

COMPUTER NETWORK ORGANIZATION

Lab 1

Q1. List the 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Answer : The different protocols are :

1. HTTP
2. TCP
3. ARP
4. MDNS
5. TLS.

No.	Time	Source	Destination	Protocol	Length	Info
107	21:14:14.675200	192.168.1.7	224.0.0.251	MDNS	268	Standard query response 0x0000 PTR 25da0aff-2c33-23ec-7af2-dc5d4c7ee8b3._googlezone._tcp.local TXT, cache-
108	21:14:14.676368	192.168.1.7	224.0.0.251	MDNS	220	Standard query response 0x0000 PTR googlerpc._googlerpc._tcp.local TXT, cache flush SRV, cache flush 0 -
109	21:14:14.682783	192.168.1.8	224.0.0.251	MDNS	268	Standard query response 0x0000 PTR 585ad3ff-0c68-41ad-aa63-ce9978ee27a2._googlezone._tcp.local TXT, cache-
110	21:14:14.683201	192.168.1.8	224.0.0.251	MDNS	222	Standard query response 0x0000 PTR googlerpc-1._googlerpc._tcp.local TXT, cache flush SRV, cache flush 0 -
111	21:14:15.644125	192.168.1.2	128.119.245.12	HTTP	487	GET /favicon.ico HTTP/1.1
112	21:14:15.647430	192.168.1.5	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
113	21:14:15.693483	128.119.245.12	192.168.1.2	HTTP	537	HTTP/1.1 404 Not Found (text/html)
114	21:14:15.733438	192.168.1.2	128.119.245.12	TCP	54	51376 + 80 [ACK] Seq=935 Ack=921 Win=130304 Len=0
115	21:14:15.809026	Netgear_ab:c2:0e	HewlettP_7f:e8:f5	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
116	21:14:15.809057	HewlettP_7f:e8:f5	Netgear_ab:c2:0e	ARP	42	192.168.1.2 is at 74:46:a0:7f:e8:f5
117	21:14:16.649212	192.168.1.5	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
118	21:14:16.789335	192.168.1.2	192.168.1.7	TCP	164	51365 + 8009 [PSH, ACK] Seq=221 Ack=221 Win=509 Len=110 [TCP segment of a reassembled PDU]
119	21:14:16.791218	192.168.1.7	192.168.1.2	TCP	164	8009 + 51365 [PSH, ACK] Seq=221 Ack=331 Win=279 Len=110 [TCP segment of a reassembled PDU]
120	21:14:16.820534	192.168.1.2	192.168.1.8	TCP	164	51366 + 8009 [PSH, ACK] Seq=221 Ack=221 Win=509 Len=110 [TCP segment of a reassembled PDU]
121	21:14:16.825631	192.168.1.8	192.168.1.2	TCP	164	8009 + 51366 [PSH, ACK] Seq=221 Ack=331 Win=279 Len=110 [TCP segment of a reassembled PDU]
122	21:14:16.835845	192.168.1.2	192.168.1.7	TCP	54	51365 + 8009 [ACK] Seq=331 Ack=331 Win=509 Len=0
123	21:14:16.877856	192.168.1.2	192.168.1.8	TCP	54	51366 + 8009 [ACK] Seq=331 Ack=331 Win=509 Len=0
124	21:14:16.952198	192.168.1.2	20.36.219.28	TCP	54	51257 + 443 [FIN, ACK] Seq=1 Ack=1 Win=516 Len=0
125	21:14:16.952631	192.168.1.2	20.36.219.28	TCP	66	51378 + 443 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
126	21:14:16.986704	20.36.219.28	192.168.1.2	TCP	60	443 + 51257 [FIN, ACK] Seq=1 Ack=2 Win=2053 Len=0
127	21:14:16.986901	192.168.1.2	20.36.219.28	TCP	54	51257 + 443 [ACK] Seq=2 Ack=2 Win=516 Len=0
128	21:14:16.987265	20.36.219.28	192.168.1.2	TCP	66	443 + 51378 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
129	21:14:16.987344	192.168.1.2	20.36.219.28	TCP	54	51378 + 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
130	21:14:16.994574	192.168.1.2	20.36.219.28	TLSv1.2	267	Client Hello
131	21:14:17.030836	20.36.219.28	192.168.1.2	TCP	1514	443 + 51378 [ACK] Seq=1 Ack=214 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
132	21:14:17.031554	20.36.219.28	192.168.1.2	TCP	1514	443 + 51378 [ACK] Seq=1461 Ack=214 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
133	21:14:17.031554	20.36.219.28	192.168.1.2	TCP	1514	443 + 51378 [ACK] Seq=2921 Ack=214 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
134	21:14:17.031554	20.36.219.28	192.168.1.2	TCP	1514	443 + 51378 [ACK] Seq=4381 Ack=214 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
135	21:14:17.031554	20.36.219.28	192.168.1.2	TLSv1.2	355	Server Hello, Certificate, Certificate Status, Server Key Exchange, Certificate Request, Server Hello Done
136	21:14:17.031666	192.168.1.2	20.36.219.28	TCP	54	51378 + 443 [ACK] Seq=214 Ack=6142 Win=132352 Len=0
137	21:14:17.034638	192.168.1.2	20.36.219.28	TLSv1.2	154	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
138	21:14:17.069835	20.36.219.28	192.168.1.2	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
139	21:14:17.071386	192.168.1.2	20.36.219.28	TLSv1.2	1657	Application Data
140	21:14:17.071465	192.168.1.2	20.36.219.28	TLSv1.2	1504	Application Data

> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0
> Ethernet II, Src: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5), Dst: Google a8:c2:4b (20:df:b9:a8:c2:4b)

wireshark_Ethernet_20200708211405_a10952.pcapng

Packets: 163 · Displayed: 163 (100.0%)

Profile: Default

Q2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select *Time Display Format*, then select *Time-of-day*.)

Answer : As seen below

- HTTP GET was sent at 21:14:13.928692 , and
- HTTP OK was received at 21:14:13.981218.
- The **delay 21:14:13.52526 secs.**

The screenshot shows the Wireshark interface with the following details:

- Packet List:** Shows 113 total packets. The 6th packet is highlighted, showing a GET request to "INTRO-wireshark-labs/k-file1.html". The 8th packet is also highlighted, showing an HTTP 200 OK response.
- Details Pane:** Displays the raw hex and ASCII data for the selected packet (6). It shows the HTTP request and response frames.
- Bytes Pane:** Displays the raw hex and ASCII data for the selected packet (6), showing the transmitted data.
- Status Bar:** Shows "Packets: 163 · Displayed: 4 (2.5%) · Dropped: 0 (0.0%) · Profile: Default".

Q3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

Answer : As shown below

- The Ip address of source (My computer) is - **192.168.1.2**
- The Ip address of destination (gaia.cs.umass.edu) is - **128.119.245.12**

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, capturing, analyzing, and saving.
- Packet List:** Shows 113 total packets. The first few are highlighted in green, indicating they are selected or belong to the current analysis.
- Selected Packet:** Frame 68 is selected, showing its details and bytes.
- Details Pane:** Displays the structure of the selected frame, including the Ethernet II header, Internet Protocol Version 4 header, and the HTTP request message.
- Bytes Pane:** Shows the raw hex and ASCII representation of the selected frame.
- Status Bar:** Shows "Packets: 163 · Displayed: 4 (2.5%) · Dropped: 0 (0.0%) · Profile: Default".

Q4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the “*Selected Packet Only*” and “*Print as displayed*” radial buttons, and then click OK.

Answer :

HTTP GET :

No.	Time	Source	Destination	Protocol	Length	Info
68	21:14:13.928692	192.168.1.2	128.119.245.12	HTTP	555	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 68: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 541

Identification: 0x178c (6028)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 51376, Dst Port: 80, Seq: 1, Ack: 1, Len: 501

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
84	21:14:13.981218	128.119.245.12	192.168.1.2	HTTP	491	HTTP/1.1 200 OK (text/html)

Frame 84: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 477

Identification: 0xd25b (53851)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 44

Protocol: TCP (6)

Header checksum: 0x4391 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

Transmission Control Protocol, Src Port: 80, Dst Port: 51376, Seq: 1, Ack: 502,
Len: 437

Hypertext Transfer Protocol

Line-based text data: text/html (3 lines)

No.	Time	Source	Destination	Protocol	Length	Info
111	21:14:15.644125	192.168.1.2	128.119.245.12	HTTP	487	GET /favicon.ico HTTP/1.1

Frame 111: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 473

Identification: 0x178f (6031)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 51376, Dst Port: 80, Seq: 502, Ack: 438, Len: 433

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol Length Info
-----	------	--------	-------------	----------------------

113 21:14:15.693483 128.119.245.12 192.168.1.2 HTTP 537
HTTP/1.1 404 Not Found (text/html)

Frame 113: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 523

Identification: 0xd25c (53852)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 44

Protocol: TCP (6)

Header checksum: 0x4362 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

Transmission Control Protocol, Src Port: 80, Dst Port: 51376, Seq: 438, Ack: 935,
Len: 483

Hypertext Transfer Protocol

Line-based text data: text/html (7 lines)

HTTP OK Message :

No.	Time	Source	Destination	Protocol	Length	Info
68	21:14:13.928692	192.168.1.2	128.119.245.12	HTTP	555	
		GET /wireshark-labs/INTRO-wireshark-file1.html		HTTP/1.1		

Frame 68: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 541

Identification: 0x178c (6028)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 51376, Dst Port: 80, Seq: 1, Ack: 1, Len: 501

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
84	21:14:13.981218	128.119.245.12	192.168.1.2	HTTP	491	HTTP/1.1 200 OK (text/html)

Frame 84: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 477

Identification: 0xd25b (53851)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 44

Protocol: TCP (6)

Header checksum: 0x4391 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

Transmission Control Protocol, Src Port: 80, Dst Port: 51376, Seq: 1, Ack: 502,
Len: 437

Hypertext Transfer Protocol

Line-based text data: text/html (3 lines)

No.	Time	Source	Destination	Protocol	Length	Info
111	21:14:15.644125	192.168.1.2	128.119.245.12	HTTP	487	GET /favicon.ico HTTP/1.1

Frame 111: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 473

Identification: 0x178f (6031)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 51376, Dst Port: 80, Seq: 502, Ack: 438, Len: 433

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol Length Info
-----	------	--------	-------------	----------------------

113 21:14:15.693483 128.119.245.12 192.168.1.2 HTTP 537
HTTP/1.1 404 Not Found (text/html)

Frame 113: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0

Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 523

Identification: 0xd25c (53852)

Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 44

Protocol: TCP (6)

Header checksum: 0x4362 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

Transmission Control Protocol, Src Port: 80, Dst Port: 51376, Seq: 438, Ack: 935,
Len: 483

Hypertext Transfer Protocol

Line-based text data: text/html (7 lines)

(File for HTTP GET And HTTP OK is attached in the Zip folder)

(continued ..)

