SHUBHAM SHANKAR
UTA ID :1001761068

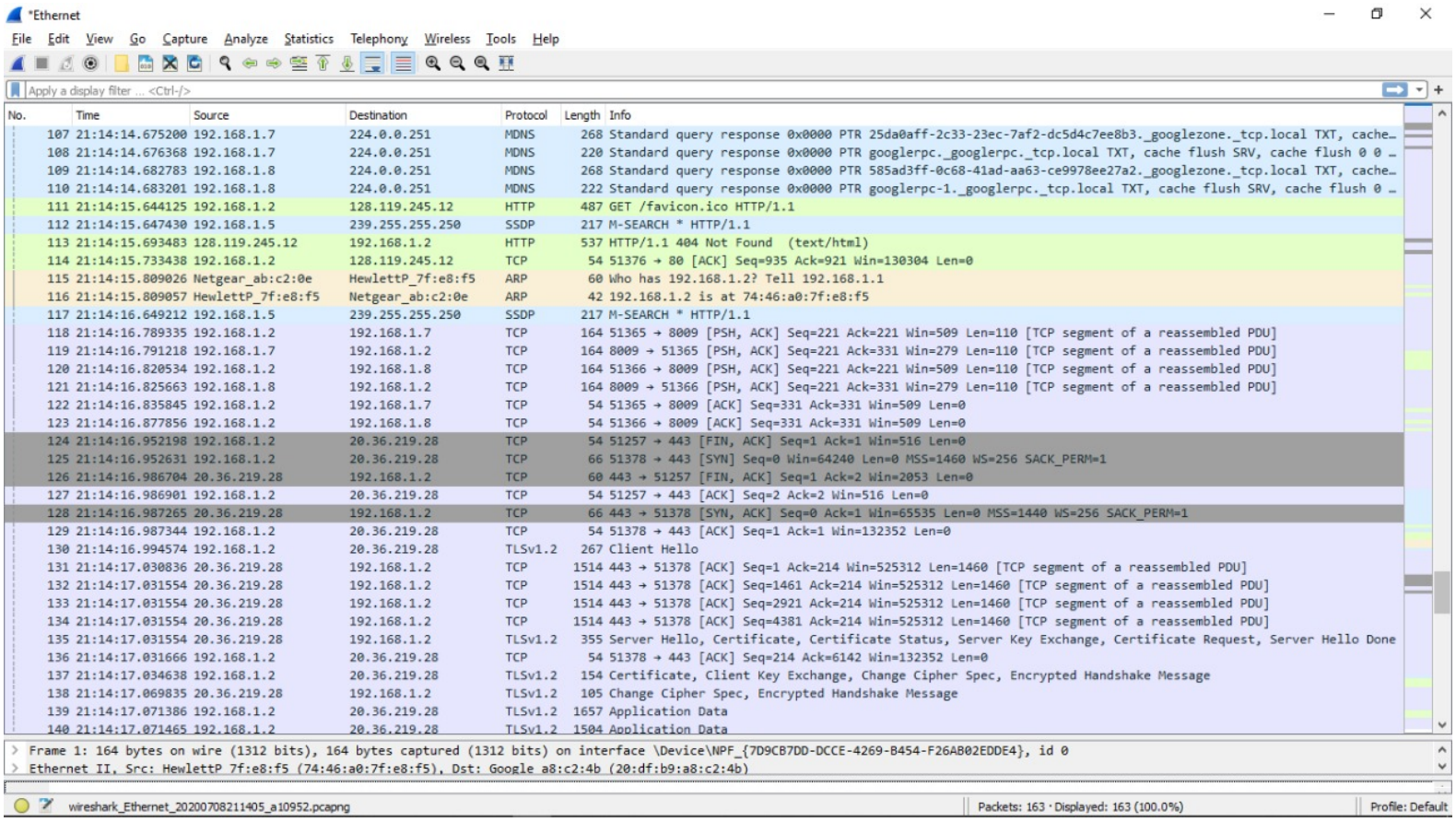
COMPUTER NETWORK ORGANIZATION

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 :

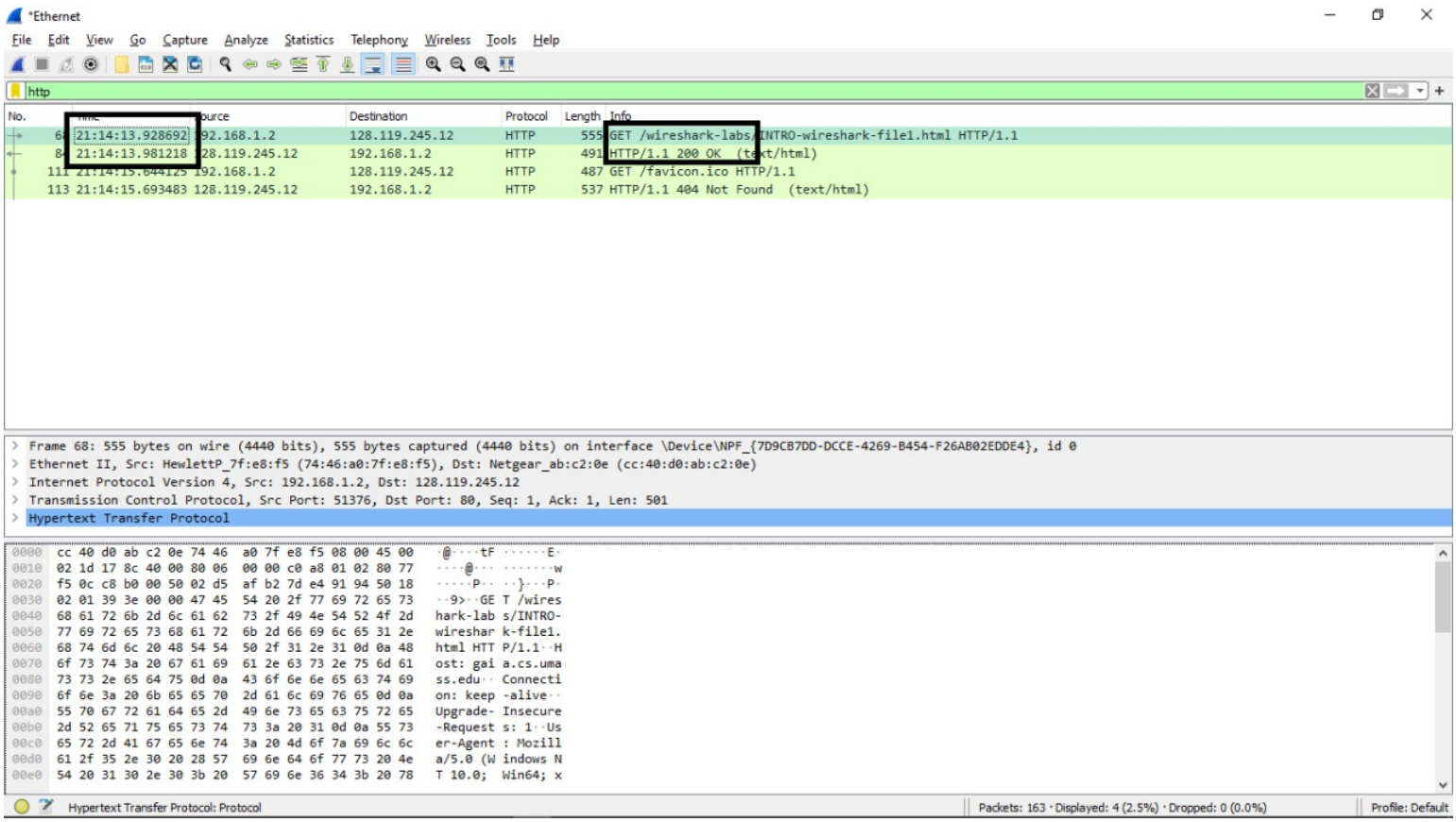
1. HTTP
2. TCP
3. ARP
4. MDNS
5. TLS.



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

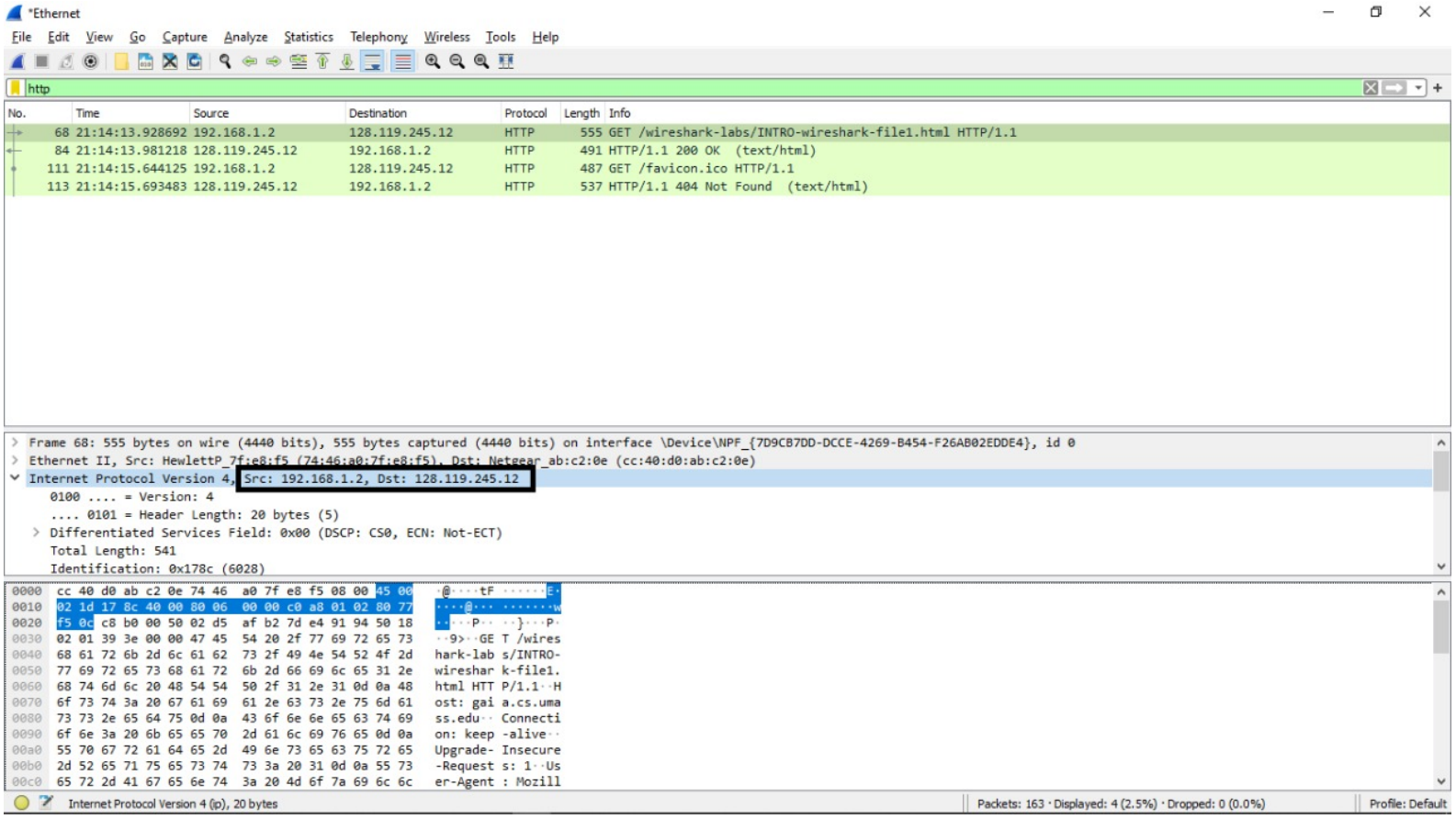
- HTTP GET was sent at 21:14:13.928692 , and
- HTTP OK was received at 21:14:13.981218.
- The **delay 21:14:13.52526 secs.**



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**



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 ..)

