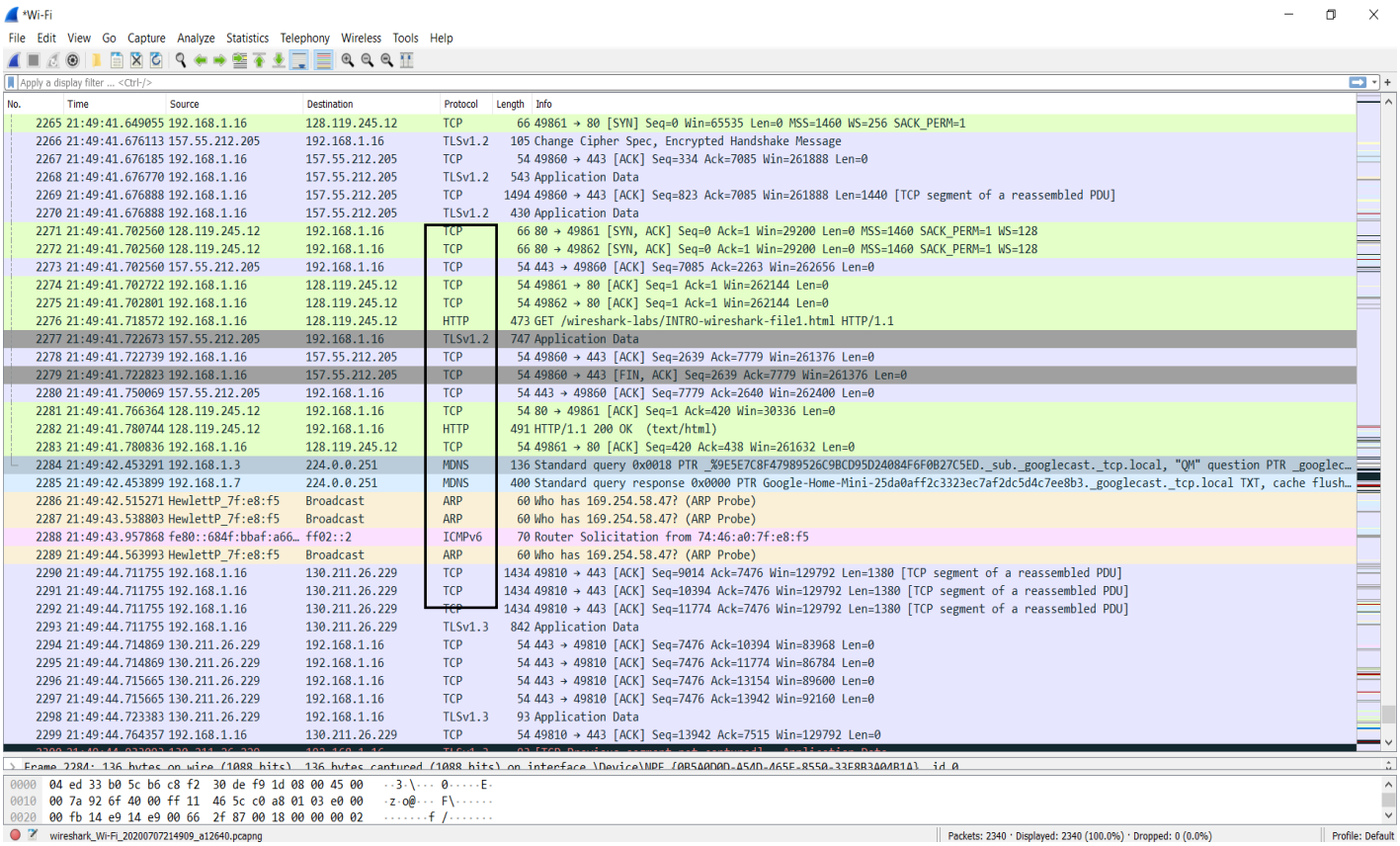
LAB 1

What to hand in

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

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

TCP, HTTP, ARP, TLSv1.2, MDNS

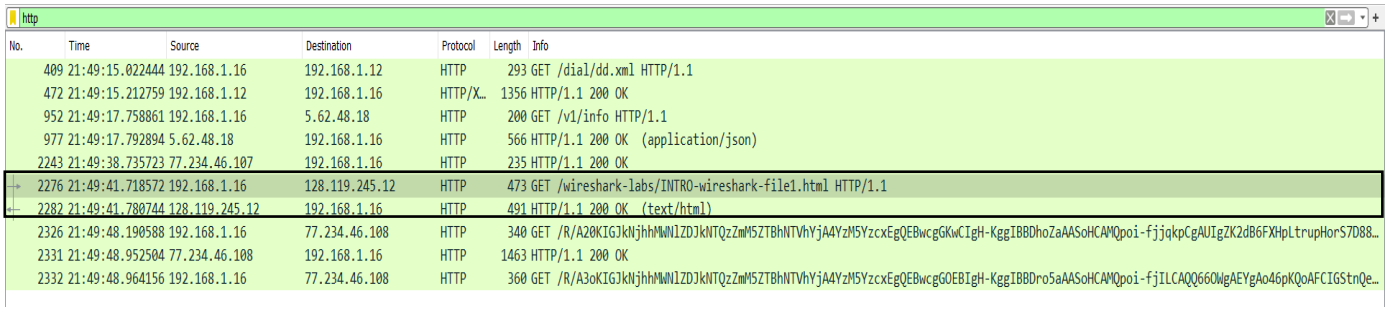


LAB 1

2. 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.)

   HTTP GET request was sent at - 21:49:41.718572
   HTTP OK reply was received at – 21:49:41.780744

   Time elapsed - 21:49:41.780744 – 21:49:41.718572 = 00:00:0.62172 Seconds

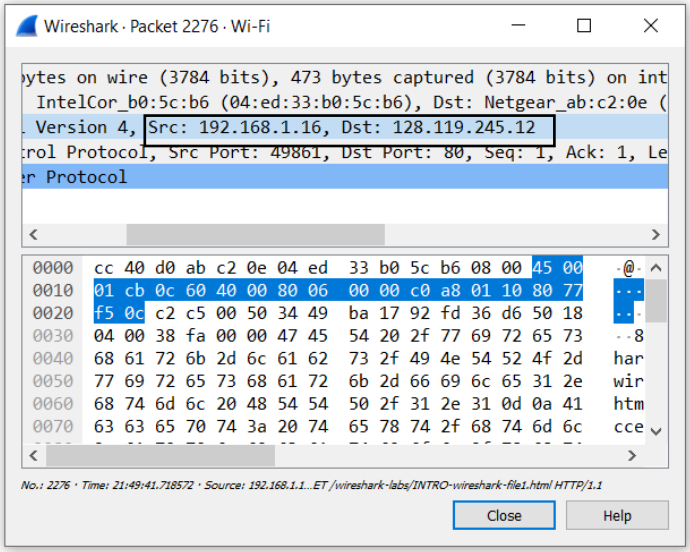


http

No.	Time	Source	Destination	Protocol	Length	Info
409	21:49:15.022444	192.168.1.16	192.168.1.12	HTTP	293	GET /dial/dd.xml HTTP/1.1
472	21:49:15.212759	192.168.1.12	192.168.1.16	HTTP/X…	1356	HTTP/1.1 200 OK
952	21:49:17.758861	192.168.1.16	5.62.48.18	HTTP	200	GET /v1/info HTTP/1.1
977	21:49:17.792894	5.62.48.18	192.168.1.16	HTTP	566	HTTP/1.1 200 OK (application/json)
2243	21:49:38.735723	77.234.46.107	192.168.1.16	HTTP	235	HTTP/1.1 200 OK
2276	21:49:41.718572	192.168.1.16	128.119.245.12	HTTP	473	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2282	21:49:41.780744	128.119.245.12	192.168.1.16	HTTP	491	HTTP/1.1 200 OK (text/html)
2326	21:49:48.190588	192.168.1.16	77.234.46.108	HTTP	340	GET /R/A20KIGJkNjhhMWNlZDJkNTQzZmM5ZTBhNTVhYjA4YzM5YzcxEgQEBwcgGKwCIgH-KggIBBDhoZaAASoHCAMQpoi-fjjqkpCgAUIgZK2dB6FXHpLtrupHorS7D88…
2331	21:49:48.952504	77.234.46.108	192.168.1.16	HTTP	1463	HTTP/1.1 200 OK
2332	21:49:48.964156	192.168.1.16	77.234.46.108	HTTP	360	GET /R/A3oKIGJkNjhhMWNlZDJkNTQzZmM5ZTBhNTVhYjA4YzM5YzcxEgQEBwcgGOEBIgH-KggIBBDro5aAASoHCAMQpoi-fjILCAQQ66OWgAEYgAo46pKQoAFCIGStnQe…

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

   Internet address of the gaia.cs.umass.edu **– 128.119.245.12 (Destination IP)**
   Internet address of your computer **– 192.168.1.16 (Source IP)**



LAB 1

4. 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.

