

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:

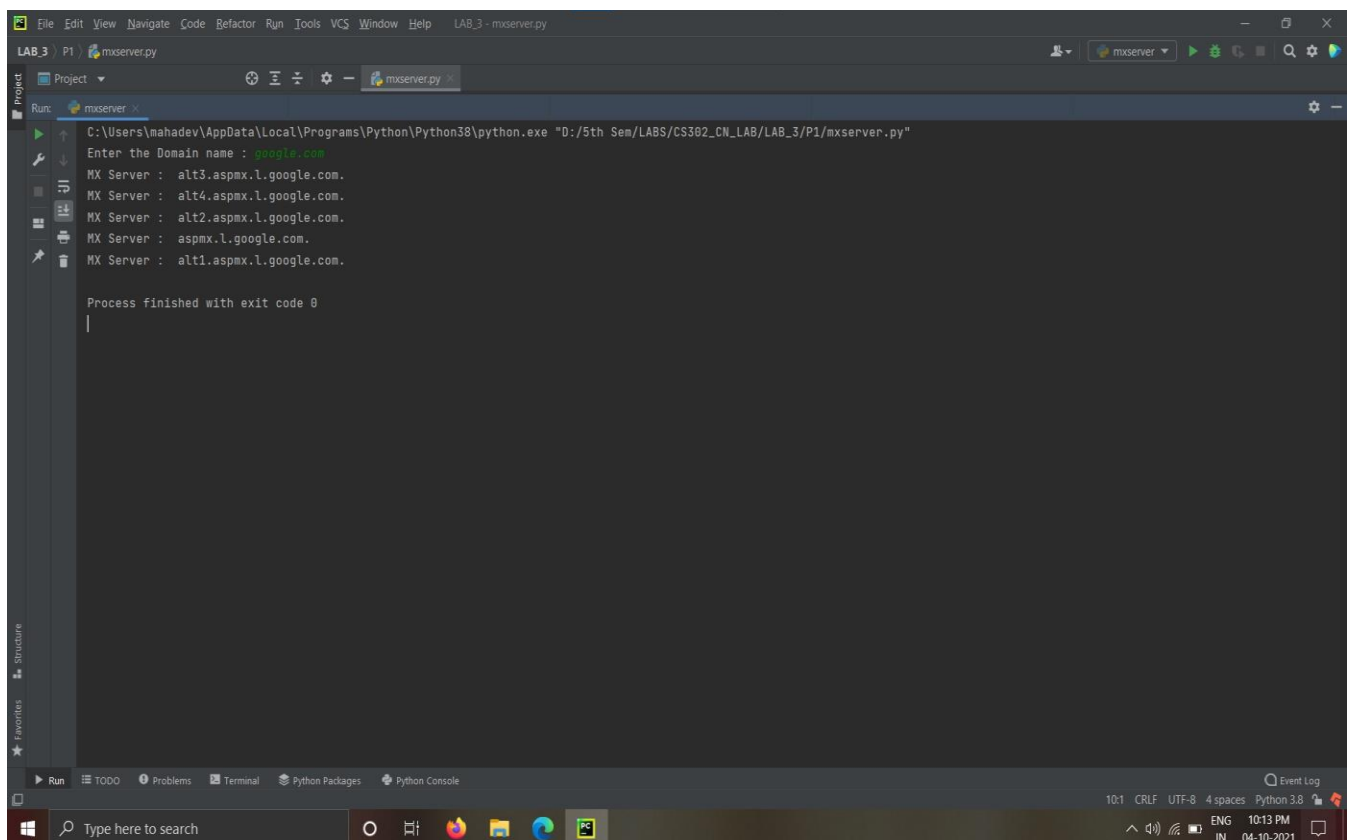
```
import dns.resolver
from distlib.compat import raw_input

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])

