CN LAB ASSIGNMENT-3

Ans.1. This is just a command line version of achieving the same results as writing a program in python. The python code along with output can be found in the next page.

```
Command Prompt - nslookup
Address:  192.168.0.1

Non-authoritative answer:
goldmansachs.com        MX preference = 10, mail exchanger = mxb-0014b501.gslb.pphosted.com
goldmansachs.com        MX preference = 10, mail exchanger = mxa-0014b501.gslb.pphosted.com
> office.com
Server:  dlinkrouter
Address:  192.168.0.1

office.com
        primary name server = ch0mgt0101dc001.prdmgt01.prod.exchangelabs.com
        responsible mail addr = msnhst.microsoft.com
        serial  = 2017259934
        refresh = 300 (5 mins)
        retry   = 120 (2 mins)
        expire  = 2419200 (28 days)
        default TTL = 60 (1 min)
> outlook.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
outlook.com     MX preference = 5, mail exchanger = outlook-com.olc.protection.outlook.com
> apple.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
apple.com       MX preference = 10, mail exchanger = rn-mailsvcp-ppex-lapp14.apple.com
apple.com       MX preference = 10, mail exchanger = rn-mailsvcp-ppex-lapp15.apple.com
apple.com       MX preference = 10, mail exchanger = rn-mailsvcp-ppex-lapp24.apple.com
apple.com       MX preference = 10, mail exchanger = rn-mailsvcp-ppex-lapp34.apple.com
apple.com       MX preference = 10, mail exchanger = rn-mailsvcp-ppex-lapp35.apple.com
apple.com       MX preference = 10, mail exchanger = rn-mailsvcp-ppex-lapp44.apple.com
apple.com       MX preference = 10, mail exchanger = rn-mailsvcp-ppex-lapp45.apple.com
apple.com       MX preference = 10, mail exchanger = ma1-aaemail-dr-lapp01.apple.com
apple.com       MX preference = 10, mail exchanger = ma1-aaemail-dr-lapp02.apple.com
apple.com       MX preference = 10, mail exchanger = ma1-aaemail-dr-lapp03.apple.com
>
```

```
Command Prompt - nslookup
Non-authoritative answer:
iris.nitk.ac.in MX preference = 0, mail exchanger = mail.nitk.ac.in
> nitk.ac.in
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
nitk.ac.in      MX preference = 1, mail exchanger = mx1.nitk.ac.in
> ibm.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com
> oracle.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
oracle.com      MX preference = 20, mail exchanger = mxb-00069f01.gslb.pphosted.com
oracle.com      MX preference = 20, mail exchanger = mxa-00069f01.gslb.pphosted.com
> yahoo.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
yahoo.com       MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
> goldmansachs.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
goldmansachs.com        MX preference = 10, mail exchanger = mxb-0014b501.gslb.pphosted.com
goldmansachs.com        MX preference = 10, mail exchanger = mxa-0014b501.gslb.pphosted.com
> office.com
Server:  dlinkrouter
Address:  192.168.0.1
```

Mail Exchange records are DNS records that are necessary for delivery of emails to any address. MX records are used because it gives the address of the server to which your mail should be delivered. No mails can be sent without DNS records.

MX records consists of two parts:

1.) Priority/preference of the particular server. Higher the value implies lower the priority.

2.) The second fields represents the actual address of the server which needs to be connected in order to reach your inbox. The actual address varies depending on which company hosts your email.

Priority is given to enable the use of primary and backup servers, so that the mail can be directed to a server which has the highest priority, and if in any case the primary server crashes, then the next server with the highest priority is given the message.

In the above tested domains for their MX servers, we observe that there could be multiple MX servers with the same priority. But there can also be domains who have different preferences/priorities for their MX servers.

Following is the program for the same to print mail servers along with their preference: (here google.com has been taken as the specefic domain, but the program will work for any domain)

```python
import dns.resolver

servers_results=dns.resolver.resolve('google.com','MX')
for i in servers_results:
    print(f"mail server {i.exchange} has priority {i.preference}")
    print("\n")
```

The corresponding output is as follows:

```
(base) C:\Users\aashi\Downloads\CN Lab 3\Q.1. DNS program>python DNS_program.py
mail server alt2.aspmx.l.google.com. has preference 30


mail server aspmx.l.google.com. has preference 10


mail server alt4.aspmx.l.google.com. has preference 50


mail server alt3.aspmx.l.google.com. has preference 40


mail server alt1.aspmx.l.google.com. has preference 20


(base) C:\Users\aashi\Downloads\CN Lab 3\Q.1. DNS program>
```

Ans.2.

IpConfig is a command that is primarily used to display the computer's IP address information. It also shows information such as system's IP address, subnet mask, and default gateway.

