# CS302 – ASSIGNMENT - 3

Ragul N S – 191CS146 & Rakshith H R – 191CS148

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

```
# Develop a program to print the Mail exchange servers of a partic
ular domain with their preferences
import dns.resolver

domainName = input("Enter the input domain: ")
mxServers = dns.resolver.resolve(domainName, 'MX')


for server in mxServers:
    print(server.to_text())
```

```
PS D:\Computer Networks Lab> python -u "d:\Computer Networks Lab\Week - 3\Q1\Q1.py"
Enter the input domain: nitk.edu.in
1 ASPMX.L.GOOGLE.COM.
5 ALT1.ASPMX.L.GOOGLE.COM.
5 ALT2.ASPMX.L.GOOGLE.COM.
10 ASPMX2.GOOGLEMAIL.COM.
10 ASPMX3.GOOGLEMAIL.COM.
PS D:\Computer Networks Lab> python -u "d:\Computer Networks Lab\Week - 3\Q1\Q1.py"
Enter the input domain: gmail.com
10 alt1.gmail-smtp-in.l.google.com.
20 alt2.gmail-smtp-in.l.google.com.
40 alt4.gmail-smtp-in.l.google.com.
30 alt3.gmail-smtp-in.l.google.com.
5 gmail-smtp-in.l.google.com.
PS D:\Computer Networks Lab> python -u "d:\Computer Networks Lab\Week - 3\Q1\Q1.py"
Enter the input domain: outlook.com
5 outlook-com.olc.protection.outlook.com.
PS D:\Computer Networks Lab> python -u "d:\Computer Networks Lab\Week - 3\Q1\Q1.py"
Enter the input domain: bugsmirror.com
1 ASPMX.L.GOOGLE.com.
5 ALT1.ASPMX.L.GOOGLE.com.
5 ALT2.ASPMX.L.GOOGLE.com.
10 ALT3.ASPMX.L.GOOGLE.com.
10 ALT4.ASPMX.L.GOOGLE.com.
PS D:\Computer Networks Lab>
```

We have used the library called dns resolver to get the mail exchange servers. The input is a domain and with the domain we call the function resolve() by passing domain and MX as parameters. The result is then converted into text and printed. Screenshot shows the output for various inputs given.

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

Ipconfig:

```
PS D:\Computer Networks Lab> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e09c:710c:9343:46a0%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::90e0:7c7f:72e3:45c6%14
   IPv4 Address. . . . . . . . . . . : 192.168.133.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 5:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8c96:a52d:b492:4ce5%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

The ipconfig command is run on PowerShell in windows and it has given details regarding the network of the machine. It prints out the windows IP Configuration as we can see from the output screenshot.

[see next page]

- Wireless LAN adapter Wi-Fi:
    - The Link-local version 4 IP address of the machine is fe80::8c96:a52d:b492:4ce5%16
    - The IPv4 address of the machine is 192.168.1.4
    - The subnet mask of the network is 255.255.255.0
    - The default gateway of 192.168.1.1
- Ethernet adapter Ethernet 3:
    - The Link-local version 4 IP address of the machine is fe80::8c96:a52d:b492:4ce5%16
    - The IPv4 address of the machine is 192.168.1.4
    - The subnet mask of the network is 255.255.255.0

```
PS D:\Computer Networks Lab> nslookup iris.nitk.ac.in
Server:  multiplay.bsnl.in
Address:  218.248.112.65

Non-authoritative answer:
Name:    iris.nitk.ac.in
Addresses:  103.225.13.13
          210.212.194.16

PS D:\Computer Networks Lab> nslookup www.nitk.ac.in
Server:  multiplay.bsnl.in
Address:  218.248.112.65

Non-authoritative answer:
Name:    www.nitk.ac.in
Addresses:  14.139.155.216
          218.248.46.85
          103.225.13.4
          210.212.194.4