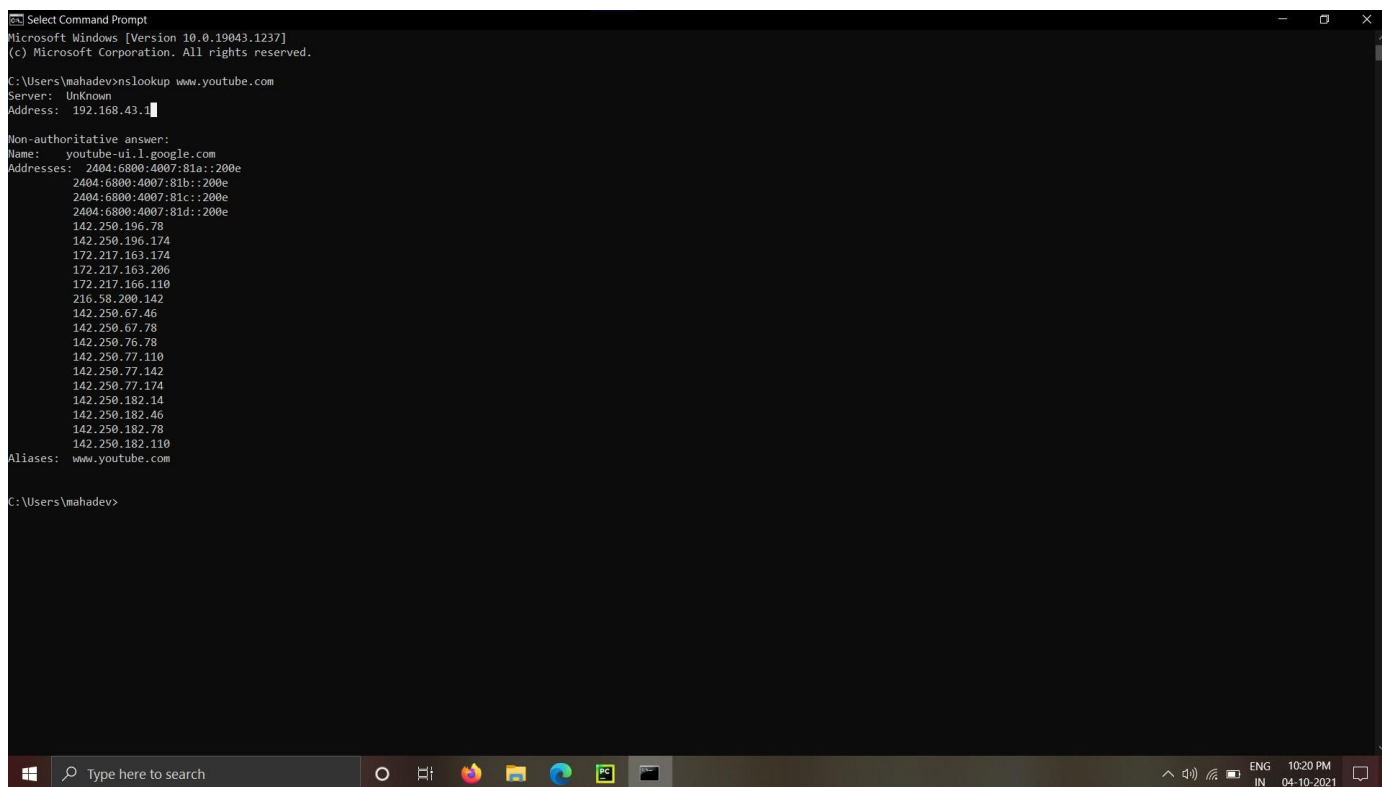
# A MX record also called mail exchanger record is a resource record in the Domain
# Name System that specifies a mail
# server responsible for accepting email messages on behalf of a recipient's domain.
```