COMPUTER NETWORK ORGANIZATION

LAB 1

part -2

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

Answer : Ran *nslookup* on a Web server in Asia

- The IP address of that server is **210.212.207.171**

```
C:\Users\ratho>nslookup www.vtu.ac.in
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: www.vtu.ac.in
Address: 210.212.207.171
```

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

Answer : Run *nslookup* on Europe University : Oxford university .

```
Command Prompt
Microsoft Windows [Version 10.0.18363.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ratho>nslookup www.vtu.ac.in
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: www.vtu.ac.in
Address: 210.212.207.171
```

```
C:\Users\ratho>nslookup -type=NS ox.ac.uk
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk
ox.ac.uk      nameserver = dns2.ox.ac.uk
ox.ac.uk      nameserver = dns0.ox.ac.uk
ox.ac.uk      nameserver = ns2.ja.net
ox.ac.uk      nameserver = dns1.ox.ac.uk
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk

C:\Users\ratho>
```

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?

Answer : **Query Gets Refused.**

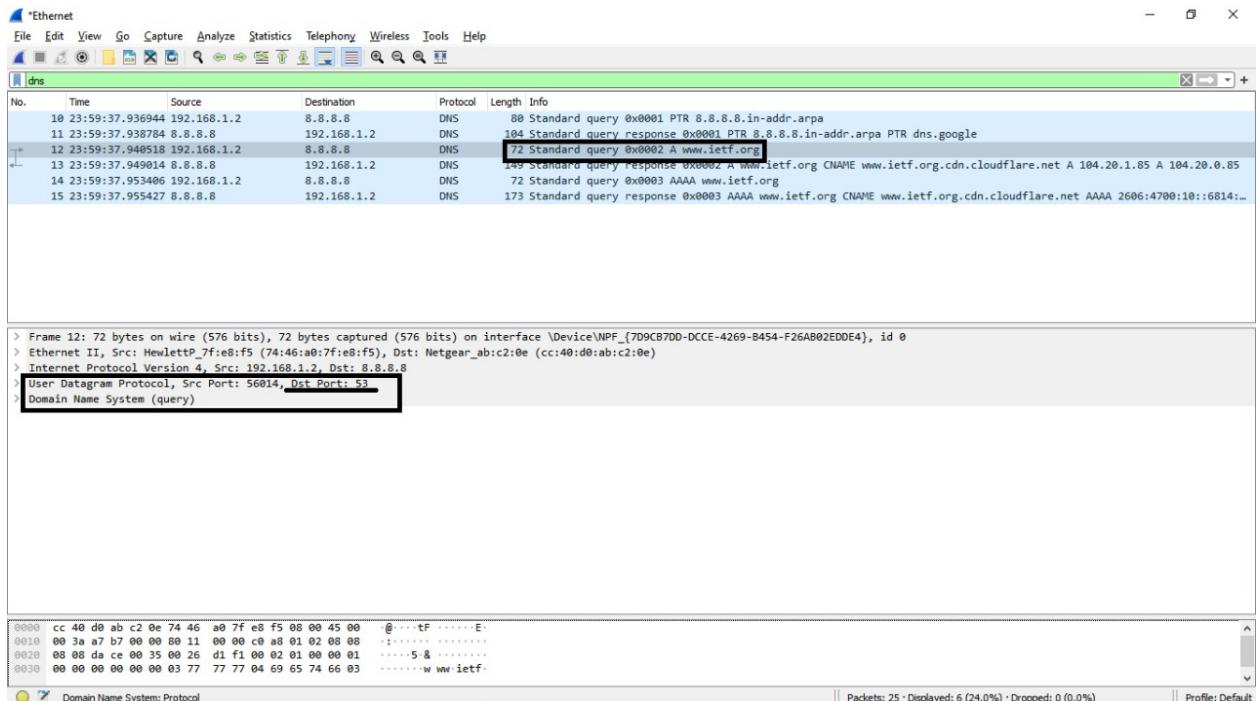
```
C:\Users\ratho>nslookup mail.yahoo.com auth4.dns.ox.ac.uk
Server:  UnKnown
Address:  45.33.127.156

*** UnKnown can't find mail.yahoo.com: Query refused
```

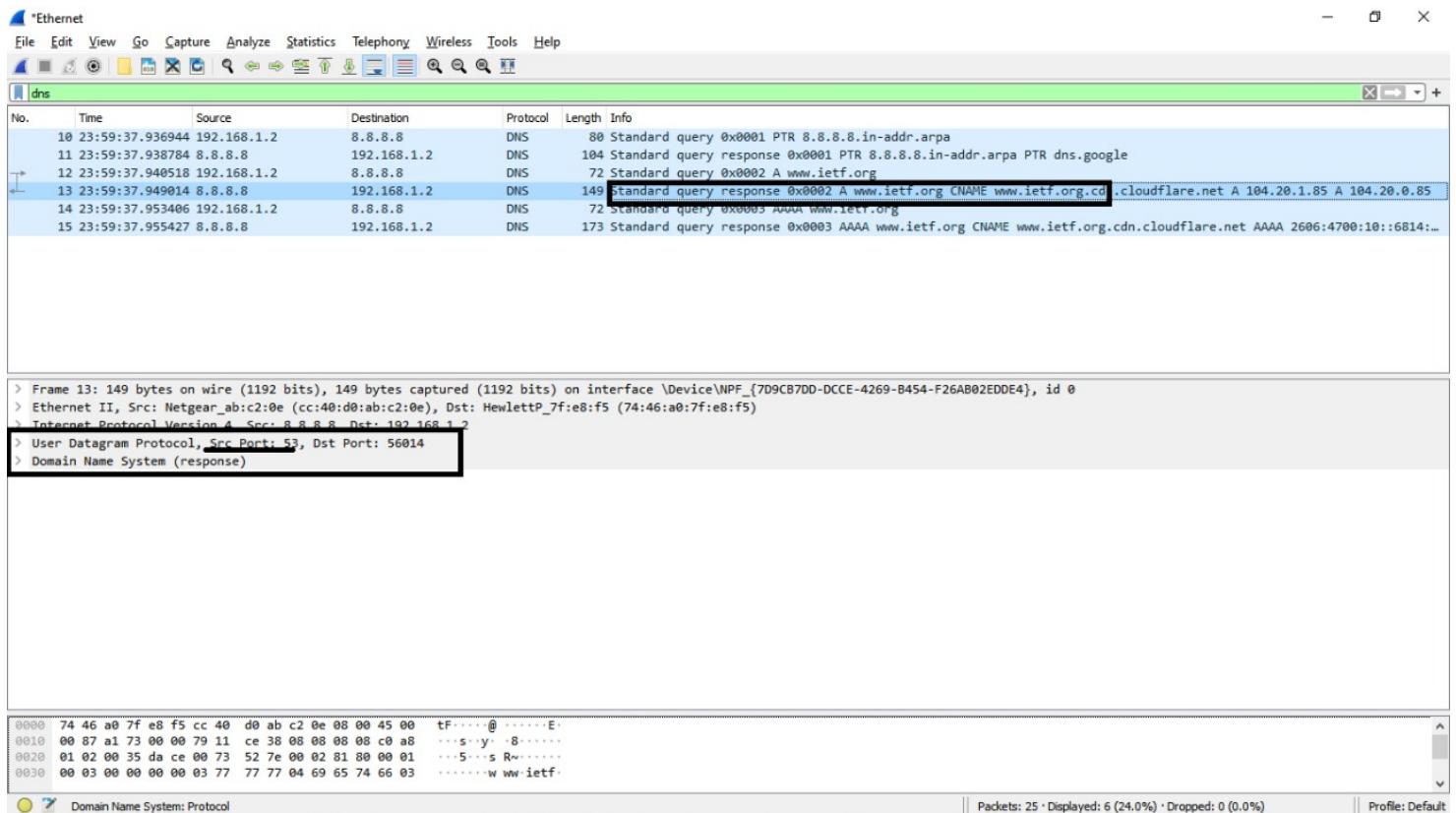
4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer :

- The DNS query and response messages are sent over **UDP**.
- DNS query Message



- DNS RESPONCE MESSAGE

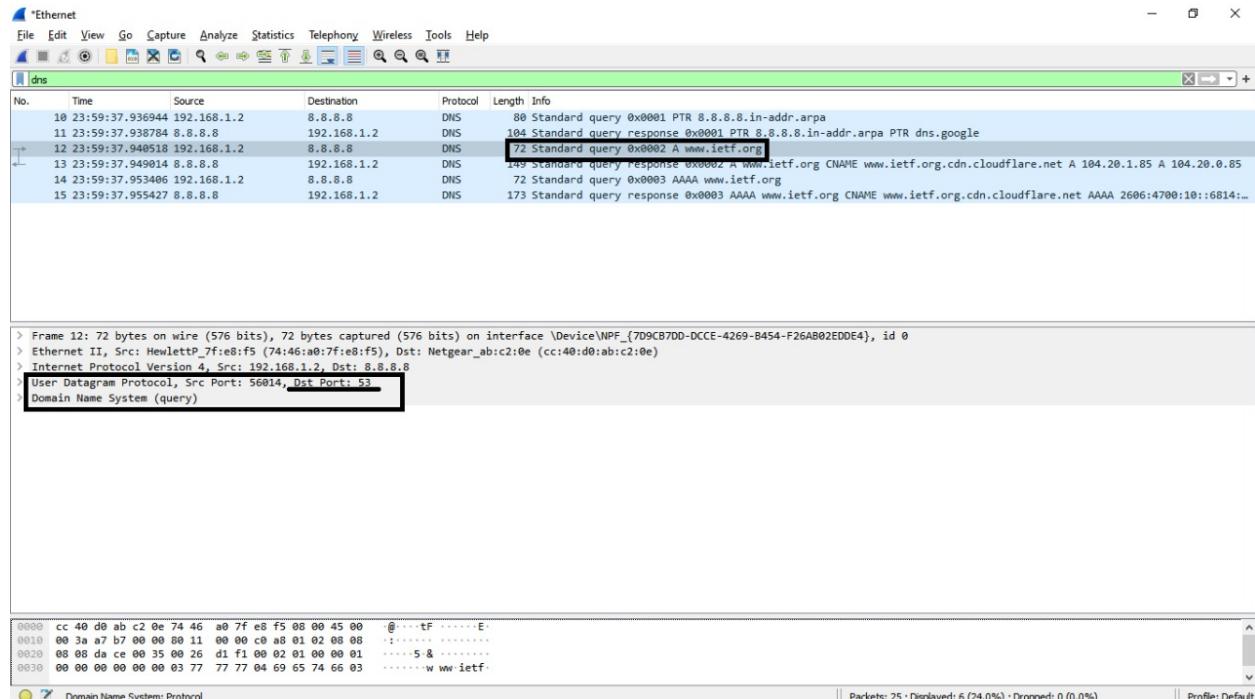


- What is the destination port for the DNS query message? What is the source port of DNS response message?

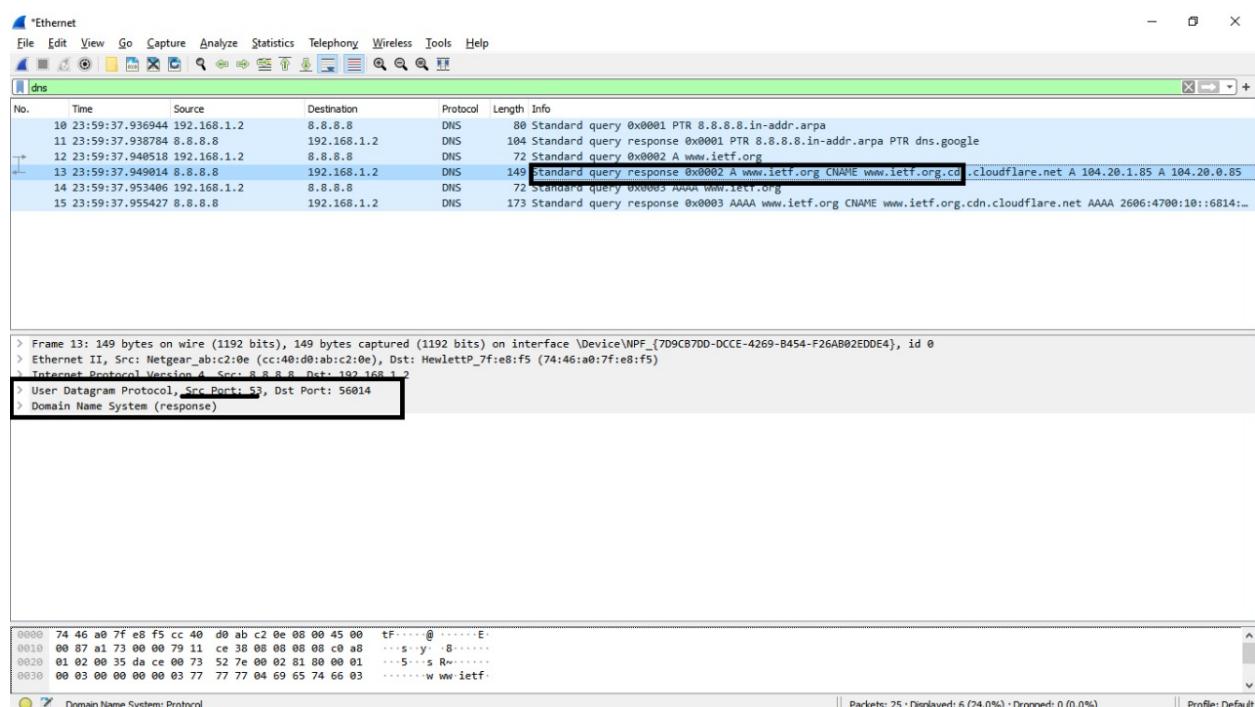
Answer :

- Destination port for the DNS query message : 53
- Source port of DNS response message : 53

- DNS query message :



- DNS response message :



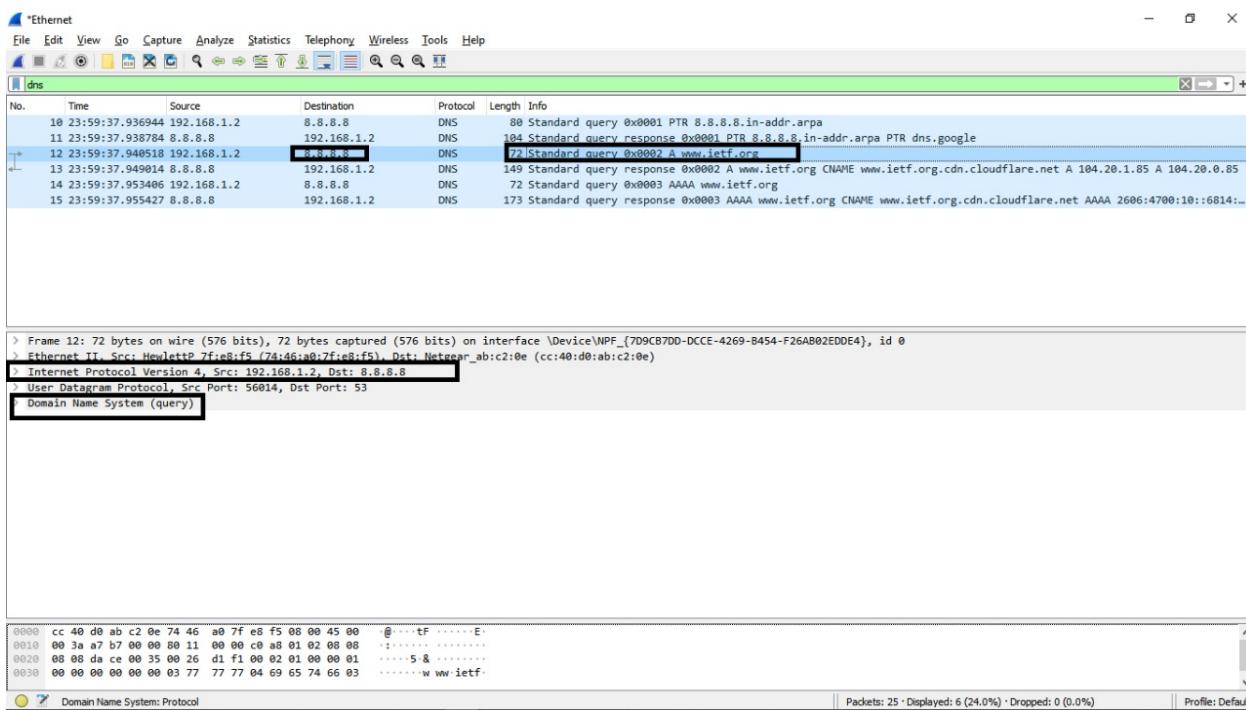
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Answer :

- DNS query message is sent to IP : **8.8.8.8**
- local DNS server : **8.8.8.8**

Yes the two IP address are the same.