No. Time Source Destination Protocol Length Info
2276 21:49:41.718572 192.168.1.16 128.119.245.12 HTTP 473 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 2276: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49861, Dst Port: 80, Seq: 1, Ack: 1, Len: 419
Hypertext Transfer Protocol

No. Time Source Destination Protocol Length Info
2282 21:49:41.780744 128.119.245.12 192.168.1.16 HTTP 491 HTTP/1.1 200 OK (text/html)

Frame 2282: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.16
Transmission Control Protocol, Src Port: 80, Dst Port: 49861, Seq: 1, Ack: 420, Len: 437
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)

PFA - Text file for the same

LAB 1

PART - 2

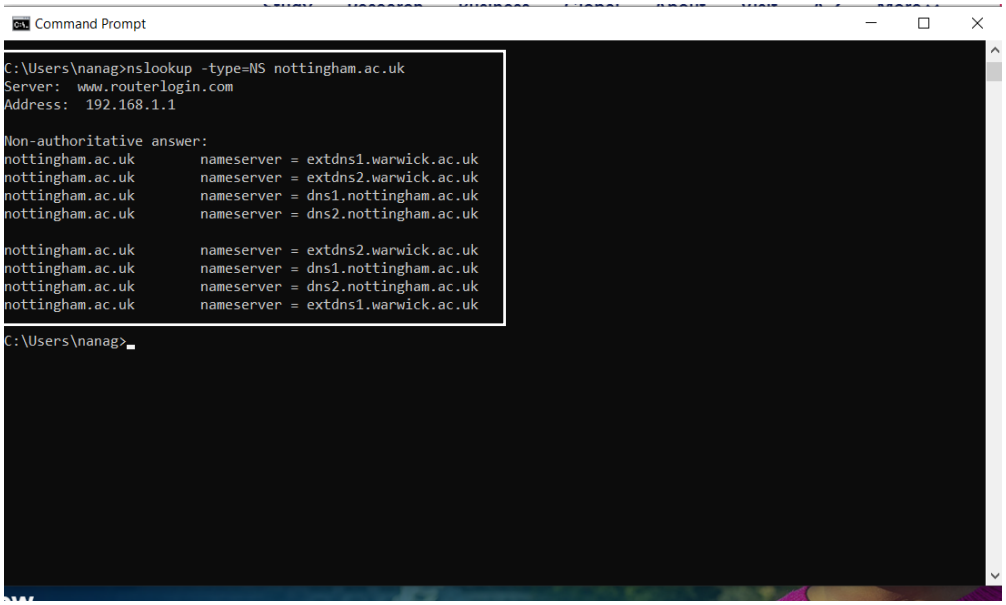
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

IP Address – 184.168.131.241

C:\Users\nanag>nslookup www.flipkart.in
Server: www.routerlogin.com
Address: 192.168.1.1

Non-authoritative answer:
Name: flipkart.in
Address: 184.168.131.241
Aliases: www.flipkart.in

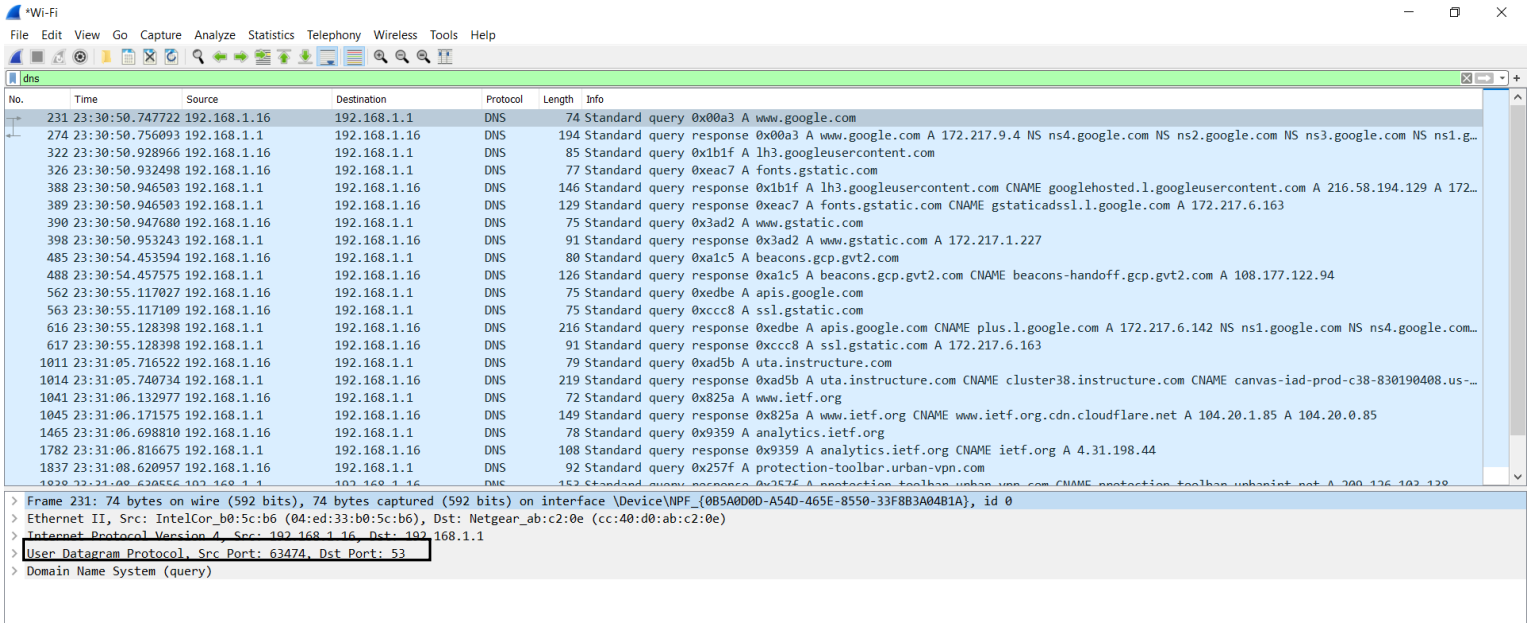
2. Run nslookup to determine the authoritative DNS servers for a university in Europe.



