Computer Networks Lab (CS302)

Report Submission: CN Assignment Lab-3

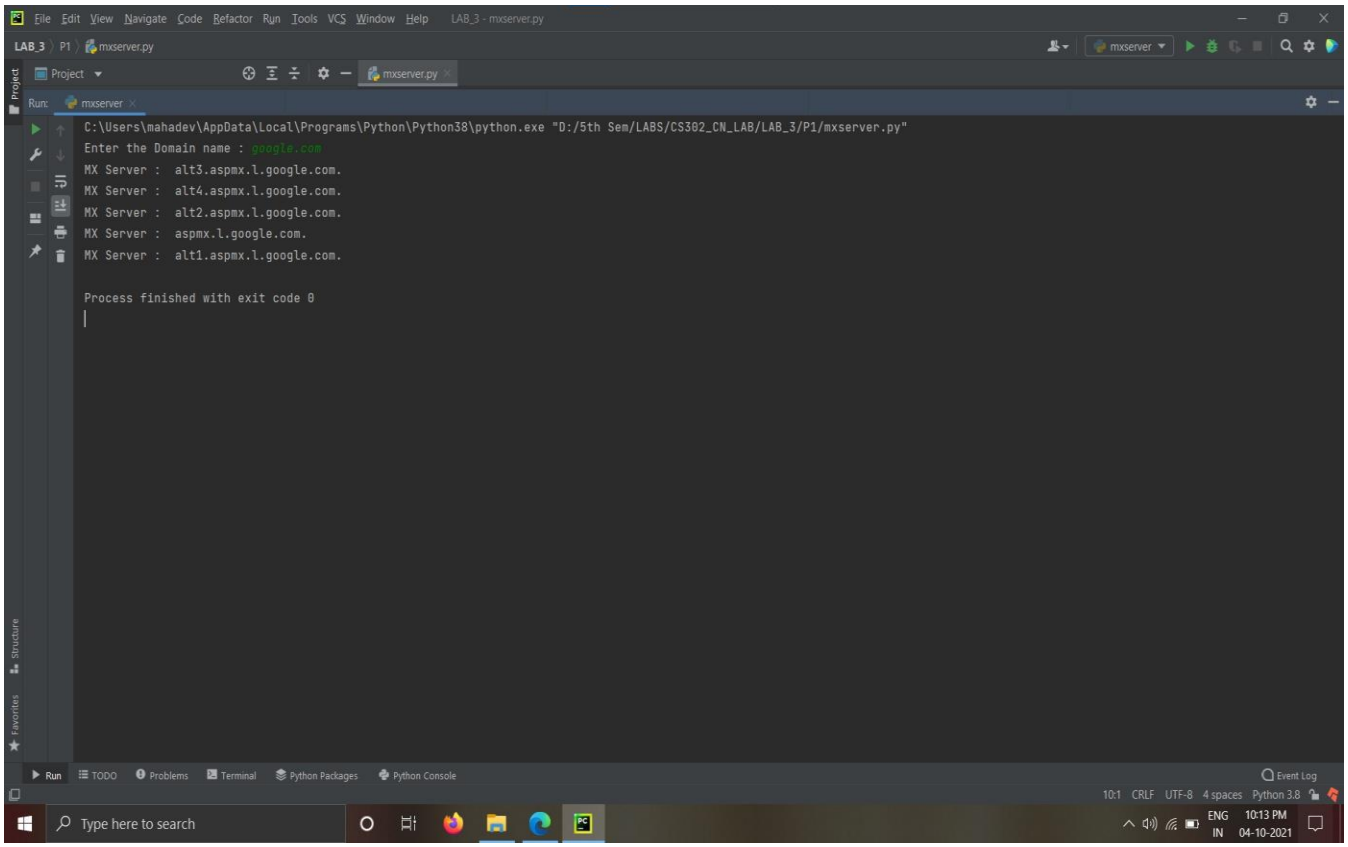
Group Member Details:

1. Mahadev M Hatti 191CS133
2. Darshan A V 191CS219

1.Develop a program to print the Mail exchange servers of a particular domain with their preferences.

Code:

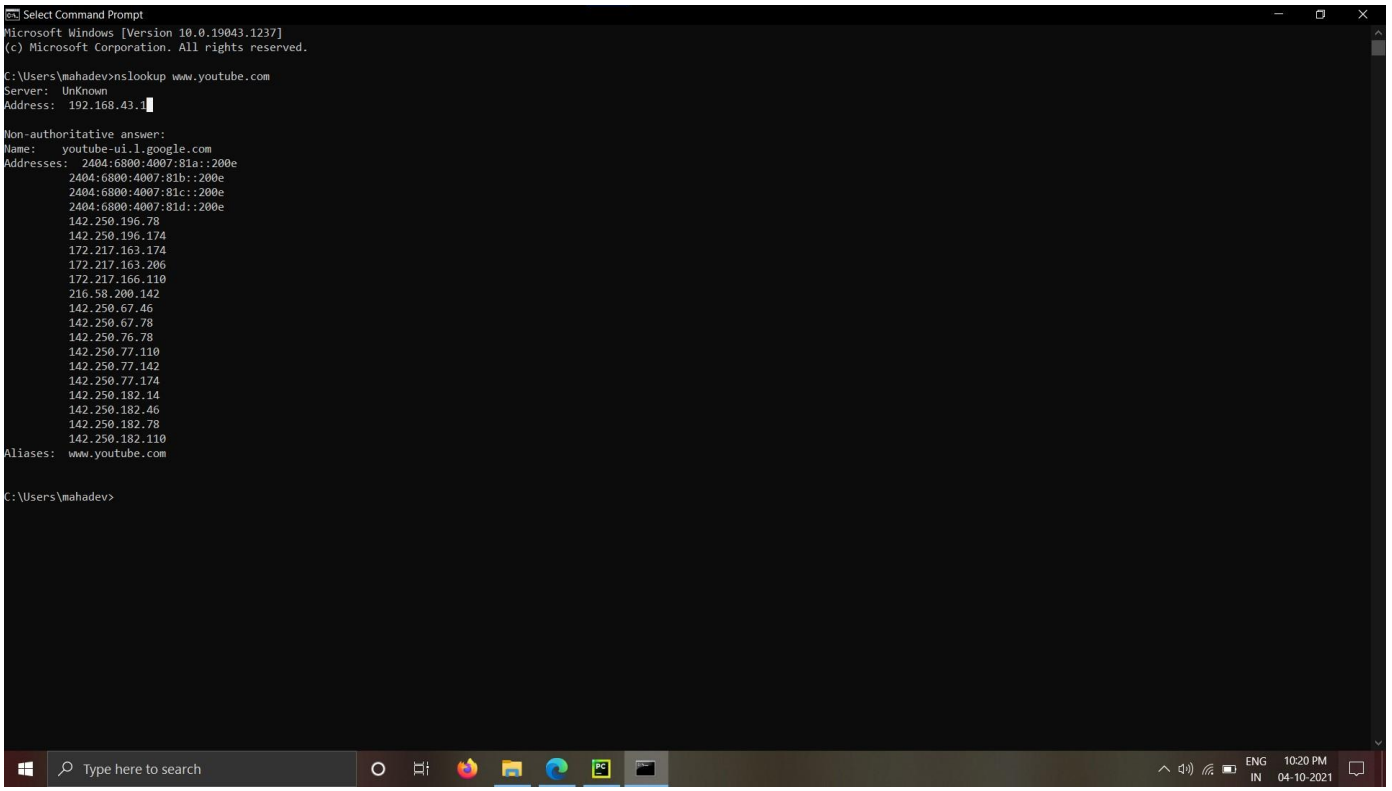
```
 import dns.resolver
from distlib.compat import raw_input

domain = raw_input('Enter the Domain name : ')

# example domain = 'nitk.edu.in'

for x in dns.resolver.resolve(domain, 'MX'):
    print('MX Server : ', (x.to_text()).split(' ', 1)[1])


# A MX record also called mail exchanger record is a resource record in the Domain
Name System that specifies a mail
# server responsible for accepting email messages on behalf of a recipient's domain.
```