DNS query message :



```
C:\Users\ratho>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-15C6NMD
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek PCIe FE Family Controller
Physical Address. . . . . : 74-46-A0-7F-E8-F5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::684f:bbaf:a66:3a2f%12(Preferred)
IPv4 Address. . . . . : 192.168.1.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 08 July 2020 08:19:48
Lease Expires . . . . . : 09 July 2020 20:53:08
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 74729120
DHCPv6 Client DUID . . . . . : 00-01-00-01-23-B0-23-E9-74-46-A0-7F-E8-F5
DNS Servers . . . . . : 8.8.8.8
                                         8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 2:

Media State . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . . . . . : Kaspersky Security Data Escort Adapter
Physical Address. . . . . . . . . : 00-FF-1E-50-48-47
DHCP Enabled. . . . . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Ethernet 8:

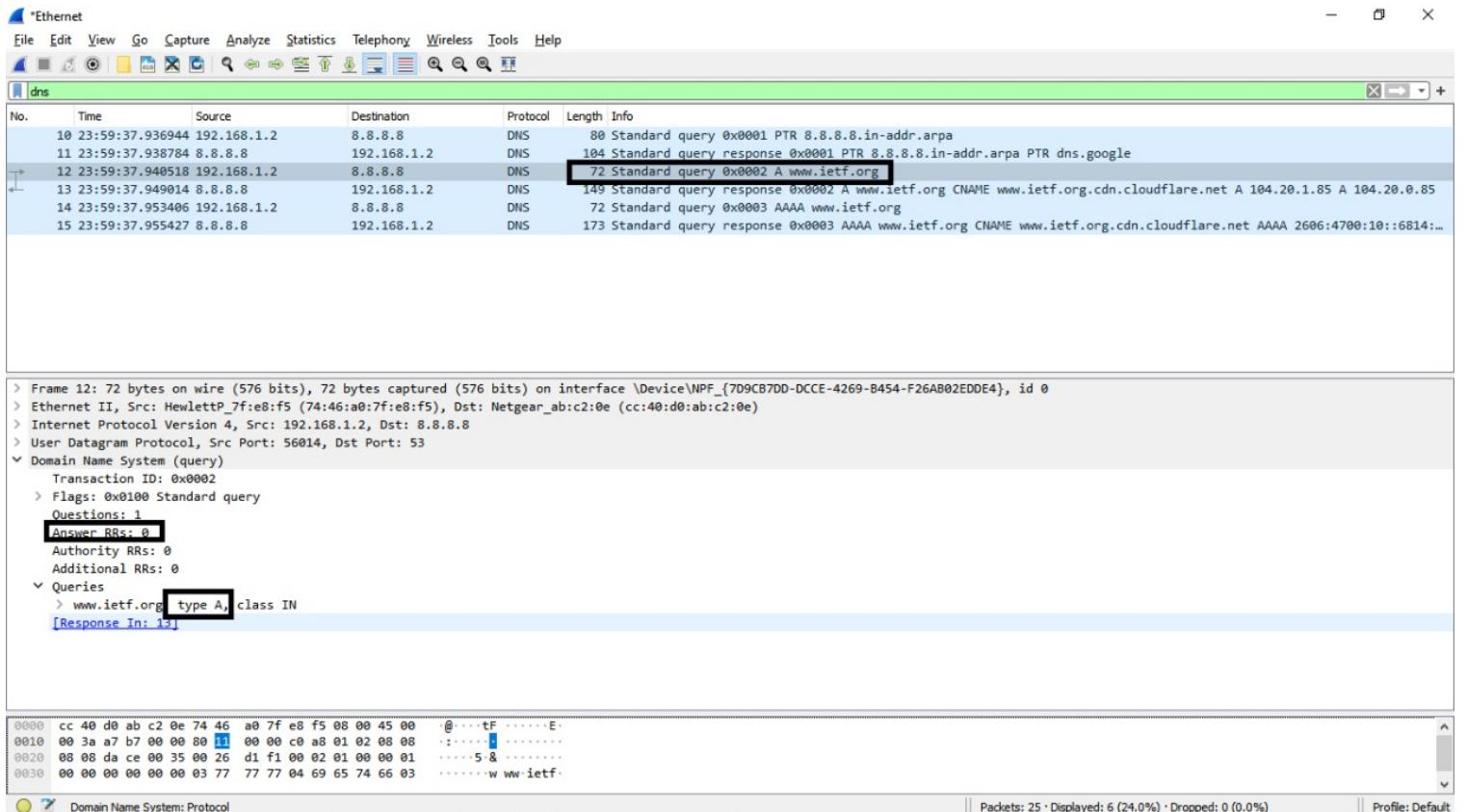
Media State . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . . . . . : Kaspersky Security Data Escort Adapter #2
Physical Address. . . . . . . . . : 00-FF-76-17-7A-08
DHCP Enabled. . . . . . . . . : Yes
```

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

Answer :

- DNS query message is of type “A”.

The query message **doesn't** contain any answer.



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

Answer :

- Dns Response contain 3 answers.

The Answer contains : Host Name , Type, Class, Time to Live, Data Length, Canonical Name.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
10	23:59:37.936044	192.168.1.2	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
11	23:59:37.938784	8.8.8.8	192.168.1.2	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
12	23:59:37.940518	192.168.1.2	8.8.8.8	DNS	72	Standard query 0x0002 A www.ietf.org
13	23:59:37.949014	8.8.8.8	192.168.1.2	DNS	149	Standard query response 0x0002 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
14	23:59:37.953406	192.168.1.2	8.8.8.8	DNS	72	Standard query 0x0003 AAAA www.ietf.org
15	23:59:37.955427	8.8.8.8	192.168.1.2	DNS	173	Standard query response 0x0003 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700:10::6814:...

```
> Frame 13: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{7D9CB7DD-DCCE-4269-B454-F26AB02EDDE4}, id 0
> Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: HewlettP_7f:e8:f5 (74:46:a0:7f:e8:f5)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.2
> User Datagram Protocol, Src Port: 53, Dst Port: 56014
└ Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  └ Queries
    > www.ietf.org: type A, class IN
  Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1748 (29 minutes, 8 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
  [Request In: 12]
  [Time: 0.008496000 seconds]
```

0000 74 46 a0 7f e8 f5 cc 40 d0 ab c2 0e 08 00 45 00 tF.....@.....E.
0010 00 87 a1 73 00 00 79 11 ce 38 08 08 08 08 c0 a8 ..s.y..8.....
0020 01 02 00 35 da ce 00 73 52 7e 00 02 81 80 00 01 ..5...s R~.....
0030 00 03 00 00 00 00 03 77 77 04 69 65 74 66 03w ww ietf.

Domain Name System: Protocol

Packets: 25 · Displayed: 6 (24.0%) · Dropped: 0 (0.0%)