SHUBHAM SHANKAR
UTA ID :1001761068

COMPUTER NETWORK ORGANIZATION

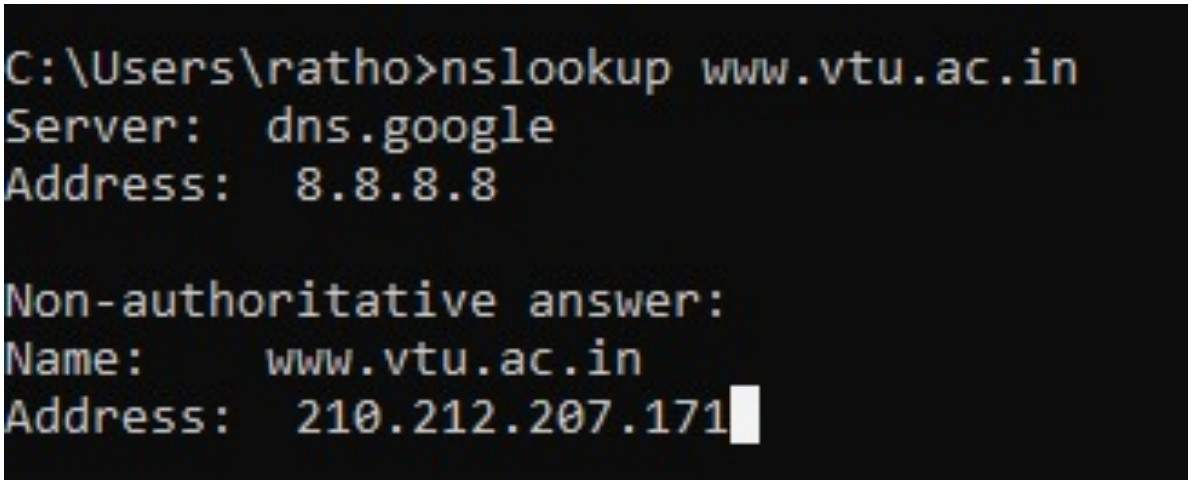
LAB 1

part -2

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

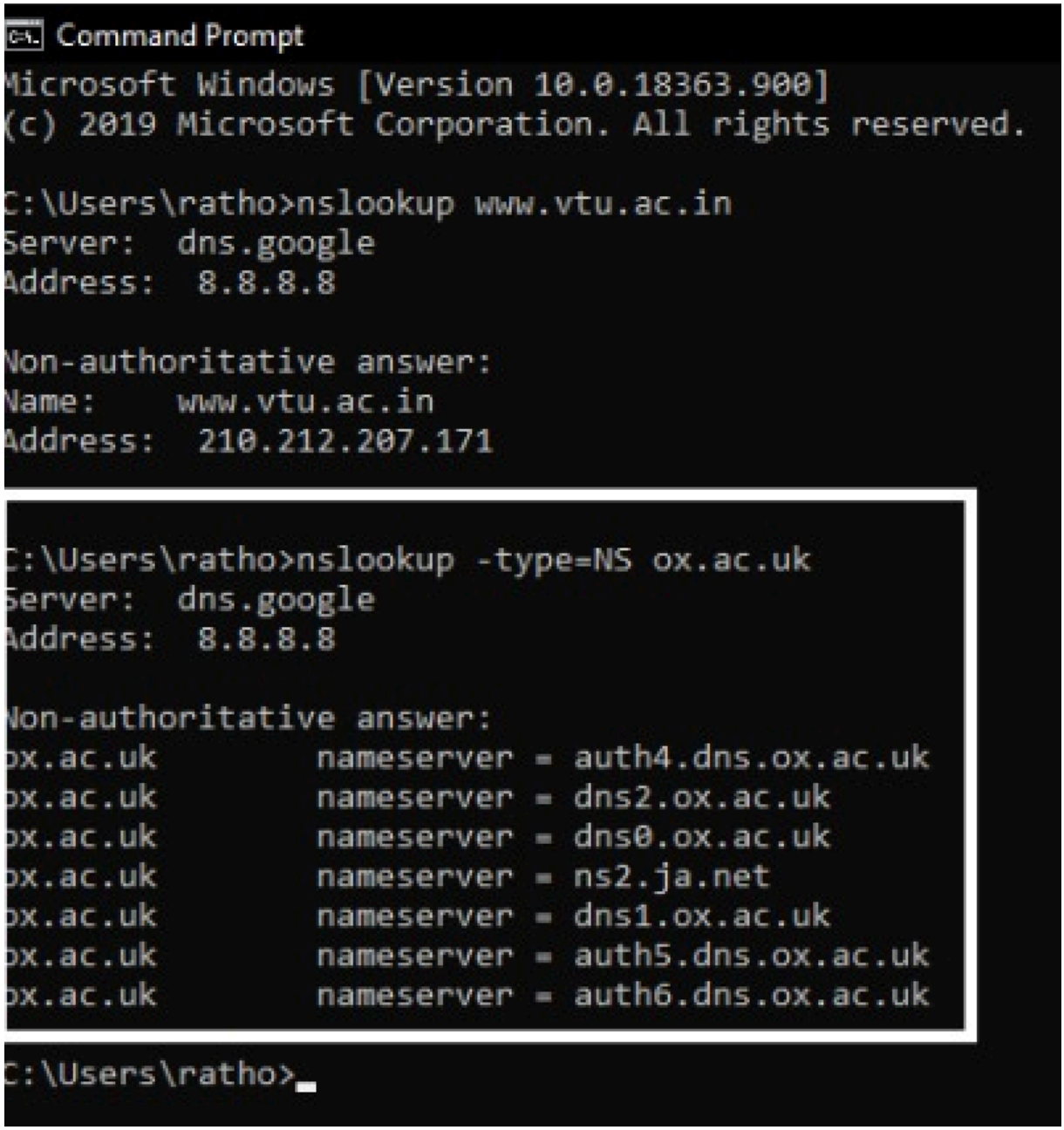
Answer : Ran *nslookup* on a Web server in Asia

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



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

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



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?

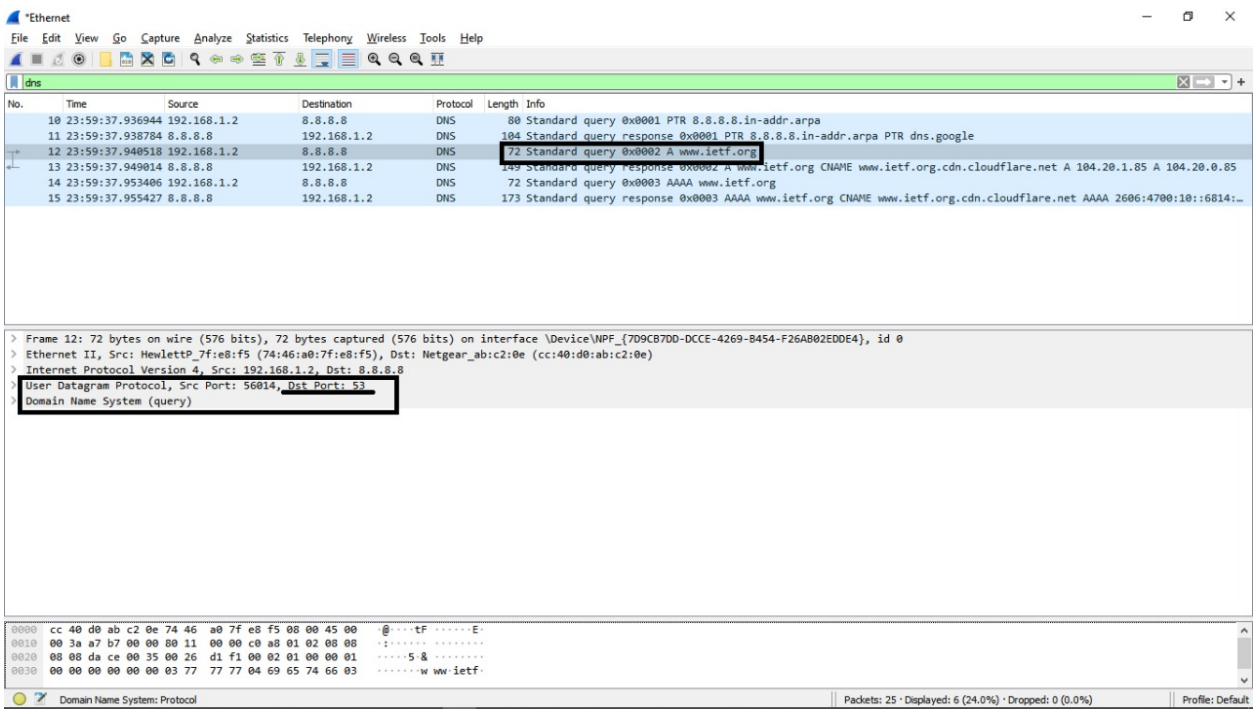
Answer : **Query Gets Refused.**

```
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
```

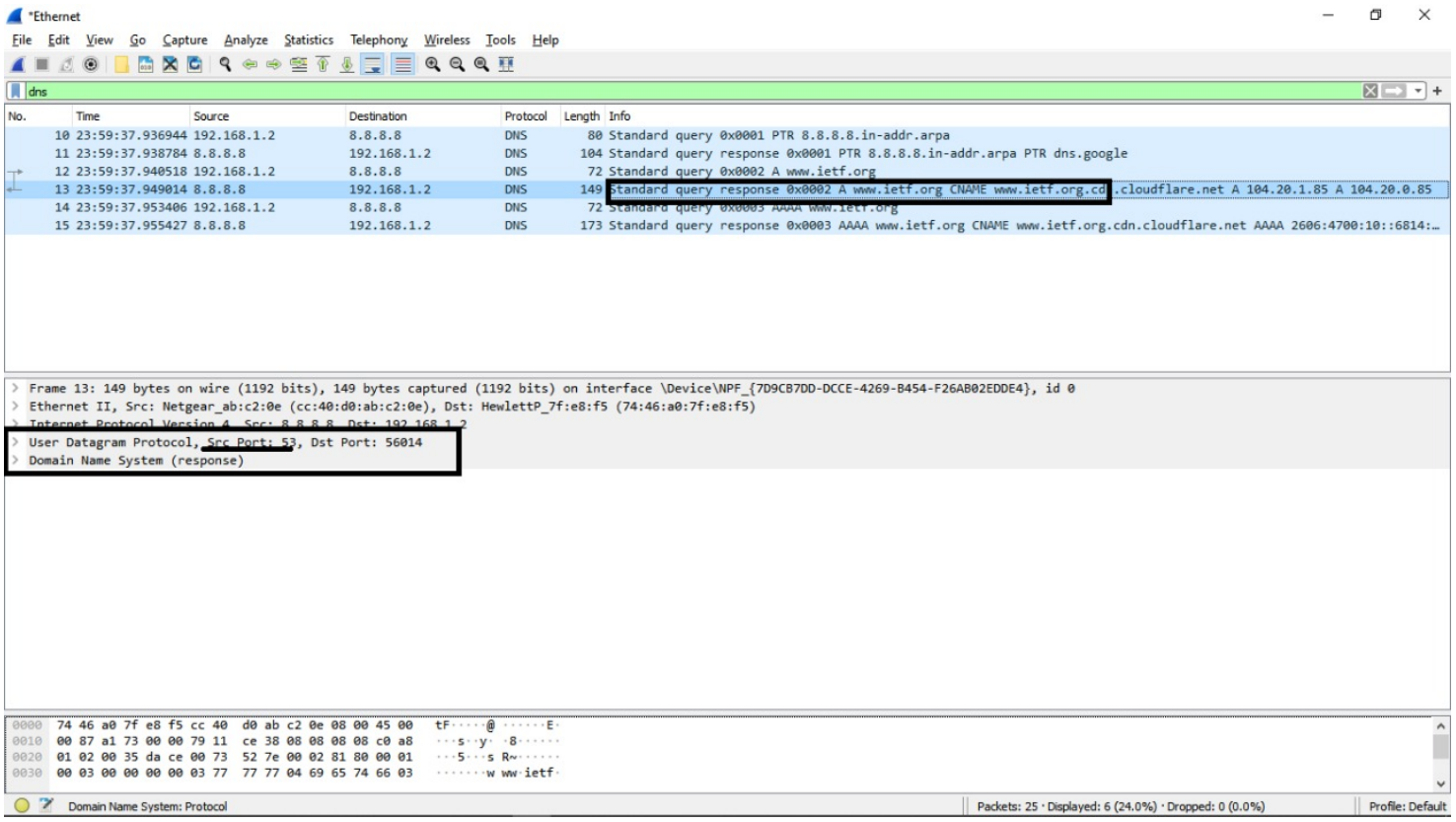
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Answer :