2. Use nslookup and ipconfig commands for finding various network related information.

nslookup:

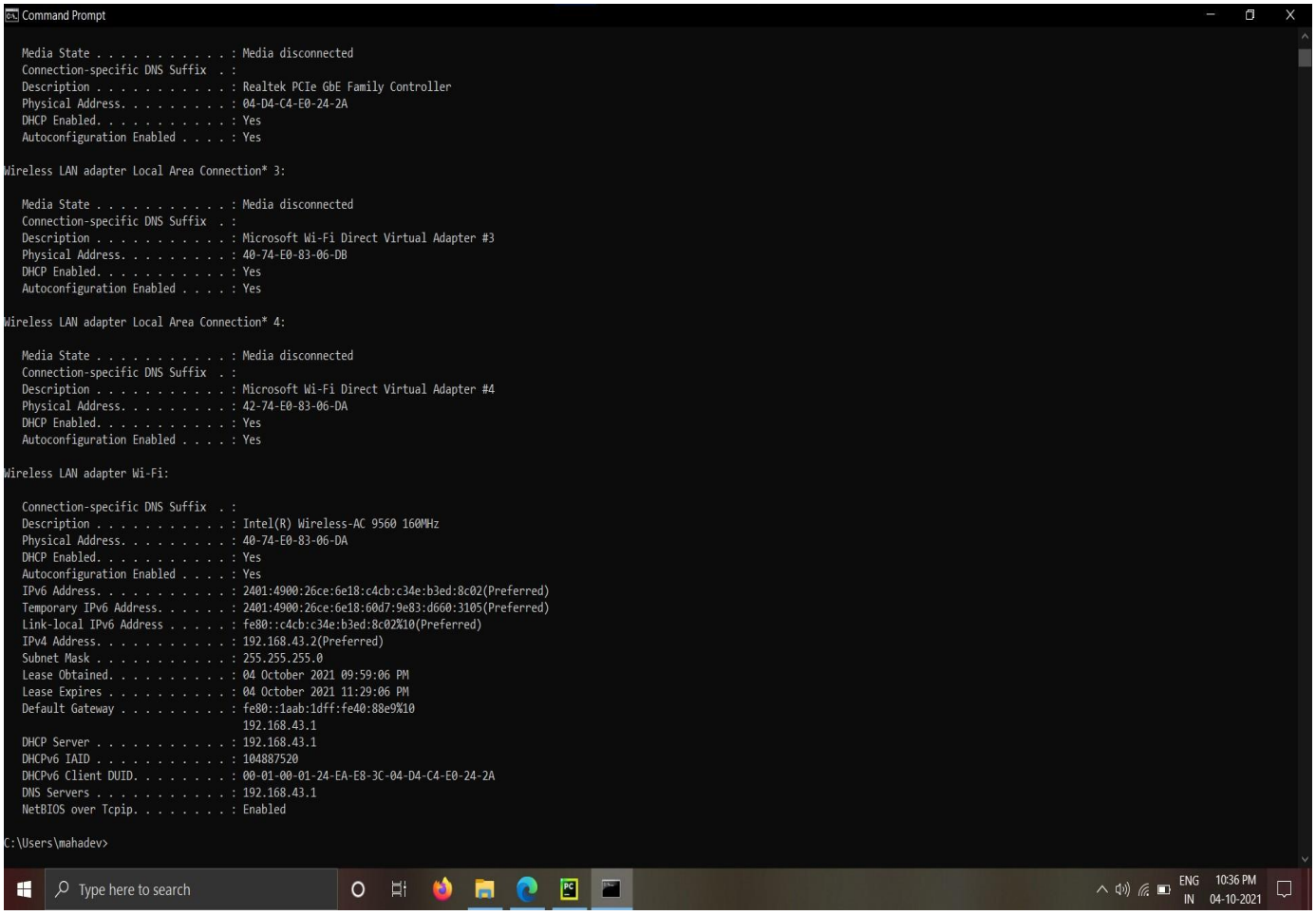
- The nslookup command will fetch the DNS records for a given domain name or an IP address.
- IP addresses and domain names are stored in DNS servers, so the nslookup command lets you query the DNS records to gather information.
- Use nslookup web_adrress command.



- The first two lines show you which DNS server was used to get these results.
- The answer that we got was the IP addresses of the youtube-ui.l.google.com server.

ipconfig:

- The “ipconfig” displays the current information about your network such as your IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNS servers.
- Use ipconfig /all command.