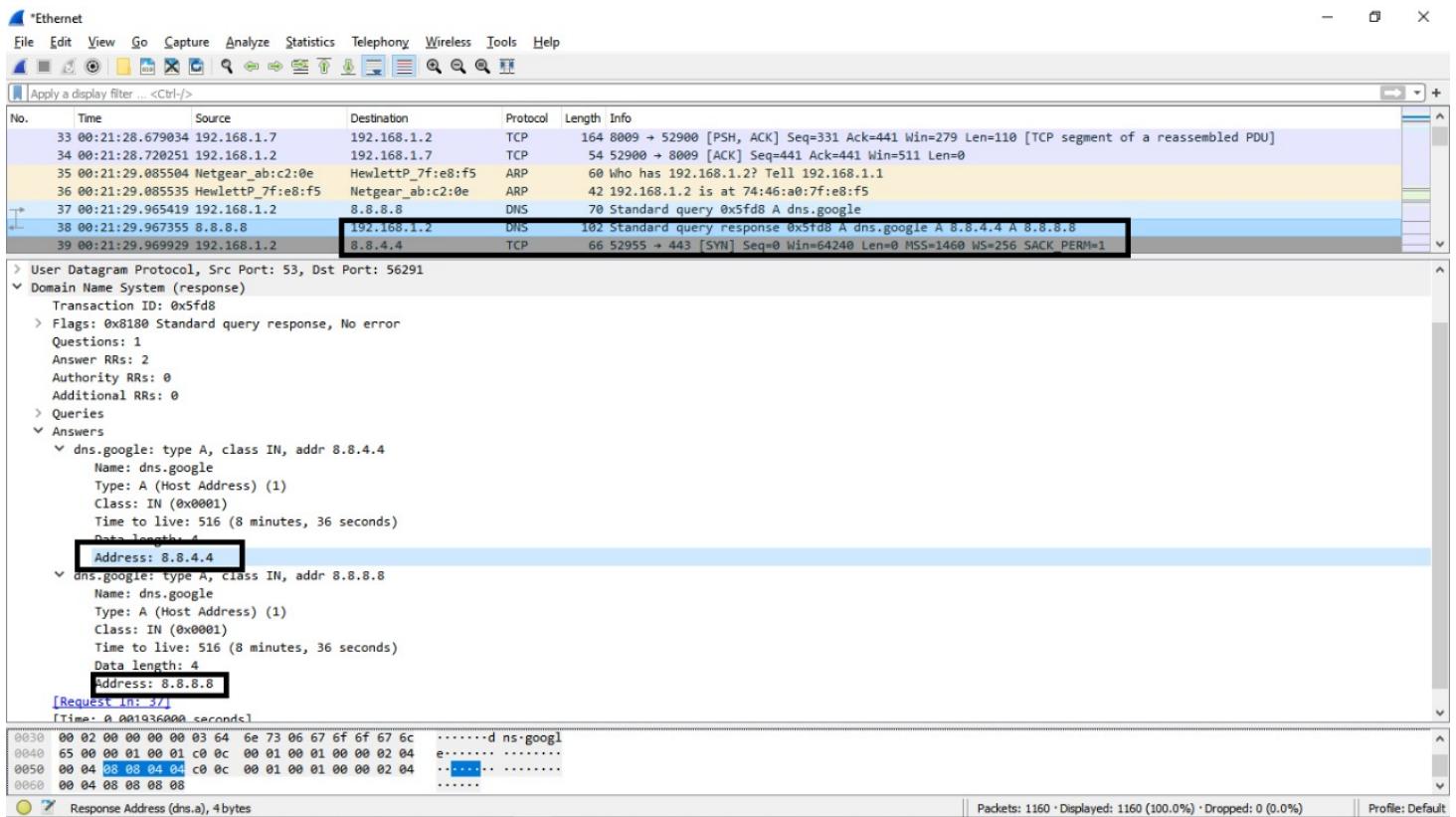
Profile: Default

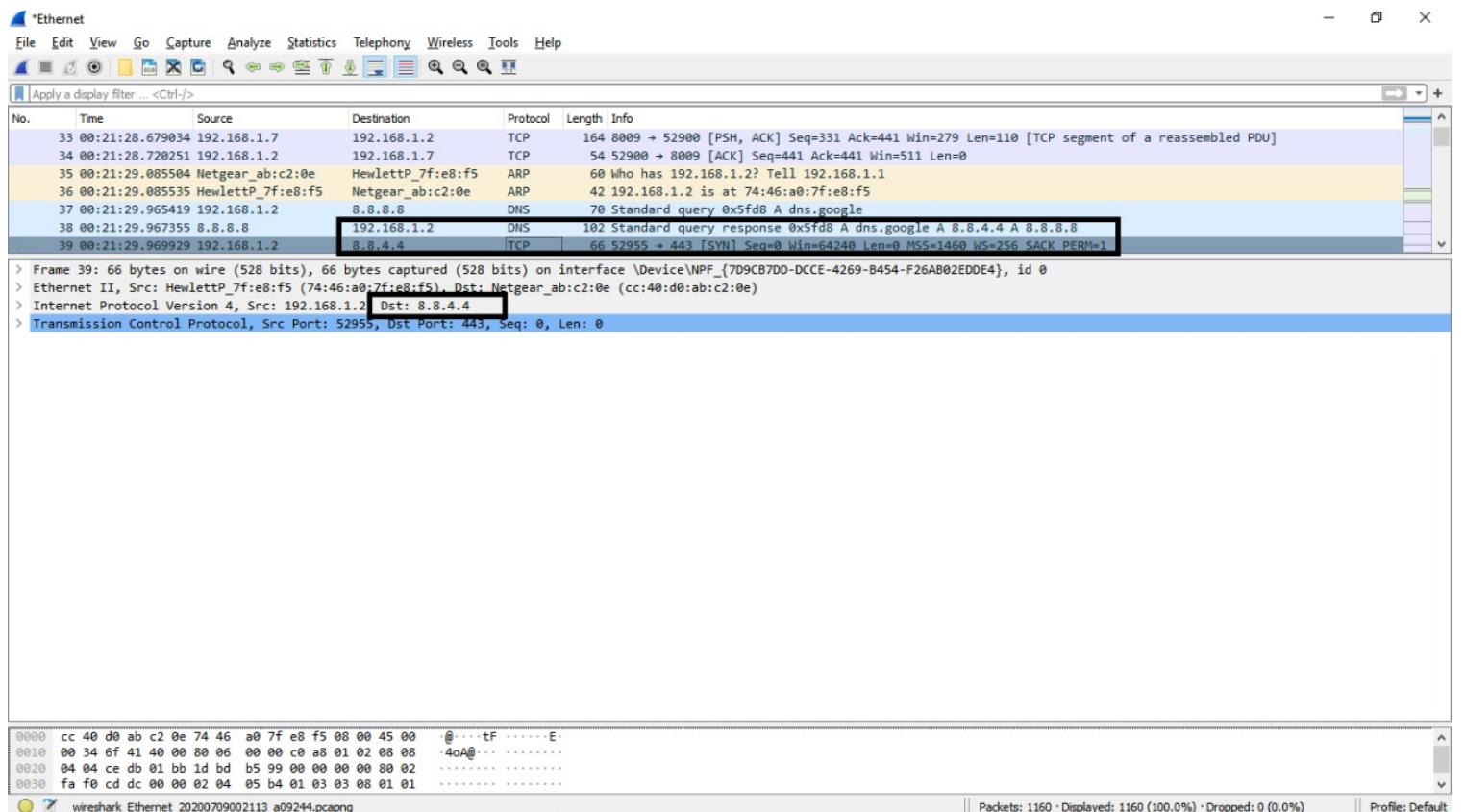
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer :

destination IP address of the SYN packet :8.8.4.4, corresponds to

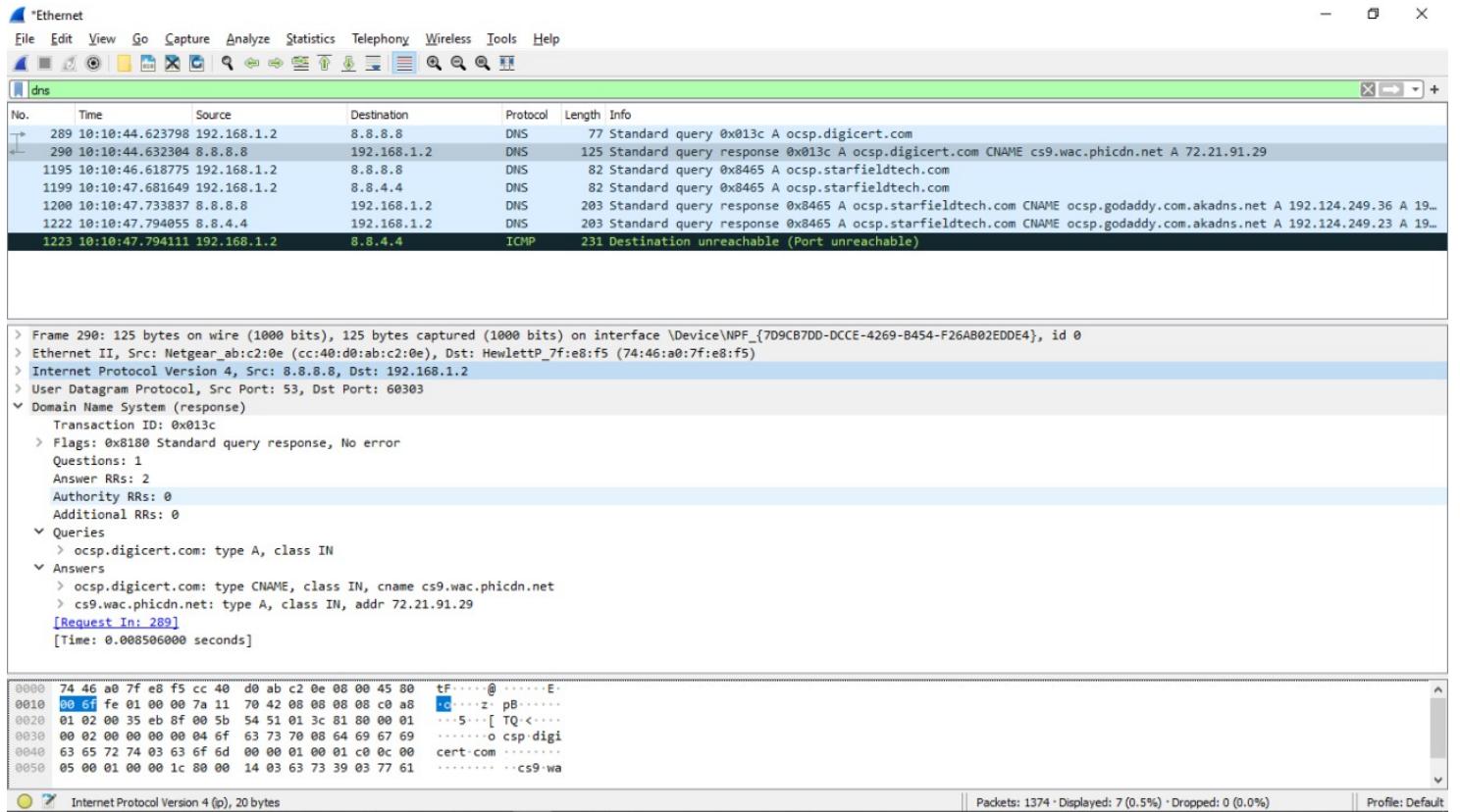
DNS response message : 8.8.4.4





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

Answer : **No**, host does not issue new DNS queries for each image retrieval.