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



- DNS RESPONCE MESSAGE



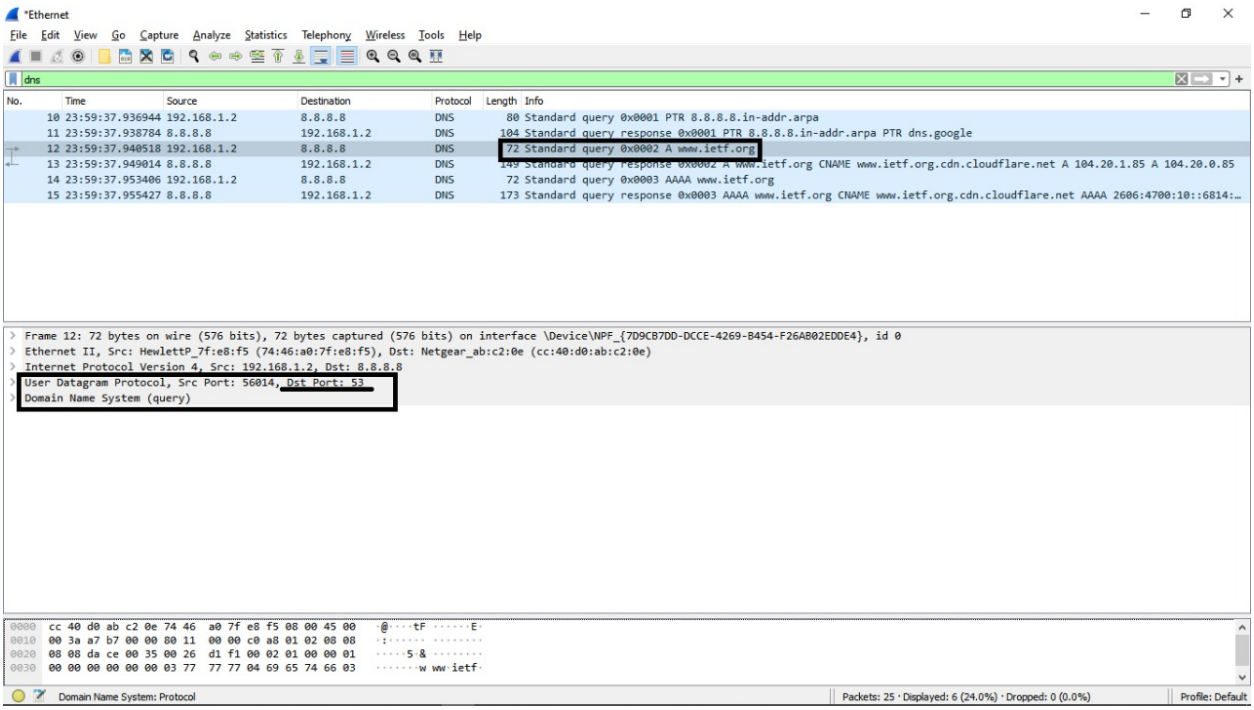
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer :

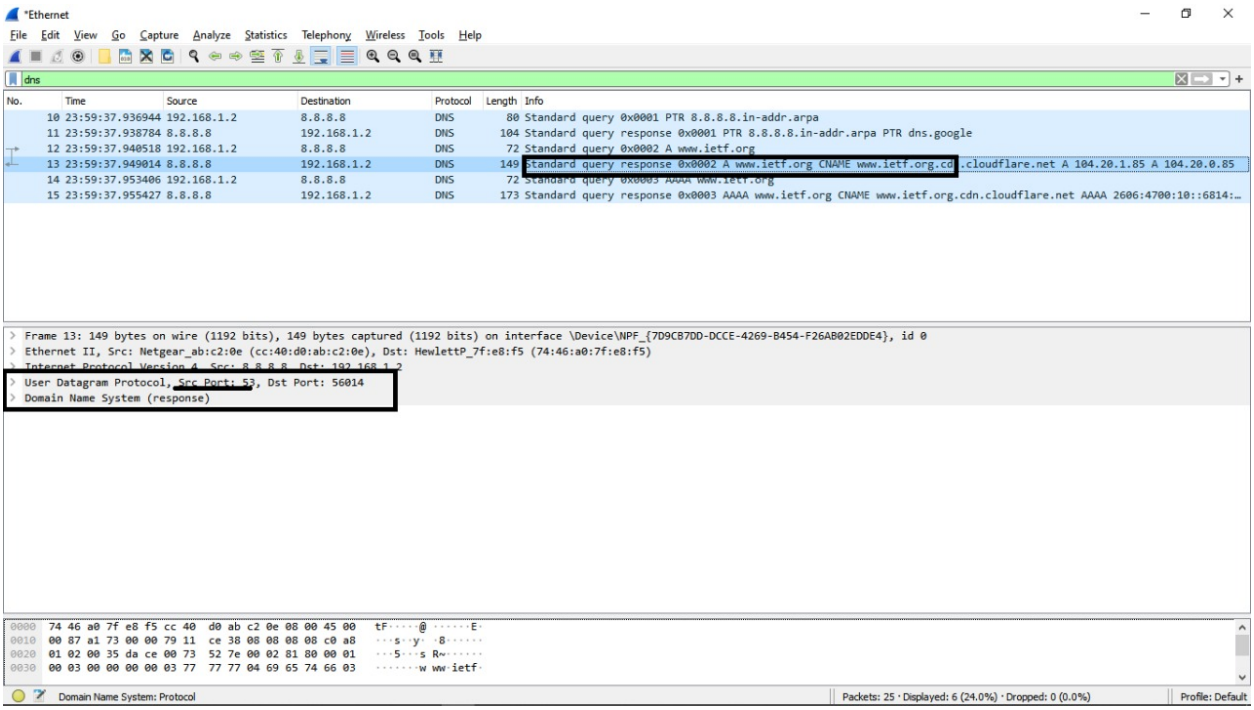
- Destination port for the DNS query message : 53

- Source port of DNS response message : 53

- DNS query message :



- DNS response message :



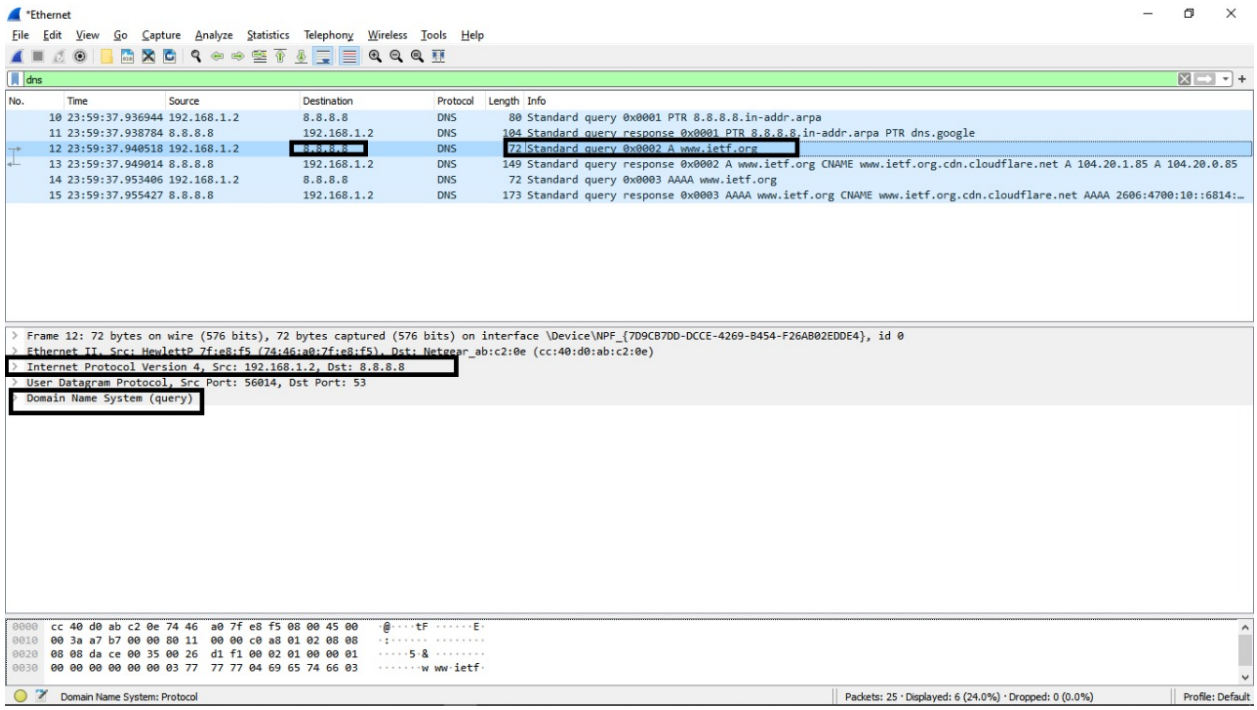
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

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 :