- Since I am connected to the WIFI, ipconfig shows results for Wireless LAN adapter Wi-Fi.
- I also found the local (ipv4) address of the computer; in my case it is 192.168.43.2.

- I also saw the Default Gateway IP = 192.168.43.1, which is our router.
- I can also observe the subnet mask = 255.255.255.0
- In My case the DHCP IP address is the same as the router address, which means that DHCP server is currently residing on the router.

  DHCP Server . . . . . : 192.168.43.1

  Default Gateway fe80::1aab:1dff:fe40:88e9%10

  192.168.43.1

- DNS server is also the same as router address which means it is also DNS server.

  DNS Servers . . . . . : 192.168.43.1

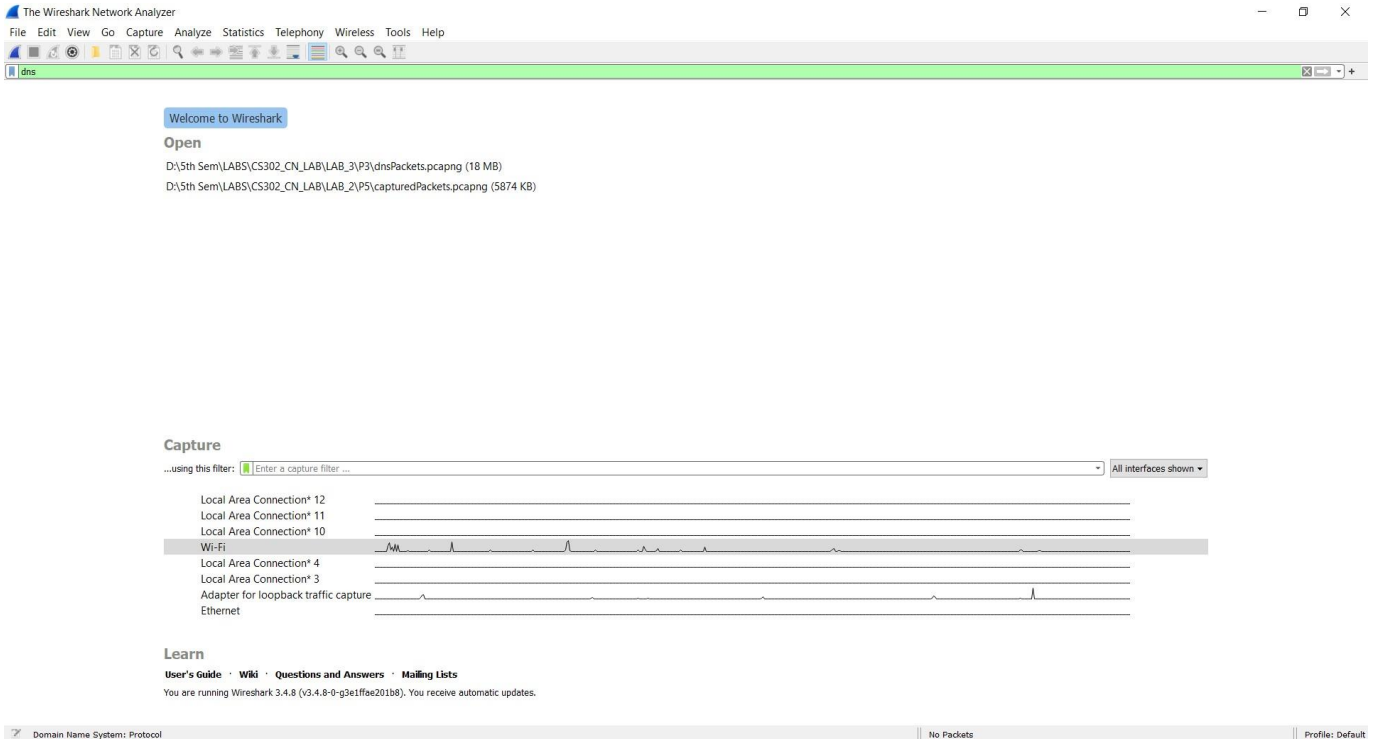
  Default Gateway fe80::1aab:1dff:fe40:88e9%10

  192.168.43.1

3. Capture and Analyse DNS Packets using Wireshark.

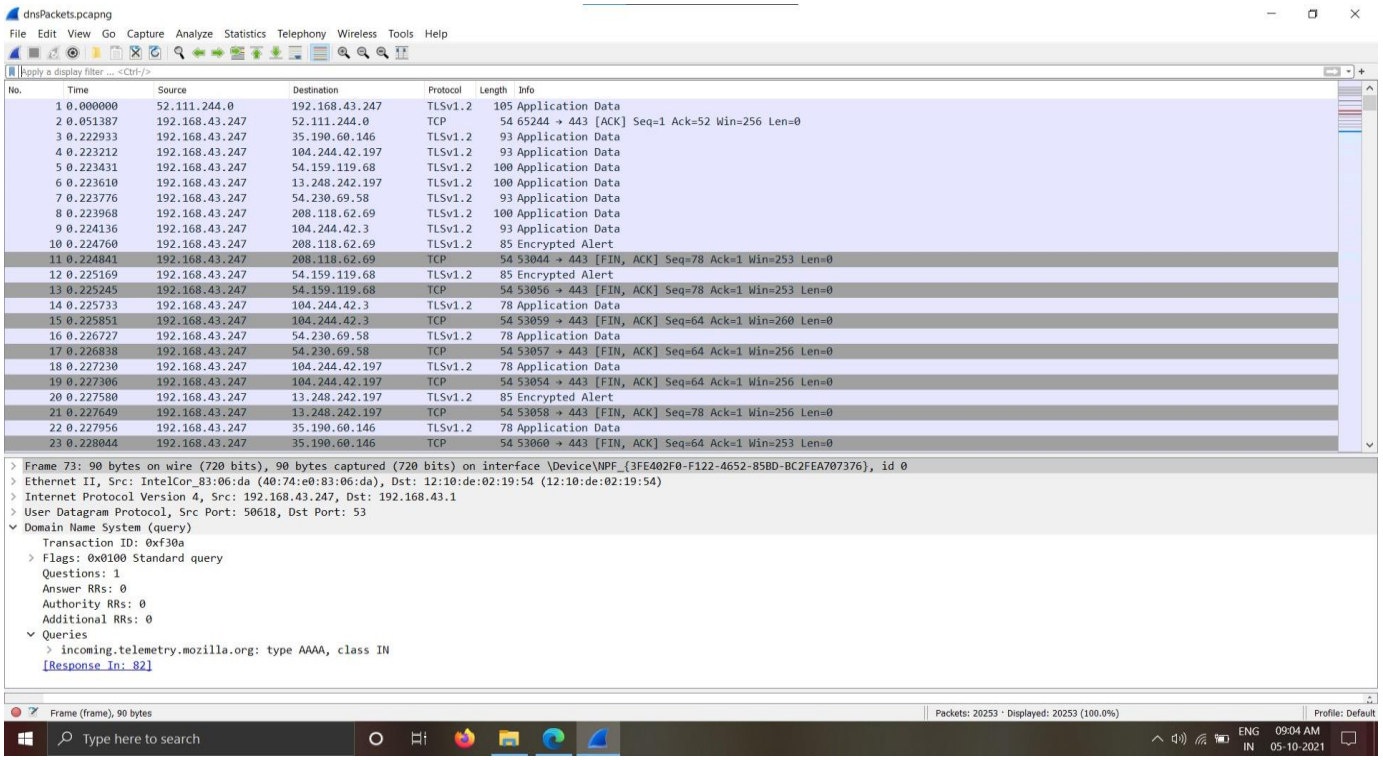
a. Analyse DNS Query and Response Packets.