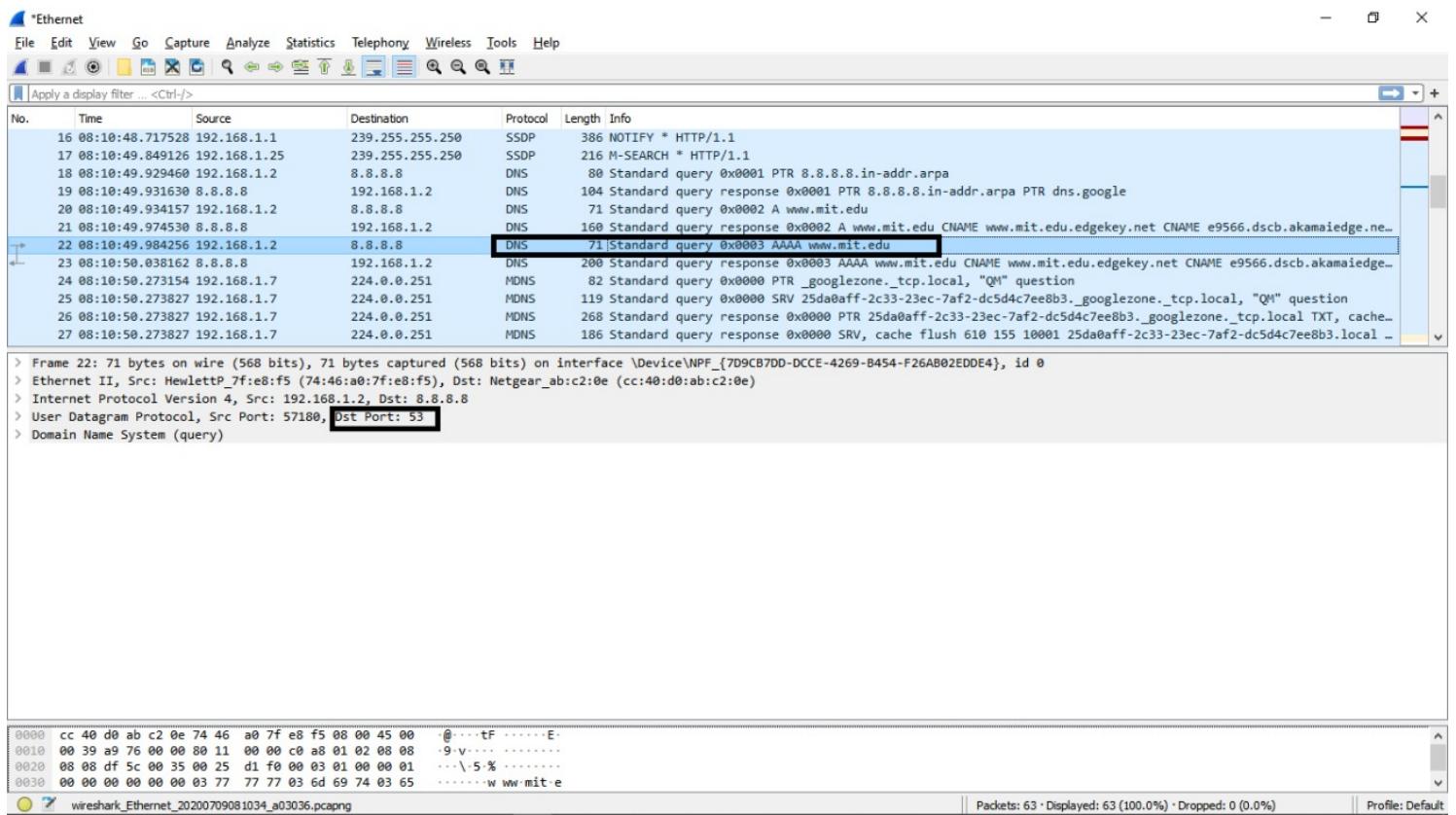


11 . What is the destination port for the DNS query message? What is the source port of DNS response message?

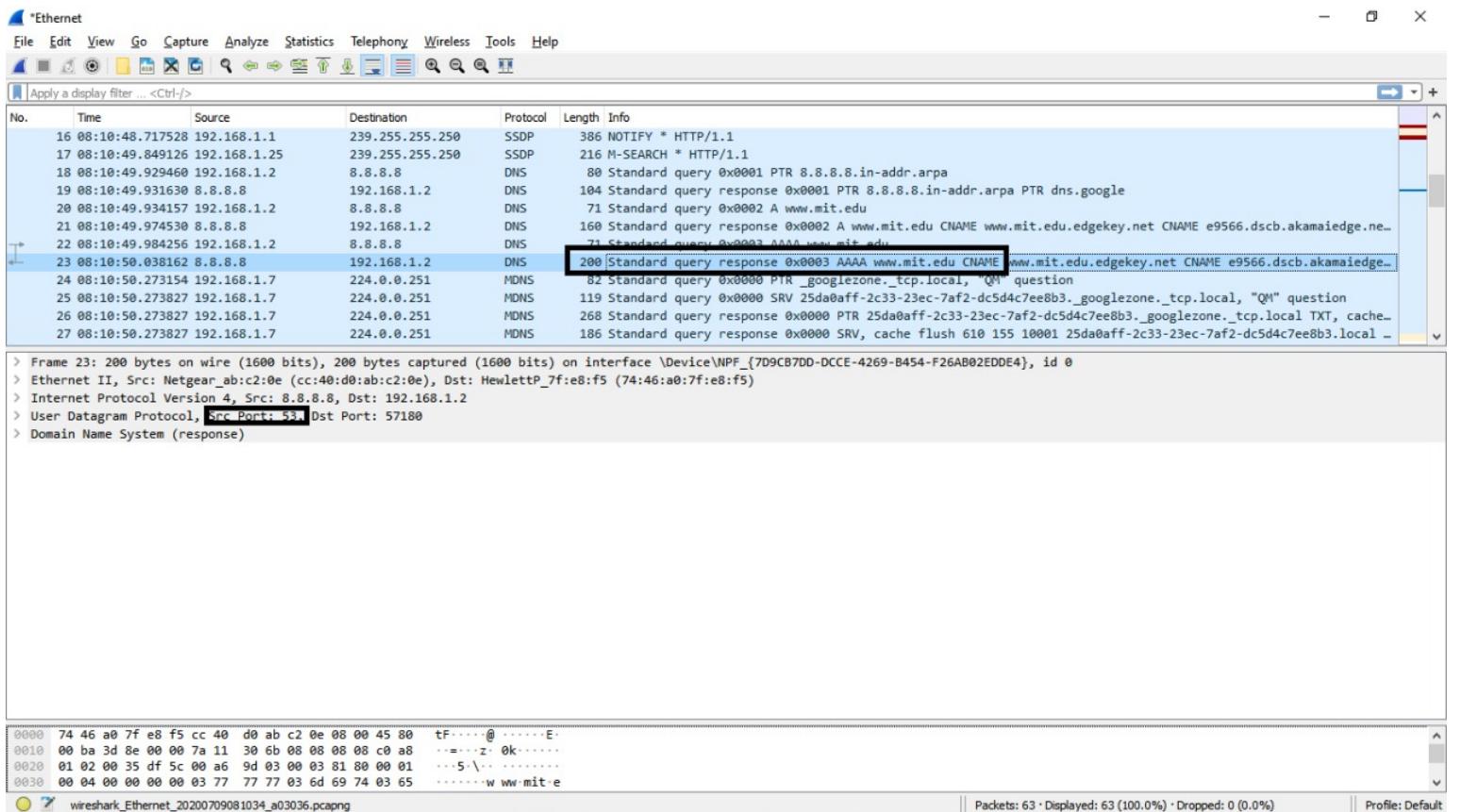
Answer :

- Destination port for the DNS query message is 53 .
- Source port of DNS response message 53 .

DNS query message :



DNS response message



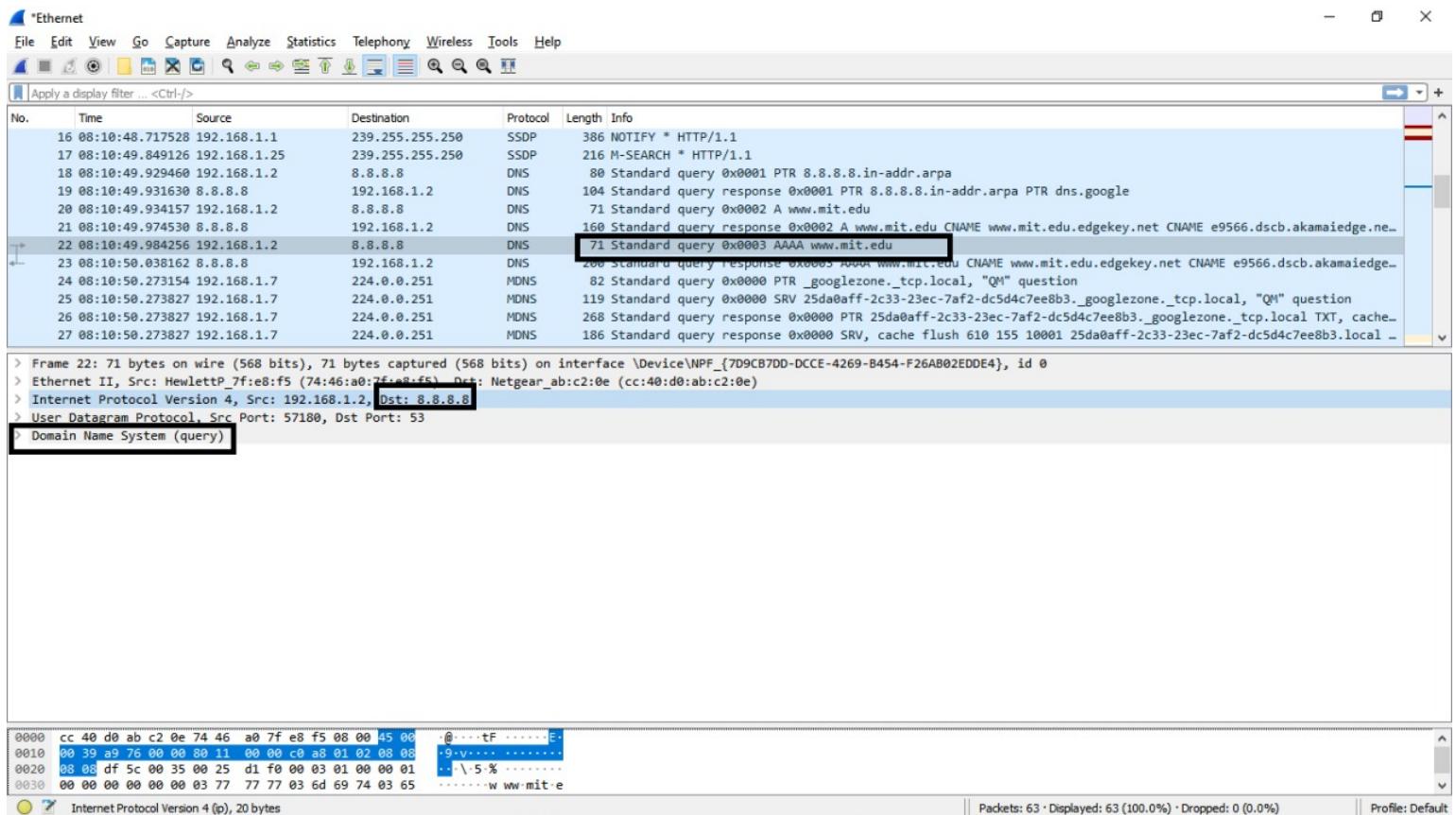
12 . To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer :

- DNS query message is sent to : 8.8.8.8
- Local DNS server : 8.8.8.8

IP address of my default local DNS server is same as IP address of DNS query message.