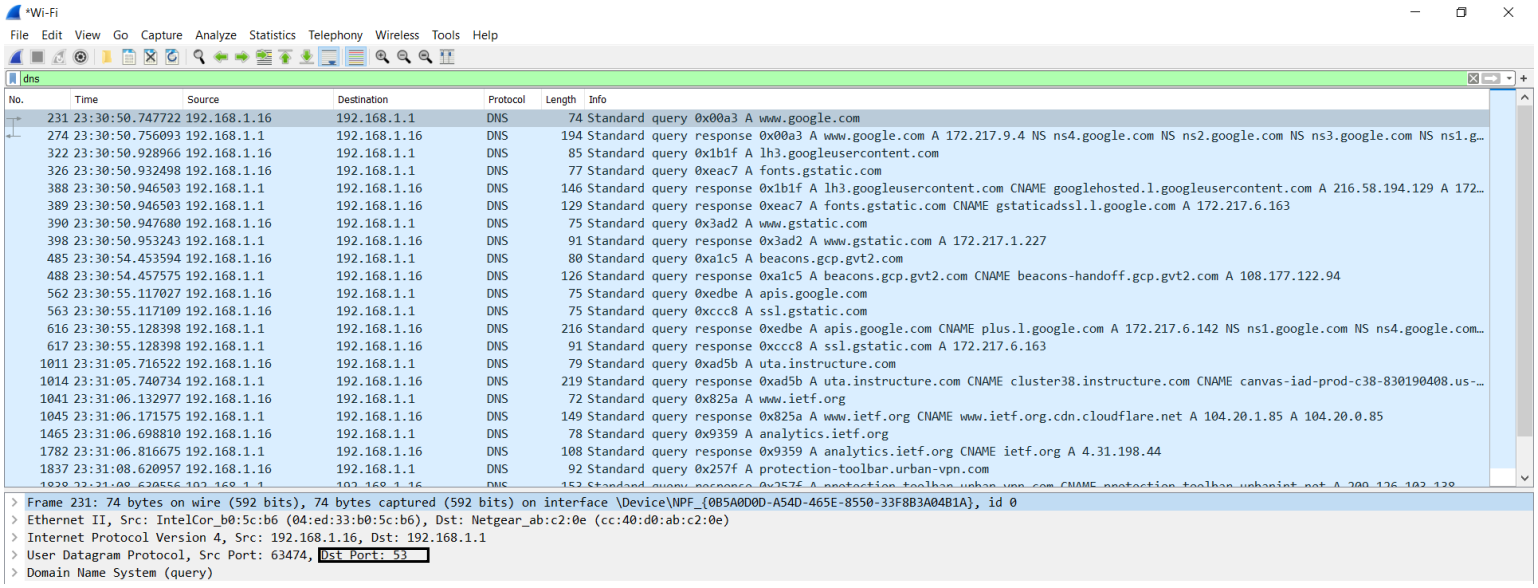
LAB 1

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

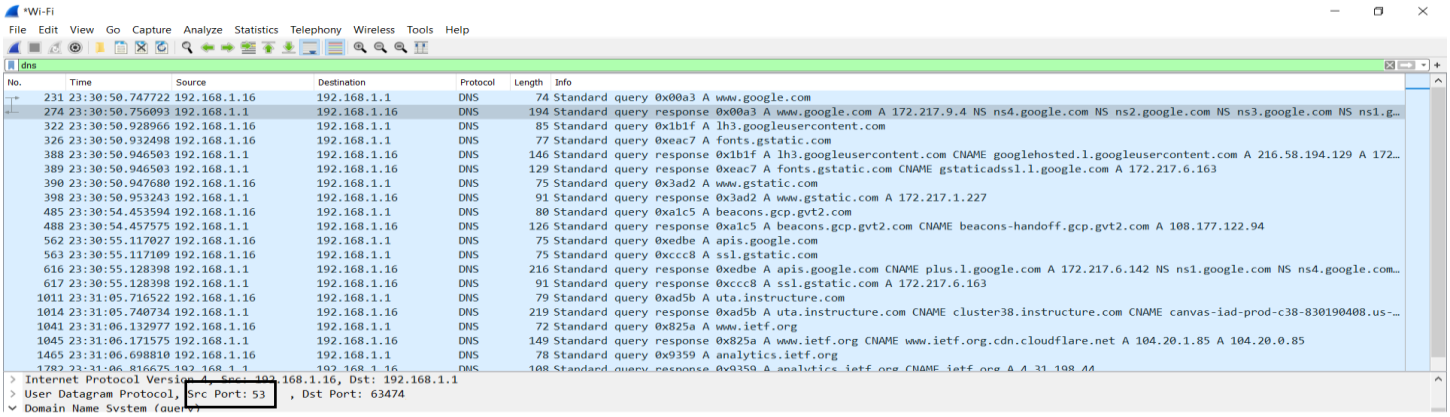
UDP



5. What is the destination port for the DNS query message? What is the source port of DNS response message?
   The destination port for the DNS query message – **53**
   The source port of DNS response message – **53**