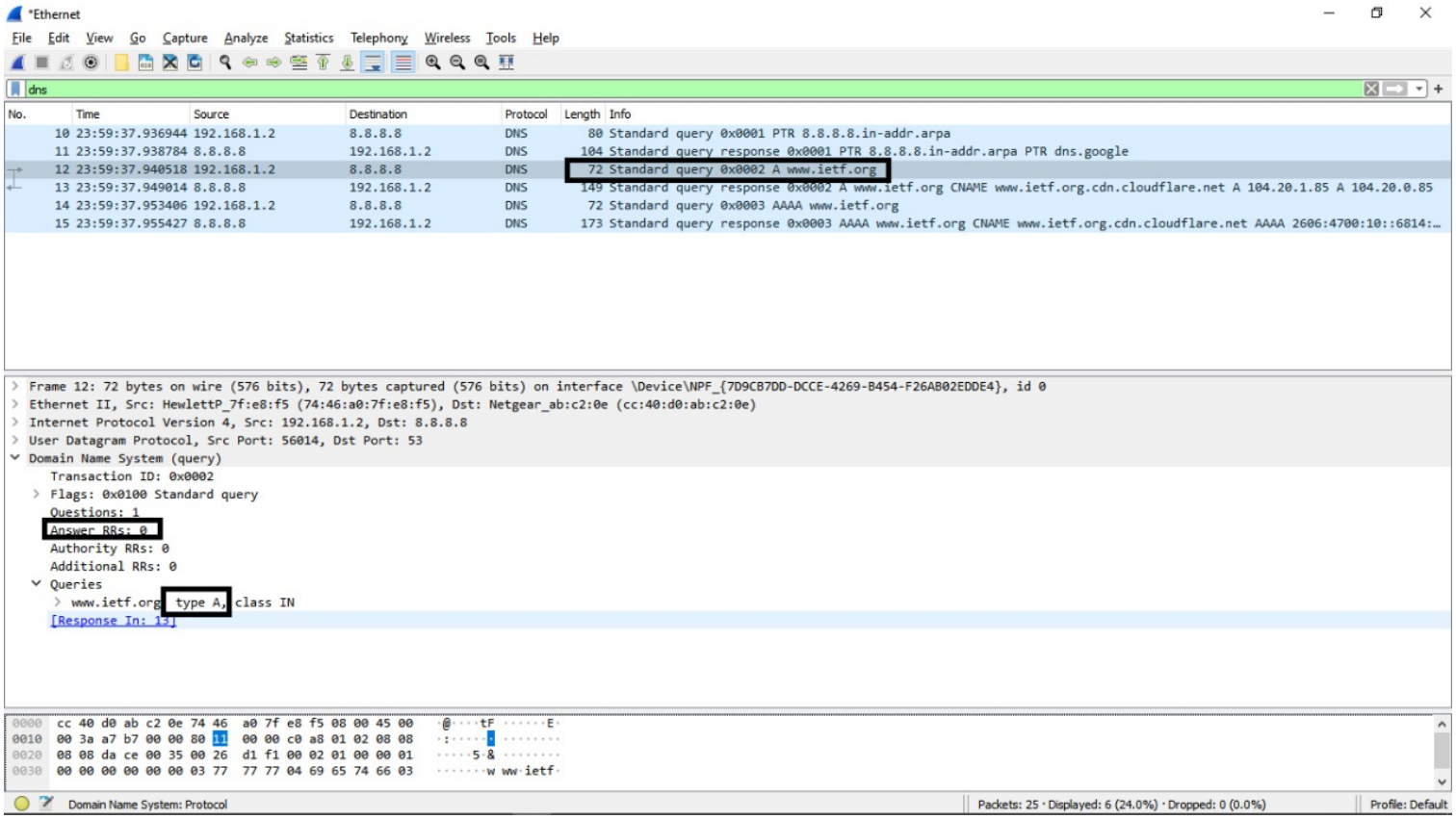
```
C:\Users\ratho>ipconfig /all

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.

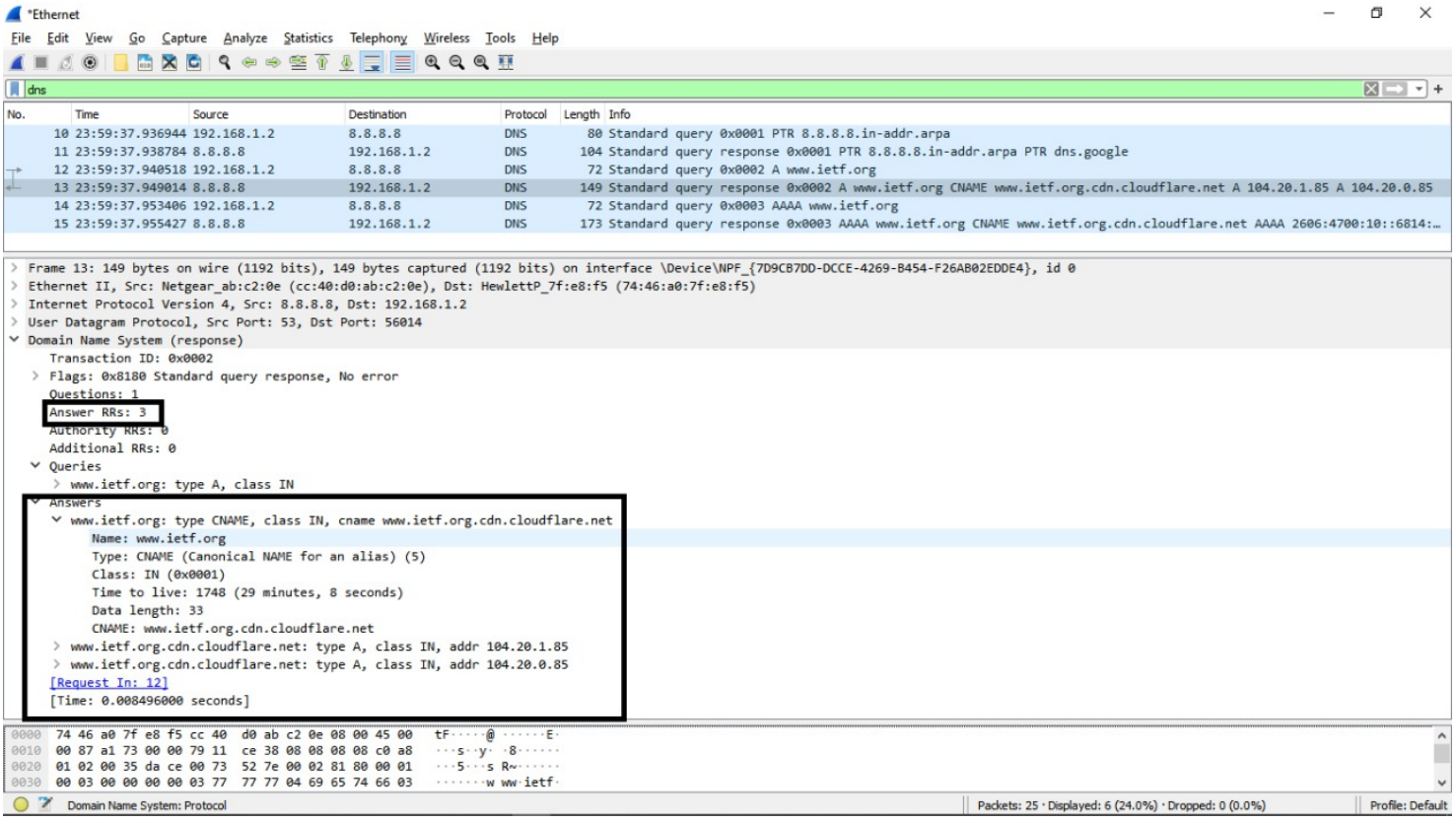


8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer :

- Dns Response contain **3** answers.

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

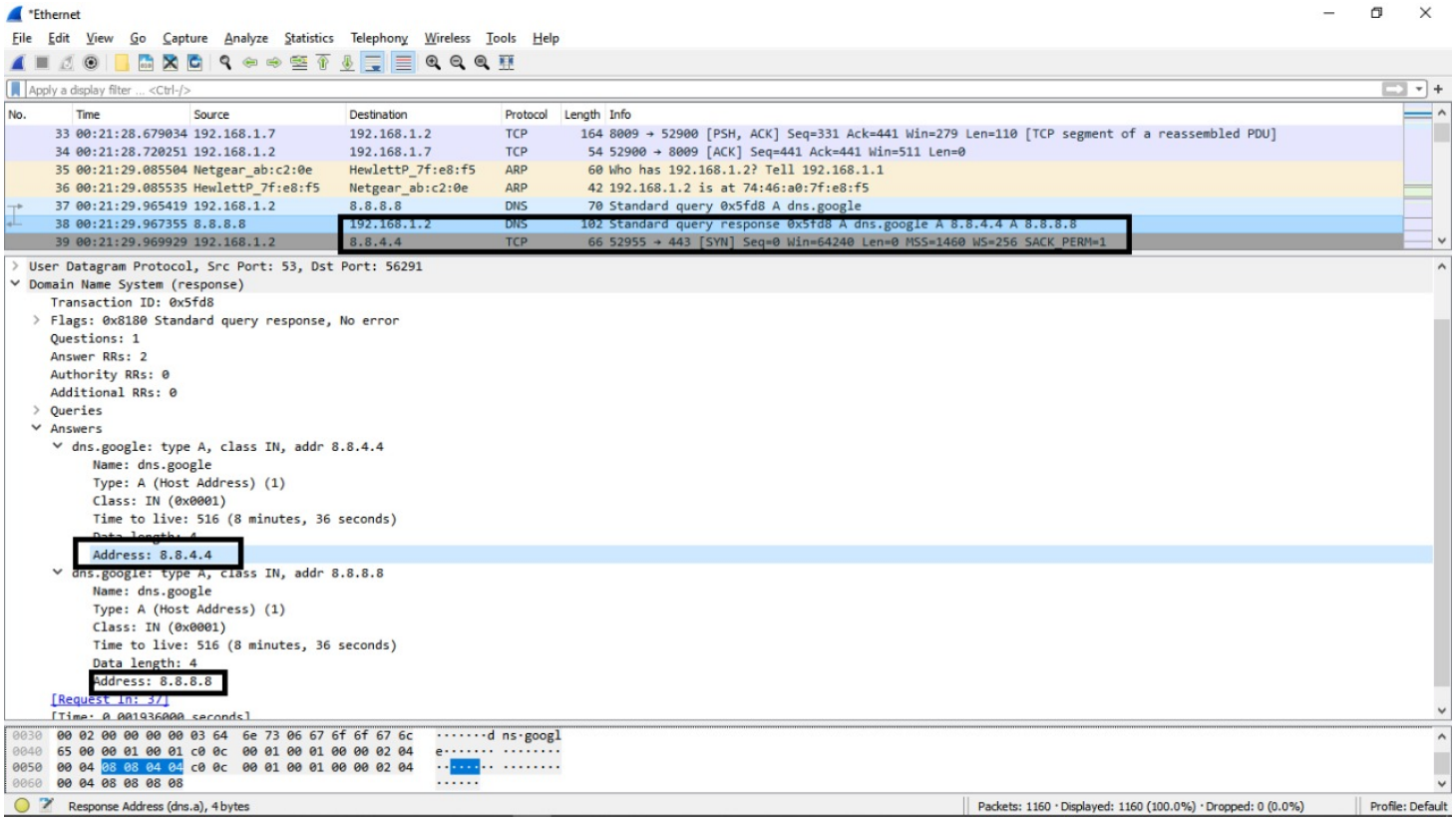


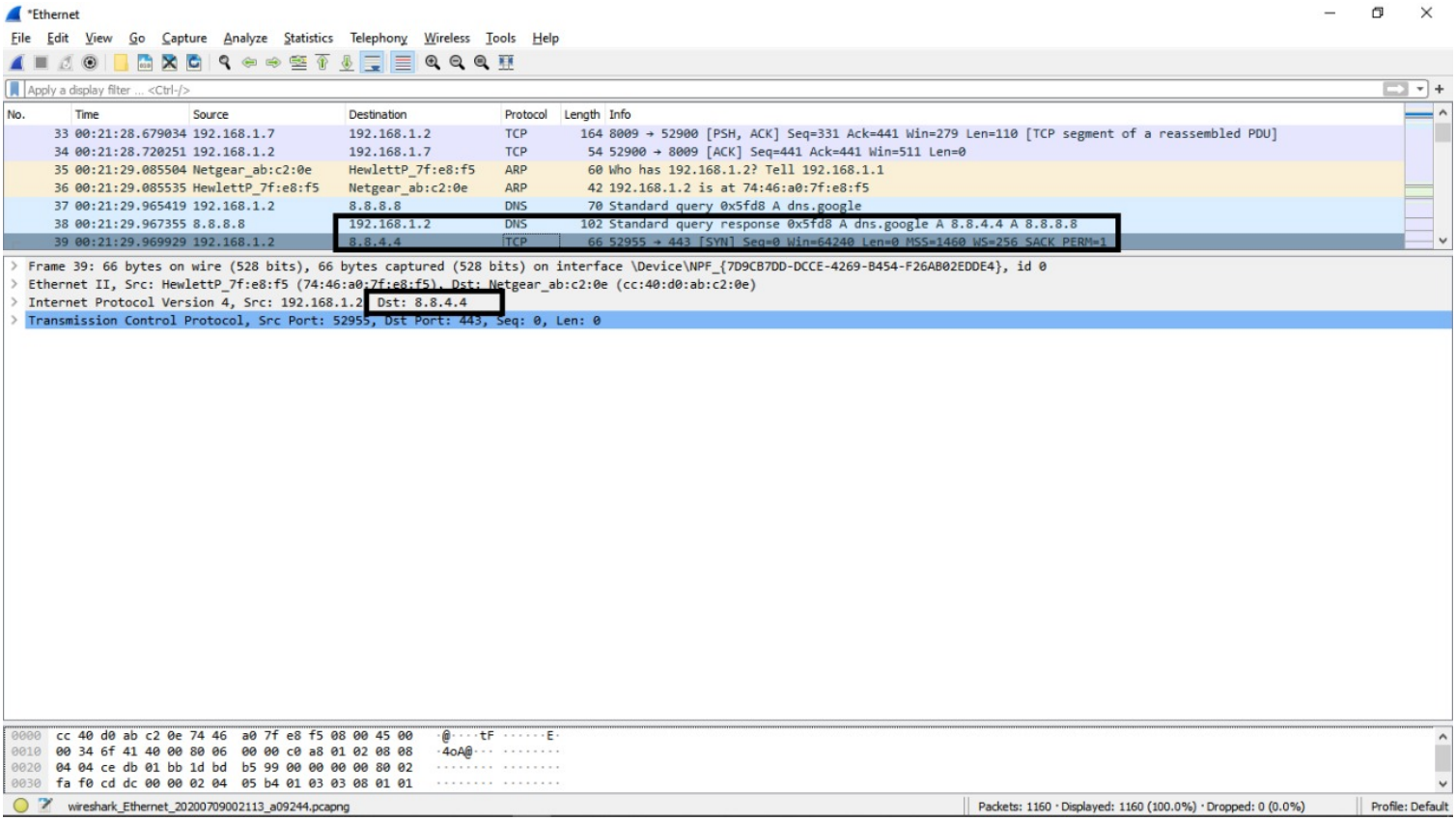
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer :

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

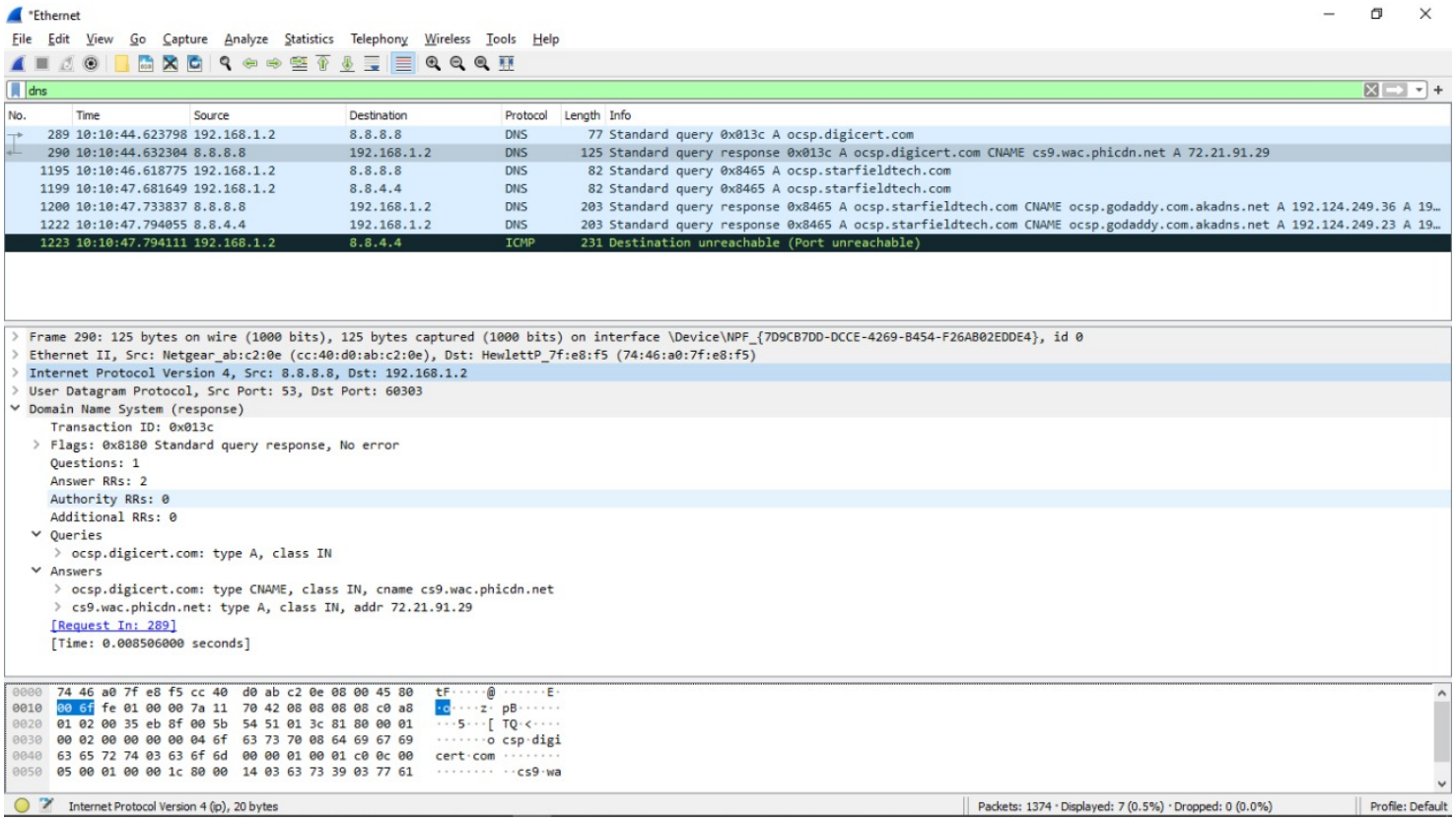
DNS response message : 8.8.4.4




*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
33 00:21:28.679034 192.168.1.7 192.168.1.2 TCP 164 8009 → 52900 [PSH, ACK] Seq=331 Ack=441 Win=279 Len=110 [TCP segment of a reassembled PDU]
