# LAB 5

Q1)

```
C:\Users\vatsal>nslookup www.google
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:805::200
          172.217.31.196
```

Q1.1)

```
C:\Users\vatsal>nslookup -type=NS www.google.com
Server:  UnKnown
Address:  192.168.43.1

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 334992334
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

```
C:\Users\Dell>nslookup -type=NS google.com
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
google.com      nameserver = ns2.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns3.google.com
google.com      nameserver = ns1.google.com

ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
```

Q1.2)

```
C:\Users\vatsal>nslookup google.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:809::200e
          172.217.167.14
```

Q1.3)

1)

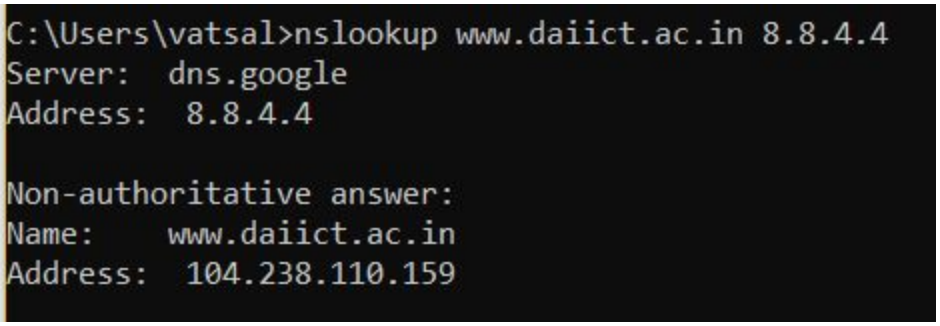
```
C:\Users\vatsal>nslookup www.daiict.ac.in
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    www.daiict.ac.in
Address:  104.238.110.159
```

2)

```
C:\Users\Dell>nslookup -type=NS daiict.ac.in
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
daiict.ac.in    nameserver = ns2.relianceada.com
daiict.ac.in    nameserver = ns3.relianceada.com
daiict.ac.in    nameserver = ns1.relianceada.com
daiict.ac.in    nameserver = ns4.relianceada.com
daiict.ac.in    nameserver = ns1.exchangenext.net
daiict.ac.in    nameserver = ns2.exchangenext.net

ns1.relianceada.com     internet address = 202.138.120.86
ns1.exchangenext.net    internet address = 202.138.120.6
ns2.relianceada.com     internet address = 202.138.120.87
ns2.exchangenext.net    internet address = 202.138.120.4
ns3.relianceada.com     internet address = 220.227.60.11
ns4.relianceada.com     internet address = 220.227.60.12
```

```
C:\Users\vatsal>nslookup -type=NS www.daiict.ac.in
Server:  UnKnown
Address:  192.168.43.1

daiict.ac.in
        primary name server = ns1.relianceada.com
        responsible mail addr = mahesh patil
        serial  = 2010090405
        refresh = 7200 (2 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 21600 (6 hours)
```

3)


C:\Users\vatsal>nslookup www.daiict.ac.in 8.8.4.4
Server:  dns.google
Address:  8.8.4.4
Non-authoritative answer:
Name:    www.daiict.ac.in
Address:  104.238.110.159

Q2)

1)

```
C:\Users\vatsal>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 3:

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

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::61b7:f457:242d:78db%10
   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 Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2405:205:c90d:b973:1928:6454:2fb3:d6fd
   Temporary IPv6 Address. . . . . . : 2405:205:c90d:b973:2886:8d1f:9c5e:3813
   Link-local IPv6 Address . . . . . : fe80::1928:6454:2fb3:d6fd%20
   IPv4 Address. . . . . . . . . . . : 192.168.43.119
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::3c46:88ff:fee7:e4c%20
                                       192.168.43.1
```

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

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bceb:4da3:ce72:1733%13
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

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

2)-

```
lh3.google.com
----------------------------------------
Record Name . . . . . : lh3.google.com
Record Type . . . . . : 5
Time To Live  . . . . : 126
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : lh2.l.google.com


Record Name . . . . . : lh2.l.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 126
Data Length . . . . . : 16
Section . . . . . . . : Answer
AAAA Record . . . . . : 2404:6800:4007:810::200e
```

