Lab - 05

Wireshark - SMTP & DNS

Program: MScIT Sem-2

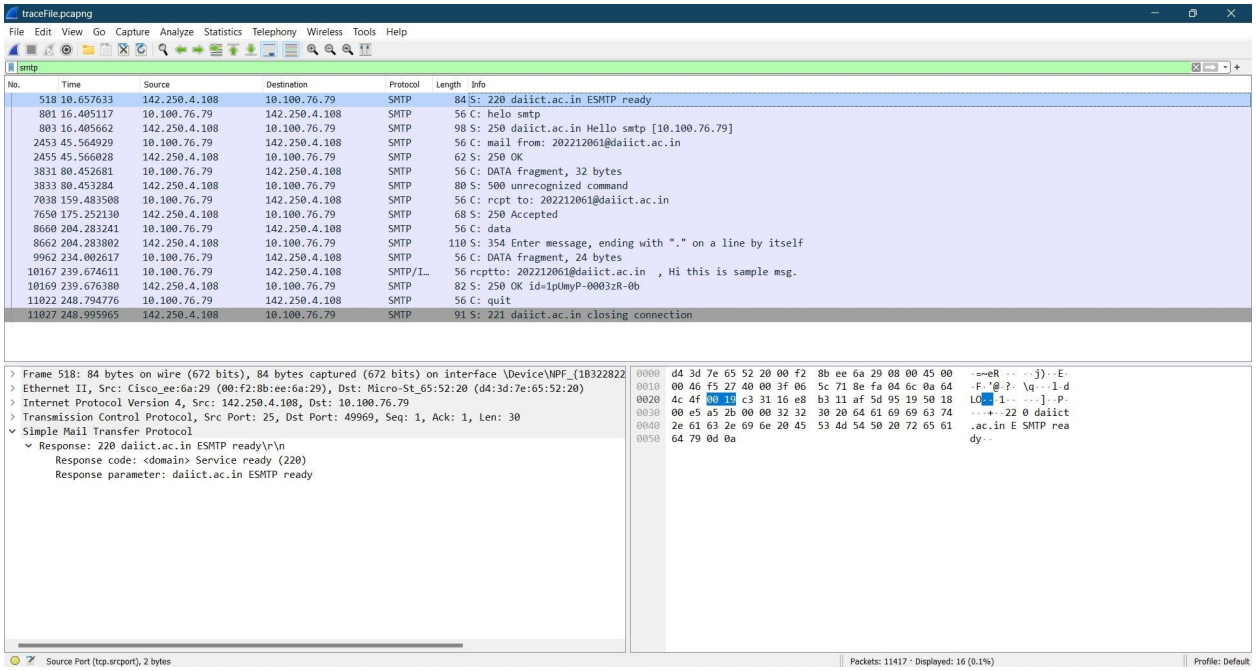
Group ID : 28

Student Name	Student ID
Dev Adnani	202212012
Saif Saiyed	202212083

1.3 Exercise

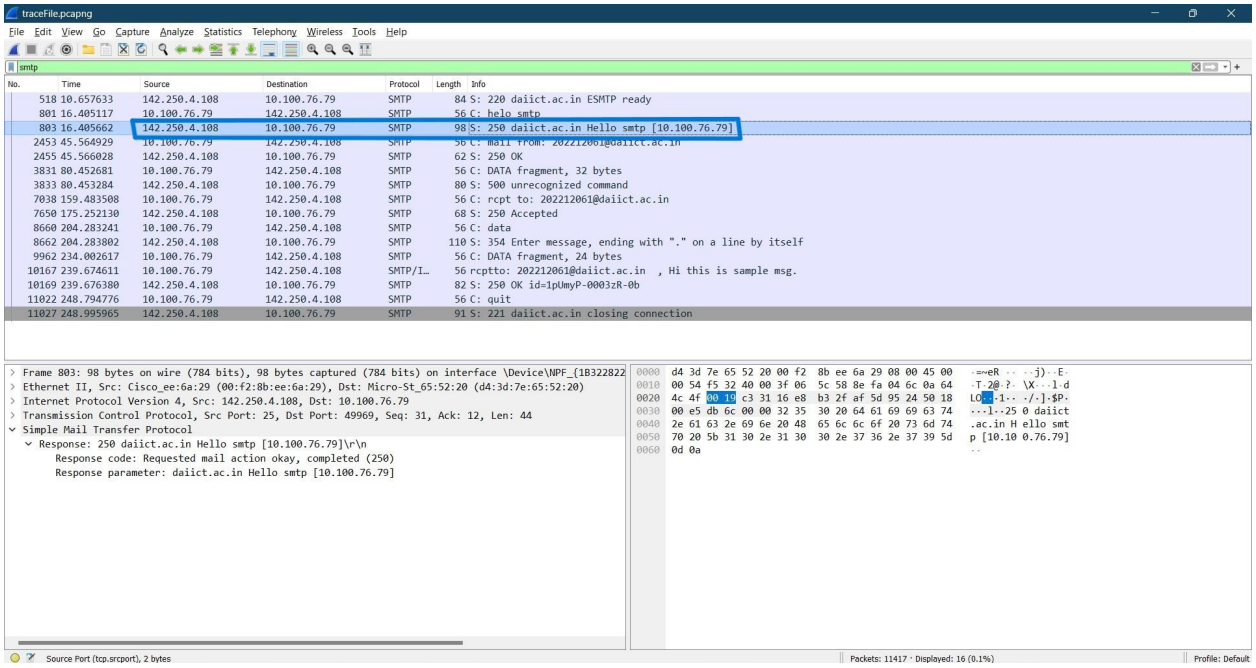
1. How do you identify that the SMTP server is ready?

Answer : We can see it is ESMTP ready.