First we have the command 'ipconfig /all' which displays the full TCP/IP configuration for all adapter.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-5RLB38B
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-11
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f575:a112:b0b5:f1c9%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 638189607
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-A2-BA-0B-00-00-10-01-23-4C
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 8C-8D-28-E6-C1-DA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

```
Command Prompt
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 8E-8D-28-E6-C1-D9
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a945:6cc4:6374:4bad%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.116.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 671109206
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-A2-BA-0B-00-00-10-01-23-4C
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::95c2:63c9:2c44:db68%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.190.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 687886422
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-A2-BA-0B-00-00-10-01-23-4C
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
```

```
   DHCPv6 IAID . . . . . . . . . . . . : 687886422
   DHCPv6 Client DUID. . . . . . . . . : 00-01-00-01-27-A2-BA-0B-00-00-10-01-23-4C
   DNS Servers . . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                         fec0:0:0:ffff::2%1
                                         fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 8C-8D-28-E6-C1-D9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:8f8:172d:b965:3069:f96:574:75f8(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:8f8:172d:b965:d535:7cfe:f951:2e3f(Preferred)
   Link-local IPv6 Address . . . . . : fe80::3069:f96:574:75f8%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.152(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 07 October 2021 18:10:55
   Lease Expires . . . . . . . . . . : 11 October 2021 16:14:12
   Default Gateway . . . . . . . . . : fe80::f68c:ebff:fe16:a426%10
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 126651688
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-A2-BA-0B-00-00-10-01-23-4C
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 8C-8D-28-E6-C1-DD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\aashi>
```

The next command we have is 'ipconfig /allcompartments' this command is used to show information about all compartments.

```
C:\Users\aashi>ipconfig /allcompartments

Windows IP Configuration


============================================================================
Network Information for Compartment 1 (ACTIVE)
============================================================================

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f575:a112:b0b5:f1c9%17
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a945:6cc4:6374:4bad%16
   IPv4 Address. . . . . . . . . . . : 192.168.116.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::95c2:63c9:2c44:db68%13
   IPv4 Address. . . . . . . . . . . : 192.168.190.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a945:6cc4:6374:4bad%16
   IPv4 Address. . . . . . . . . . . : 192.168.116.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::95c2:63c9:2c44:db68%13
   IPv4 Address. . . . . . . . . . . : 192.168.190.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:8f8:172d:b965:3069:f96:574:75f8
   Temporary IPv6 Address. . . . . . : 2001:8f8:172d:b965:d535:7cfe:f951:2e3f
   Link-local IPv6 Address . . . . . : fe80::3069:f96:574:75f8%10
   IPv4 Address. . . . . . . . . . . : 192.168.0.152
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::f68c:ebff:fe16:a426%10
                                       192.168.0.1

Ethernet adapter Bluetooth Network Connection:

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

Another command of ipconfig is thr ‘ipconfig /displaydns’ which displays all the contents of the DNS resolver cache. Following is a part of the lengthy result of our running of this command.

```
C:\Users\aashi>ipconfig /displaydns

Windows IP Configuration

    tr.blismedia.com
    ----------------------------------------
    Record Name . . . . . : tr.blismedia.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 12305
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 34.96.105.8


    gem.gbc.criteo.com
    ----------------------------------------
    Record Name . . . . . : gem.gbc.criteo.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 12307
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : gbc4.nl.eu.criteo.com


    Record Name . . . . . : gbc4.nl.eu.criteo.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 12307
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 178.250.6.113


    Record Name . . . . . : gbc4.nl.eu.criteo.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 12307
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 178.250.6.135
```

Here are some of the subcommands that can be used with ipconfig

```
where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.
```

Next we have the NSLOOKUP command. NsLookup queries the specified DNS server and retrieves the requested records that are associated with the domain name you provided. These records contain information like the domain name's IP addresses. Here we have used nslookup in interactive mode and used set type=mx command inorder to display mail server information of a specefic domain.

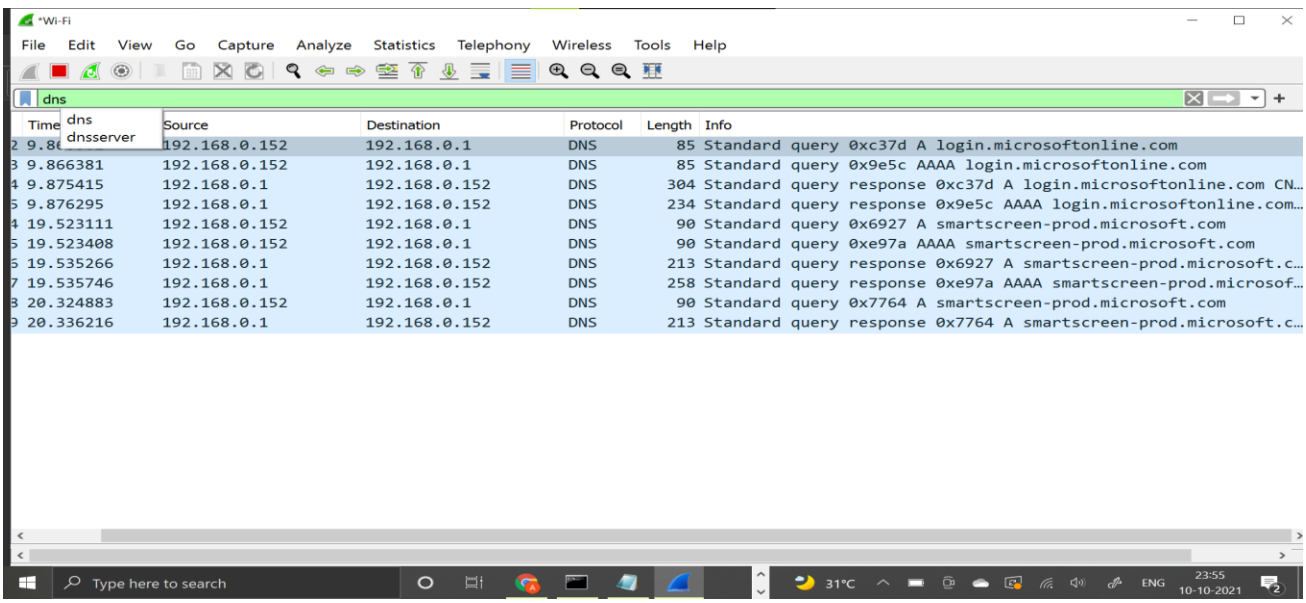
```
C:\Users\aashi>nslookup
Default Server:  dlinkrouter
Address:  192.168.0.1