PS D:\Computer Networks Lab>
```

nslookup: The command stands for name server lookup. It is used to query the dns service. The tool is typically used to obtain a domain name via your command line interface (CLI), receive IP address mapping details, and lookup DNS records. This information is retrieved from the DNS cache of your chosen DNS server.

In the output screenshot you can see that the command has given the address of the inputed domain name, and the server used to resolve the given name into ip address.

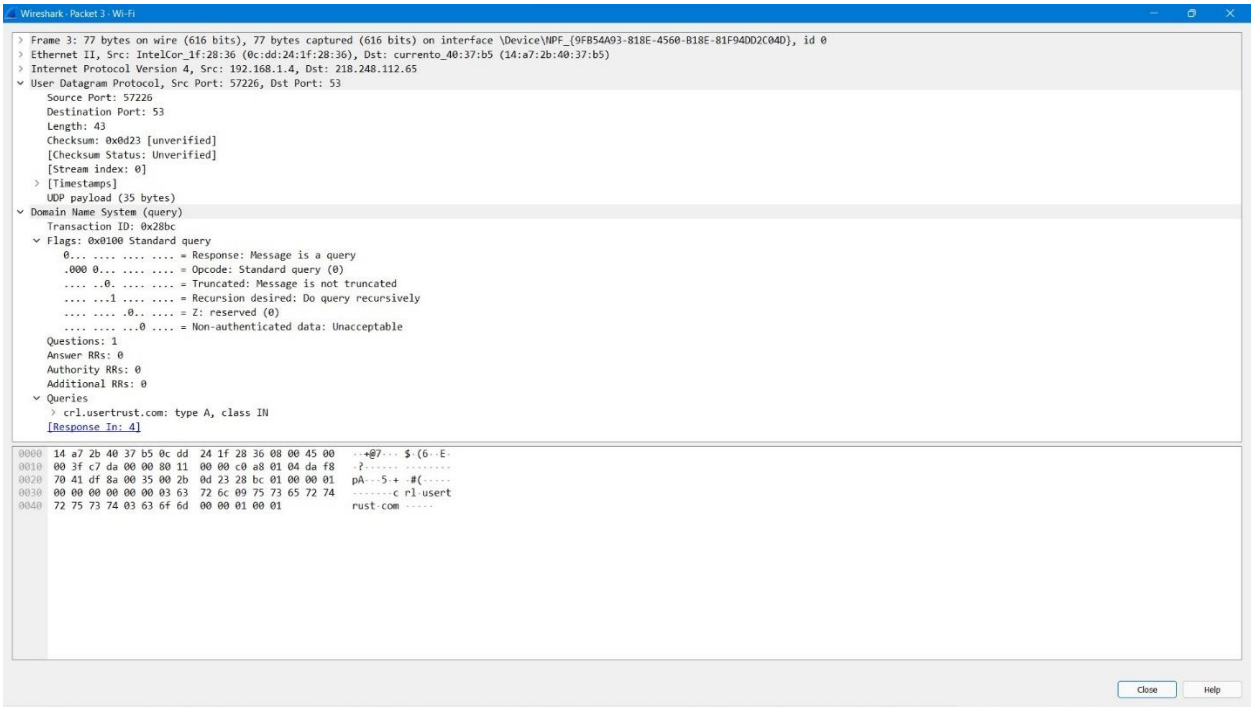
## 3.Capture and Analyze DNS Packets using Wireshark.

## a. Analyze DNS Query and Response Packets.

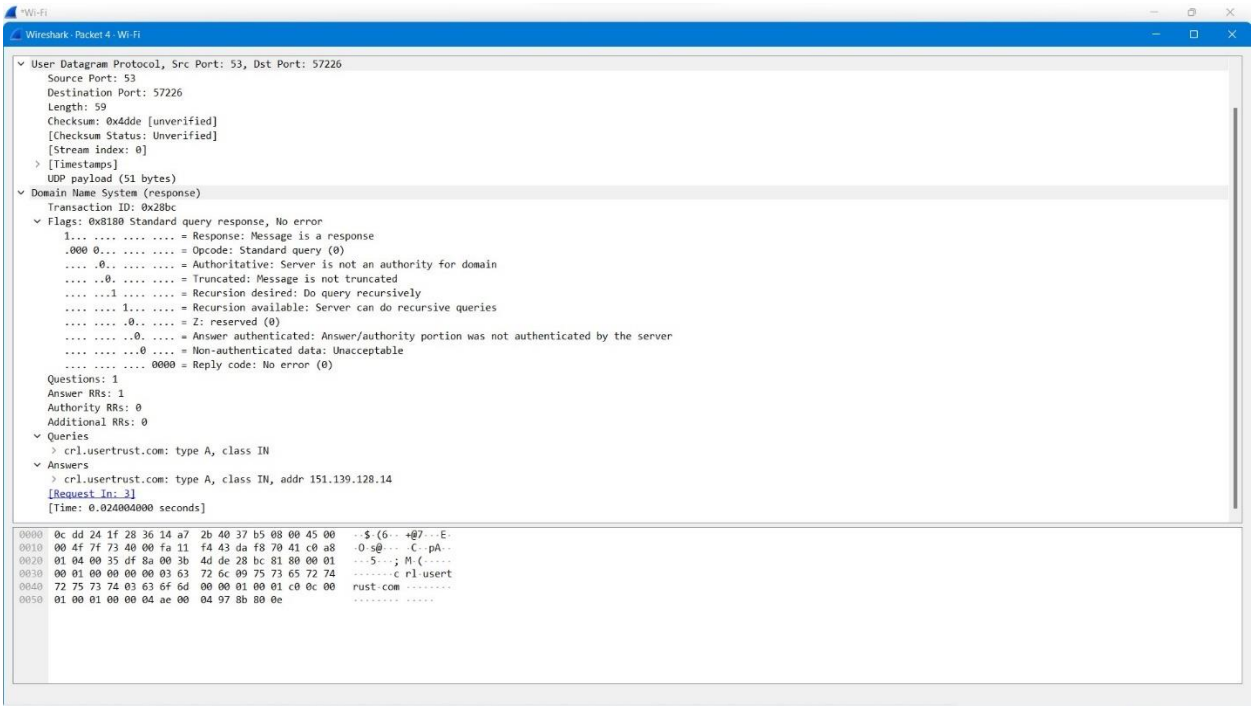
## b. By using the captured packets identify the source and destination ports query and response messages.

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

DNS request packet:



DNS response packet:




a) The DNS request packet has a question which corresponds to the domain name which we want to resolve in to IP address. In our case that is crl.usertrust.com. The DNS response packet has a field called answers which has the ipv4 address which corresponds to crl.usertrust.com. The IP address in the answers field is 151.139.128.14.

There are other fields with the information such as mac and IP addresses of the source and destination machine, information related to the transfer control protocol etc. The DNS response packet also has the time in which the response is sent to the DNS request. In our case that is 0.024004000 seconds.

b) By the captured packets we can find that the source port and destination ports used for request and response.

DNS request: source port – 57226 Destination port – 53

DNS response: source port – 53 Destination port – 57226

c) A client program picking an IP address from a list will generally try the addresses in the order they were returned by the DNS server (round robin). If the client cannot connect to the first IP address returned, it should try the second and so on. For example, all major browsers do this, however many other Internet client programs "forget" this step and fail if they cannot connect to the first IP address.