```
moodle.daiict.ac.in
----------------------------------------
Record Name . . . . . : moodle.daiict.ac.in
Record Type . . . . . : 1
Time To Live  . . . . : 16117
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 14.139.122.116
```

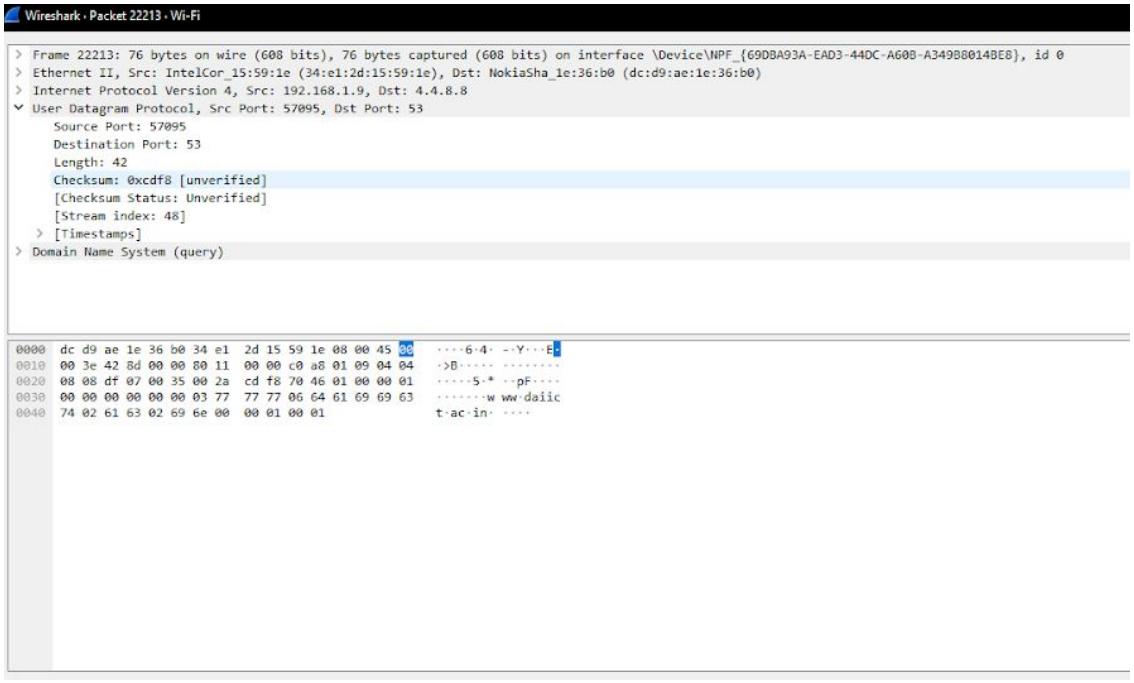
```
zoomva193-123-132-126mmr.cloud.zoom.us
----------------------------------------
Record Name . . . . . : zoomva193-123-132-126mmr.cloud.zoom.us
Record Type . . . . . : 1
Time To Live  . . . . : 84502
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 193.123.132.126
```

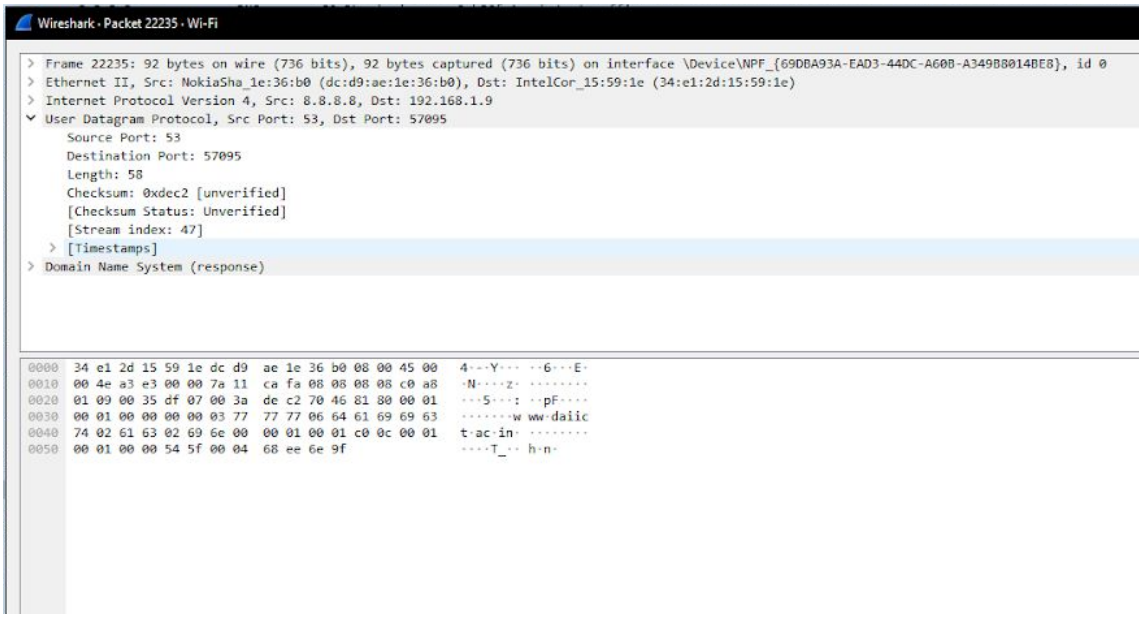
3)