- DNS query message



```
C:\Users\ratho>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-15C6NMD
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Realtek PCIe FE Family Controller
  Physical Address. . . . . : 74-46-A0-7F-E8-F5
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::684f:bbaf:a66:3a2f%12(PREFERRED)
  IPv4 Address. . . . . : 192.168.1.2(PREFERRED)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : 08 July 2020 08:19:48
  Lease Expires . . . . . : 09 July 2020 20:53:08
  Default Gateway . . . . . : 192.168.1.1
  DHCP Server . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . : 74729120
  DHCPv6 Client DUID . . . . . : 00-01-00-01-23-B0-23-E9-74-46-A0-7F-E8-F5
  DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
  NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 2:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Kaspersky Security Data Escort Adapter
  Physical Address. . . . . : 00-FF-1E-50-48-47
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes

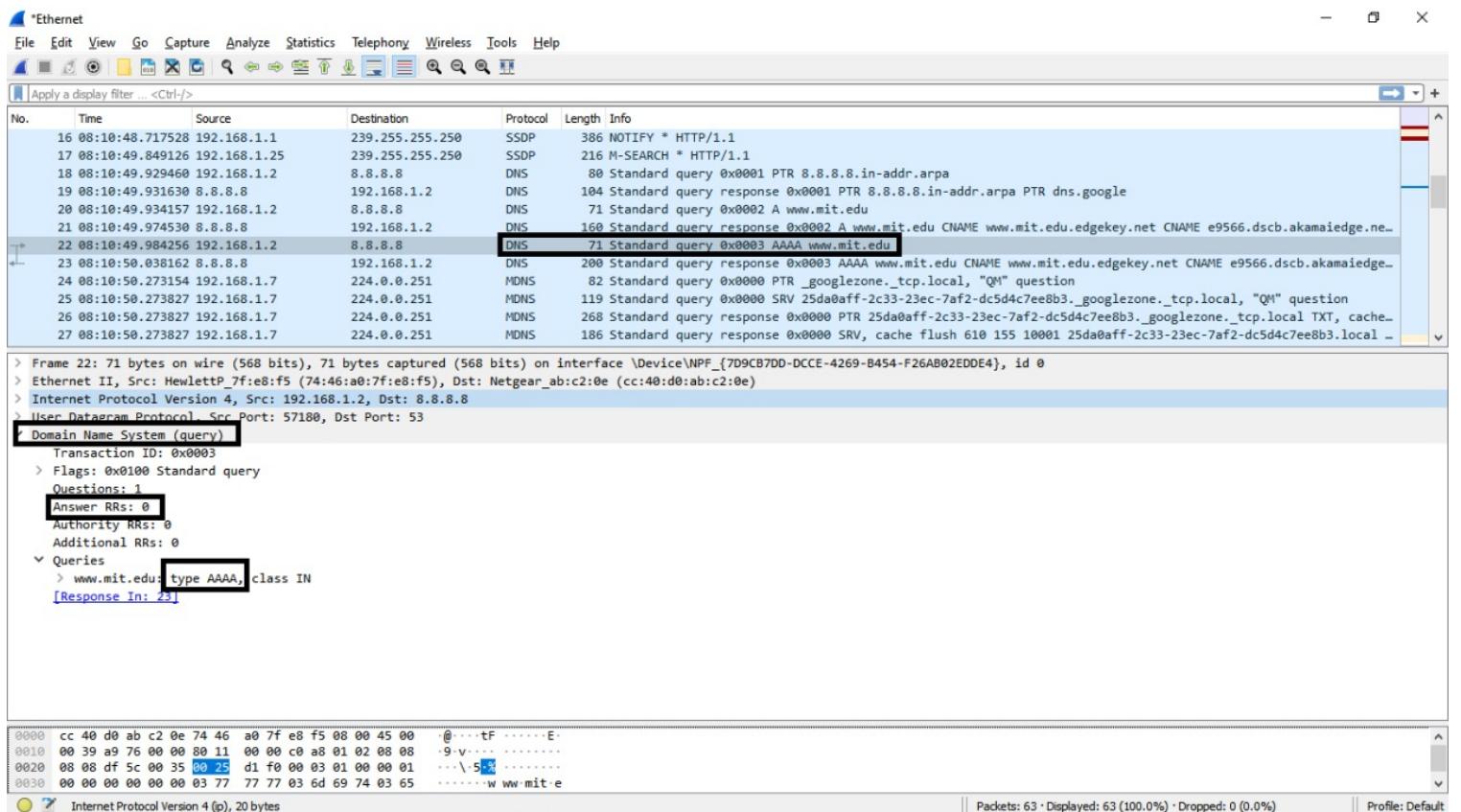
Ethernet adapter Ethernet 8:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Kaspersky Security Data Escort Adapter #2
  Physical Address. . . . . : 00-FF-76-17-7A-08
  DHCP Enabled. . . . . : Yes
```

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

Answer :

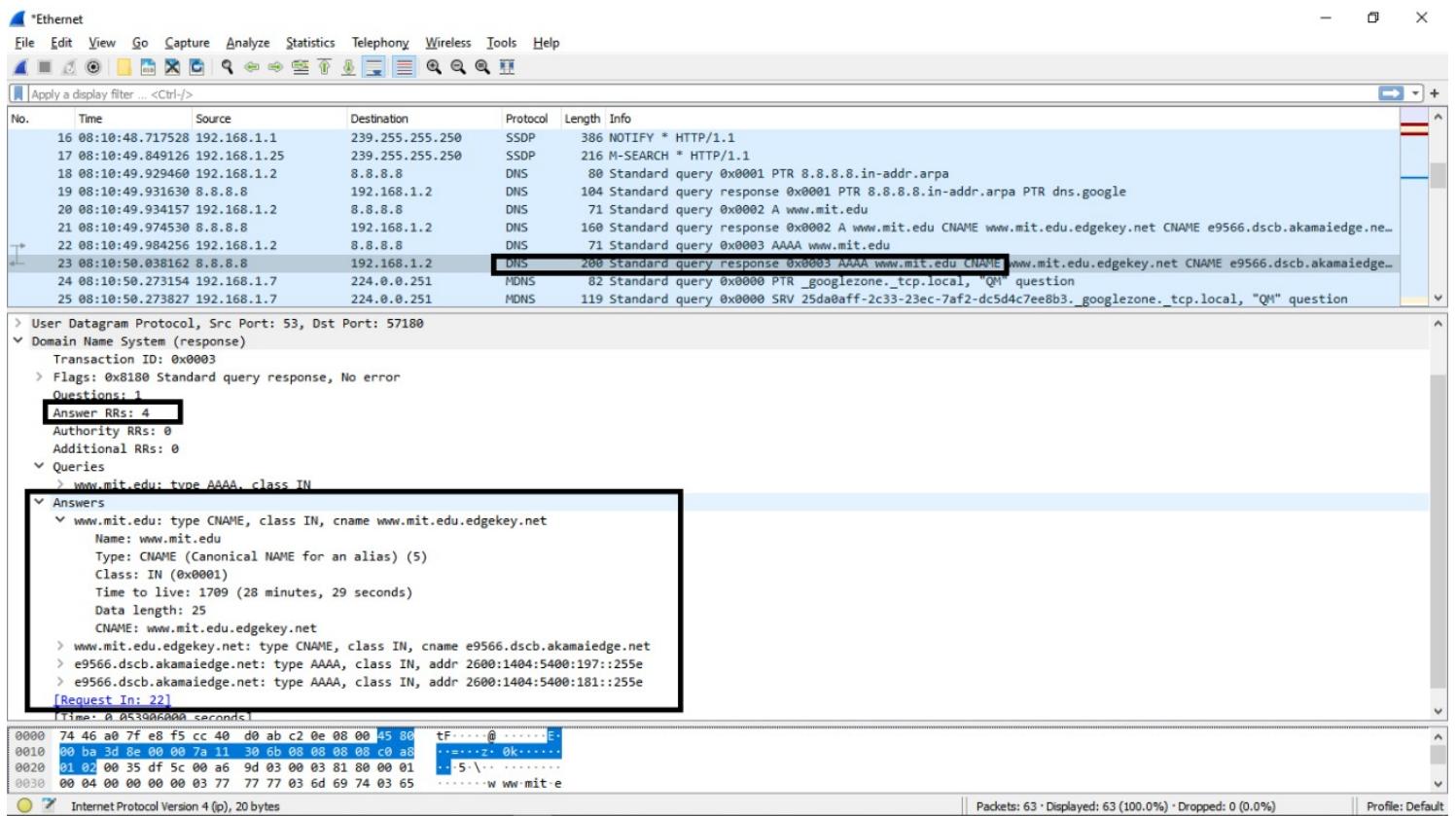
- DNS query message is of type “AAAA” .
- The query message **does not** contain any answer.