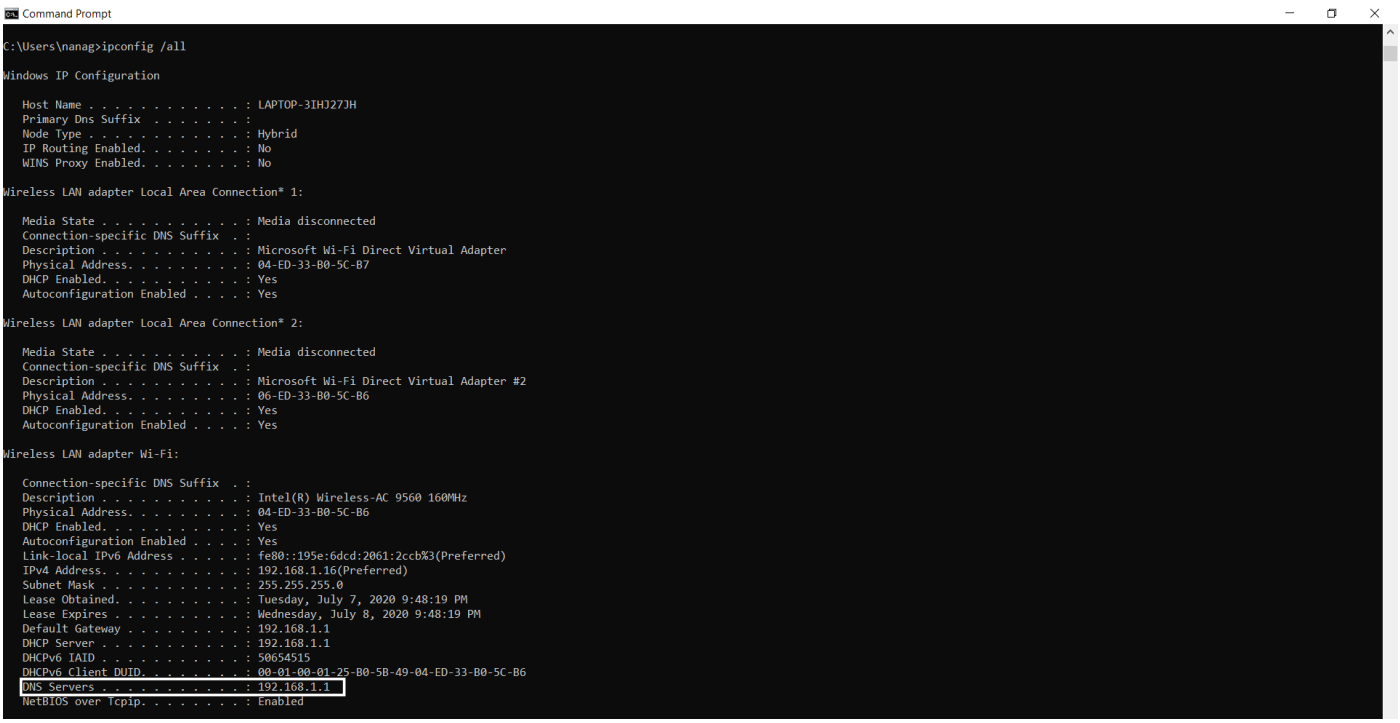


LAB 1

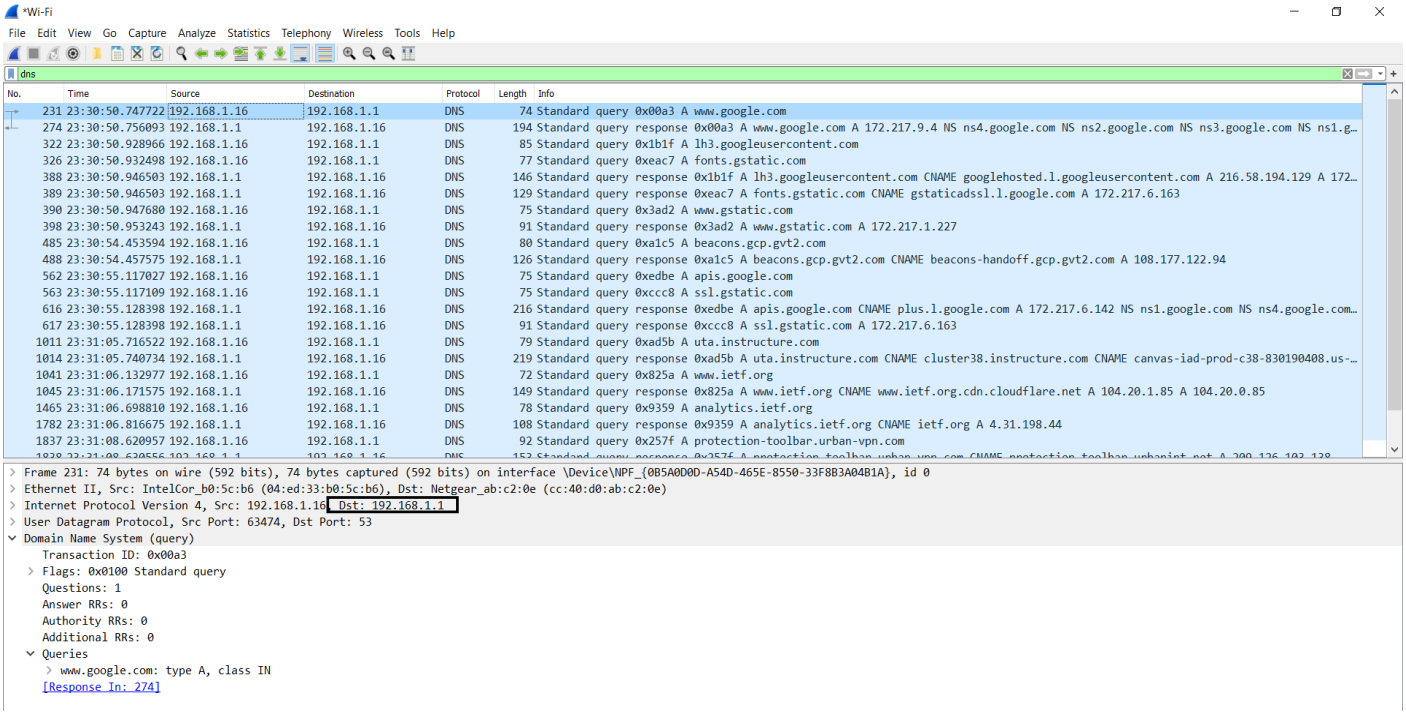


6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

YES, Both the IP Addresses are Same – 192.168.1.1



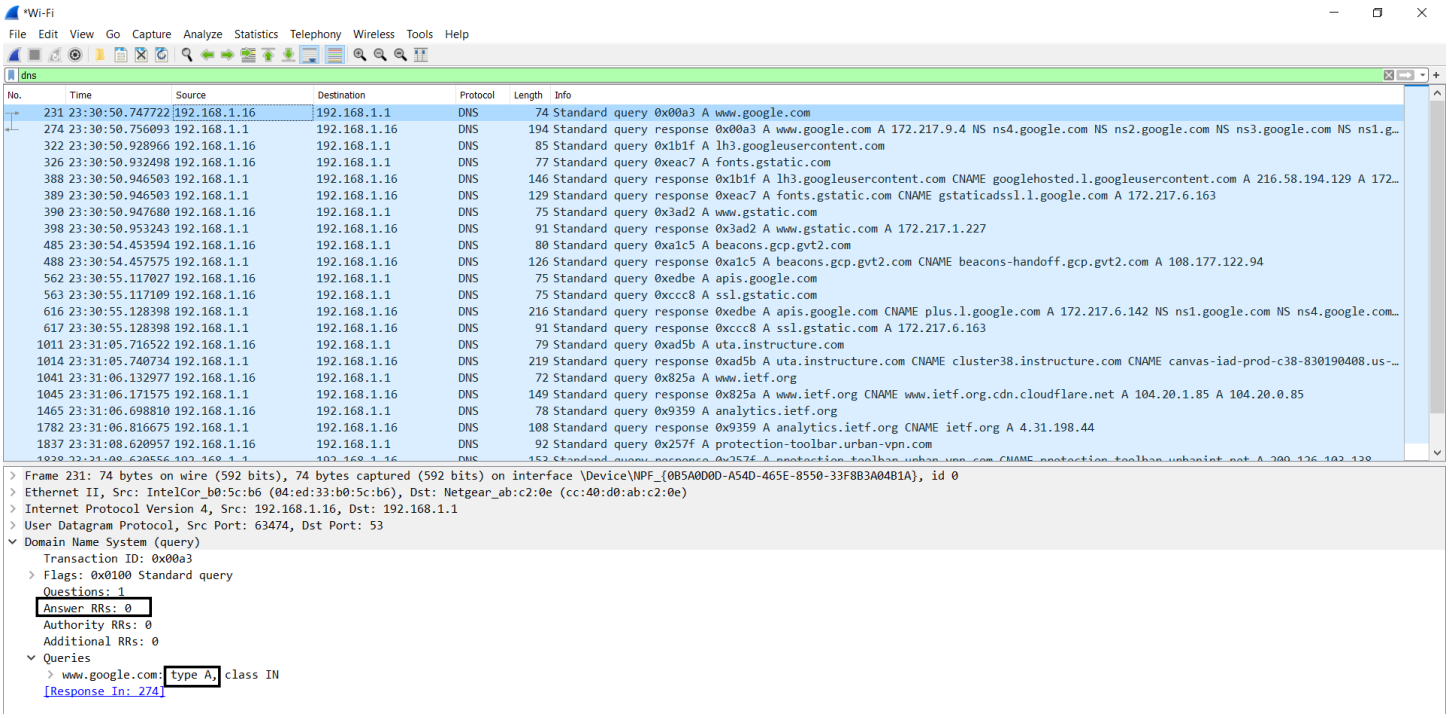
LAB 1



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

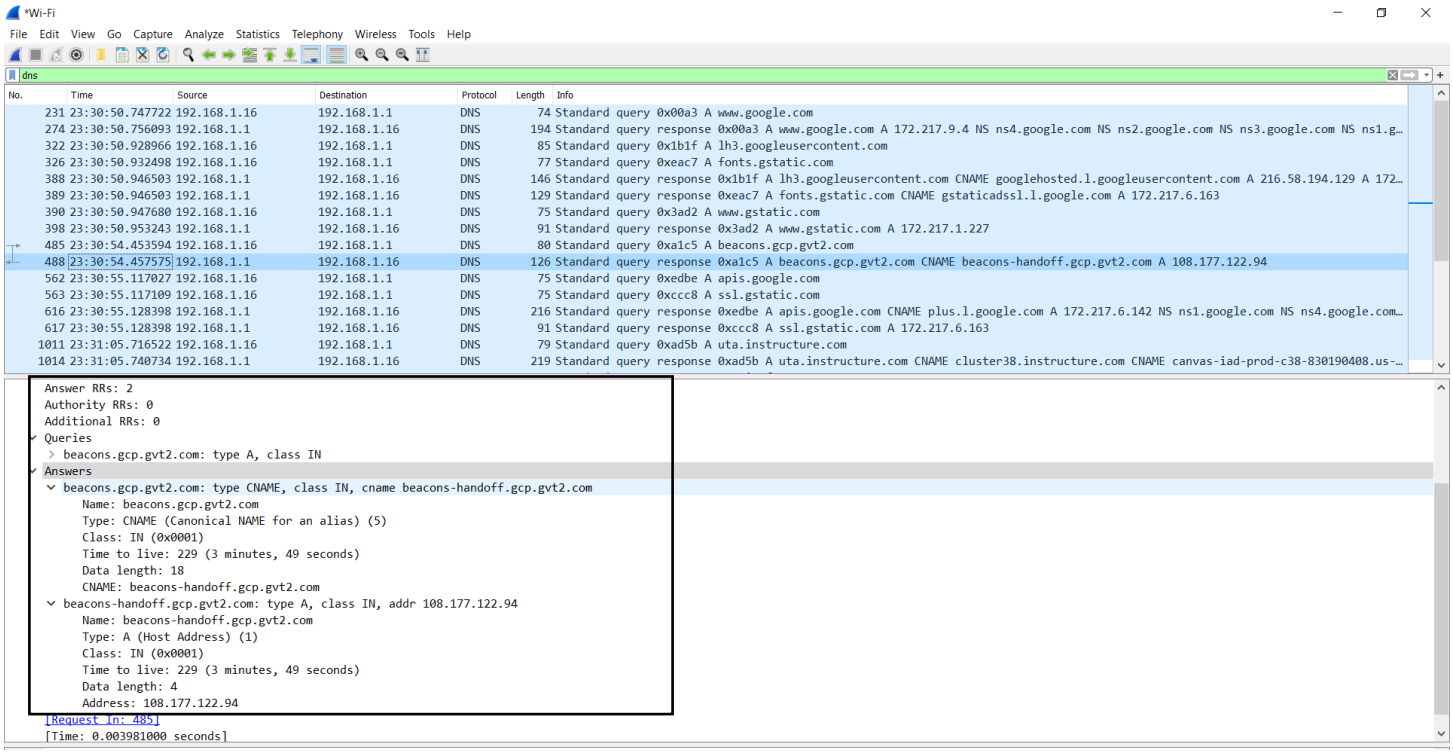
   DNS Querry – TYPE- A

   No querry message contains 0 Answers



LAB 1

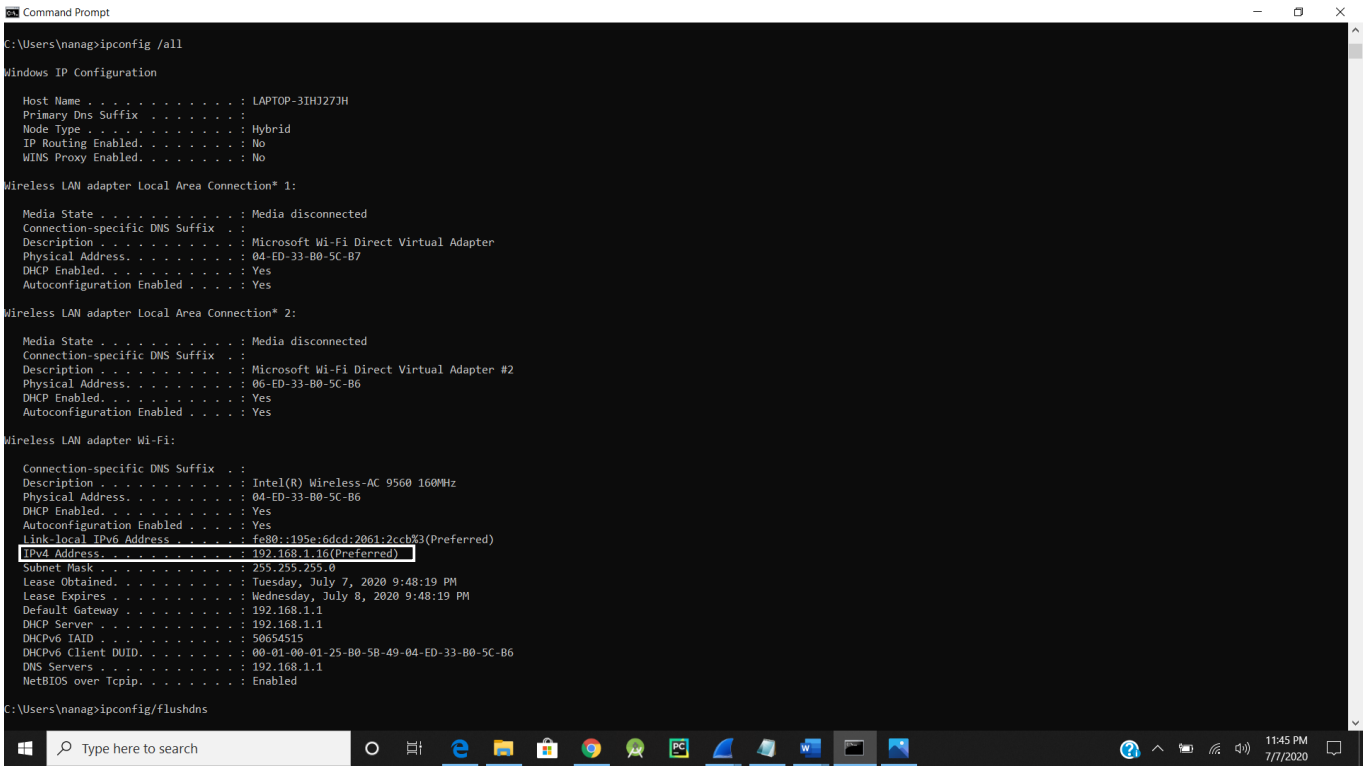