```
C:\Users\vatsal>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

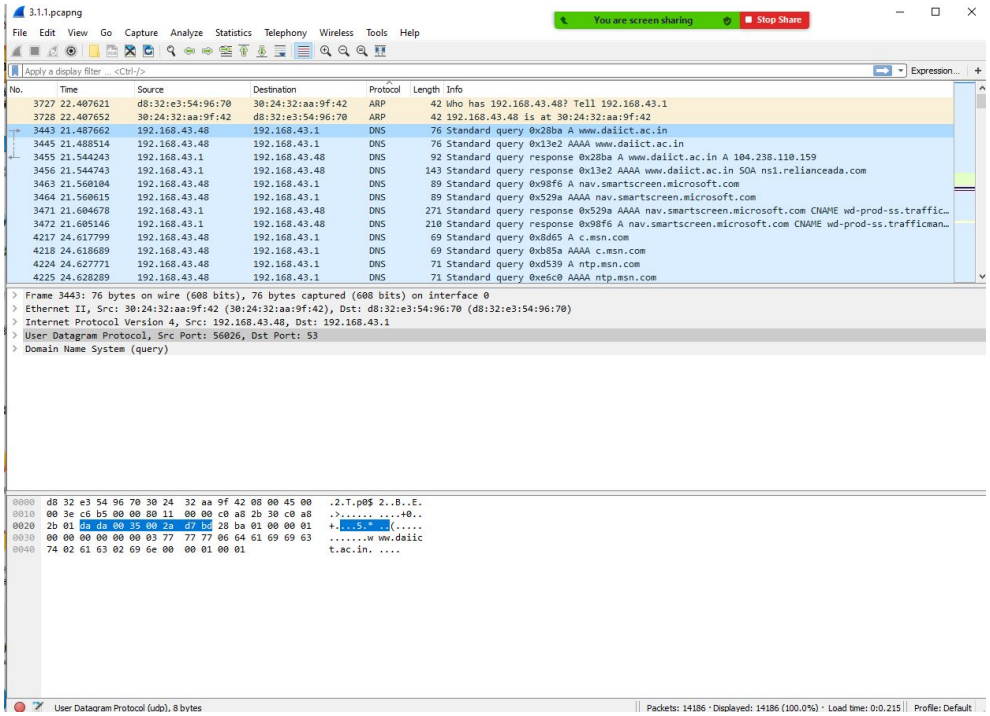
Q3.1)

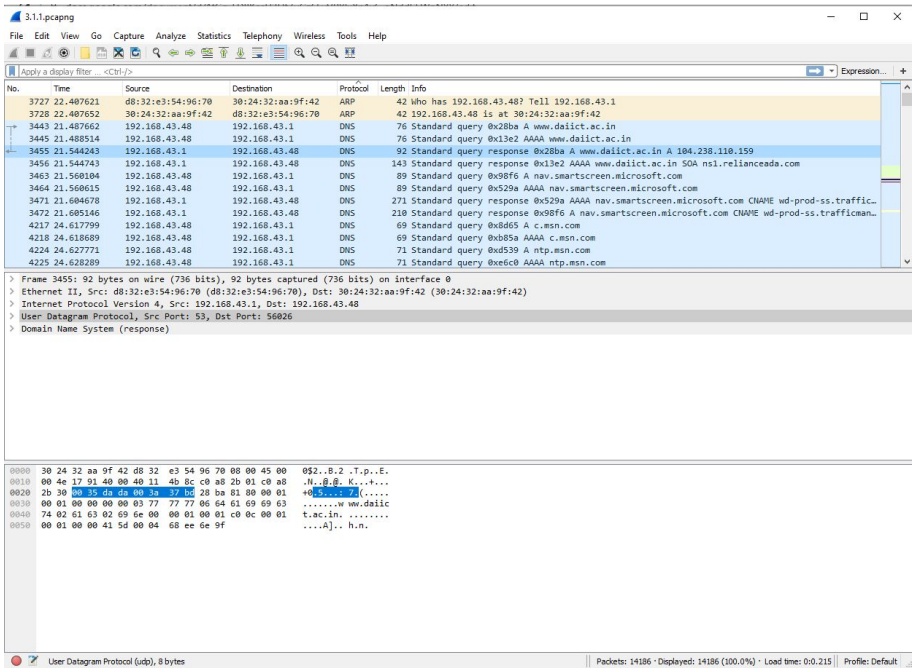
1. Both the query and the response message are sent over UDP.