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_address command.



```
Select Command Prompt
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mahadev>nslookup www.youtube.com
Server:      Unknown
Address:     192.168.43.1

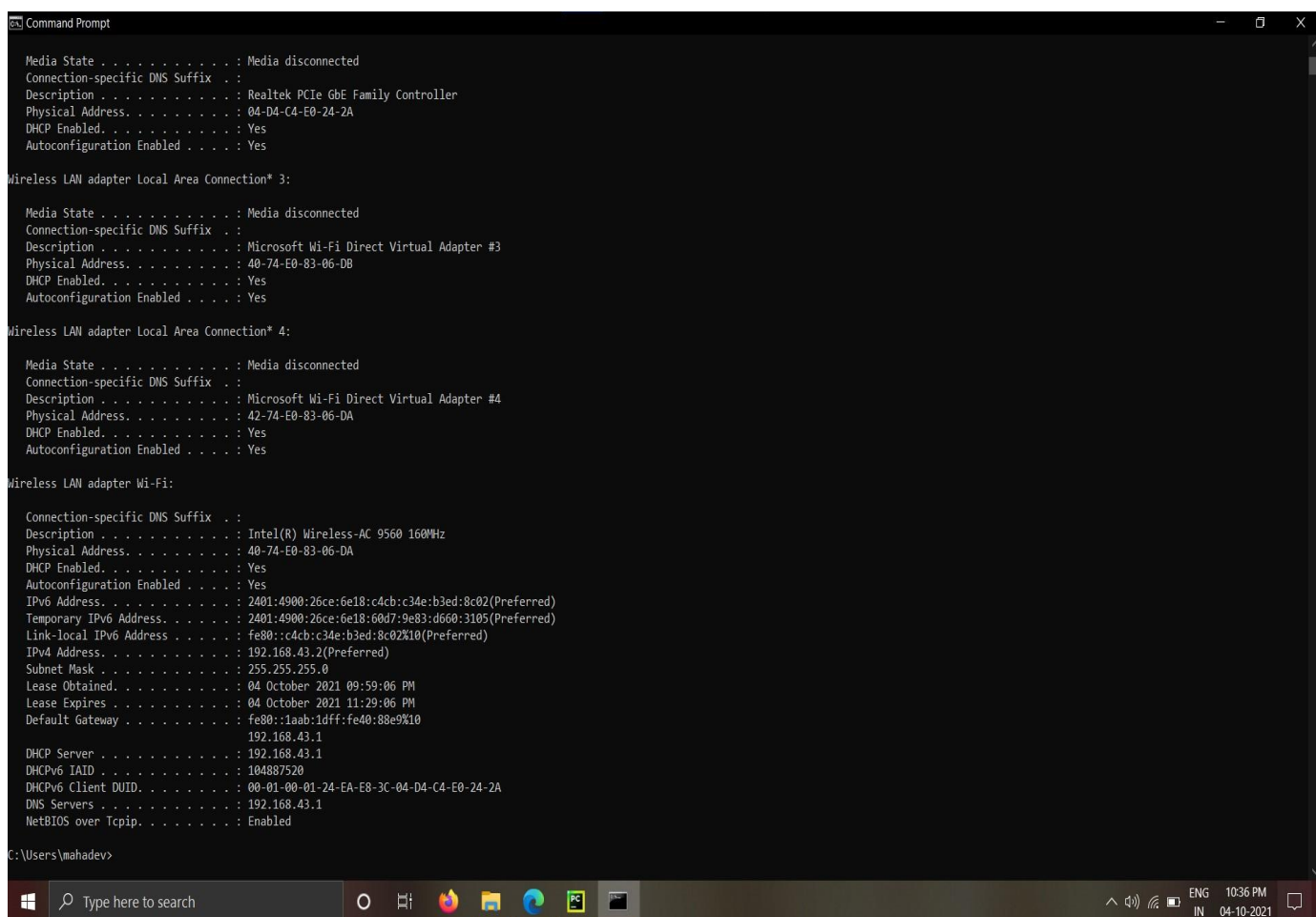
Non-authoritative answer:
Name:   youtube-ui.l.google.com
Addresses:  2404:6800:4007:81a::200e
            2404:6800:4007:81b::200e
            2404:6800:4007:81c::200e
            2404:6800:4007:81d::200e
            142.250.196.78
            142.250.196.174
            172.217.163.174
            172.217.163.206
            172.217.166.110
            216.58.200.142
            142.250.67.46
            142.250.67.78
            142.250.76.78
            142.250.77.110
            142.250.77.142
            142.250.77.174
            142.250.182.14
            142.250.182.46
            142.250.182.78
            142.250.182.110
Aliases:  www.youtube.com

C:\Users\mahadev>
```