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
   ANSWERS = 2
   Each answer contains NAME, TYPE, Class, Time to Live, Data length, CNAME, Address

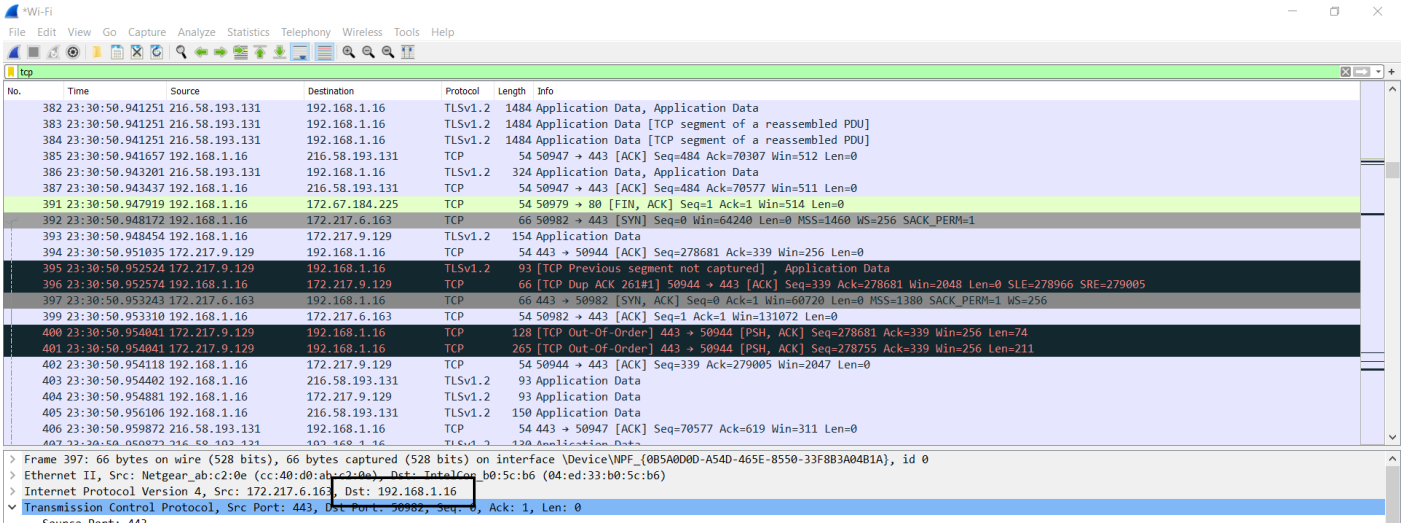


LAB 1

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?

The destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message – **YES, local IP – 192.168.1.16**

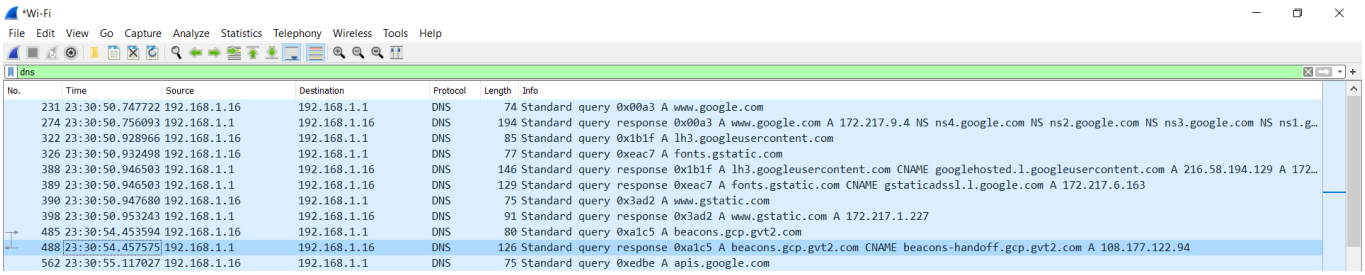




LAB 1

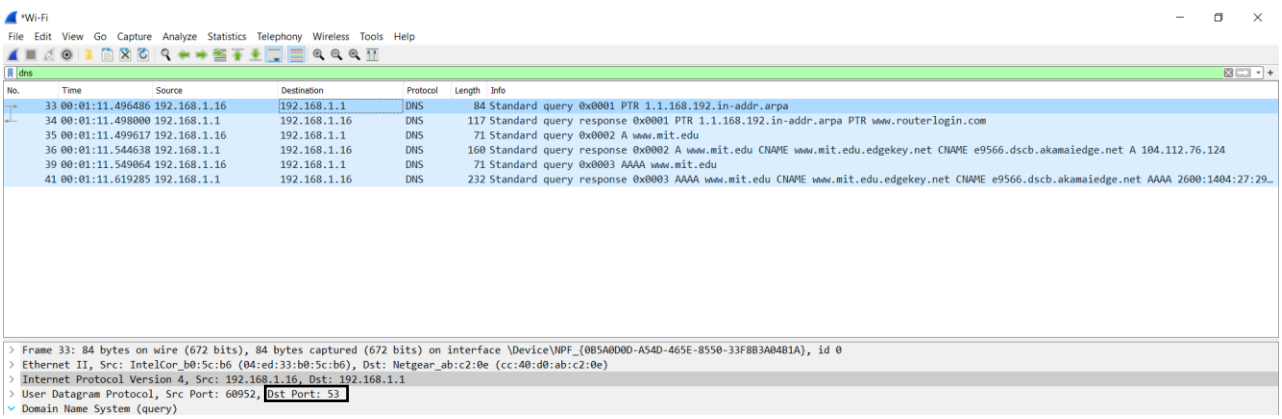
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