34 00:21:28.720251 192.168.1.2 192.168.1.7 TCP 54 52900 → 8009 [ACK] Seq=441 Ack=441 Win=511 Len=0
35 00:21:29.085504 Netgear_ab:c2:0e HewlettP_7f:e8:f5 ARP 60 Who has 192.168.1.2? Tell 192.168.1.1
36 00:21:29.085535 HewlettP_7f:e8:f5 Netgear_ab:c2:0e ARP 42 192.168.1.2 is at 74:46:a0:7f:e8:f5
37 00:21:29.965419 192.168.1.2 8.8.8.8 DNS 70 Standard query 0x5fd8 A dns.google
38 00:21:29.967355 8.8.8.8 192.168.1.2 DNS 102 Standard query response 0x5fd8 A dns.google A 8.8.4.4 A 8.8.8.8
39 00:21:29.969929 192.168.1.2 8.8.4.4 TCP 66 52955 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
Frame 39: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 8.8.4.4
Transmission Control Protocol, Src Port: 52955, Dst Port: 443, Seq: 0, Len: 0
0000 cc 40 d0 ab c2 0e 74 46 a0 7f e8 f5 08 00 45 00
0010 00 34 6f 41 40 00 80 06 00 00 c0 a8 01 02 08 08
0020 04 04 ce db 01 bb 1d bd b5 99 00 00 00 00 80 02
0030 fa f0 cd dc 00 00 02 04 05 b4 01 03 03 08 01 01
wireshark_Ethernet_20200709002113_a09244.pcapng
Packets: 1160 · Displayed: 1160 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

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.

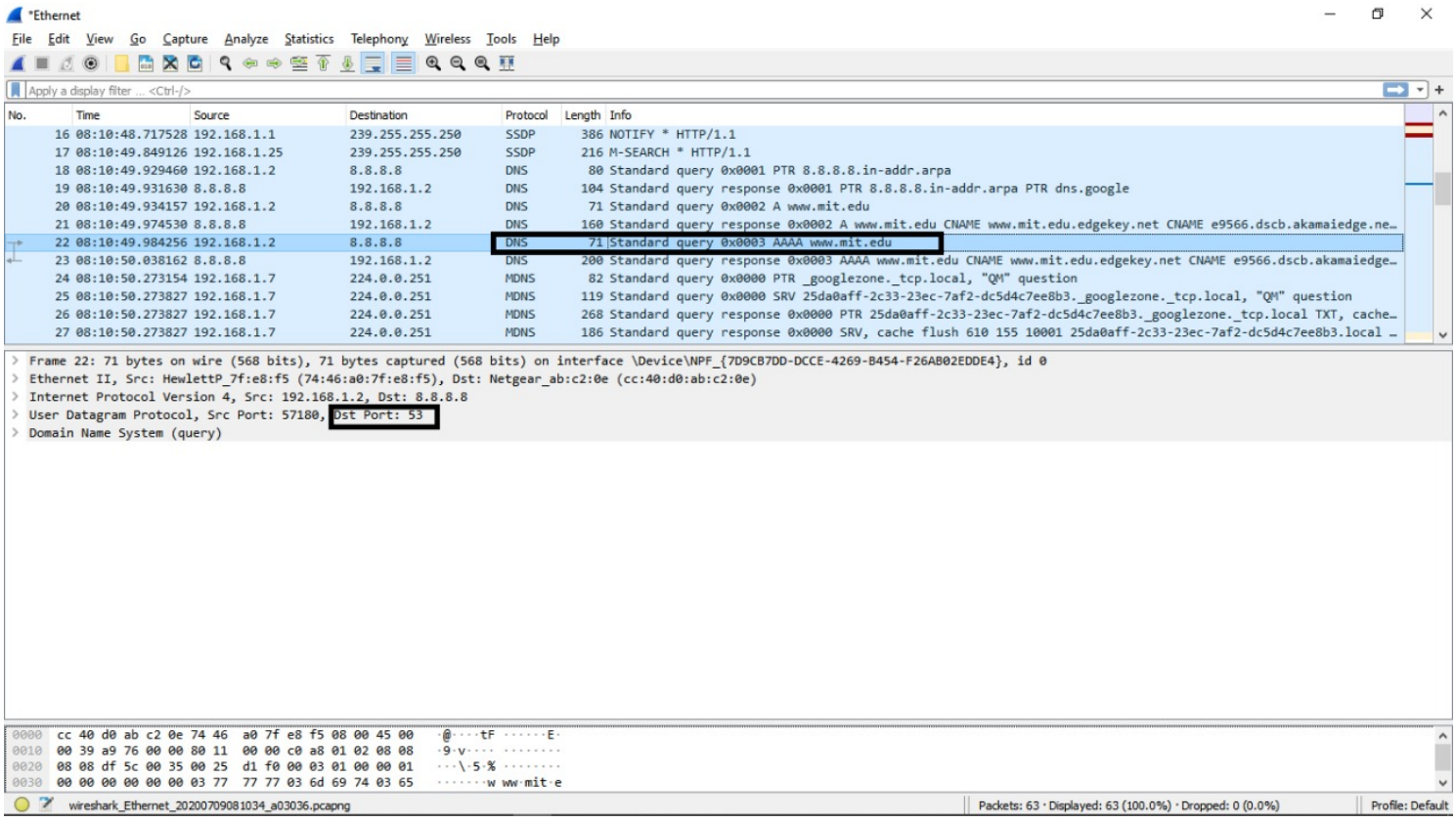


11 . What is the destination port for the DNS query message? What is the source port of DNS response message?

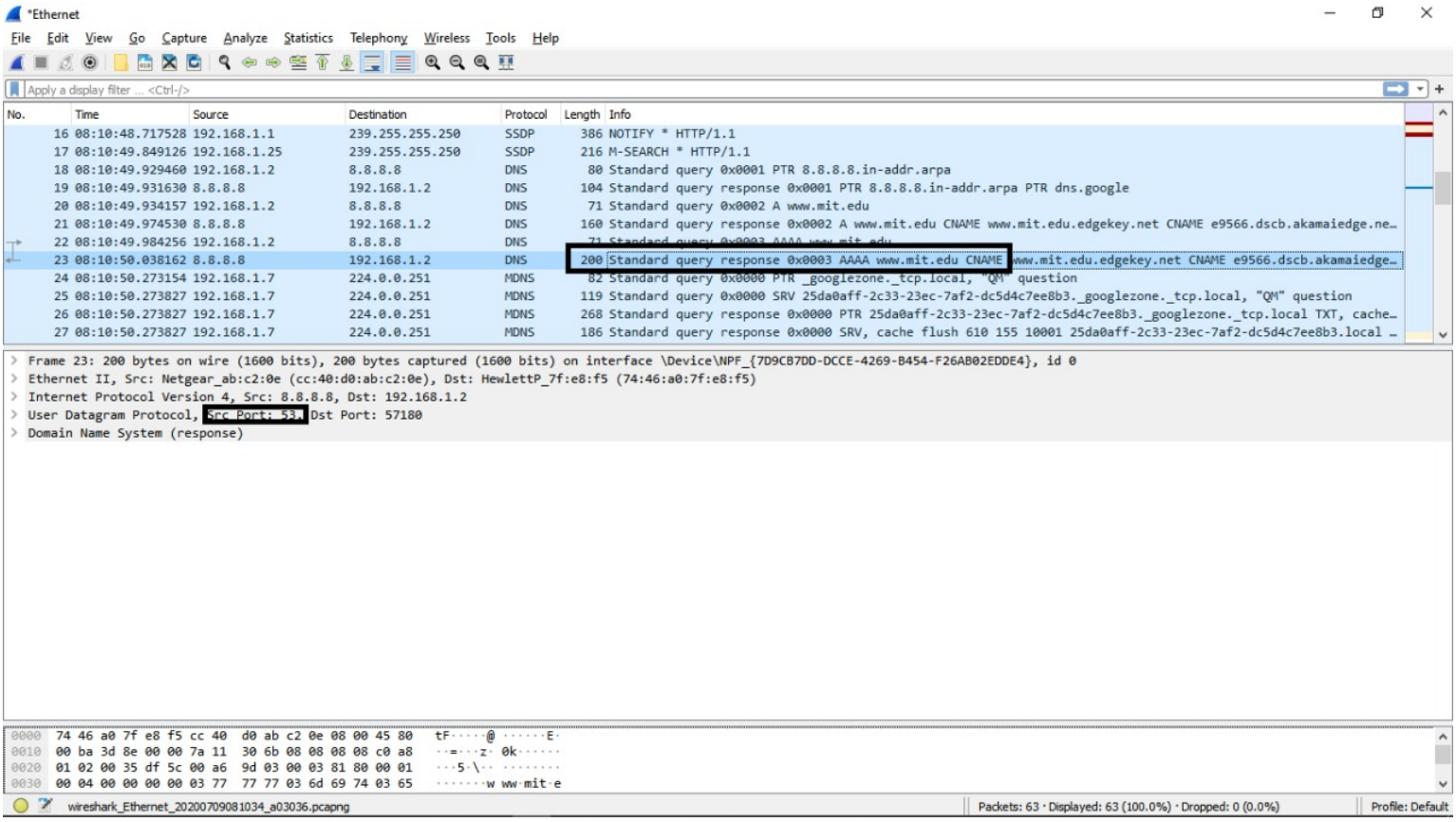
Answer :

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

DNS query message :



DNS response message



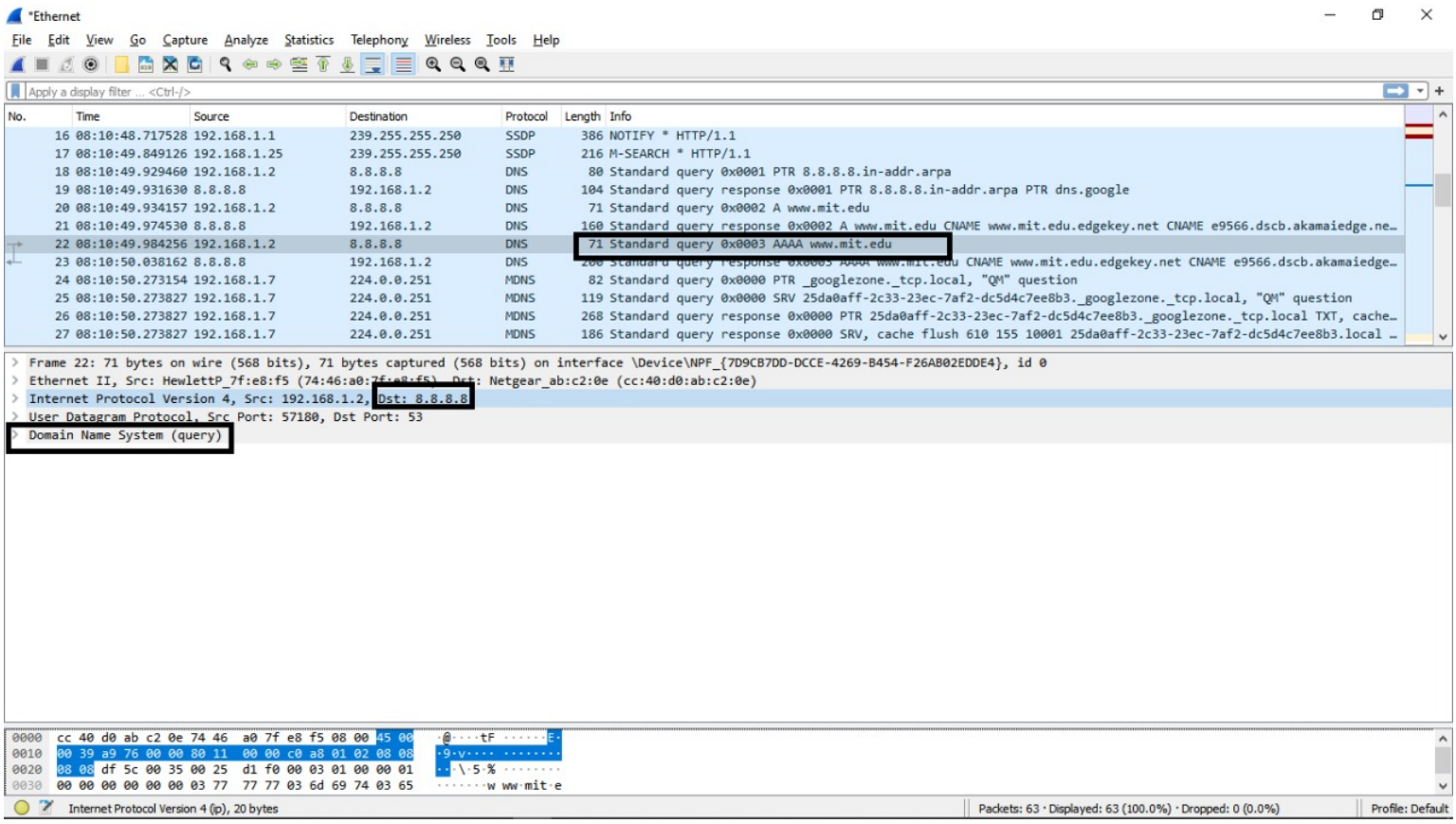
12 . To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
Answer :

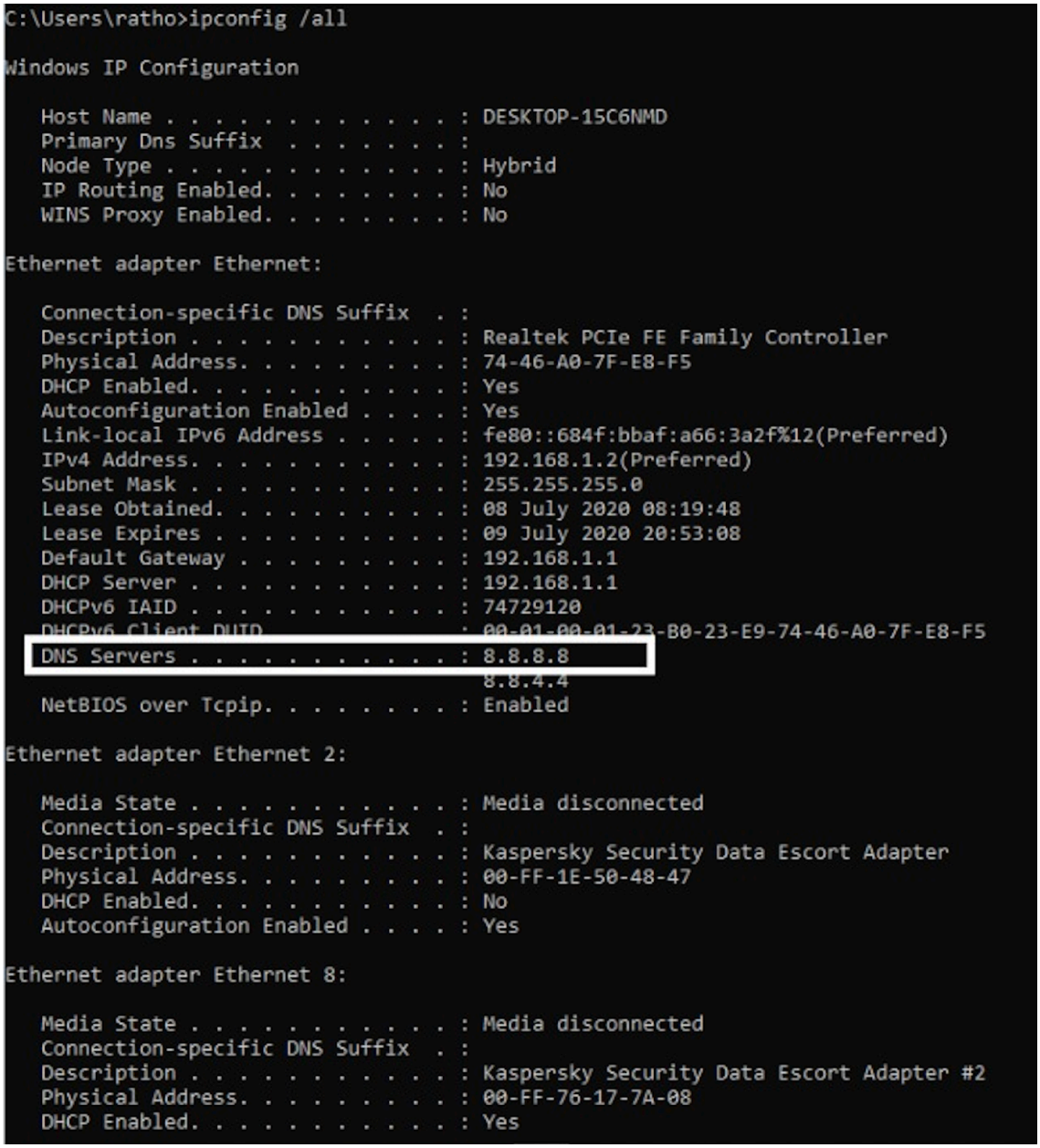
- DNS query message is sent to : 8.8.8.8

- 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**