1. In the below fig. selects the Wi-Fi option from the Interface list options.



- DNS traffic normally goes to or from port 53, and traffic to and from that port is normally DNS traffic.

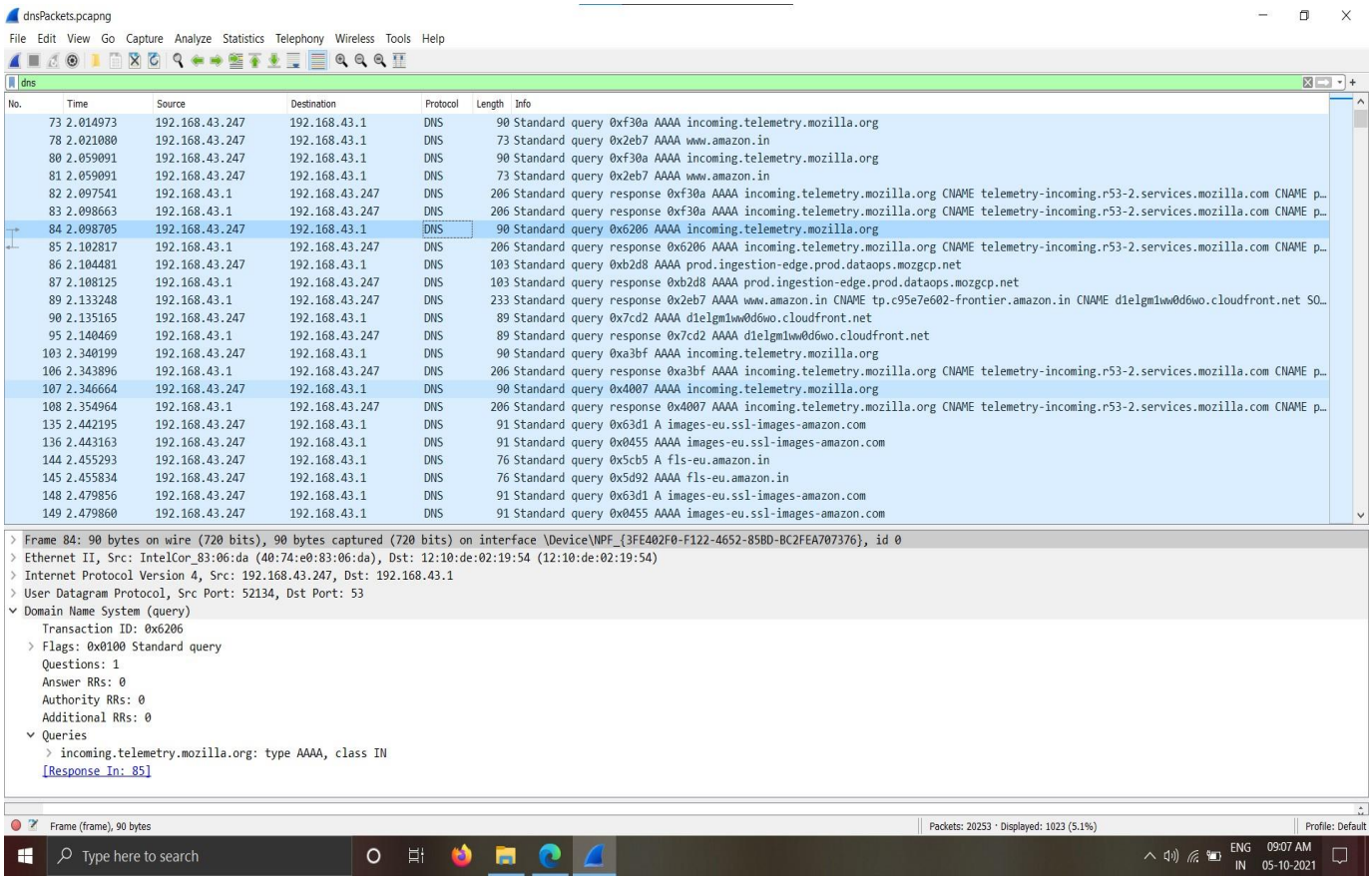
2. In the new window you can see all the current traffic on the network. (Clear cache – Before capturing the traffic, you need to clear your browser's cache.)