> google.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:4019:80d::200e
          142.250.181.14

> set type=mx
> google.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
> microsoft.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
microsoft.com   MX preference = 10, mail exchanger = microsoft-com.mail.protection.outlook.com
> bing.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
bing.com        MX preference = 10, mail exchanger = bing-com.mail.protection.outlook.com
>
```

Next we have used the set type=ns command for nslookup in interactive mode as it displays the names of all authoritative servers of a domain. Following is a screenshot of the same for twitter.com as domain:

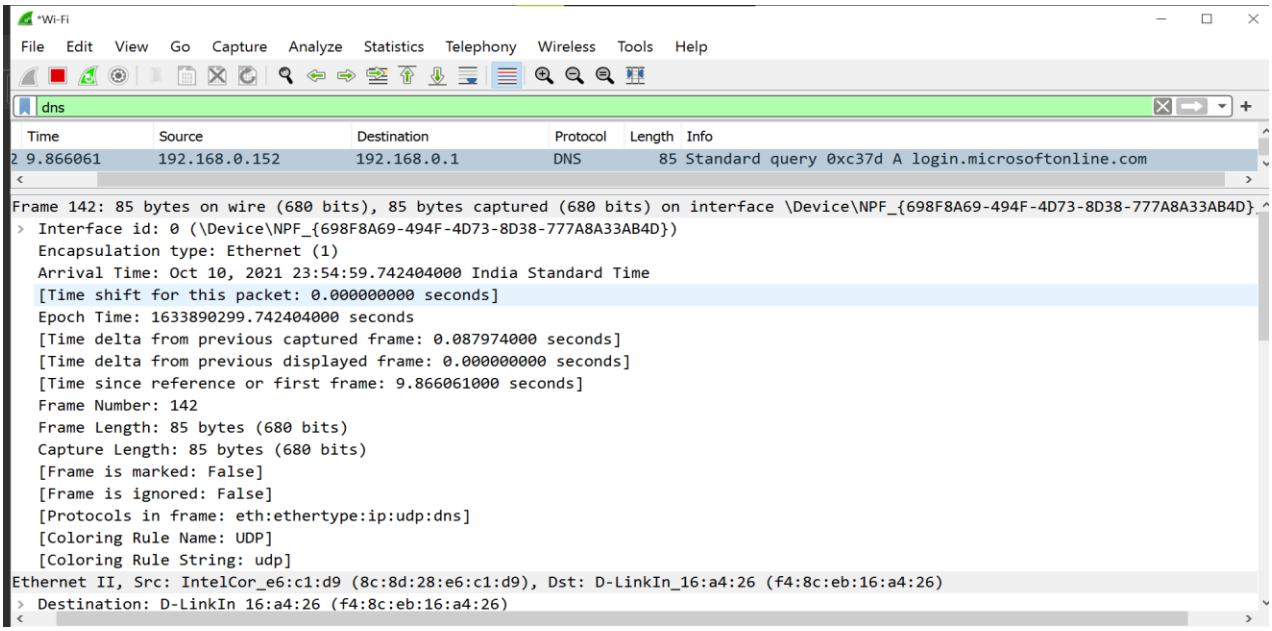
```
> set query=ns
> twitter.com
Server:  dlinkrouter
Address:  192.168.0.1