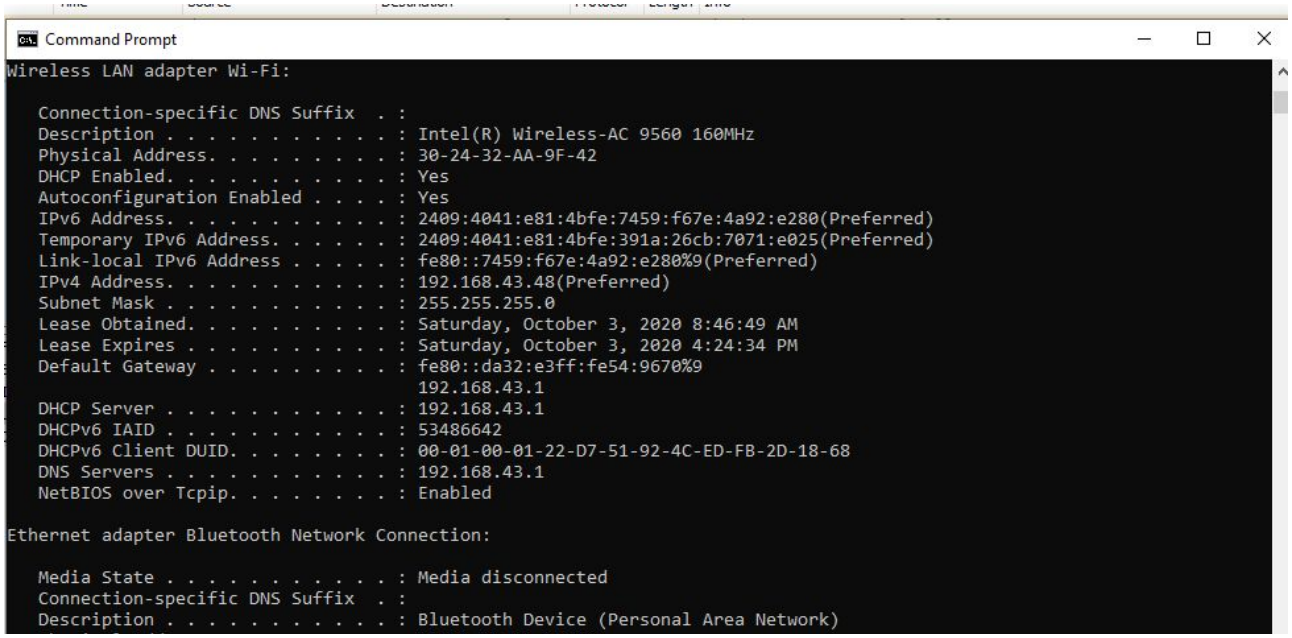



2. Destination port of DNS query message-53
   Source port of DNS response message-53

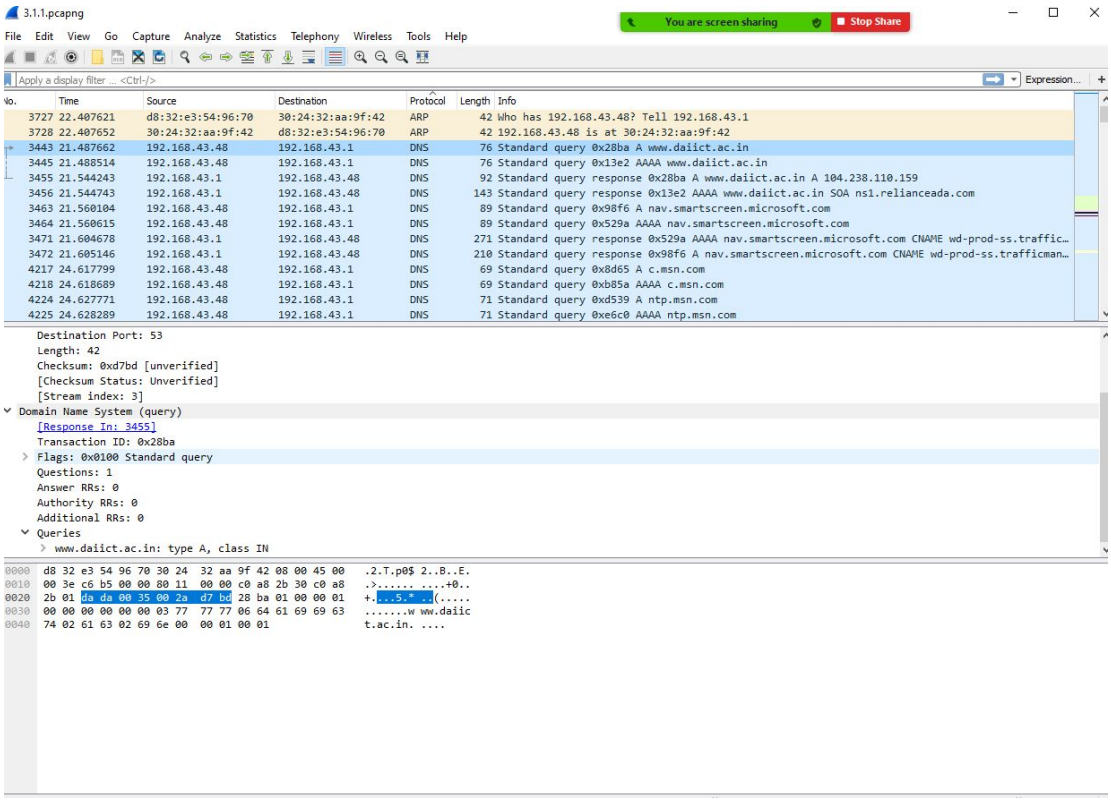