3. Use filter section to filter out Specific Packets related to dns Server.

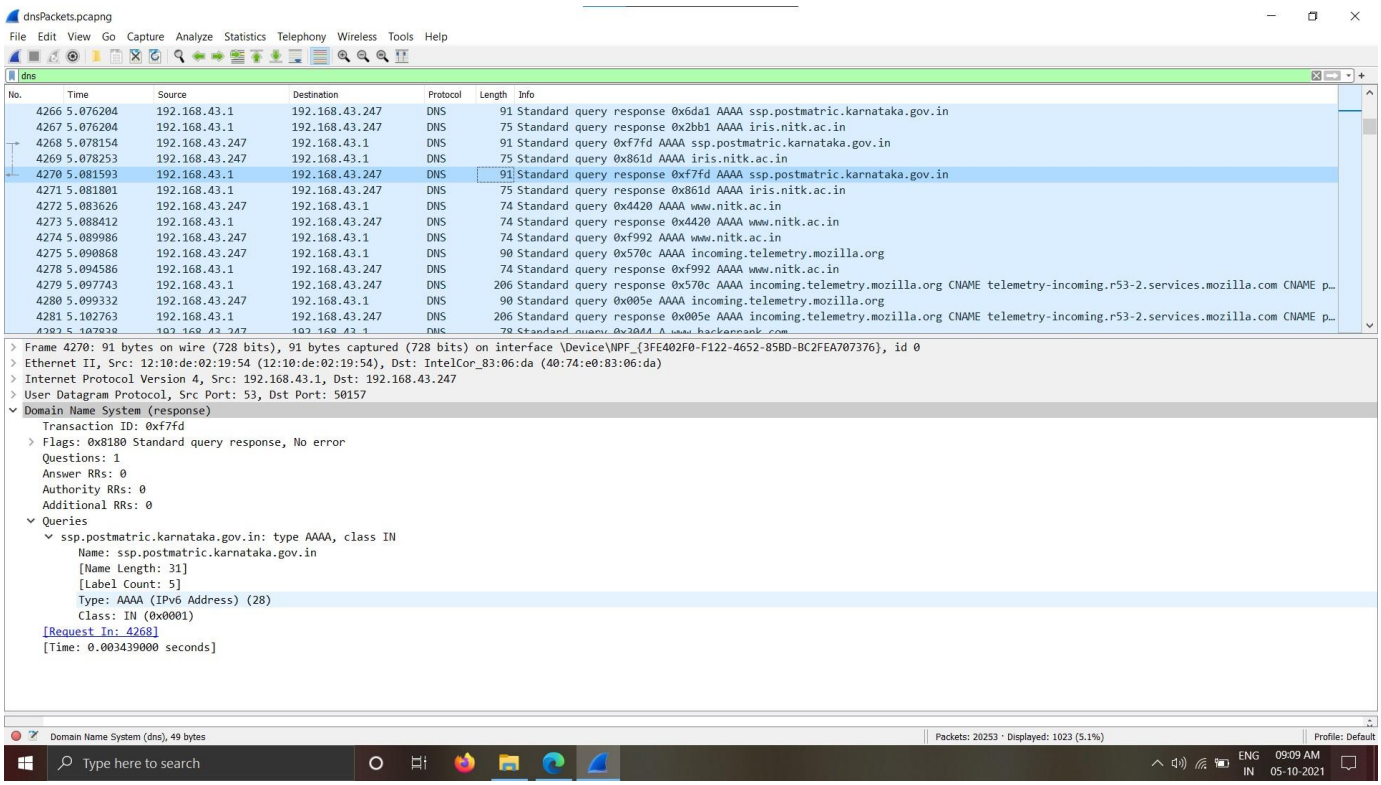
From this Pane you can observe:

- No. – The number of a captured packet.
- Time – This shows you when the packet was captured with regards to when you started capturing.
- Source – This is the origin of a captured packet in the form of an address.
- Destination – The destination address of a captured packet.
- Protocol – The type of a captured packet.
- Length – This shows you the length of a captured packet. This is expressed in bytes.