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

Answer :

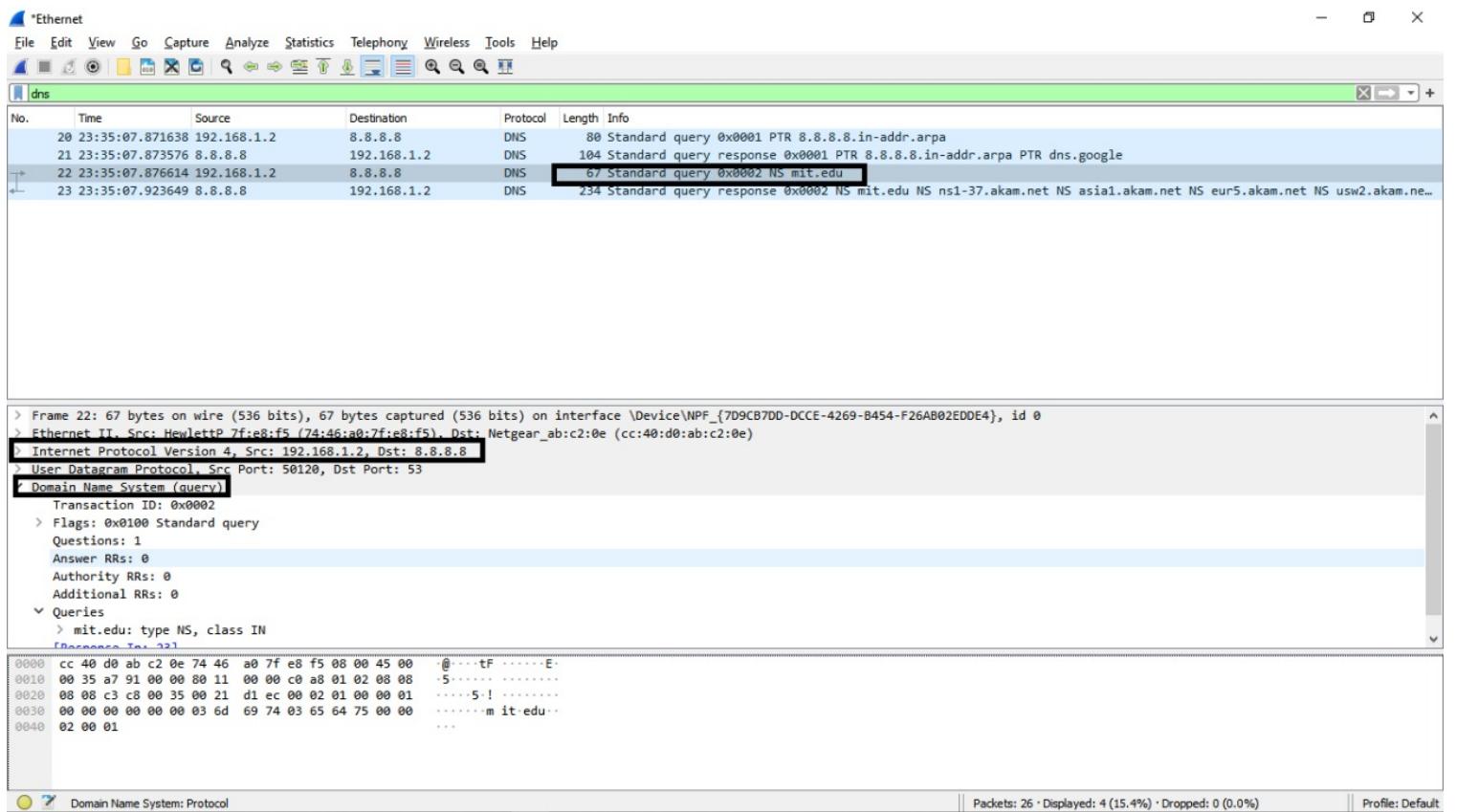
- DNS response message contain 4 answer.
- Each of these answers contain
 - Name , Type, Class, Time to Live, Date Length, Canonical Name.



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

Answer :

- DNS query message sent to 8.8.8.8
- Yes this is the IP address of your default local DNS server.



```
C:\Users\ratho>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-15C6NMD
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek PCIe FE Family Controller
Physical Address. . . . . : 74-46-A0-7F-E8-F5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::684f:bbaf:a66:3a2f%12(Preferred)
IPv4 Address. . . . . : 192.168.1.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 08 July 2020 08:19:48
Lease Expires . . . . . : 09 July 2020 20:53:08
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 74729120
DHCPv6 Client DUID . . . . . : 00-01-00-01-23-B0-23-E9-74-46-A0-7F-E8-F5
DNS Servers . . . . . : 8.8.8.8
                                         8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Kaspersky Security Data Escort Adapter
Physical Address. . . . . : 00-FF-1E-50-48-47
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

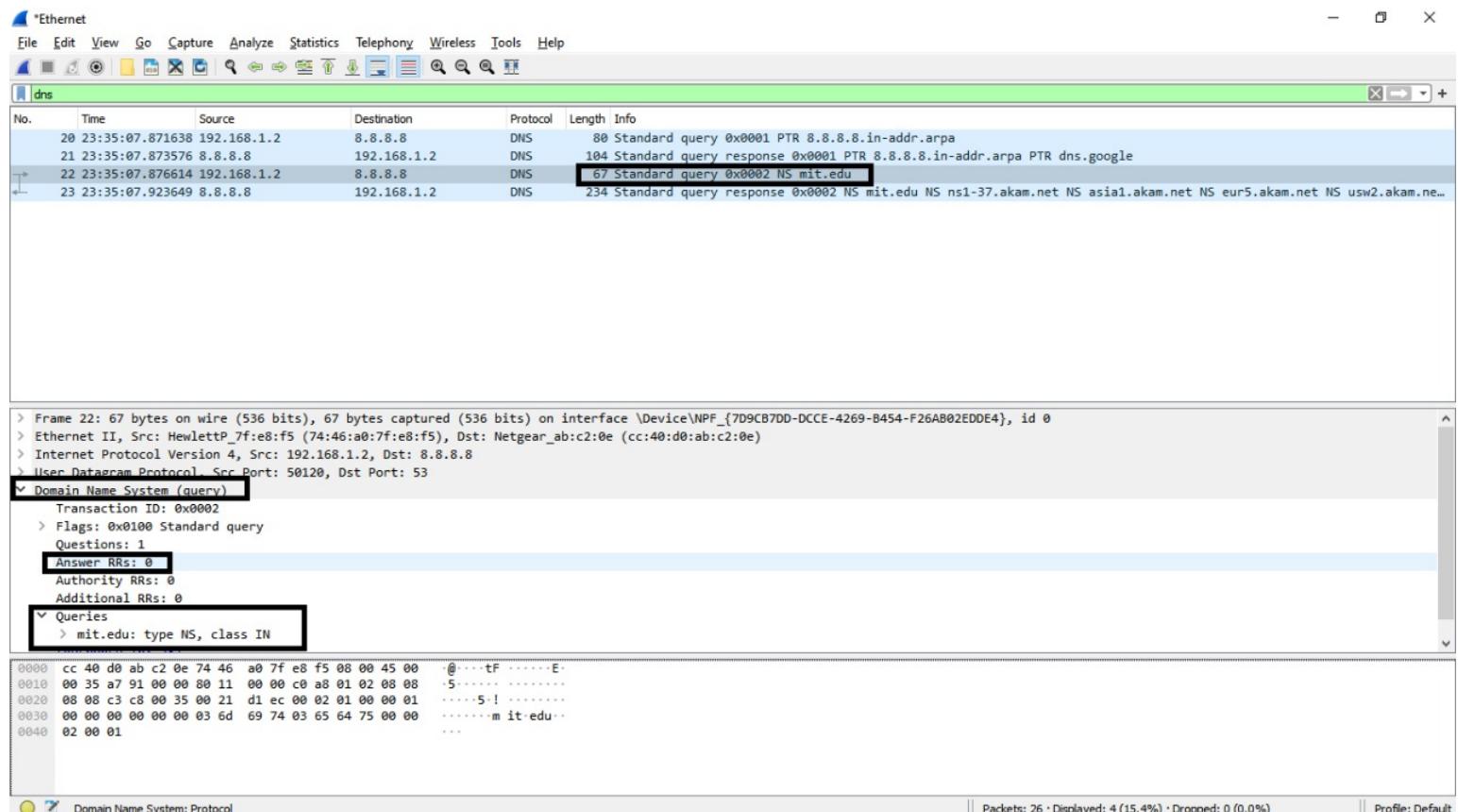
Ethernet adapter Ethernet 8:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Kaspersky Security Data Escort Adapter #2
Physical Address. . . . . : 00-FF-76-17-7A-08
DHCP Enabled. . . . . : Yes
```

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

Answer :

- DNS query message is of type “NS”.
- The query message **does not contain** any answer .



18. 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 namesers?

Answer : Name servers are

1. ns ns1-37.akam.net
2. ns asia1.akam.net
3. ns eur5.akam.net
4. ns usw2.akam.net
5. ns use5.akam.net
6. ns use2.akam.net
7. ns asia2.akam.net
8. ns ns1-173.akam.net

No , it does not provide IP addresses of the MIT nameservers.