- 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.

A screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the output of the "ipconfig /all" command. The output is organized into sections for different network adapters. The first section is for a Realtek PCIe GbE Family Controller, showing it is disconnected. The next two sections are for Microsoft Wi-Fi Direct Virtual Adapters #3 and #4, also showing they are disconnected. The final section is for the Intel(R) Wireless-AC 9560 160MHz Wi-Fi adapter, which is connected. This section displays a wealth of information including the physical address, DHCP status, IPv6 and IPv4 addresses (with preferred status), subnet mask, lease times, default gateway, DHCP server, and DNS servers. The command prompt shows the user is logged in as mahadev.

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 04-D4-C4-E0-24-2A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 3:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address. . . . . : 40-74-E0-83-06-DB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 4:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : 42-74-E0-83-06-DA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wireless-AC 9560 160MHz
Physical Address. . . . . : 40-74-E0-83-06-DA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2401:4900:26ce:6e18:c4cb:b3ed:8c02(Preferred)
Temporary IPv6 Address. . . . : 2401:4900:26ce:6e18:60d7:9e83:d660:3105(Preferred)
Link-local IPv6 Address . . . . : fe80::c4cb:c34e:b3ed:8c02%10(Preferred)
IPv4 Address. . . . . : 192.168.43.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 04 October 2021 09:59:06 PM
Lease Expires . . . . . : 04 October 2021 11:29:06 PM
Default Gateway . . . . . : fe80::1aab:1dff:fe40:88e9%10