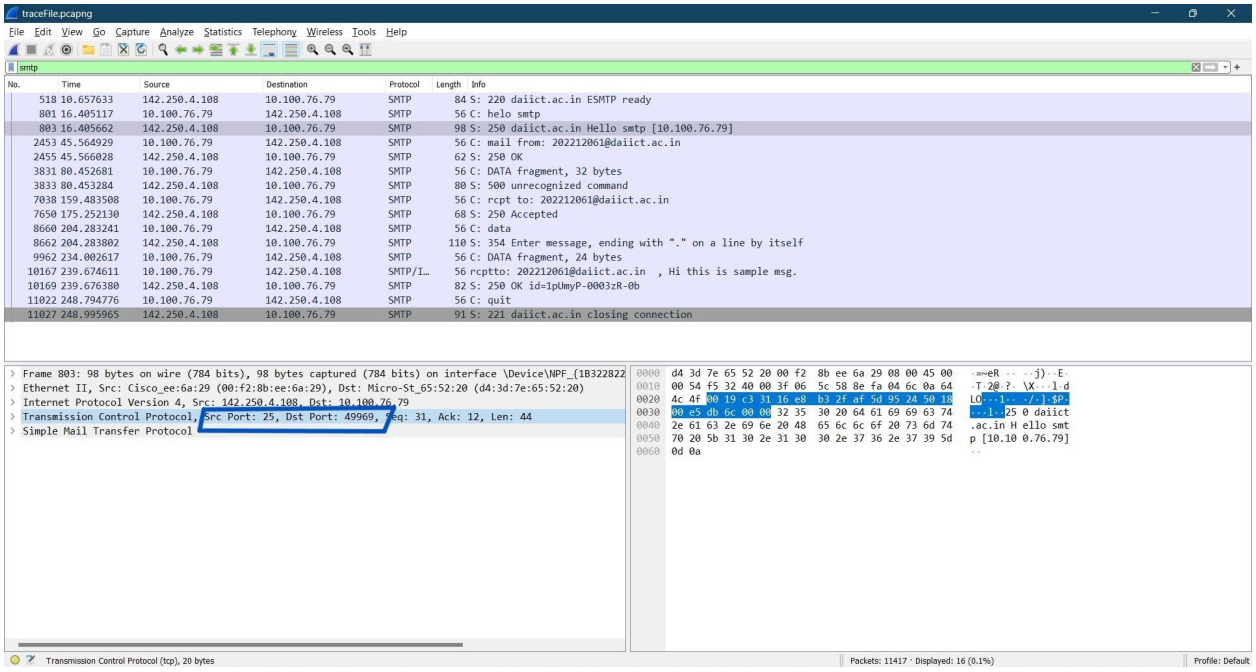
2. Identify the connection establishment packet.

Answer : Shown in screenshot.



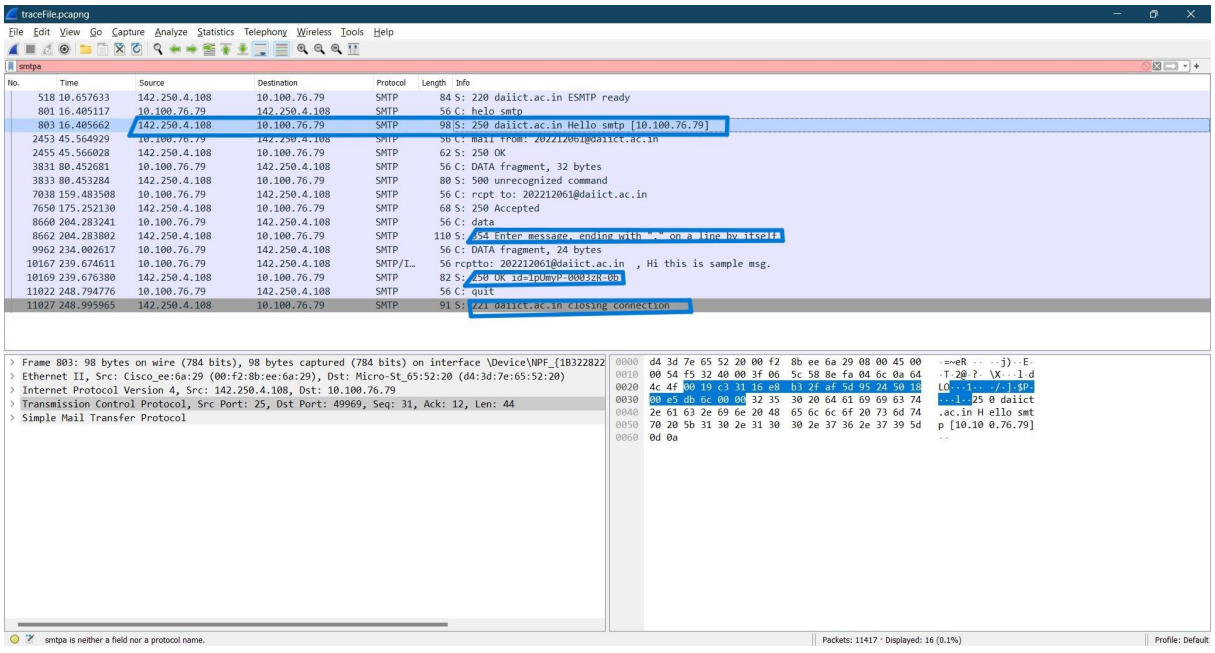
3. What is the ip address and port number of the SMTP server? Identify in a packet.

Answer : IP address is 10.100.76.79 and Port Number is 25.



4. Write down responses for, 1) connection establishment, 2) Request completing response 3) Sending a message 4) Closing connection

Answer : Shown in screenshot.



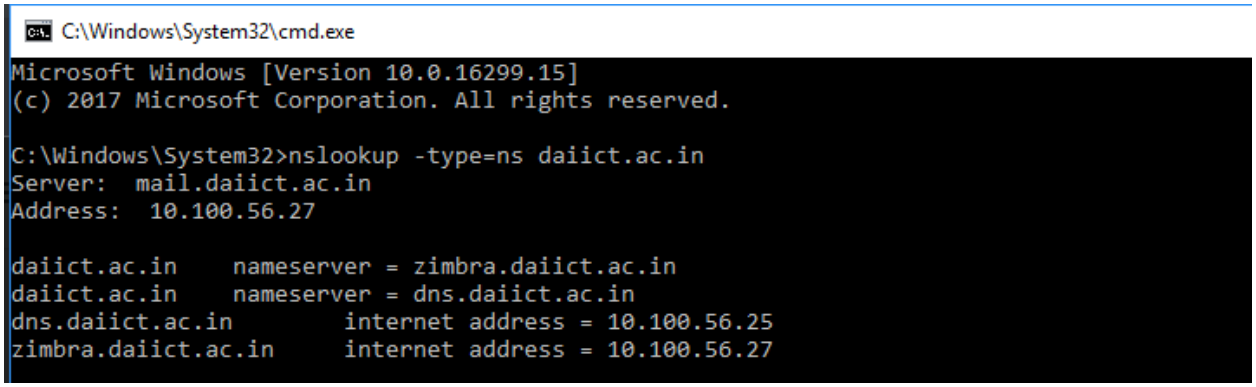
2.3 Exercise

2.3.1 Exercise 1

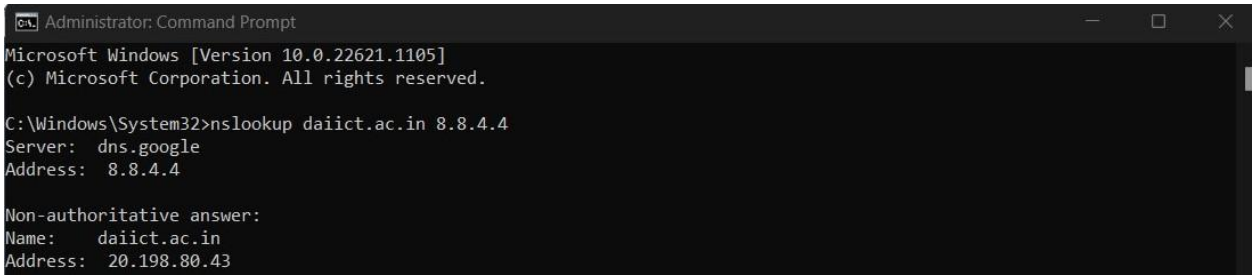
1. Run nslookup to obtain the IP address of daiict.ac.in server.

```
C:\Windows\System32>nslookup daiict.ac.in
Server:  csp3.zte.com.cn
Address:  fe80::1

Non-authoritative answer:
Name:    daiict.ac.in
Address:  20.198.80.43


C:\Windows\System32>
```