Non-authoritative answer:
twitter.com     nameserver = d01-02.ns.twtrdns.net
twitter.com     nameserver = ns1.p34.dynect.net
twitter.com     nameserver = ns2.p34.dynect.net
twitter.com     nameserver = d.r06.twtrdns.net
twitter.com     nameserver = d01-01.ns.twtrdns.net
twitter.com     nameserver = a.r06.twtrdns.net
twitter.com     nameserver = ns3.p34.dynect.net
twitter.com     nameserver = ns4.p34.dynect.net
twitter.com     nameserver = c.r06.twtrdns.net
twitter.com     nameserver = b.r06.twtrdns.net
>
```

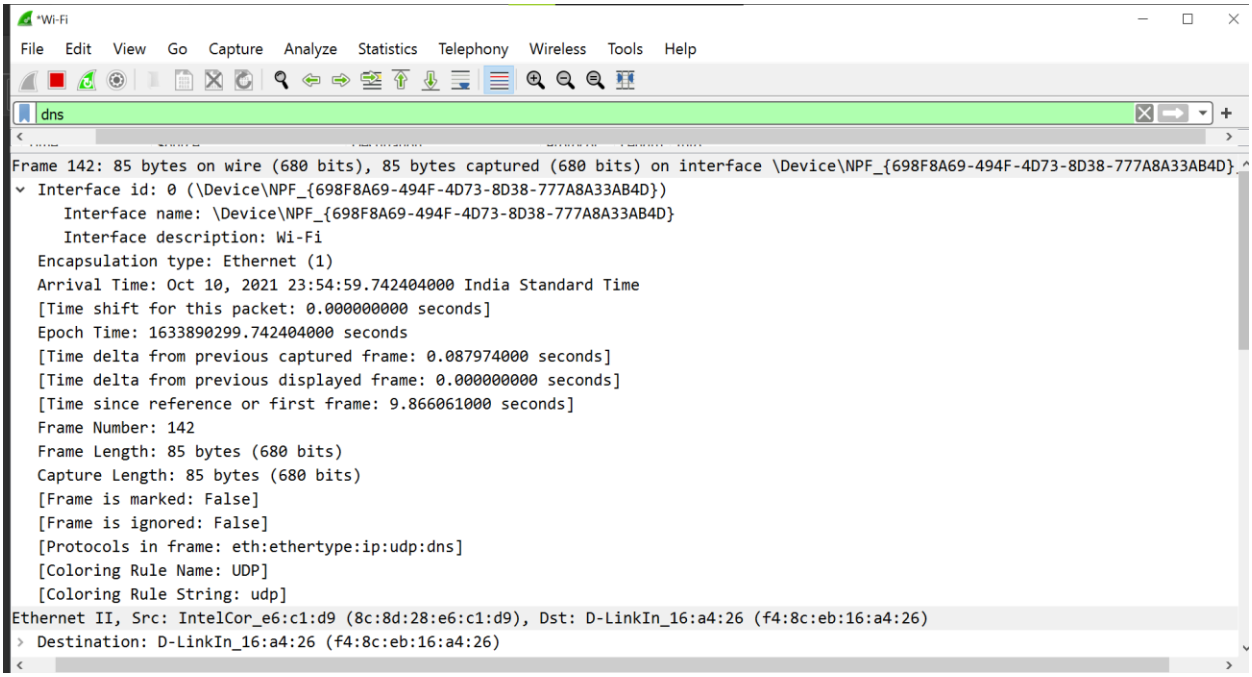
Ans.3.

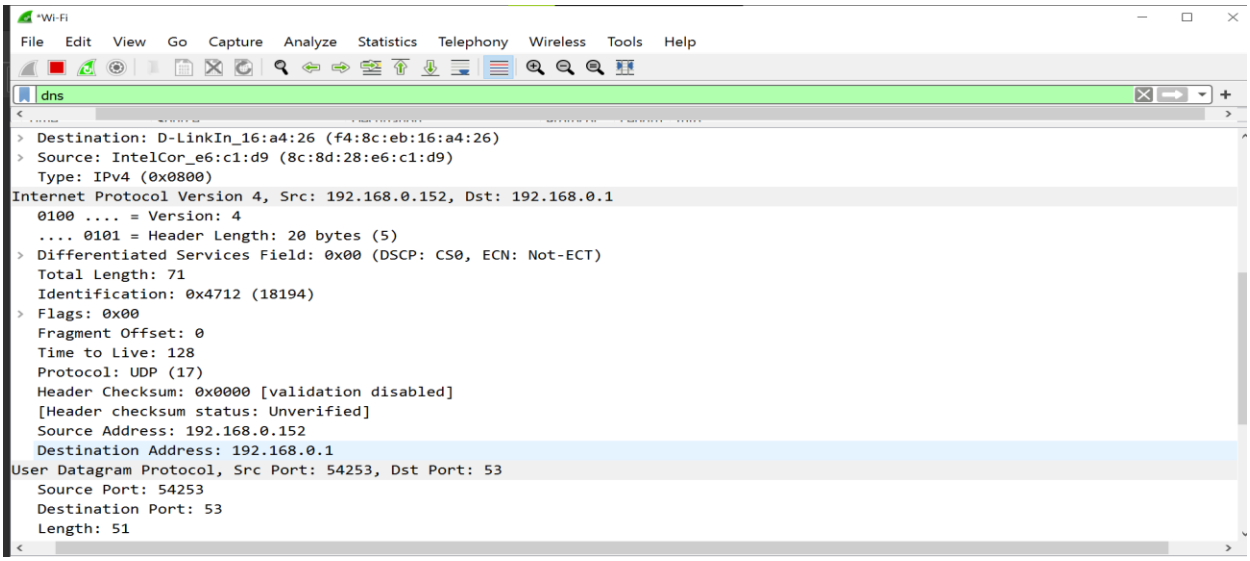
(a.)

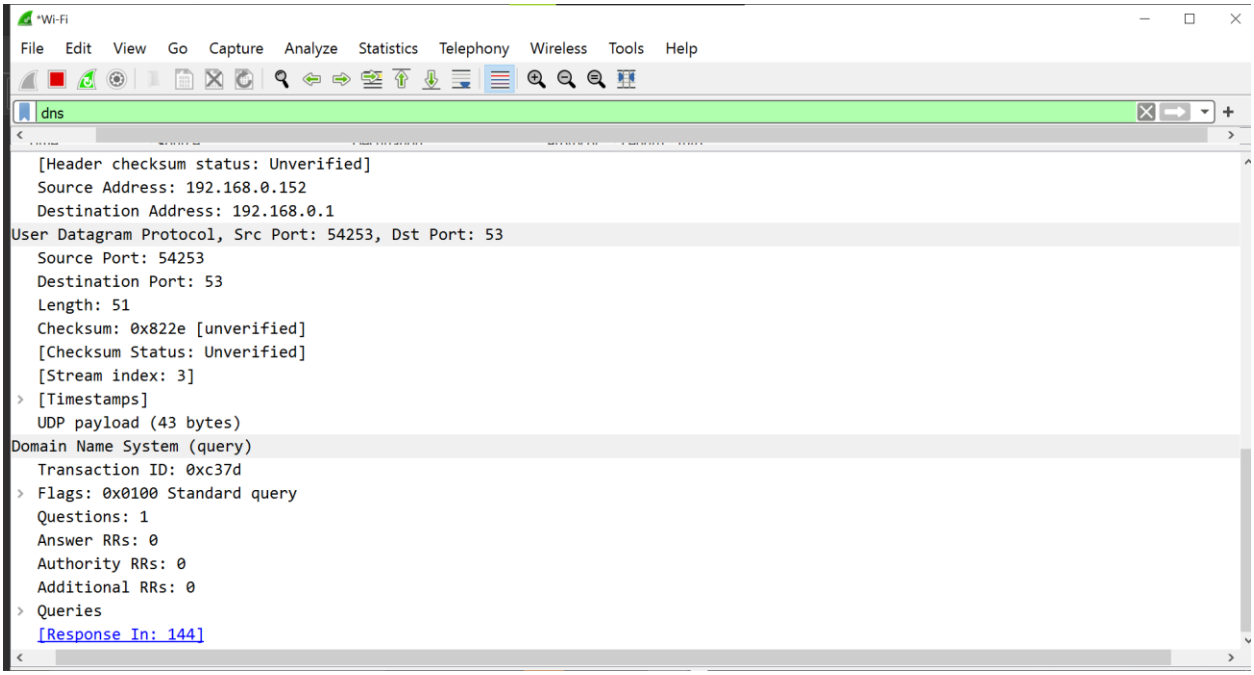


This is for the first query detail/analysis:

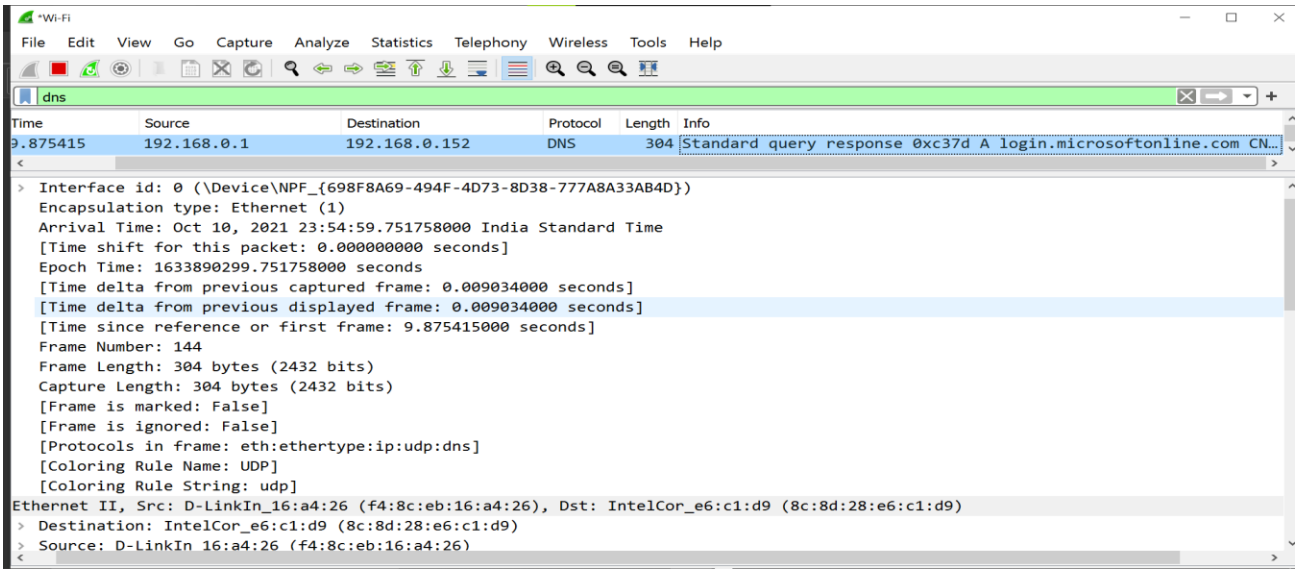

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Time Source Destination Protocol Length Info
2 9.866061 192.168.0.152 192.168.0.1 DNS 85 Standard query 0xc37d A login.microsoftonline.com
Frame 142: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{698F8A69-494F-4D73-8D38-777A8A33AB4D}
Interface id: 0 (\Device\NPF_{698F8A69-494F-4D73-8D38-777A8A33AB4D})
Encapsulation type: Ethernet (1)