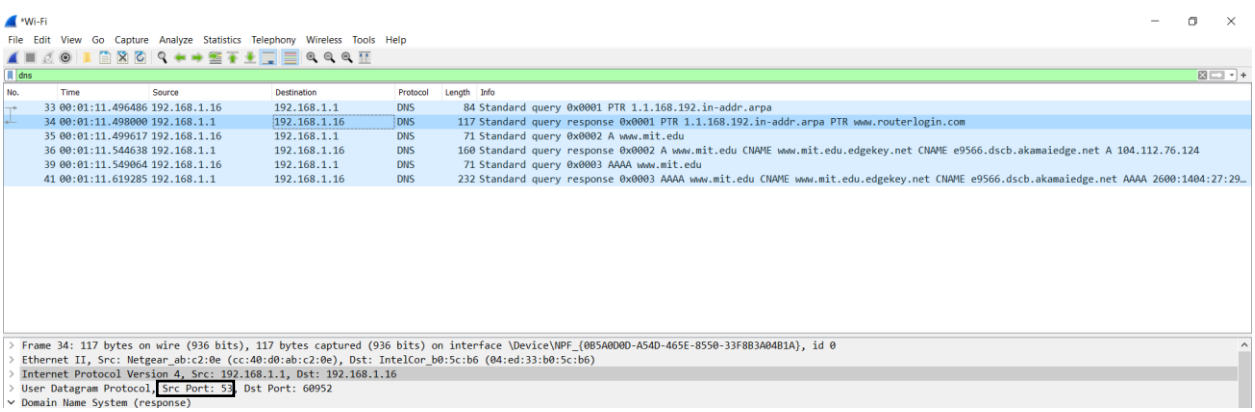
NO it does not issue new DNS querries.



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

The destination port for the DNS query message – **53**
The source port of DNS response message – **53**

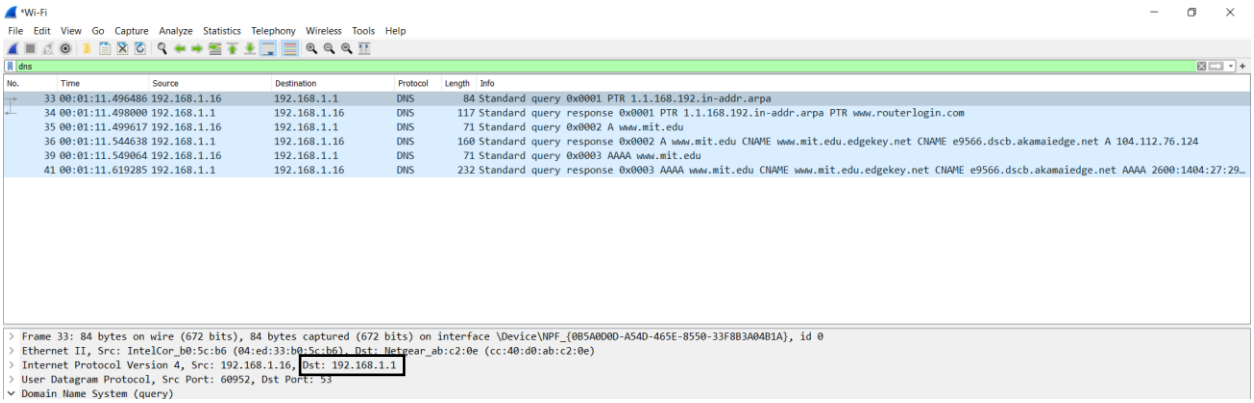


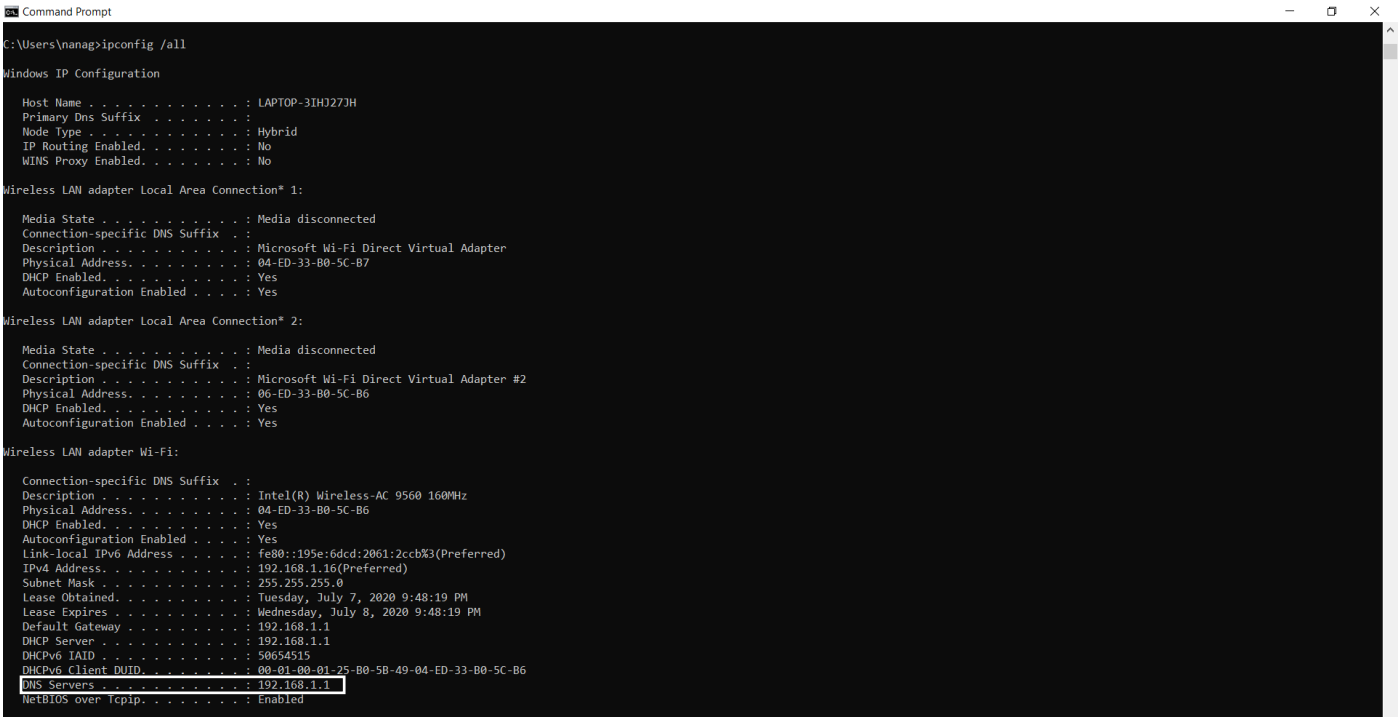


LAB 1

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

DNS query message IP address sent And the IP address of your default local DNS server are same – **192.168.1.1**