                          192.168.43.1
DHCP Server . . . . . : 192.168.43.1
DHCPv6 IAID . . . . . : 104887520
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-EA-E8-3C-04-D4-C4-E0-24-2A
DNS Servers . . . . . : 192.168.43.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\mahadev>
```

- 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.

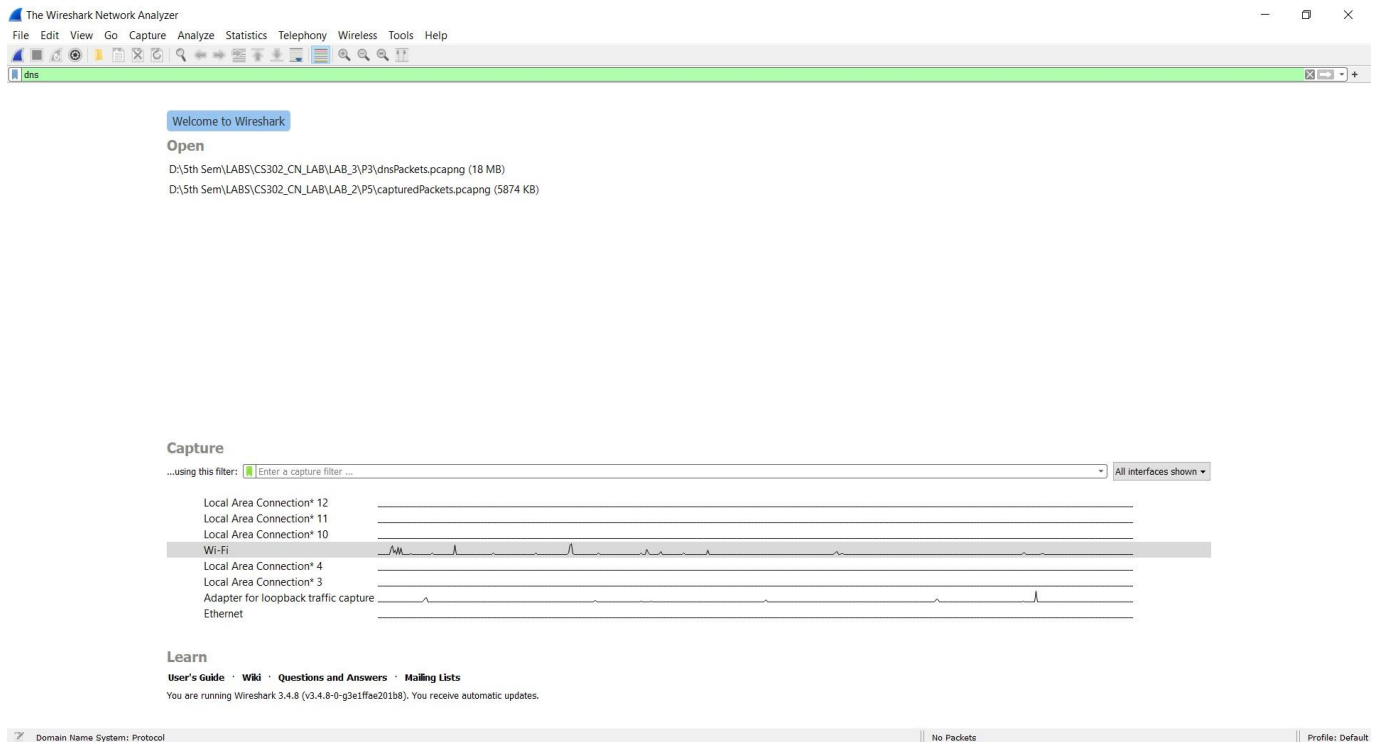
DNS Servers : 192.168.43.1

Default Gateway fe80::1aab:1dff:fe40:88e9%10
192.168.43.1

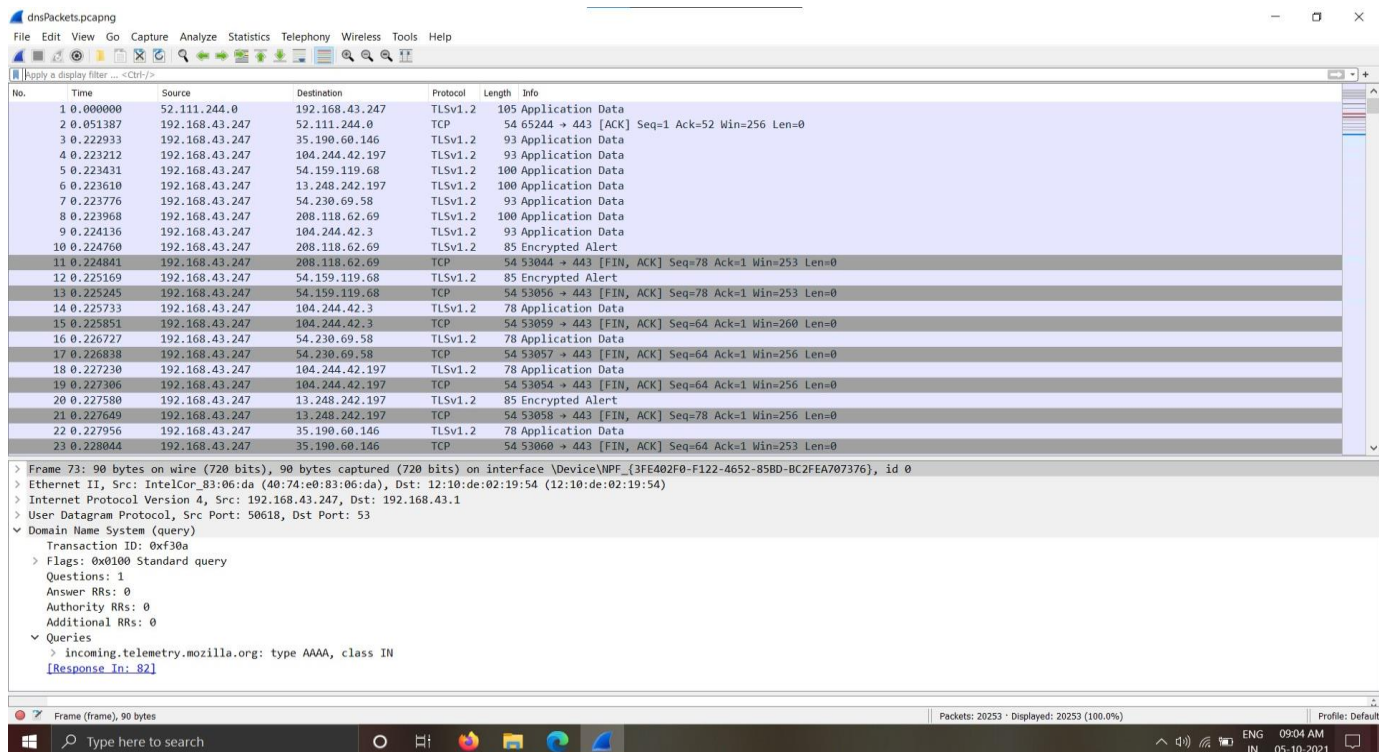
3. Capture and Analyse DNS Packets using Wireshark.

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.

Frame 84: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85B0-BC2FEA707376}, id 0

Ethernet II, Src: IntelCor_83:06:da (48:74:e0:83:06:da), Dst: 12:10:de:02:19:54 (12:10:de:02:19:54)

Internet Protocol Version 4, Src: 192.168.43.247, Dst: 192.168.43.1

User Datagram Protocol, Src Port: 52134, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x6206

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

incoming.telemetry.mozilla.org: type AAAA, class IN

[Response In: 85]

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

◆ This is a DNS Response Packet

Frame 4270: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85B0-BC2FEA707376}, id 0

Ethernet II, Src: 12:10:de:02:19:54 (12:10:de:02:19:54), Dst: IntelCor_83:06:da (48:74: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: 50157

Domain Name System (response)

Transaction ID: 0xf7fd

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

ssp.postmatric.karnataka.gov.in: type AAAA, class IN

Name: ssp.postmatric.karnataka.gov.in

[Name Length: 31]

[Label Count: 5]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

[Request In: 4268]

[Time: 0.003439000 seconds]