Arrival Time: Oct 10, 2021 23:54:59.742404000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1633890299.742404000 seconds
[Time delta from previous captured frame: 0.087974000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 9.866061000 seconds]
Frame Number: 142
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: IntelCor_e6:c1:d9 (8c:8d:28:e6:c1:d9), Dst: D-LinkIn_16:a4:26 (f4:8c:eb:16:a4:26)
Destination: D-LinkIn_16:a4:26 (f4:8c:eb:16:a4:26)

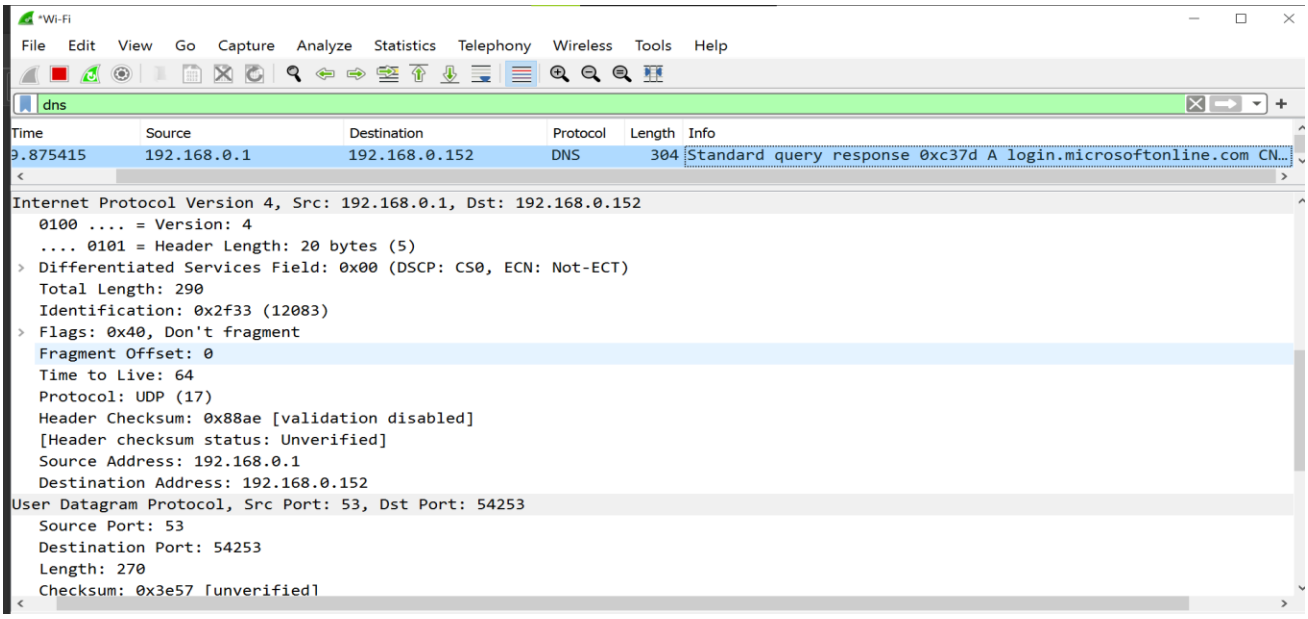

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Frame 142: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{698F8A69-494F-4D73-8D38-777A8A33AB4D}
Interface id: 0 (\Device\NPF_{698F8A69-494F-4D73-8D38-777A8A33AB4D})
Interface name: \Device\NPF_{698F8A69-494F-4D73-8D38-777A8A33AB4D}
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Oct 10, 2021 23:54:59.742404000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1633890299.742404000 seconds
[Time delta from previous captured frame: 0.087974000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 9.866061000 seconds]
Frame Number: 142