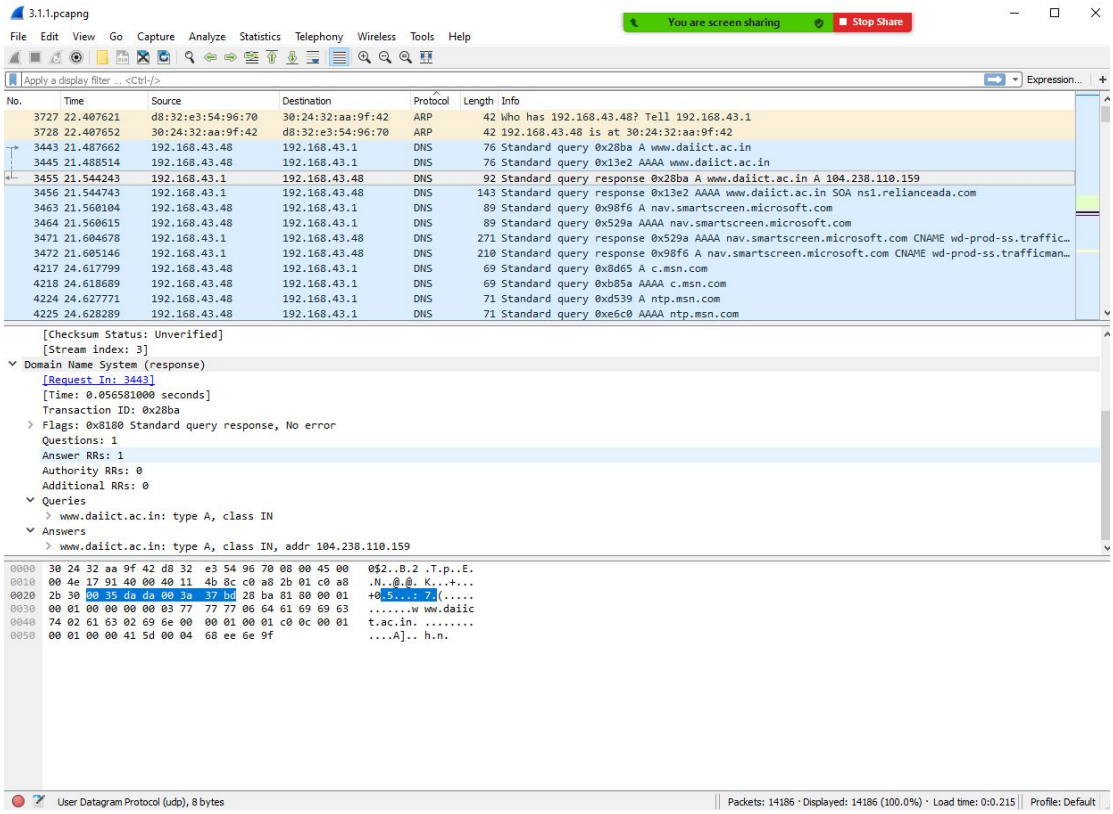
3. The IP address to which the DNS query is sent is the same as that of the IP of the local DNS server.