2. Run nslookup to determine the authoritative DNS servers for daiict.ac.in server.



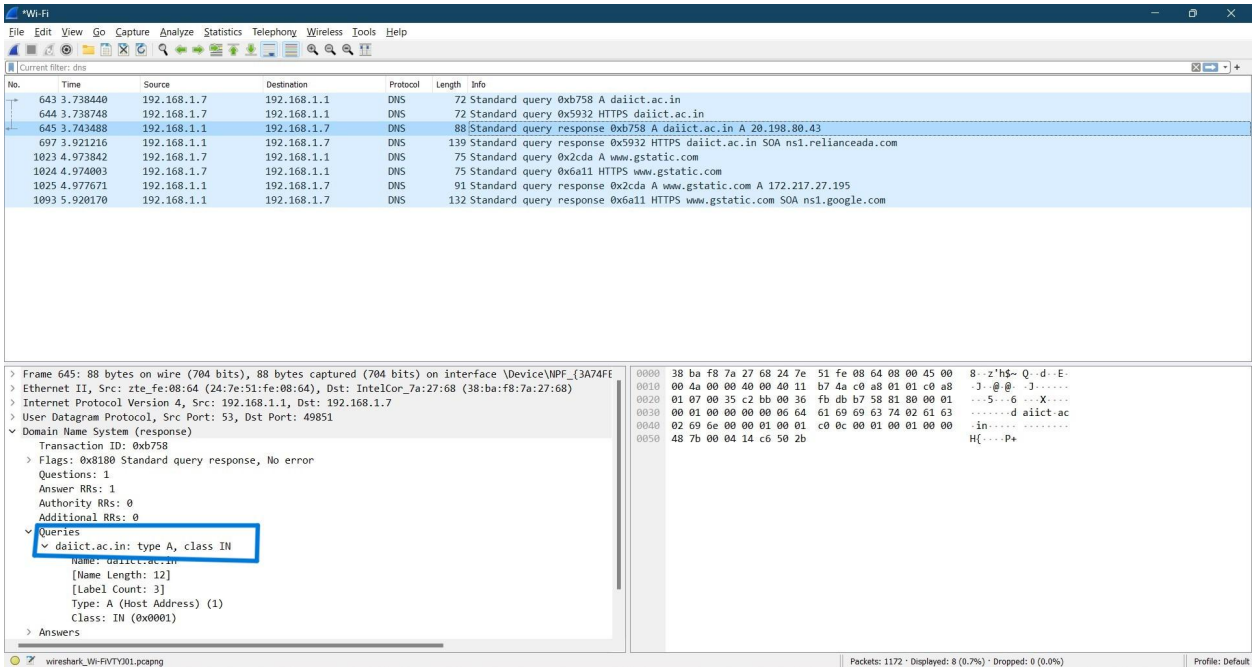
3. Run nslookup so that 8.8.4.4 is queried for the mail servers for google.com



2.3.2
Exercise 2: DNS query from browser

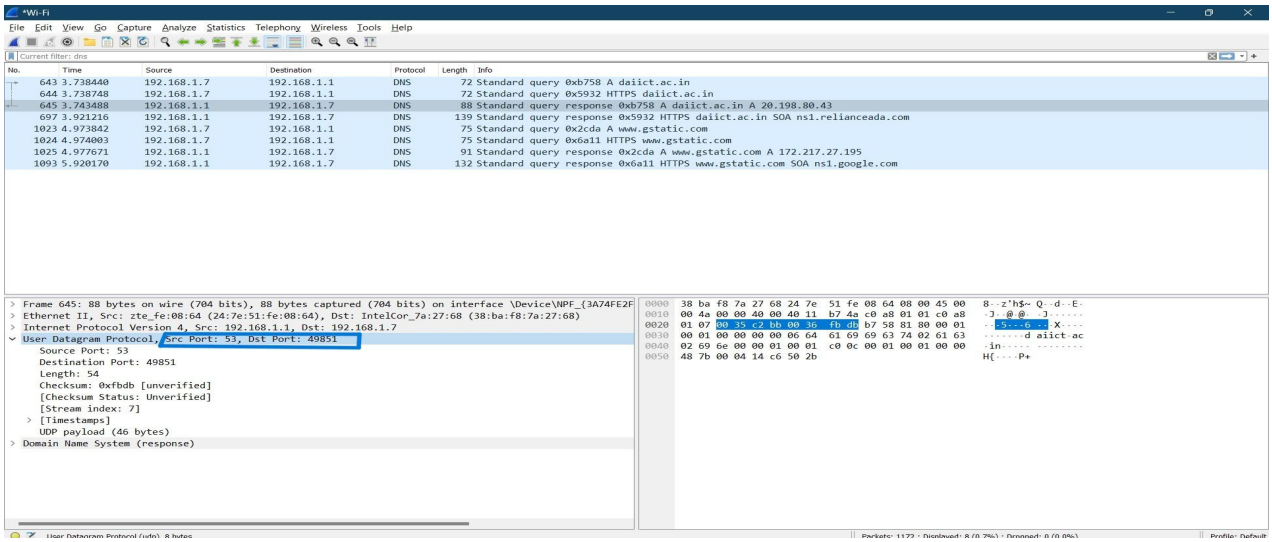
1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer : They are sent over UDP.