4. Choose the packet you want to read. Double-click on it.

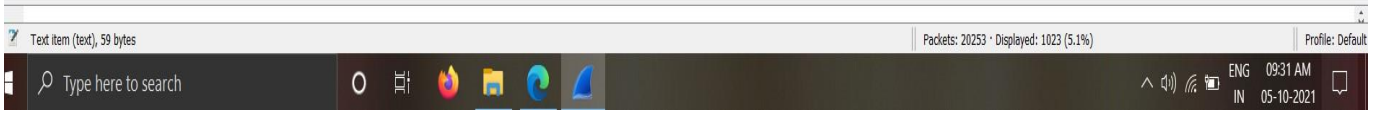
♦ This is a DNS Response Packet



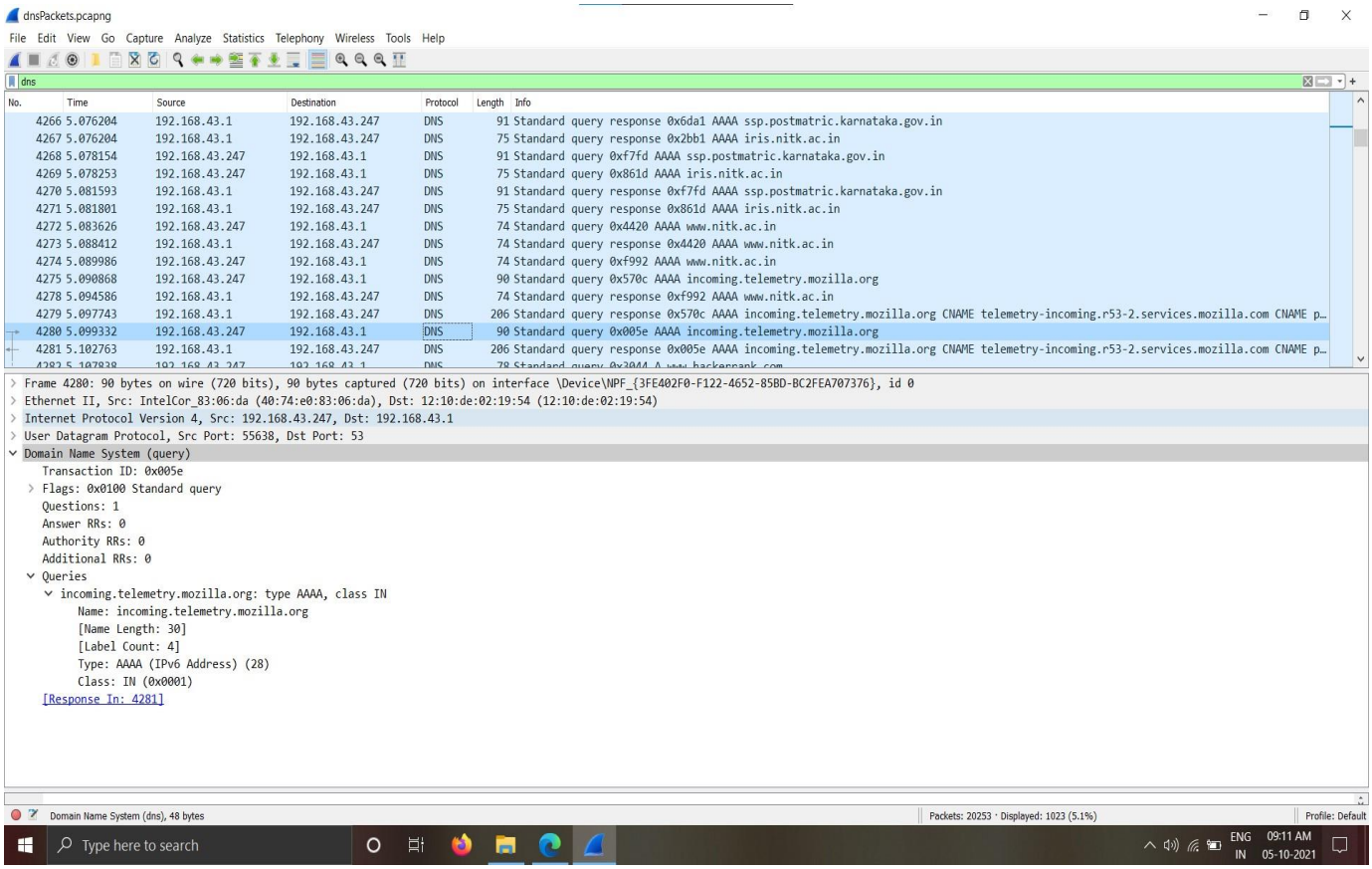
```
> Frame 4281: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: 12:10:de:02:19:54 (12:10:de:02:19:54), Dst: IntelCor_83:06:da (40:74:e0:83:06:da)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.247
> User Datagram Protocol, Src Port: 53, Dst Port: 55638
v Domain Name System (response)
    Transaction ID: 0x005e
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v incoming.telemetry.mozilla.org: type AAAA, class IN
        Name: incoming.telemetry.mozilla.org
        [Name Length: 30]
        [Label Count: 4]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  v Answers
    > incoming.telemetry.mozilla.org: type CNAME, class IN, cname telemetry-incoming.r53-2.services.mozilla.com
    > telemetry-incoming.r53-2.services.mozilla.com: type CNAME, class IN, cname prod.ingestion-edge.prod.dataops.mozgcp.net
    [Request In: 4280]
    [Time: 0.003431000 seconds]
```

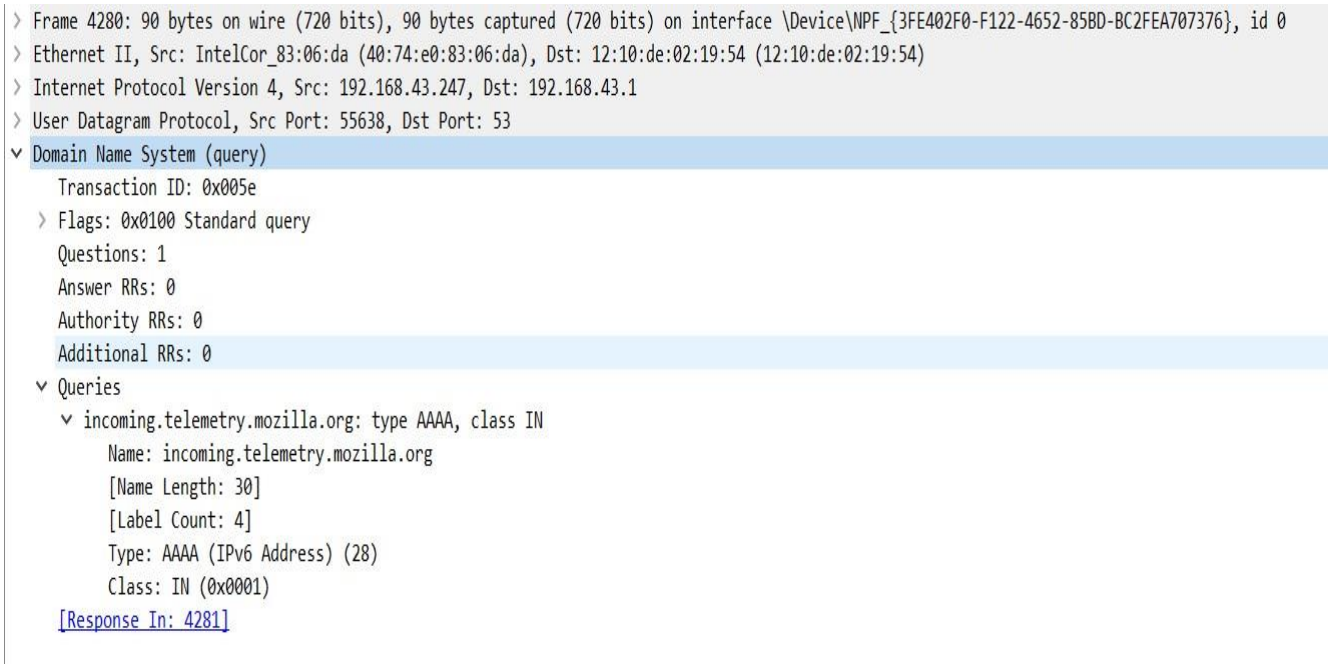
- The request data structure: Response
- The number of questions: 1
- The number of answers : 2 (Since it's a dns Response,answers cannot be zero)
- Data in the queries
    - The questions sent by the client are included in the response as well.

```
v Answers
  v incoming.telemetry.mozilla.org: type CNAME, class IN, cname telemetry-incoming.r53-2.services.mozilla.com
      Name: incoming.telemetry.mozilla.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 15 (15 seconds)
      Data length: 47
      CNAME: telemetry-incoming.r53-2.services.mozilla.com
  v telemetry-incoming.r53-2.services.mozilla.com: type CNAME, class IN, cname prod.ingestion-edge.prod.dataops.mozgcp.net
      Name: telemetry-incoming.r53-2.services.mozilla.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 92 (1 minute, 32 seconds)
      Data length: 45
      CNAME: prod.ingestion-edge.prod.dataops.mozgcp.net
  [Request In: 4280]
  [Time: 0.003431000 seconds]
```