```

> 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]

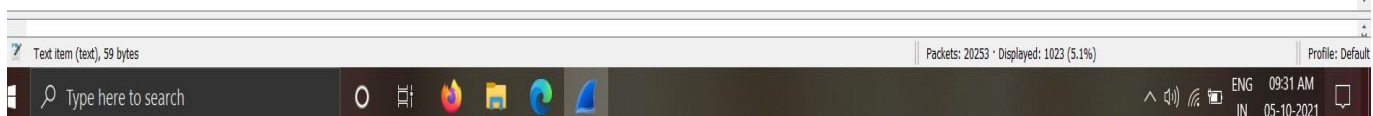
```

- 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 screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list pane shows several DNS packets. Packet 4281 is selected, showing a standard query from 192.168.43.1 to 192.168.43.247. The packet details pane shows the structure of the DNS query:

```

Domain Name System (query)
  Transaction ID: 0x005e
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    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)
      [Response In: 4281]
  
```

```

> Frame 4280: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: IntelCor_83:06:da (40:74:e0:83:06:da), Dst: 12:10:de:02:19:54 (12:10:de:02:19:54)
> Internet Protocol Version 4, Src: 192.168.43.247, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 55638, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x005e
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    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)
      [Response In: 4281]
  
```

- 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 :)

The screenshot shows the Wireshark interface with the filter `dns.id == 0x861d` applied. The packet list displays two packets:

No.	Time	Source	Destination	Protocol	Length	Info
4269	5.078253	192.168.43.247	192.168.43.1	DNS	75	Standard query 0x861d AAAA iris.nitk.ac.in
4271	5.081801	192.168.43.1	192.168.43.247	DNS	75	Standard query response 0x861d AAAA iris.nitk.ac.in

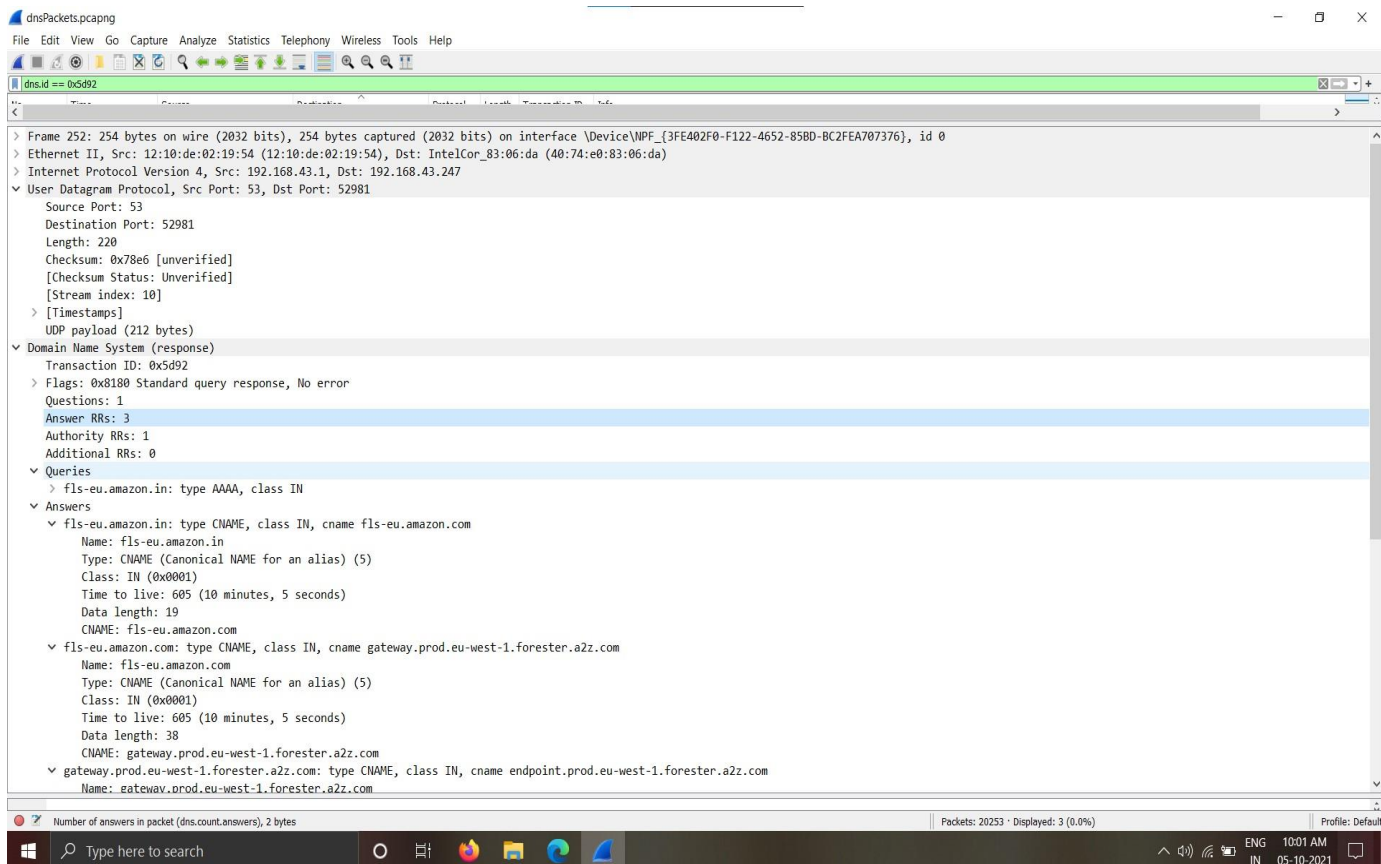
The packet details pane for packet 4271 shows the following structure:

- Frame 4271: 75 bytes on wire (600 bits), 75 bytes captured (600 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: 65185
 - Source Port: 53
 - Destination Port: 65185
 - Length: 41
 - Checksum: 0x685f [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 42]
 - [Timestamps]
 - UDP payload (33 bytes)
- Domain Name System (response)
 - Transaction ID: 0x861d
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - iris.nitk.ac.in: type AAAA, class IN
 - [Request In: 4269]
 - [Time: 0.003548000 seconds]

- 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:



```

  gateway.prod.eu-west-1.forester.a2z.com: type CNAME, class IN, cname endpoint.prod.eu-west-1.forester.a2z.com
    Name: gateway.prod.eu-west-1.forester.a2z.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 212 (3 minutes, 32 seconds)
    Data length: 11
    CNAME: endpoint.prod.eu-west-1.forester.a2z.com
  Authoritative nameservers
  prod.eu-west-1.forester.a2z.com: type SOA, class IN, mname ns-644.awsdns-16.net
    Name: prod.eu-west-1.forester.a2z.com
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 605 (10 minutes, 5 seconds)
    Data length: 62
    Primary name server: ns-644.awsdns-16.net
    Responsible authority's mailbox: awsdns-hostmaster.amazon.com
    Serial Number: 1
    Refresh Interval: 7200 (2 hours)
    Retry Interval: 900 (15 minutes)
    Expire limit: 1209600 (14 days)
    Minimum TTL: 86400 (1 day)
  [Request In: 145]
  [Time: 0.079450000 seconds]

```

Number of answers in packet (dns.count.answers): 2 bytes

Packets: 20253 · Displayed: 3 (0.0%)

Profile: Default

1001 AM 05-10-2021

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