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

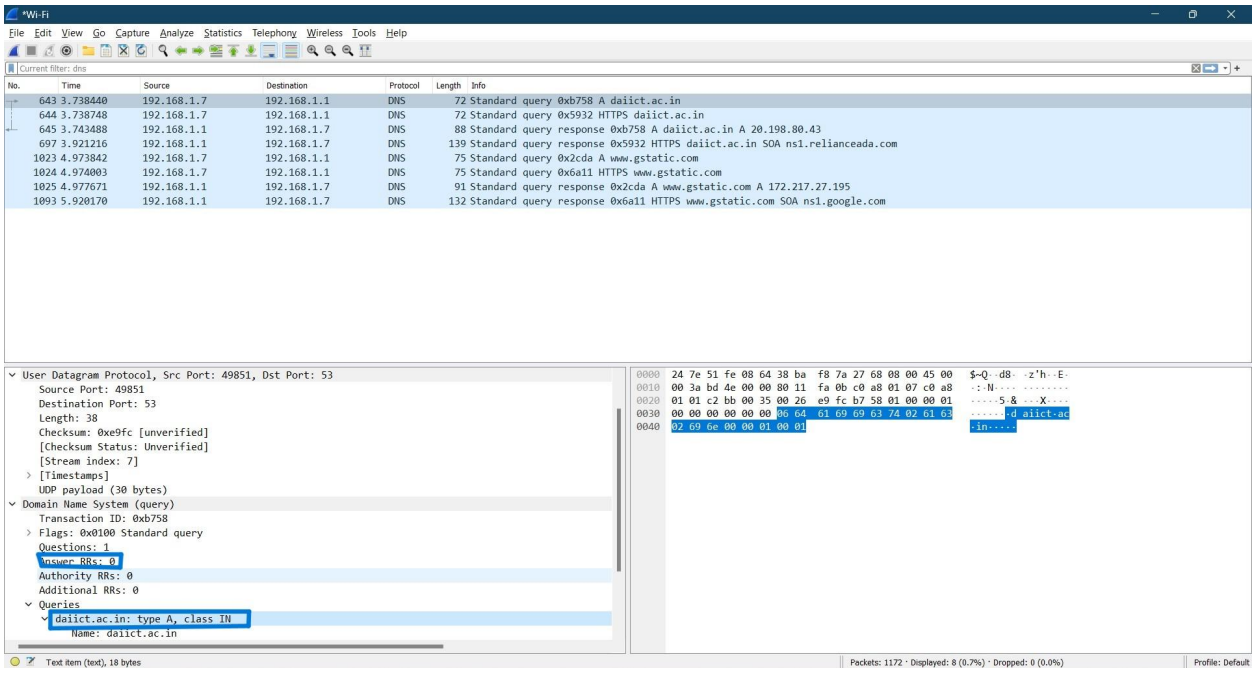
Answer : Source Port is 53 & Destination Port is 49851



3. 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 : It is sent to 192.168.1.1 & yes these two IP addresses are the same.