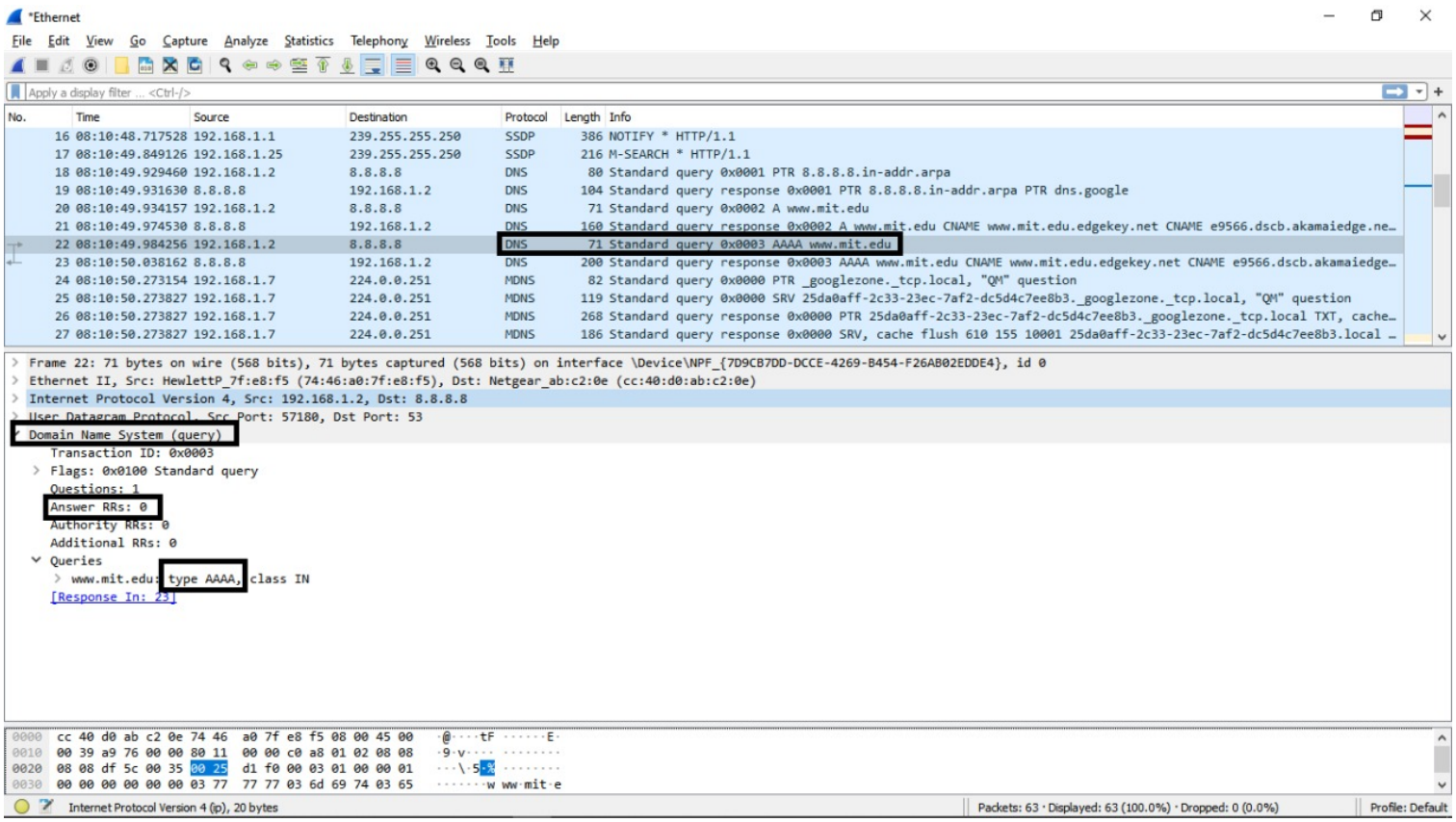



C:\Users\ratho>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-15C6NMD
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Description . . . . . : 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 :.

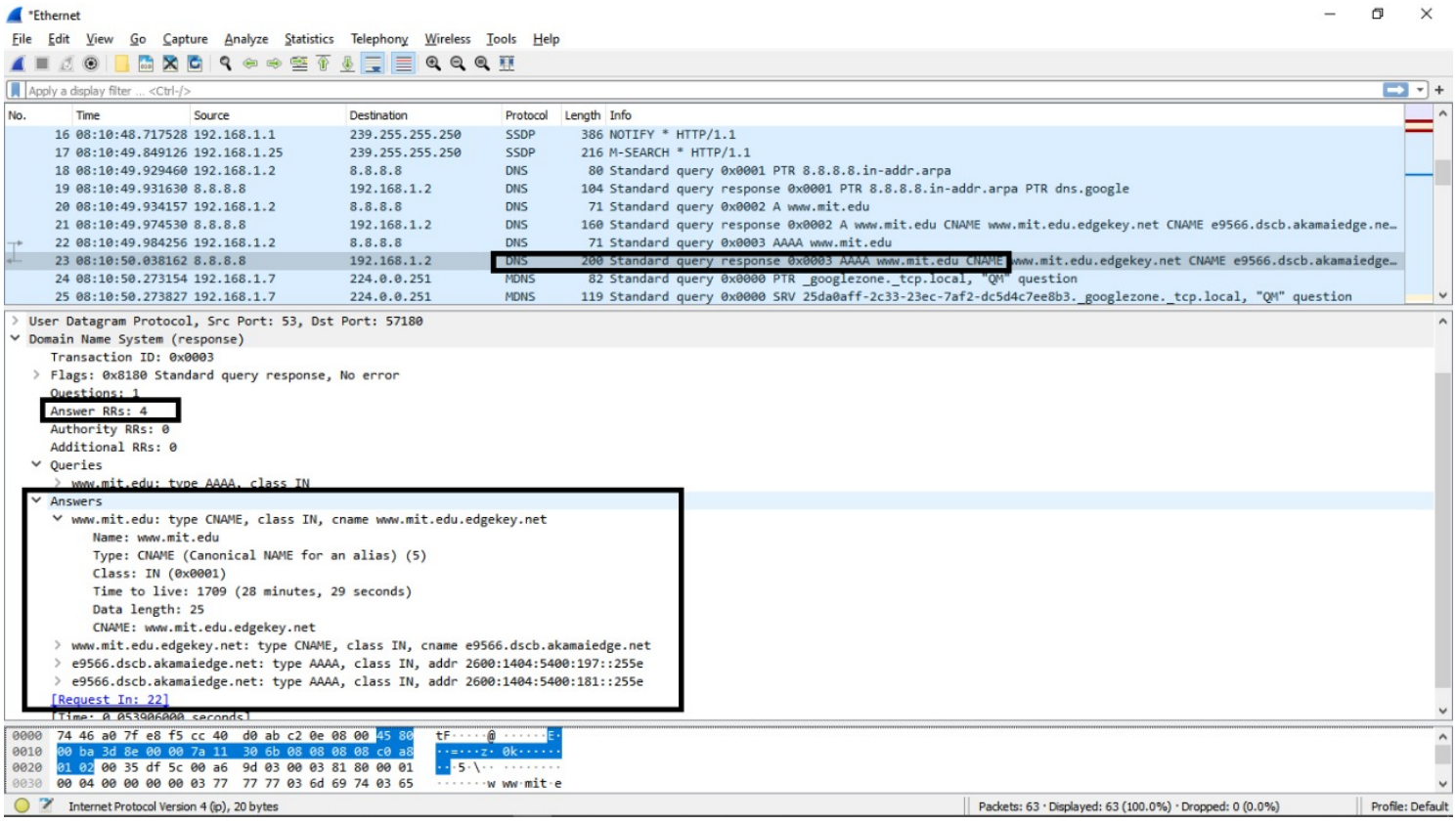
- DNS query message is of type "**AAAA**" .
- The query message **does not** contain any answer.



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

Answer :

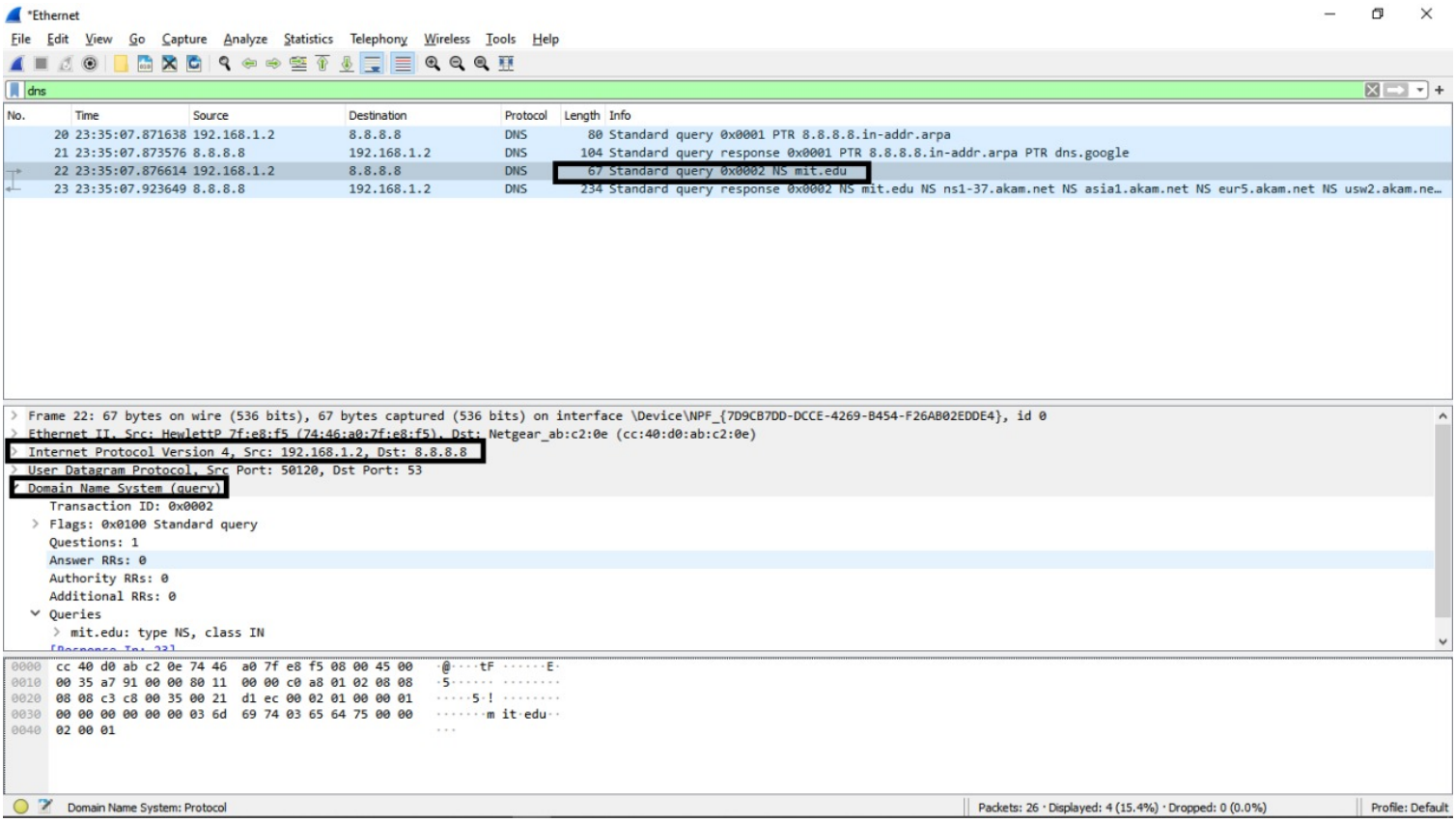
- DNS response message contain **4** answer.
- Each of these answers contain
    - Name , Type, Class, Time to Live, Date Length, Canonical Name.



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 Is this the IP address of your default local DNS server.

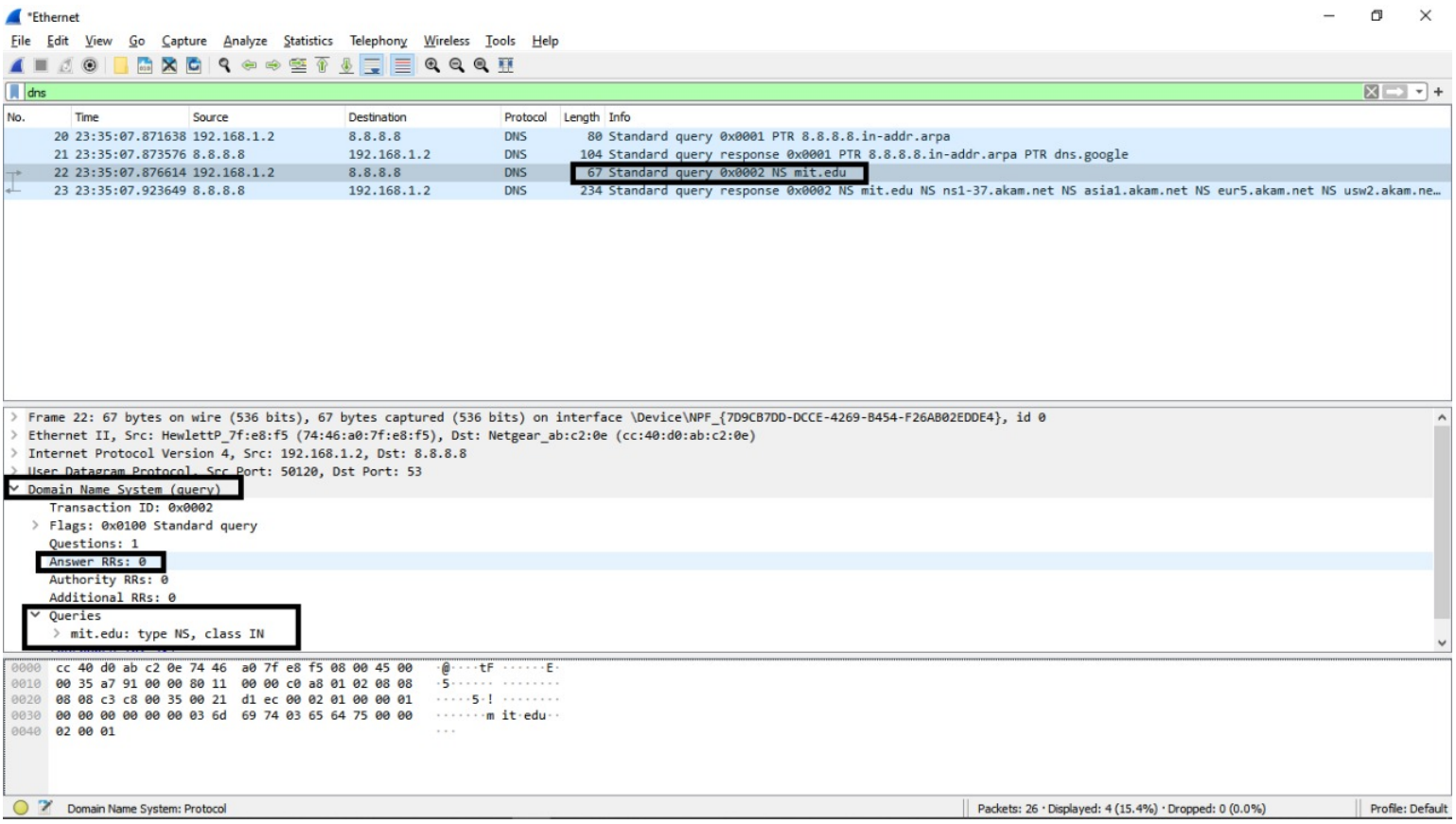