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: IntelCor_e6:c1:d9 (8c:8d:28:e6:c1:d9), Dst: D-LinkIn_16:a4:26 (f4:8c:eb:16:a4:26)
Destination: D-LinkIn_16:a4:26 (f4:8c:eb:16:a4:26)

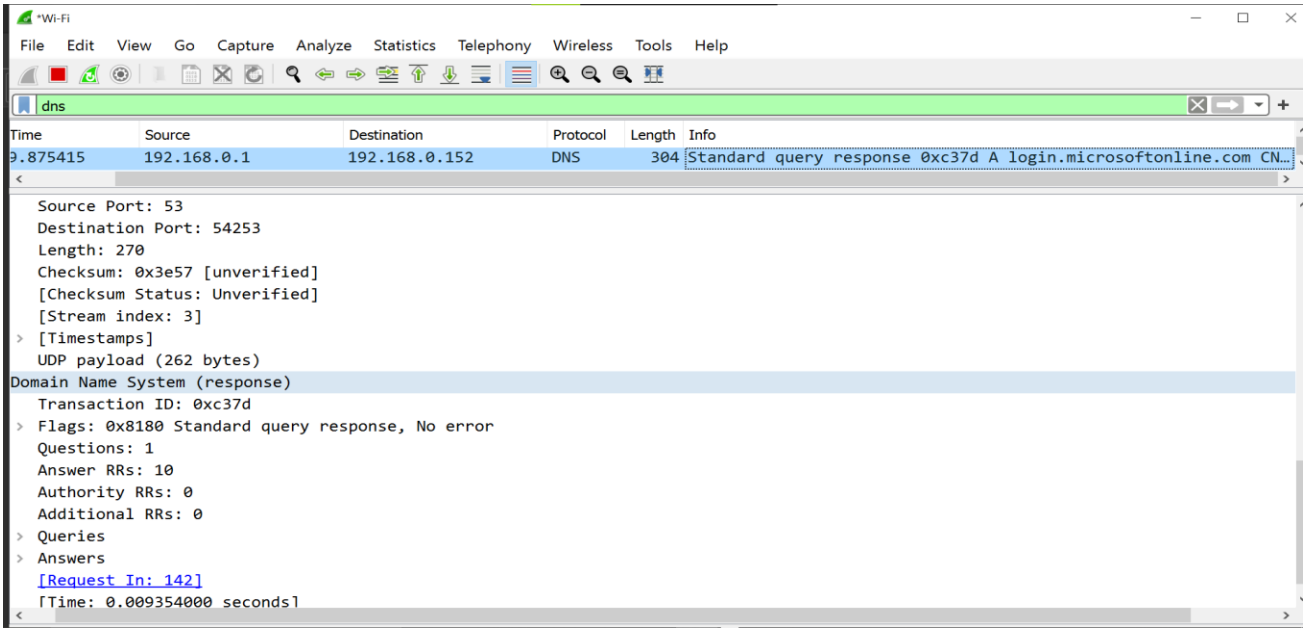




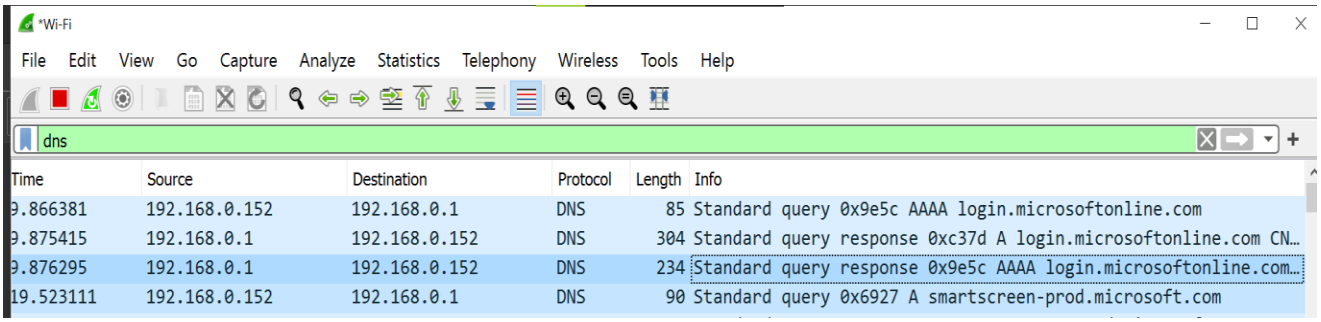
Analysis of response:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Time Source Destination Protocol Length Info
9.875415 192.168.0.1 192.168.0.152 DNS 304 Standard query response 0xc37d A login.microsoftonline.com CN…
Interface id: 0 (\Device\NPF_{698F8A69-494F-4D73-8D38-777A8A33AB4D})
Encapsulation type: Ethernet (1)
Arrival Time: Oct 10, 2021 23:54:59.751758000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1633890299.751758000 seconds
[Time delta from previous captured frame: 0.009034000 seconds]
[Time delta from previous displayed frame: 0.009034000 seconds]
[Time since reference or first frame: 9.875415000 seconds]
Frame Number: 144
Frame Length: 304 bytes (2432 bits)
Capture Length: 304 bytes (2432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: D-LinkIn_16:a4:26 (f4:8c:eb:16:a4:26), Dst: IntelCor_e6:c1:d9 (8c:8d:28:e6:c1:d9)
Destination: IntelCor_e6:c1:d9 (8c:8d:28:e6:c1:d9)