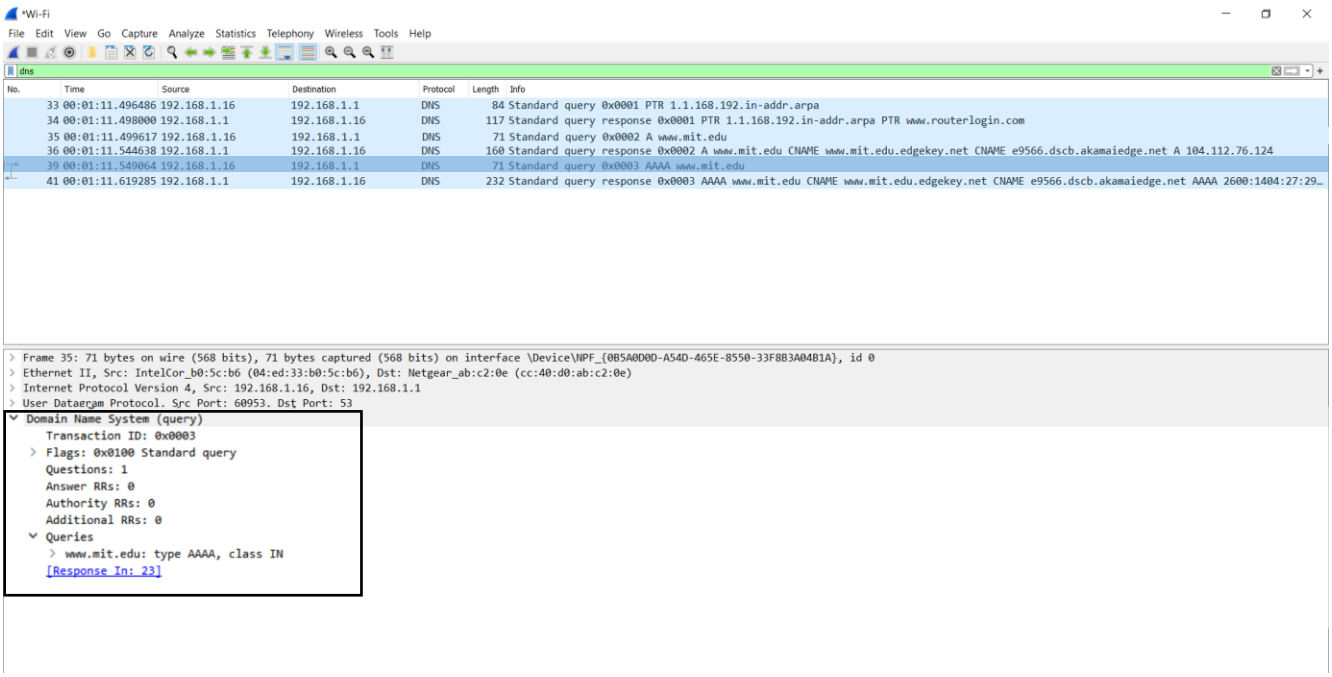


LAB 1

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

TYPE – AAAA

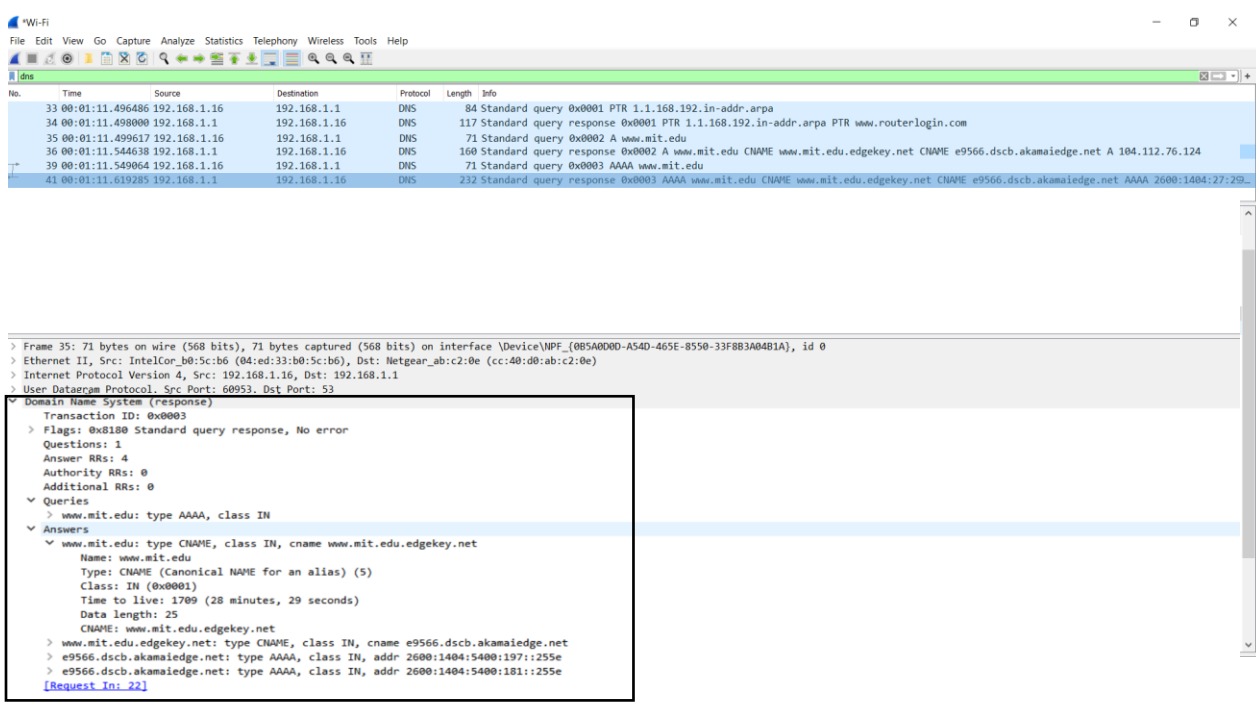
No query message does not contain any Answers. Answers = 0



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

ANSWERS = 4

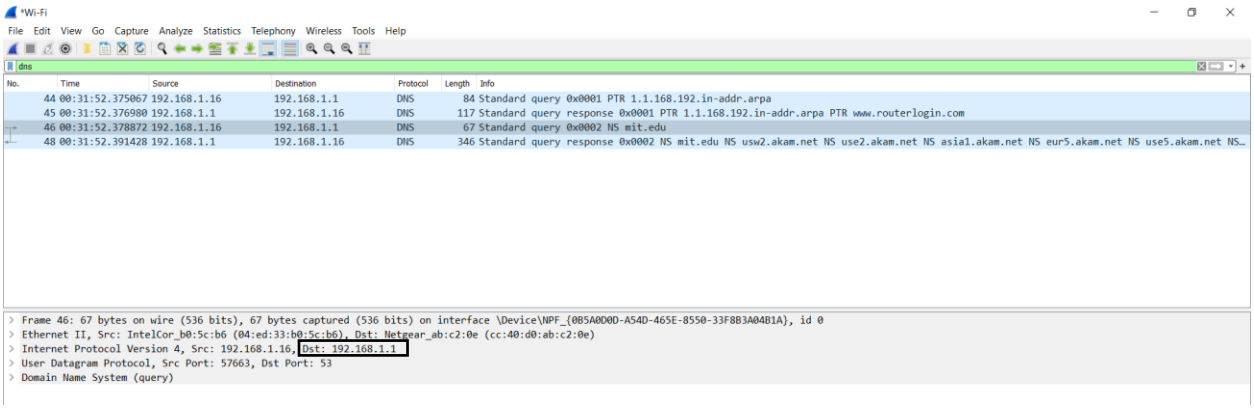
Each answer contains NAME, TYPE, Class, Time to Live, Data length, CNAME, Address