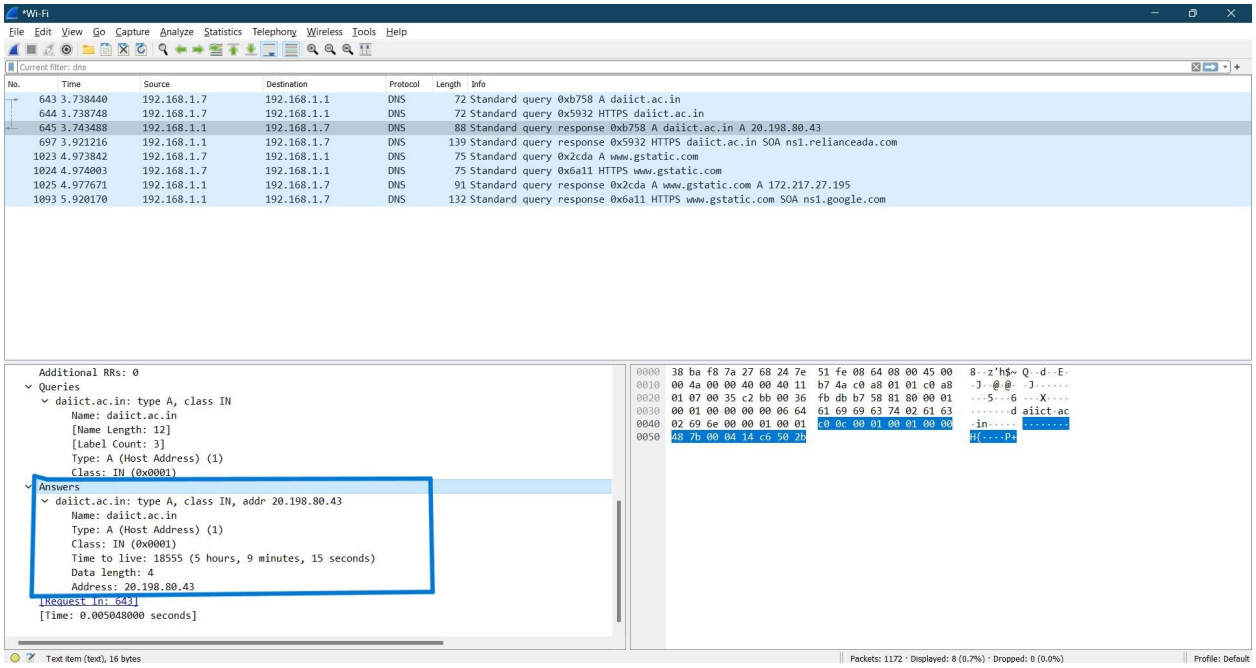
```
IPv4 Address. . . . . . . . . . . : 192.168.1.7(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : 25 February 2023 10.03.00 PM
Lease Expires . . . . . . . . . . : 26 February 2023 10.03.00 PM
Default Gateway . . . . . . . . . : fe80::1%9
                                    192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . . . . . . . : 104381176
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-1F-53-45-E8-6A-64-15-9F-1F
DNS Servers . . . . . . . . . . . : fe80::1%9
                                    192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
Answer : The query is type 'A' and it does not contain any answer.



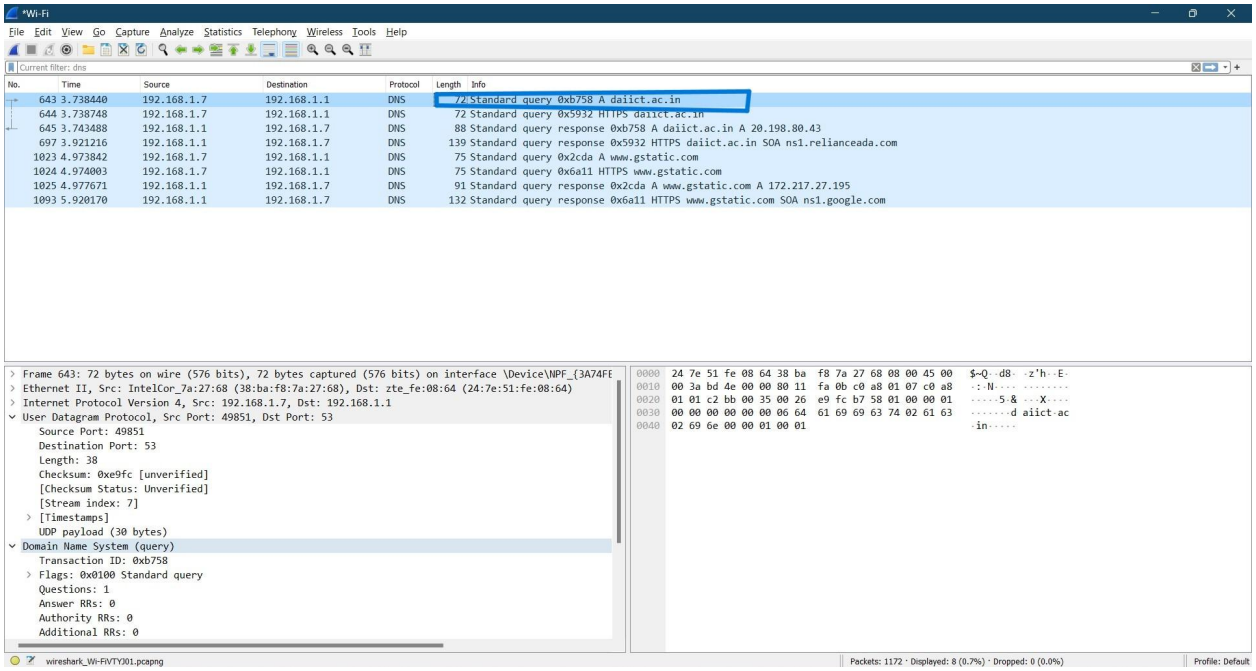
5. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Answer : There is 1 answer which contains its name, type, class, time to live (TTL), the data length and IP address.



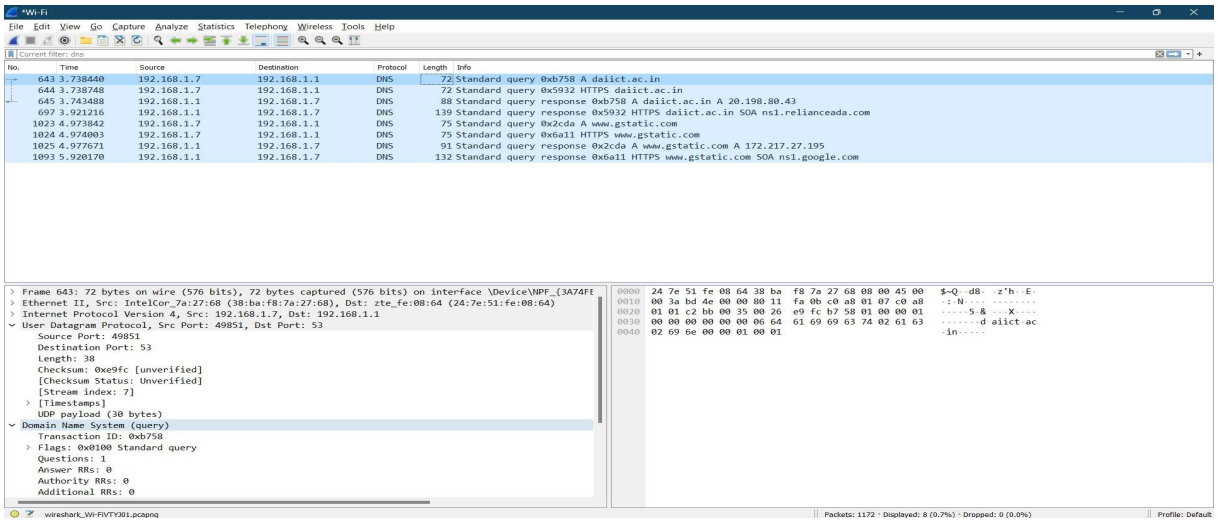
6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer : The SYN packet was sent to 192.168.1.1 which corresponds to the first IP address provided in the DNS response message.



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

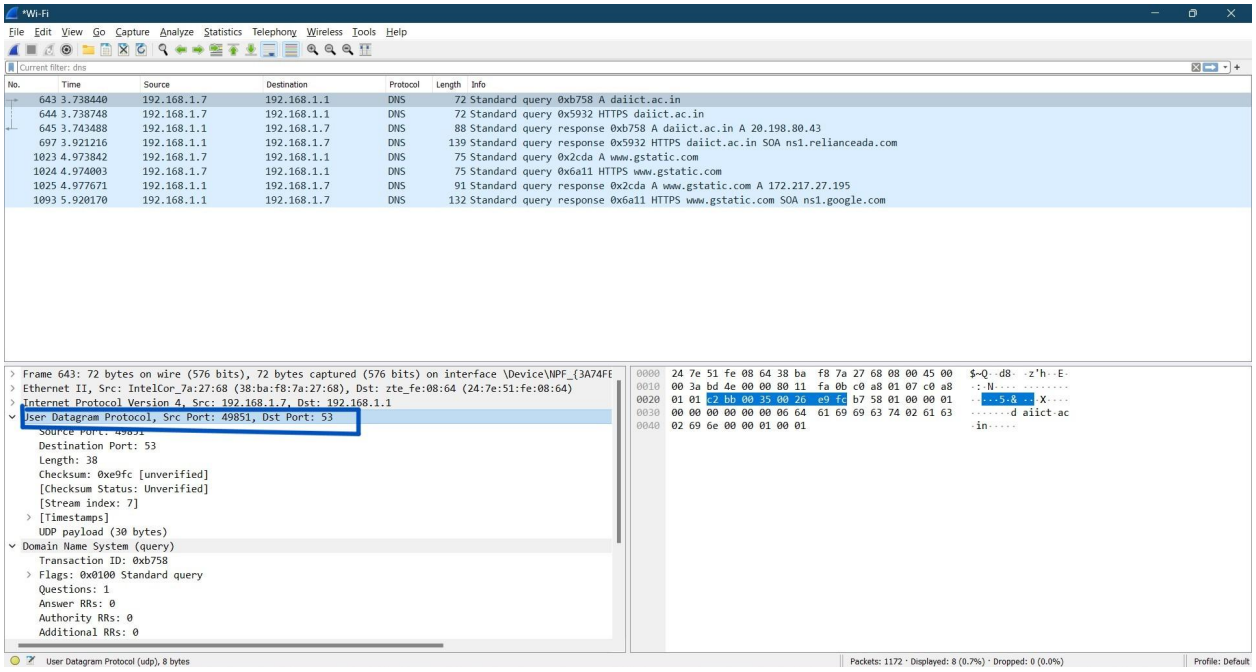
Answer : No



2.3.3
Exercise 3: DNS query using nslookup

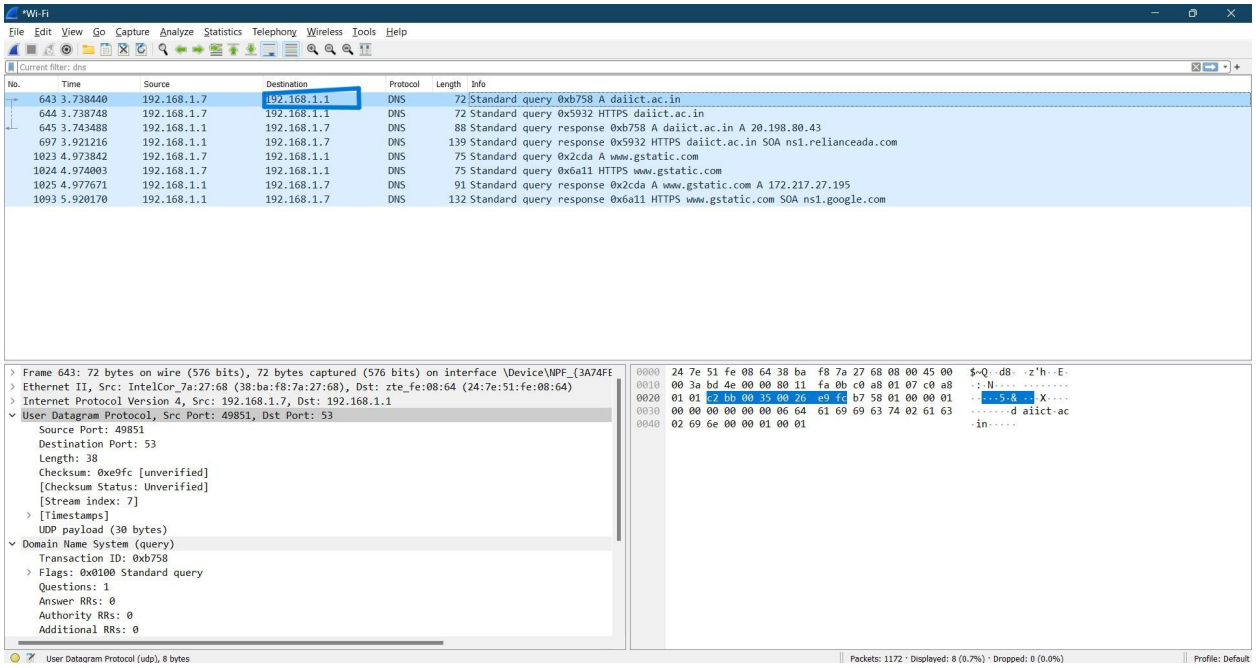
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

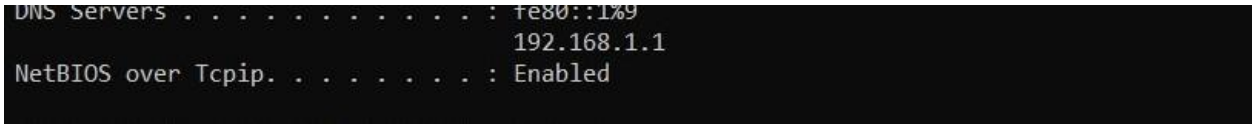
Answer : The destination port for DNS query message is 53 and the source port of DNS response message is 49851.



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