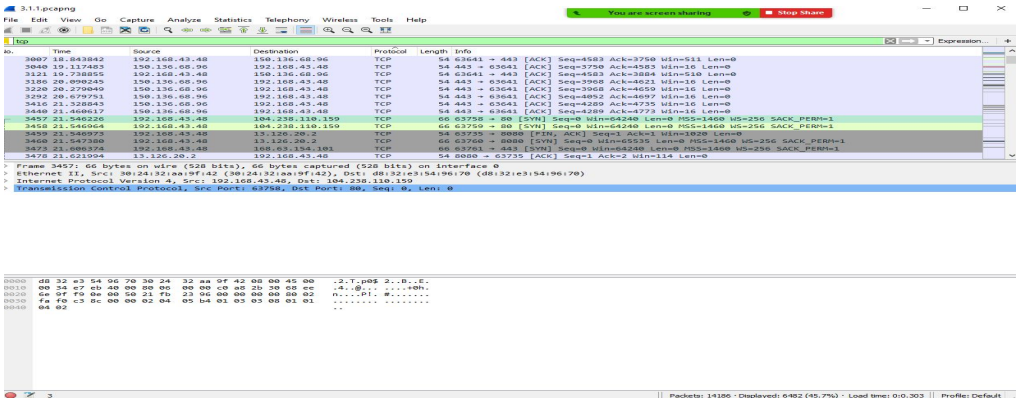

4. The DNS query is of type A and it did not contain any “answers”.



5. The DNS response message shows only 1 answer which contains the address of the website that it was queried for.



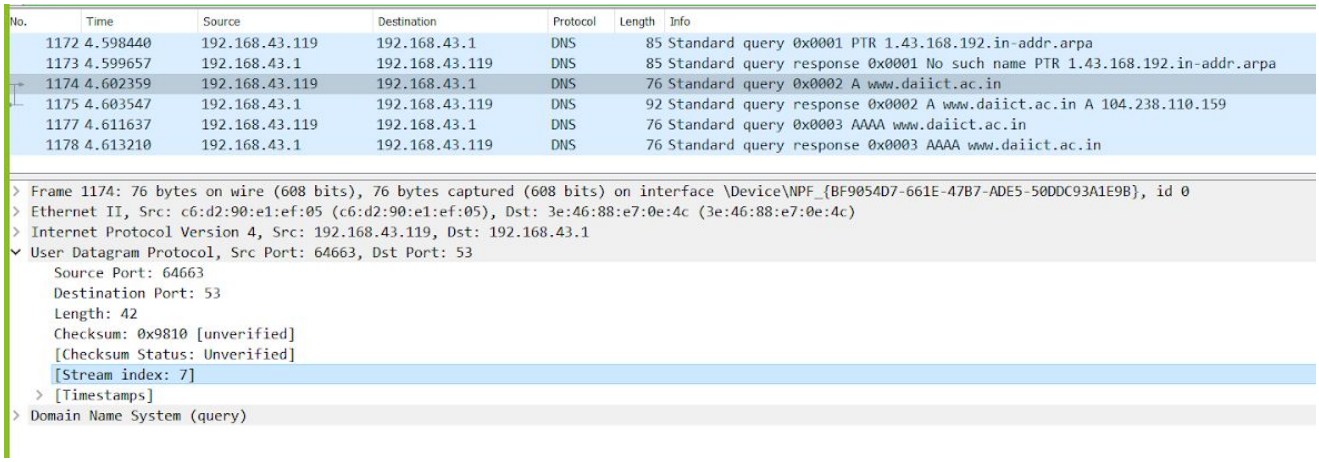

6. The destination IP address of the SYN packet corresponds to the address provided by the DNS response, which is 104.238.110.159