```
C:\Users\ratho>ipconfig /all

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 .

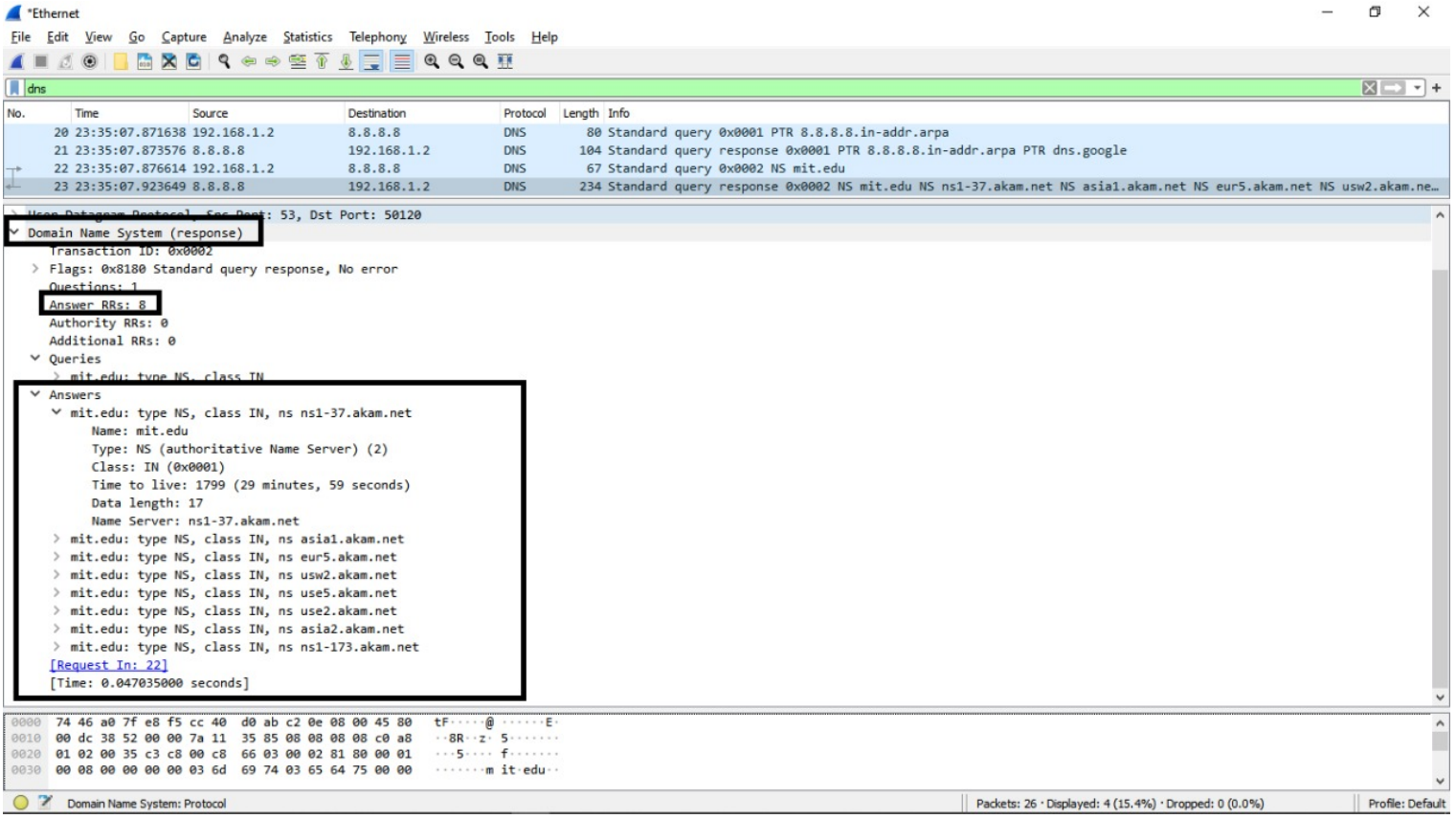


18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

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.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
20 23:35:07.871638 192.168.1.2 8.8.8.8 DNS 80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
21 23:35:07.873576 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
22 23:35:07.876614 192.168.1.2 8.8.8.8 DNS 67 Standard query 0x0002 NS mit.edu
23 23:35:07.923649 8.8.8.8 192.168.1.2 DNS 234 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS asia1.akam.net NS eur5.akam.net NS usw2.akam.ne…
Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 8
Authority RRs: 0
Additional RRs: 0
Queries
Answers
mit.edu: type NS, class IN, ns ns1-37.akam.net
Name: mit.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1799 (29 minutes, 59 seconds)
Data length: 17
Name Server: ns1-37.akam.net
mit.edu: type NS, class IN, ns asia1.akam.net
mit.edu: type NS, class IN, ns eur5.akam.net
mit.edu: type NS, class IN, ns usw2.akam.net
mit.edu: type NS, class IN, ns use5.akam.net
mit.edu: type NS, class IN, ns use2.akam.net
mit.edu: type NS, class IN, ns asia2.akam.net
mit.edu: type NS, class IN, ns ns1-173.akam.net
[Request In: 22]
[Time: 0.047035000 seconds]
0000 74 46 a0 7f e8 f5 cc 40 d0 ab c2 0e 08 00 45 80
0010 00 dc 38 52 00 00 7a 11 35 85 08 08 08 08 c0 a8
0020 01 02 00 35 c3 c8 00 c8 66 03 00 02 81 80 00 01
0030 00 08 00 00 00 00 03 6d 69 74 03 65 64 75 00 00
Domain Name System: Protocol
Packets: 26 · Displayed: 4 (15.4%) · Dropped: 0 (0.0%)
Profile: Default