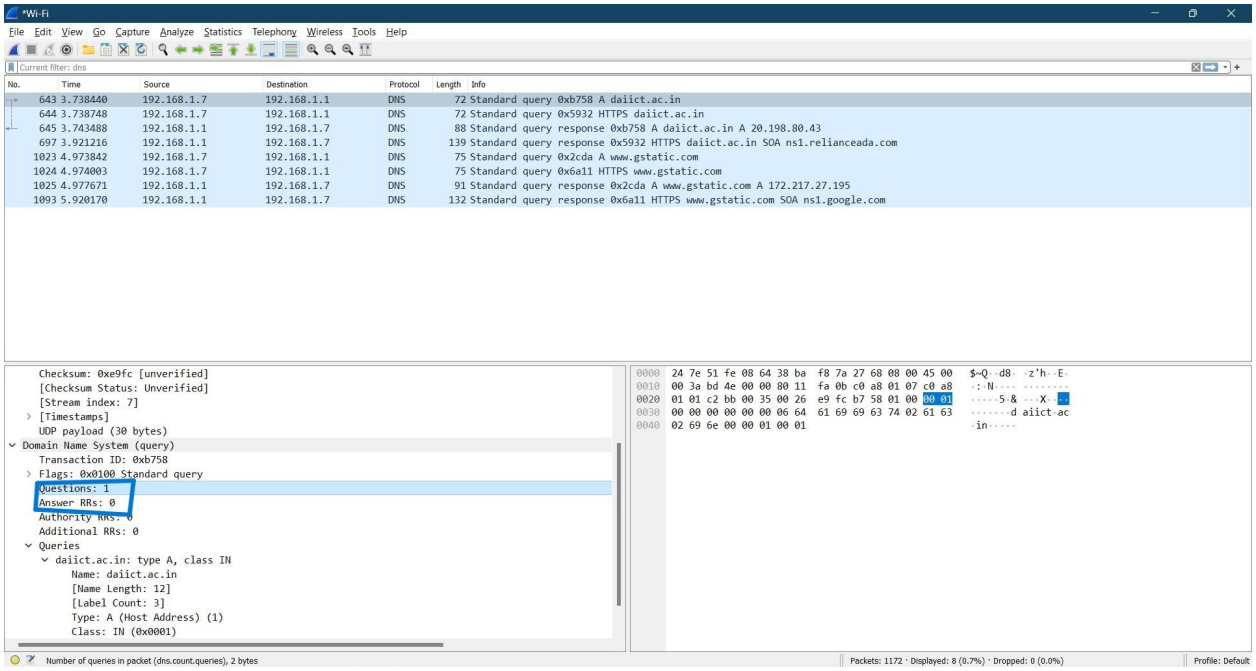
Answer : It is sent to 192.168.1.1, which is the default local DNS server. Can be seen in the screenshot below.





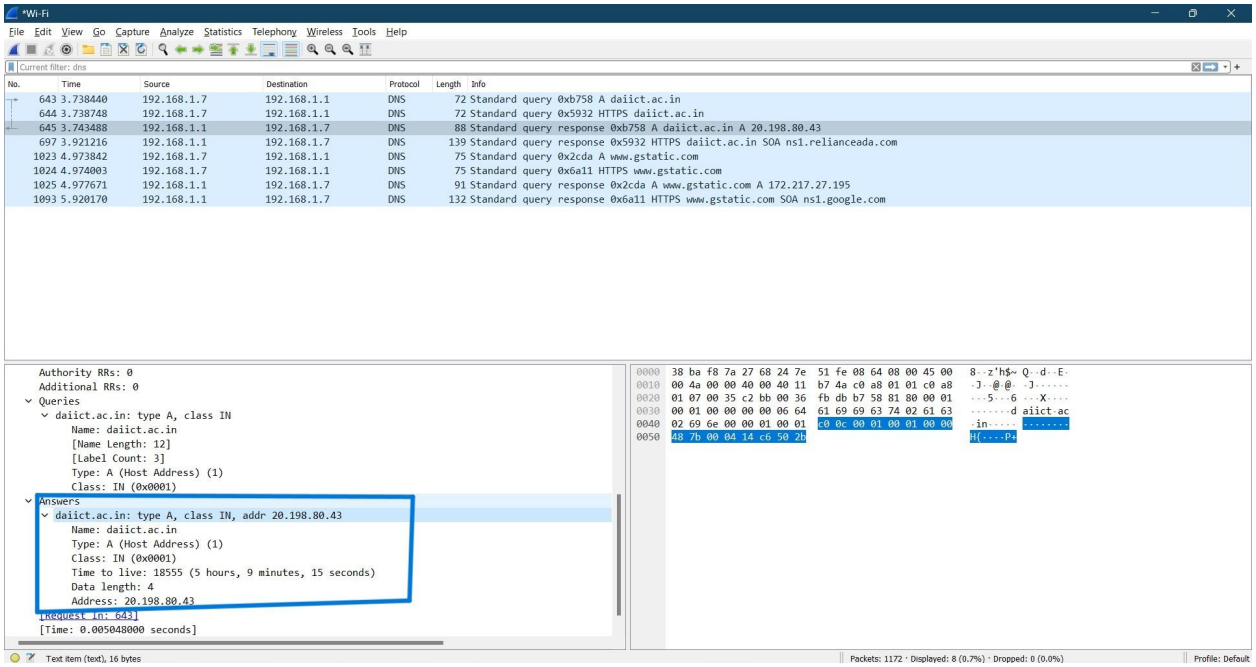
3. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer : The query type is “A” and it doesn't contain any answer.



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

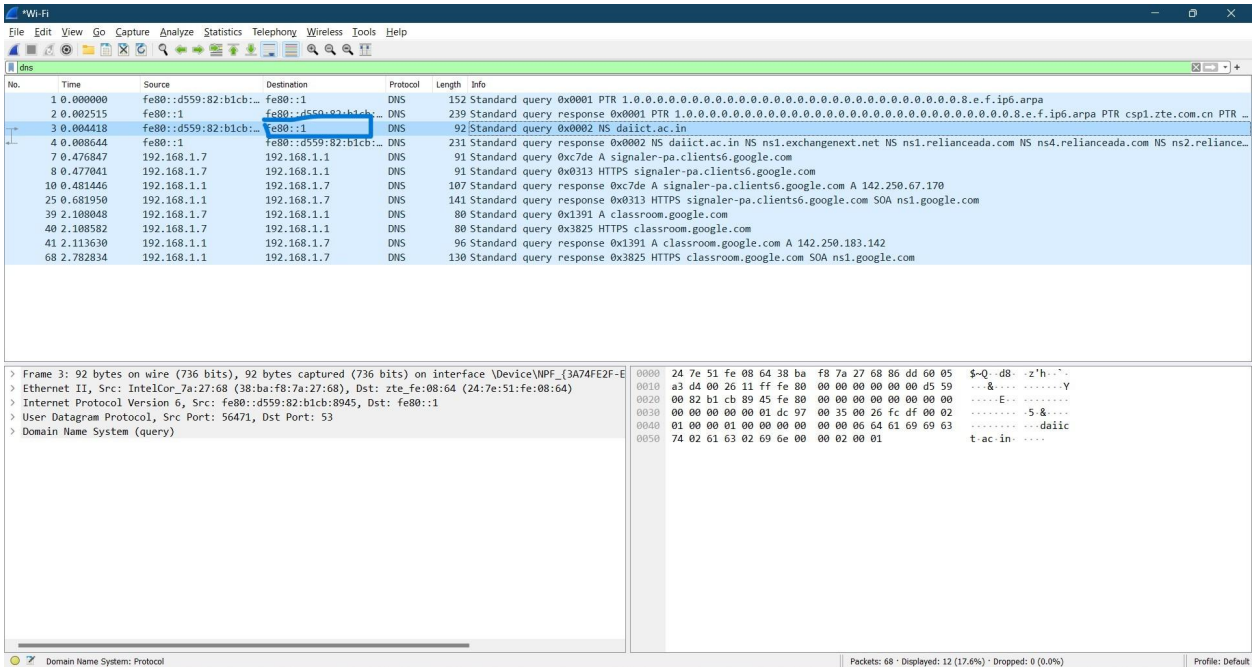
Answer : There is 1 answer which contains its name, type, class, time to live (TTL), the data length and IP address.



2.3.4
Exercise 4: Finding name servers

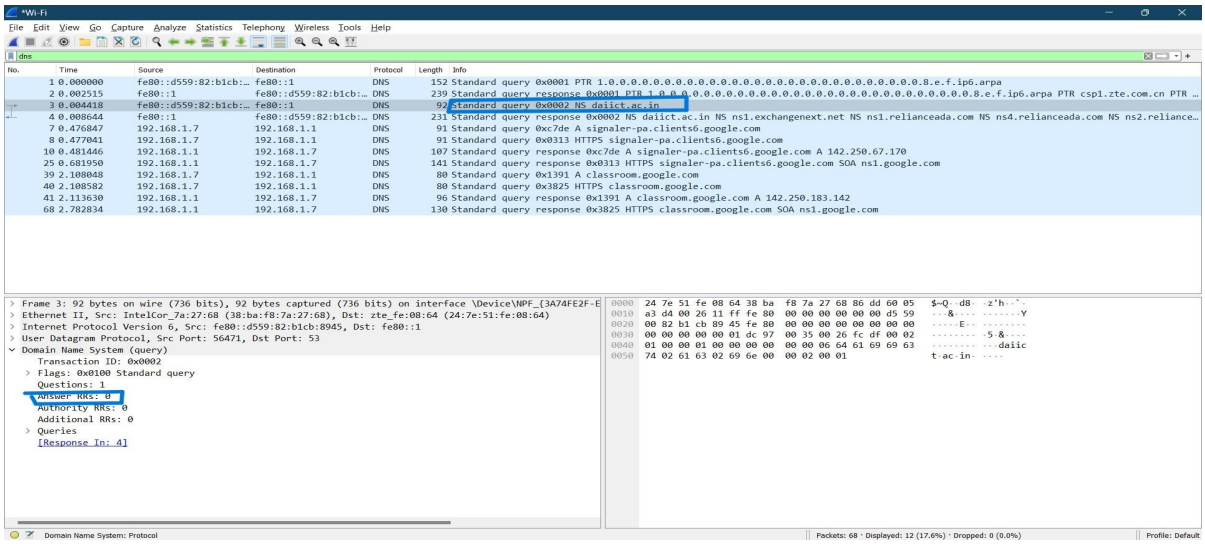
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer : It was sent to fe80::1 which is the default DNS server.



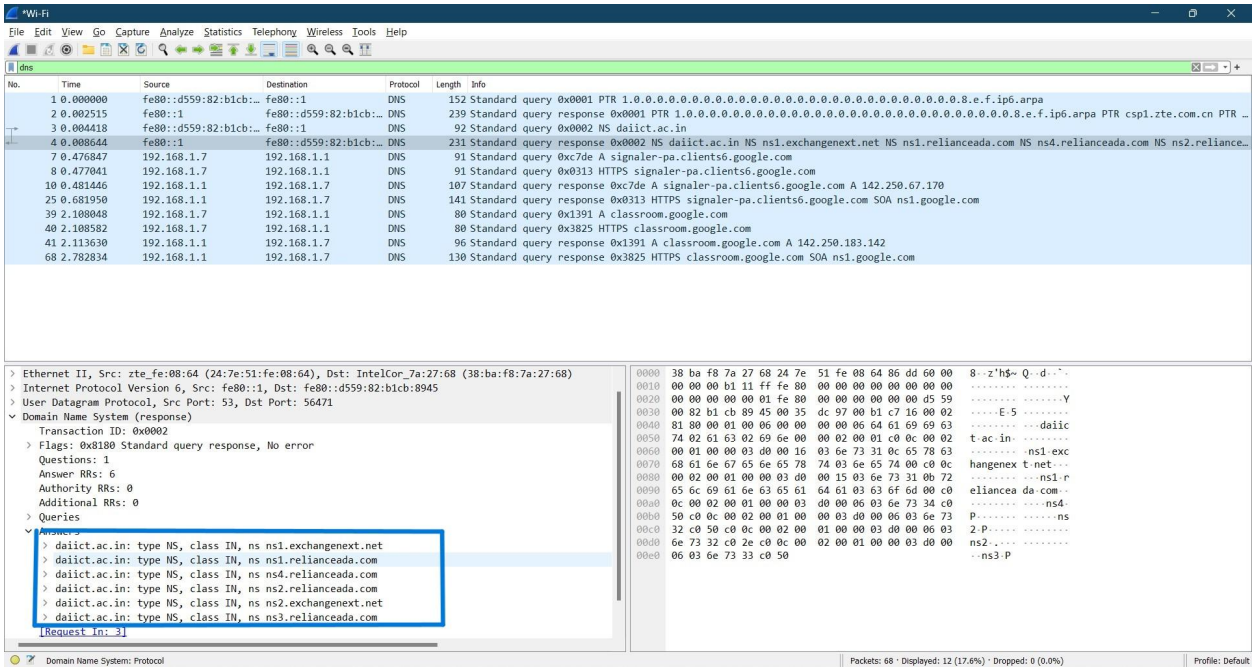
2. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer : The type is “NS” and it does not contain any answer.



3. Examine the DNS response message. What daiict name servers does the response message provide?

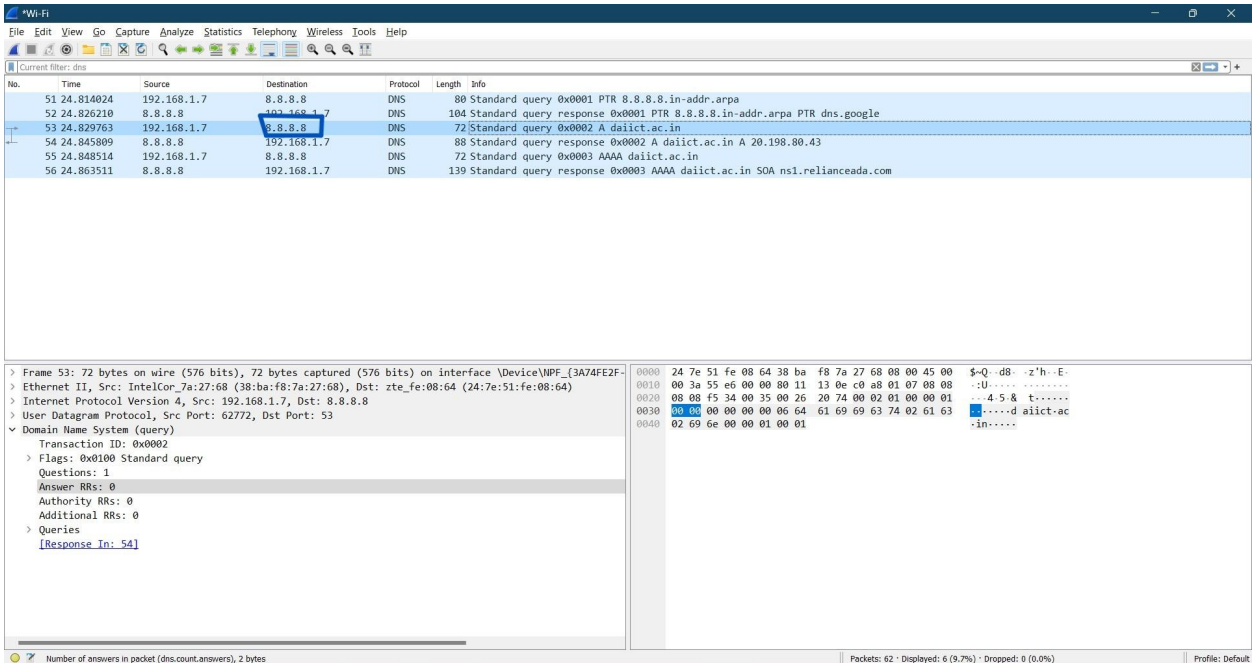
Answer : Names are exchangenet, relianceada.



2.3.5 Exercise 5: DNS query to specific DNS server

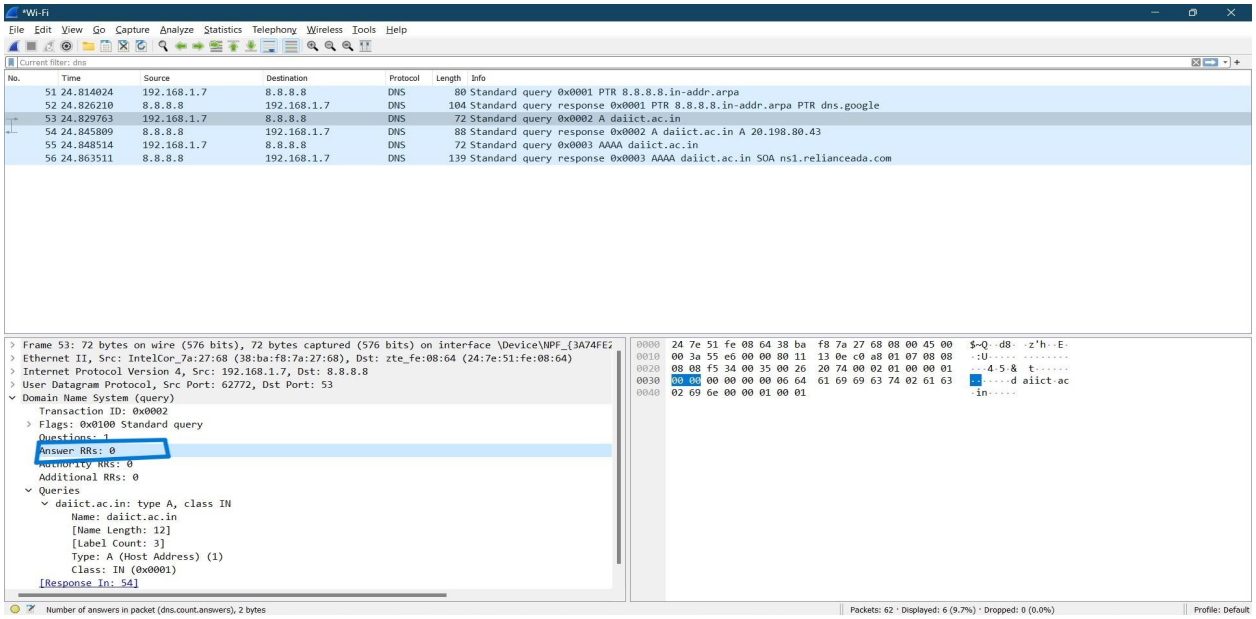
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Answer : The query is sent to 8.8.8.8



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

Answer : It's of the standard type 'A' query which does not contain any answers.



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

Answer : There is 1 answer which contains its name, type, class, time to live (TTL), the data length and IP address.