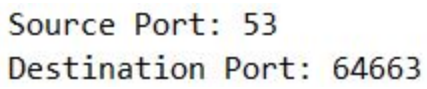

7. Yes, the host issues new DNS queries for each image.

3.2)

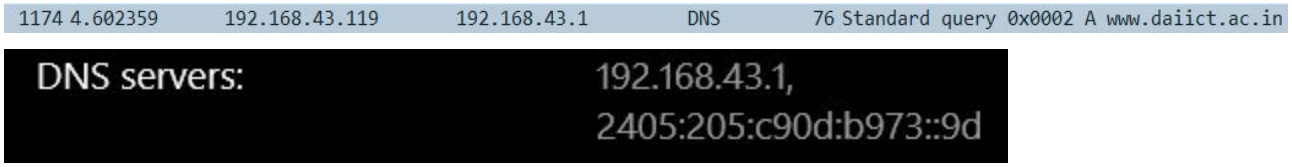
1) Destination Port for DNS Query : 53



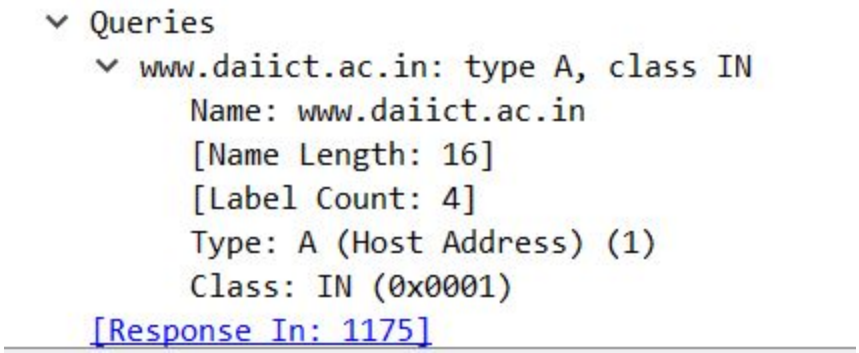

Source Port for DNS message/response: 53




2)The DNS query message was sent to 192.168.43.1 This is the same IP address as the local DNS server.




3)This query was a type A query. It did not contain any “answers”.




4)This DNS response message provided us with only one answer. The answer contains the address of the website that it was queried for.

```
Queries
  > www.daiict.ac.in: type A, class IN
Answers
  v www.daiict.ac.in: type A, class IN, addr 104.238.110.159
      Name: www.daiict.ac.in
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 10273 (2 hours, 51 minutes, 13 seconds)
      Data length: 4
      Address: 104.238.110.159
  [Request In: 1174]
```

3.3)

1) DNS Query is sent to 192.168.43.1
   This is the IP address of our local DNS Server.

```
Source: 192.168.43.119
Destination: 192.168.43.1
```

2)There were multiple query types : A,AAAA,NS. None of them had any answers.

```
Queries
  v daiict.ac.in: type A, class IN
      Name: daiict.ac.in
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 5610]

v daiict.ac.in: type AAAA, class IN
    Name: daiict.ac.in
    [Name Length: 12]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
```

```
Queries
  daiict.ac.in: type NS, class IN
      Name: daiict.ac.in
      [Name Length: 12]
      [Label Count: 3]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
```

3) We received the following response messages. The answers can be seen in the screenshots below.

