page 239 in text from Kurose Book) after the receipt of each ACK? Assume that the value of the Estimated RTT is equal to the measured RTT for the first segment.
[Hint: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu
server. Select as Statistics->TCP Stream Graph->Round Trip Time Graph.]

Soln:

4-
Estimated rtt- (1-0.125)*0+0.125*0=0
5-
Estimated rtt- (1-0.125)*0+0.125*0.0122=0.001525
13-
Estimated rtt-(1-0.125)*very small value+0.125*0.0001=0.0000125