- This is a DNS Query Packet:



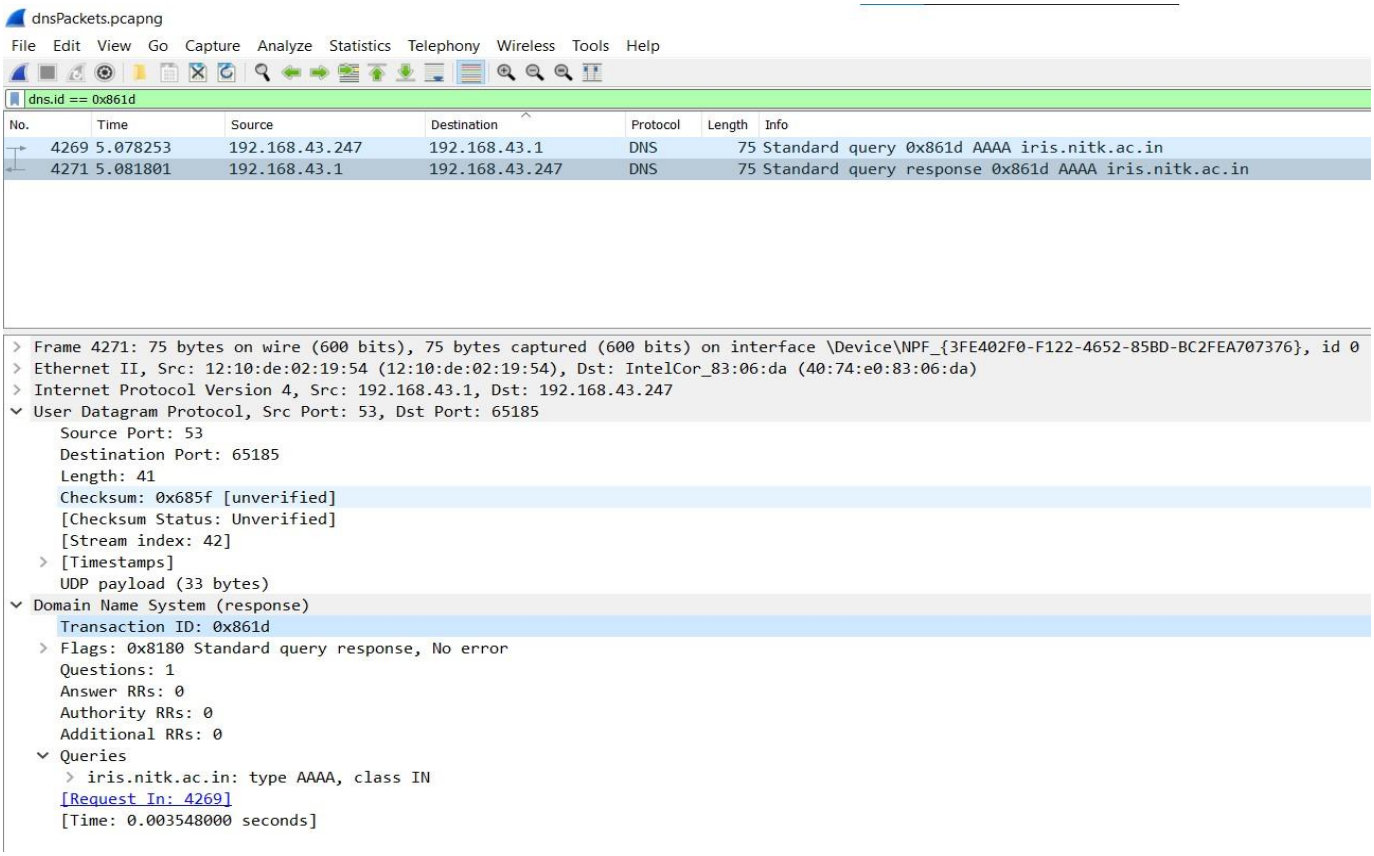


- The request data structure: query

- The number of questions: 1
- The number of answers : 0 (Since it's a dns query)
- Data in the queries
    - In my case, the request is for the AAAA record for incoming.telemetry.mozilla.org

b. By using the captured packets identify the source and destination ports query and response messages.