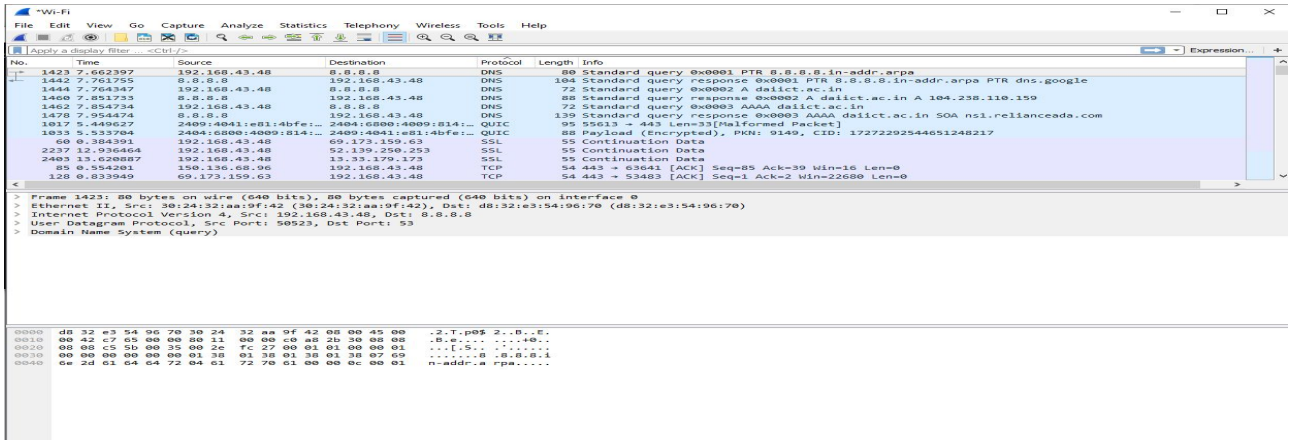
```
  Answers
    daiict.ac.in: type A, class IN, addr 104.238.110.159
        Name: daiict.ac.in
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 9432 (2 hours, 37 minutes, 12 seconds)
        Data length: 4
        Address: 104.238.110.159
    [Request In: 5606]
    [Time: 0.031635000 seconds]

Authoritative nameservers
  daiict.ac.in: type SOA, class IN, mname ns1.relianceada.com
      Name: daiict.ac.in
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 2353 (39 minutes, 13 seconds)
      Data length: 55
      Primary name server: ns1.relianceada.com
      Responsible authority's mailbox: mahesh patil
      Serial Number: 2010090405
      Refresh Interval: 7200 (2 hours)
      Retry Interval: 3600 (1 hour)
      Expire limit: 604800 (7 days)
      Minimum TTL: 21600 (6 hours)
```

```
▾ Answers
    > daiict.ac.in: type NS, class IN, ns ns1.relianceada.com
    > daiict.ac.in: type NS, class IN, ns ns2.relianceada.com
    > daiict.ac.in: type NS, class IN, ns ns3.relianceada.com
    > daiict.ac.in: type NS, class IN, ns ns4.relianceada.com
    > daiict.ac.in: type NS, class IN, ns ns1.exchangenext.net
    > daiict.ac.in: type NS, class IN, ns ns2.exchangenext.net
  [Request In: 8454]
  [Time: 0.031992000 seconds]
```

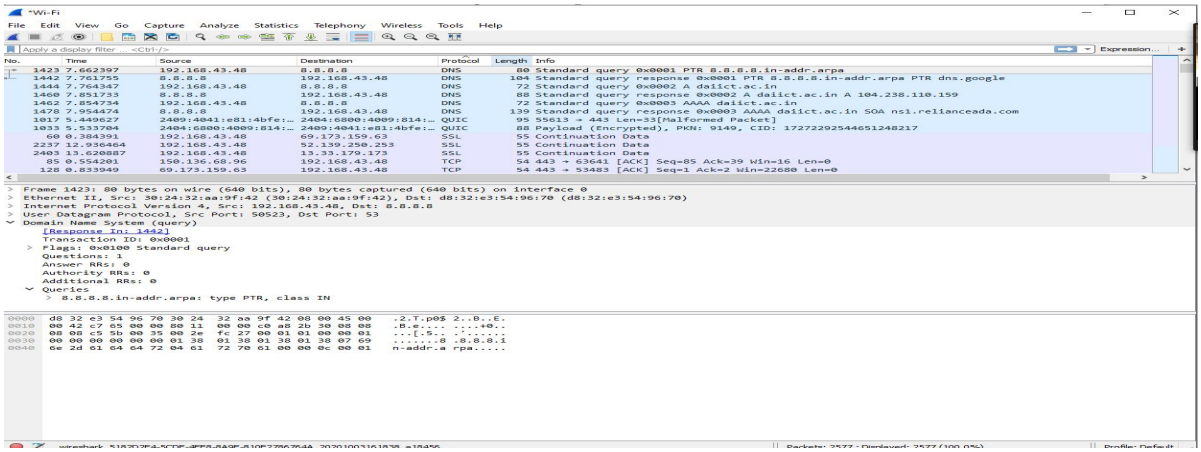
We obtained 6 name servers as can be seen in the above screenshot.

3.4)

1. This time the destination was 8.8.8.8 which is not the same as that of the local DNS server. This time it corresponds to google's public DNS server.




2. The DNS query message is a Domain name pointer, type PTR, and it does not contain any answers as shown in the screenshot.



3. This time we get answers. The DNS response message shows only 1 answer which contains the address of the website that it was queried for.