Source: D-LinkIn_16:a4:26 (f4:8c:eb:16:a4:26)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Time Source Destination Protocol Length Info
9.875415 192.168.0.1 192.168.0.152 DNS 304 Standard query response 0xc37d A login.microsoftonline.com CN…
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.152
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 290
Identification: 0x2f33 (12083)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x88ae [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.1
Destination Address: 192.168.0.152
User Datagram Protocol, Src Port: 53, Dst Port: 54253
Source Port: 53
Destination Port: 54253
Length: 270
Checksum: 0x3e57 [unverified]

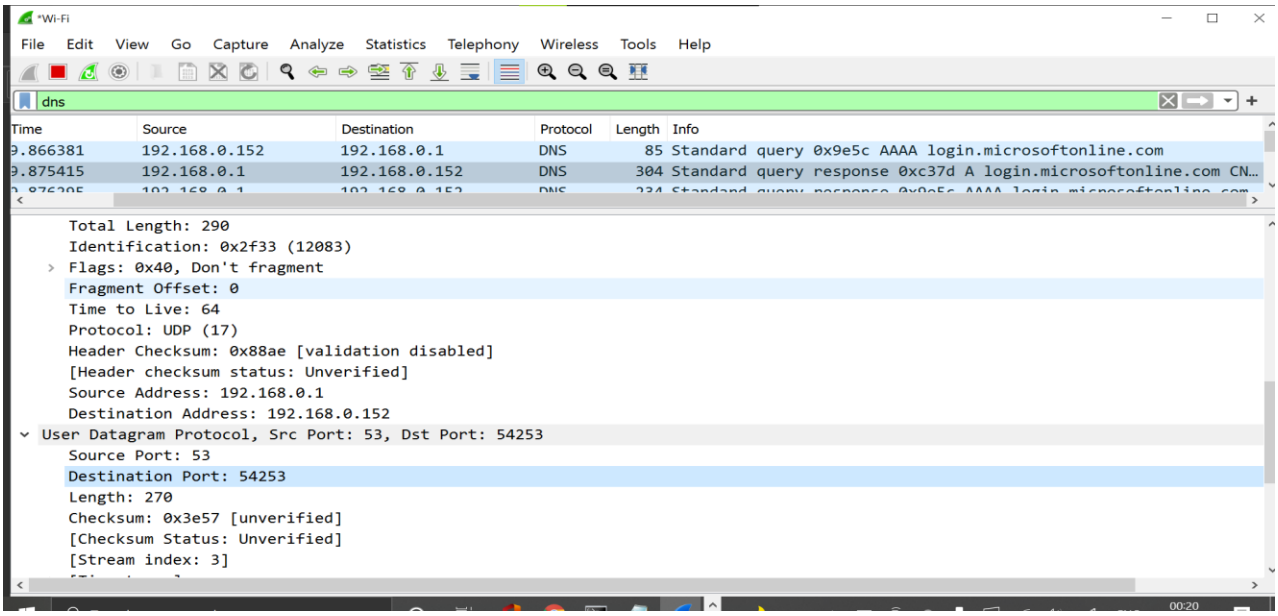


(b.)



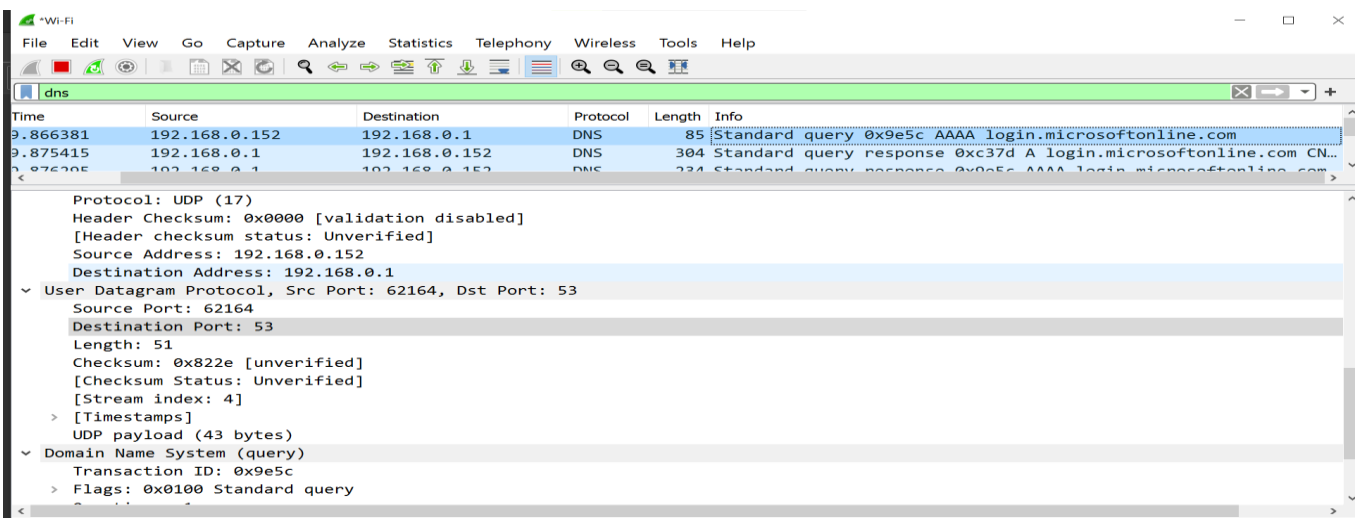
Here we observe that for the query which is in the first row, there are two responses for that query following it. The destination address for the query going from my laptop(IP address: 192.168.0.152) which is the source to the destination whose IP address is 192.168.0.1.

For the responses, the source and destination IP addresses are basically swapped. Now my computer is on the receiving end(IP address: 192.168.0.152) and login.microsoftonline.com(IP address: 192.168.0.1) is the source from which the response is sent. The details of source and destination ports is as follows for the query response:



Here the response coming from Microsoft originates in port 53 and my laptop receives it in port 54253.

For the same query the following is the source and destination port:



Here my laptop is sending a query from port 62164 and Microsoft receives the query in port 53.

The DNS uses TCP Port 53 for **zone transfers.**

(c.) the reason for multiple responses to a single query is since the same domain can have multiple IP addresses and hence when a response is sent it is sent from all the IP addresses of that domain and the DNS server to return all records for

that name. For example Microsoft.com can revolve to 4 different IP addresses. And since a socket is being used to receive responses from the server, hence it can also receive multiple responses.

Another main reason is because the DNS server returns all the IPs for services matching that A record. It is up to the client to resolve which IP to use, hence multiple responses.