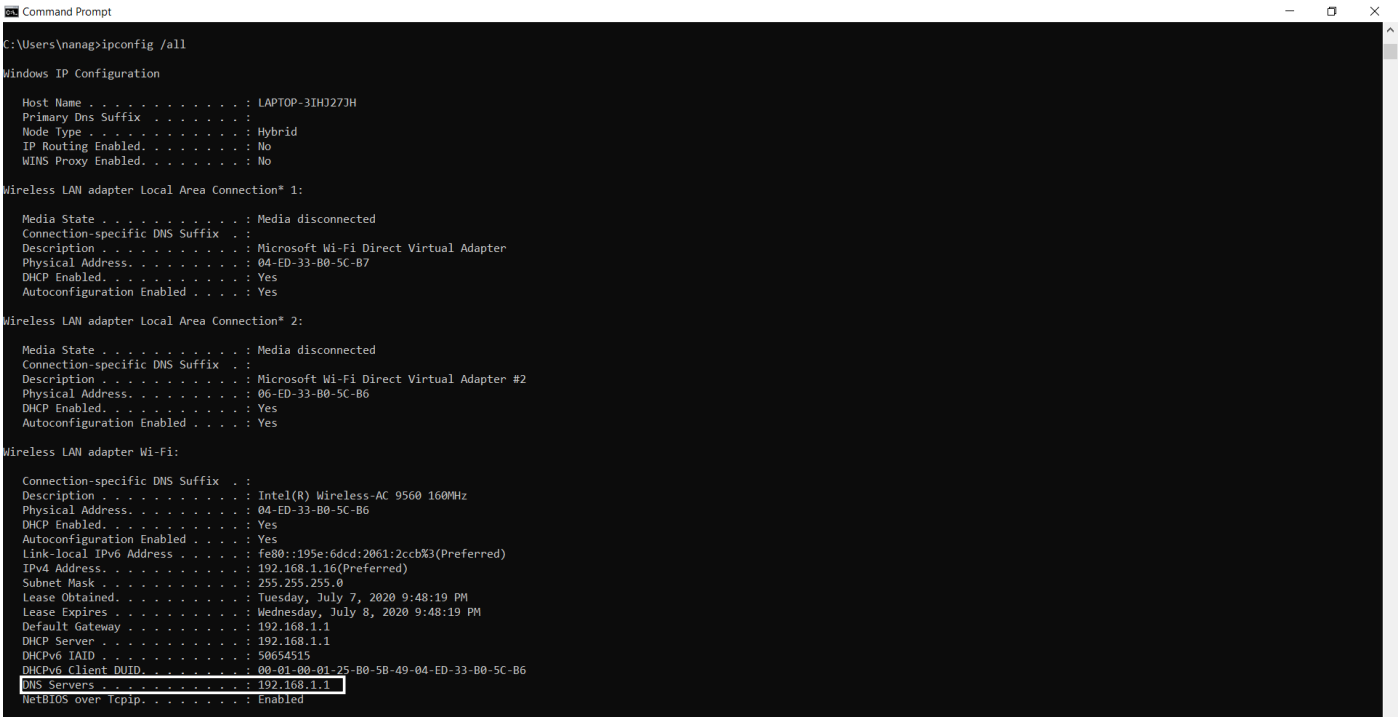


LAB 1

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

YES, IP address the DNS query message is sent is same as my default local DNS server-



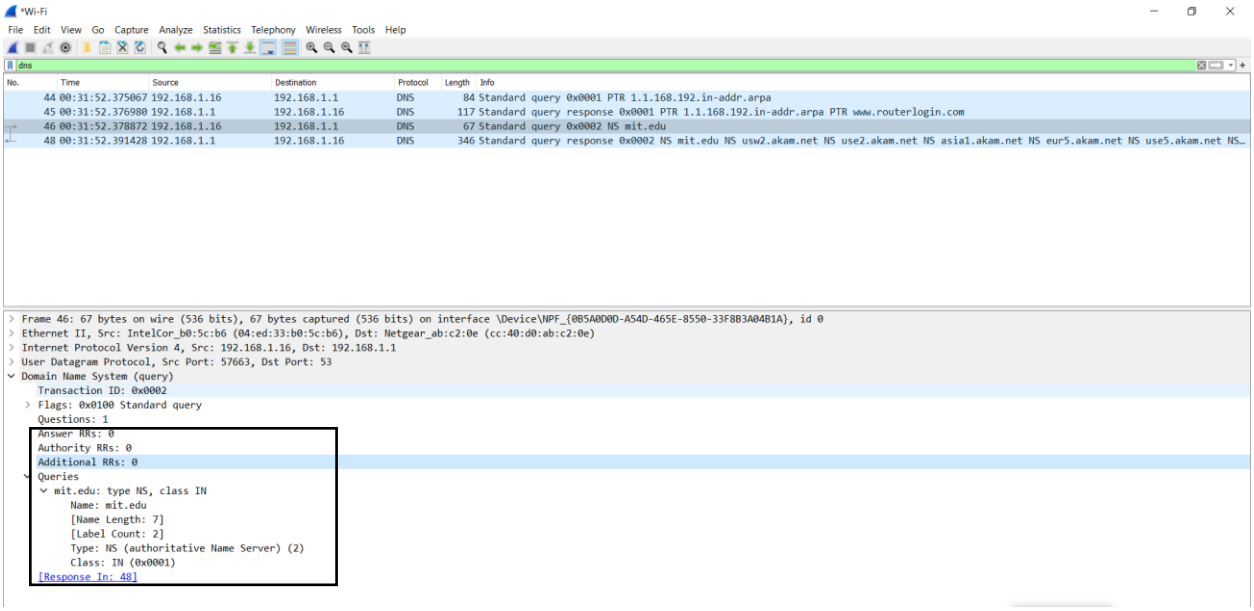


LAB 1

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

TYPE – NS

No query message does not contain any Answers. Answers = 0

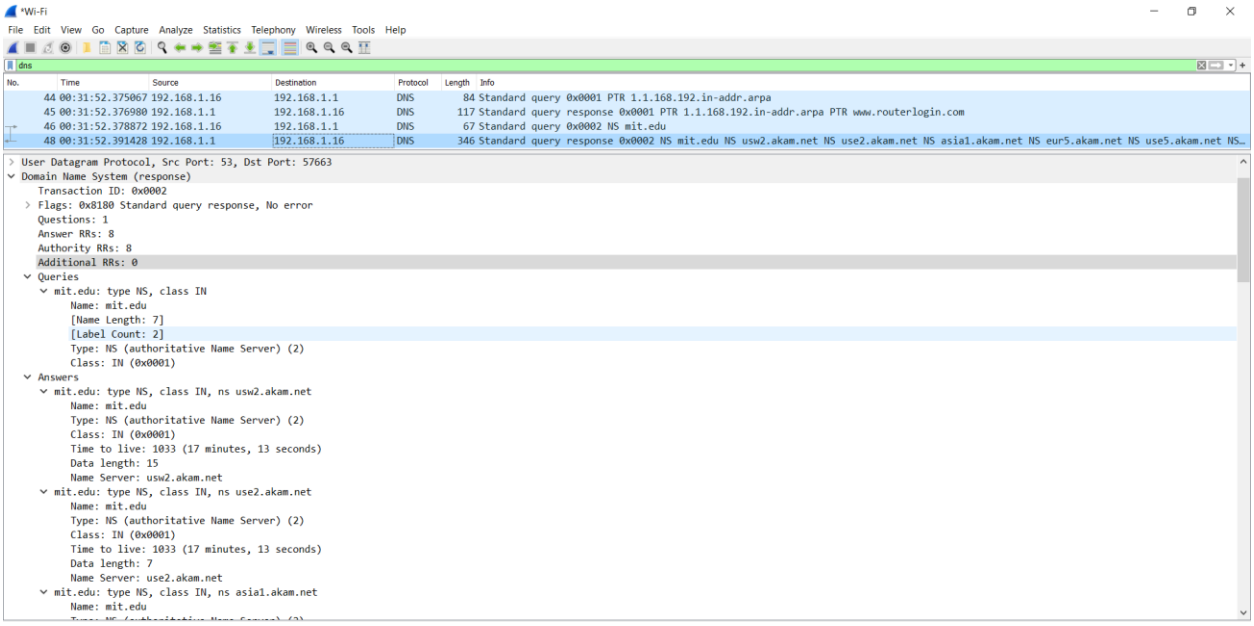


18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

usw2.akam.net
asia1.akam.net
eur5.akam.net
use5.akam.net
ns1-173.akam.net
asia2.akam.net
ns1-37.akam.net
use2.akam.net

YES, it does provide IP address of MIT nameservers

LAB 1


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
44 00:31:52.375067 192.168.1.16 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
45 00:31:52.376980 192.168.1.1 192.168.1.16 DNS 117 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR www.routerlogin.com
46 00:31:52.378872 192.168.1.16 192.168.1.1 DNS 67 Standard query 0x0002 NS mit.edu
48 00:31:52.391428 192.168.1.1 192.168.1.16 DNS 346 Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS use2.akam.net NS asia1.akam.net NS eur5.akam.net NS use5.akam.net NS…
User Datagram Protocol, Src Port: 53, Dst Port: 57663
Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 8
Authority RRs: 8
Additional RRs: 0
Queries
mit.edu: type NS, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Answers
mit.edu: type NS, class IN, ns usw2.akam.net
Name: mit.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1033 (17 minutes, 13 seconds)
Data length: 15
Name Server: usw2.akam.net
mit.edu: type NS, class IN, ns use2.akam.net
Name: mit.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1033 (17 minutes, 13 seconds)
Data length: 7
Name Server: use2.akam.net
mit.edu: type NS, class IN, ns asia1.akam.net
Name: mit.edu