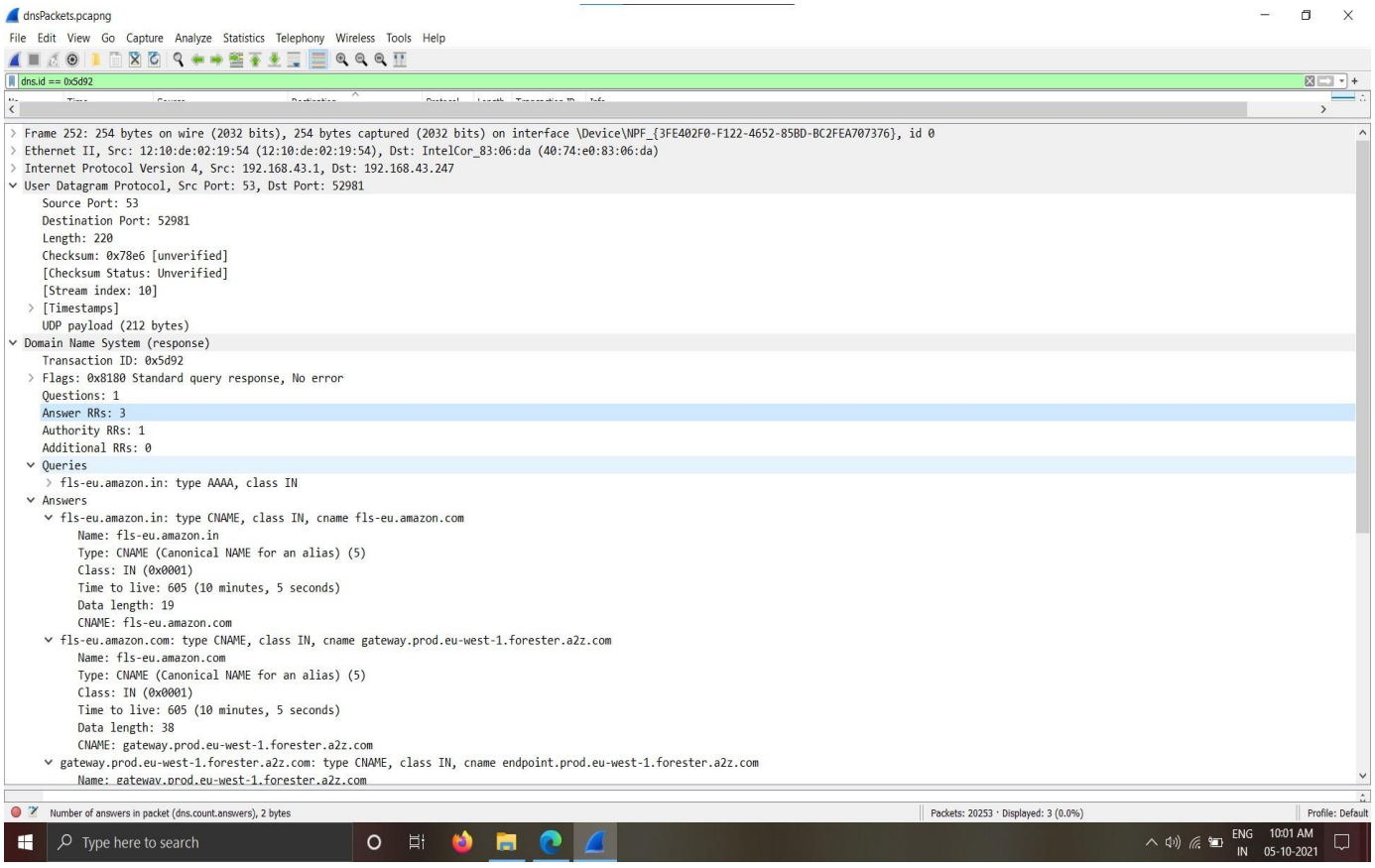
→ Since I wanted to know the source and destination ports query and response messages, I applied a filter on the particular dns query and found its transaction id, and based on that I filtered the queries and I got this (see fig. Below :)

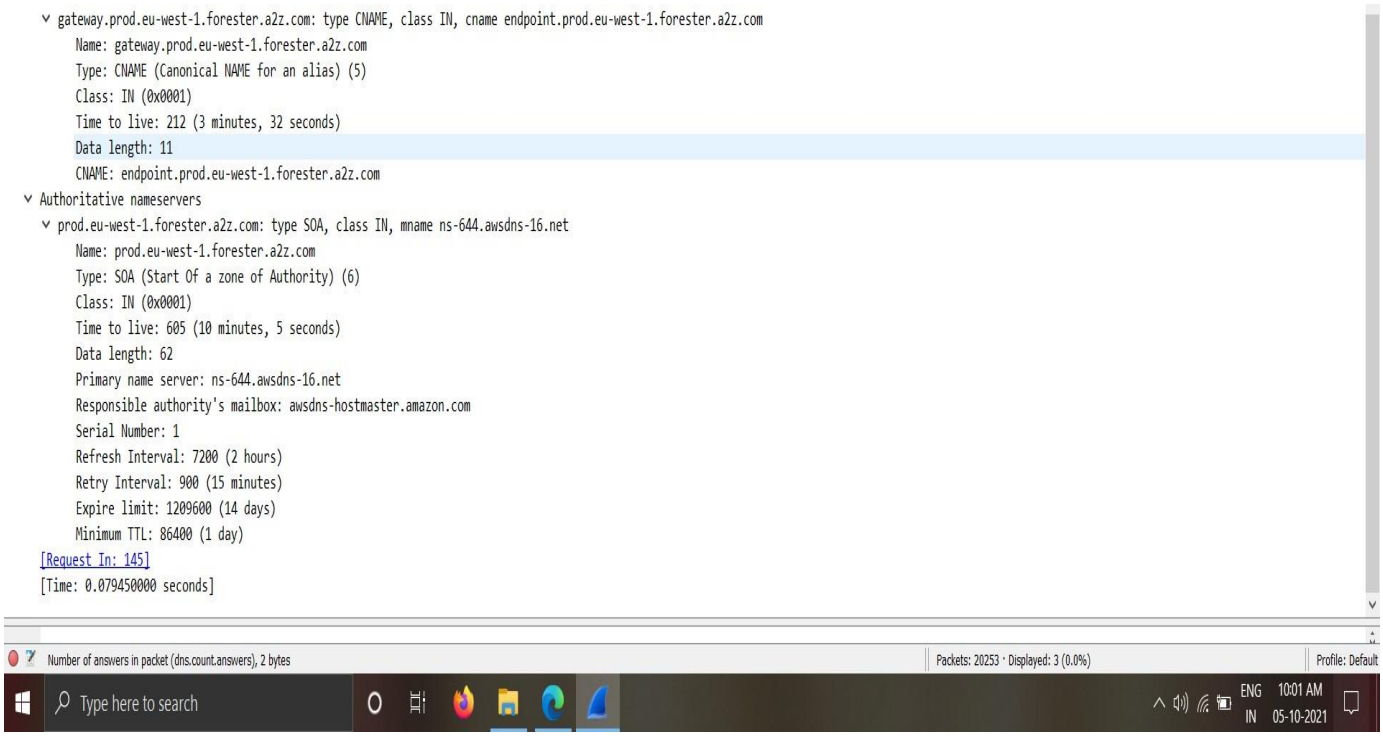


- Now for the selected query and response their particular source and destination ports are:
- Domain Name System (response):
  - ✓ Src Port: 53, Dst Port: 65185
  - ✓ Src: 192.168.43.1, Dst: 192.168.43.247
- Domain Name System (query):
  - ✓ Src Port: 65185, Dst Port: 53
  - ✓ Src: 192.168.43.247, Dst: 192.168.43.1

c. Check whether a DNS request receives multiple responses, if so, determine the reason for this

- Yes, one dns request, received multiple responses:





★ An authoritative nameserver MAY include any additional records that help name resolution. These additional records are appended to the additional section of the response.