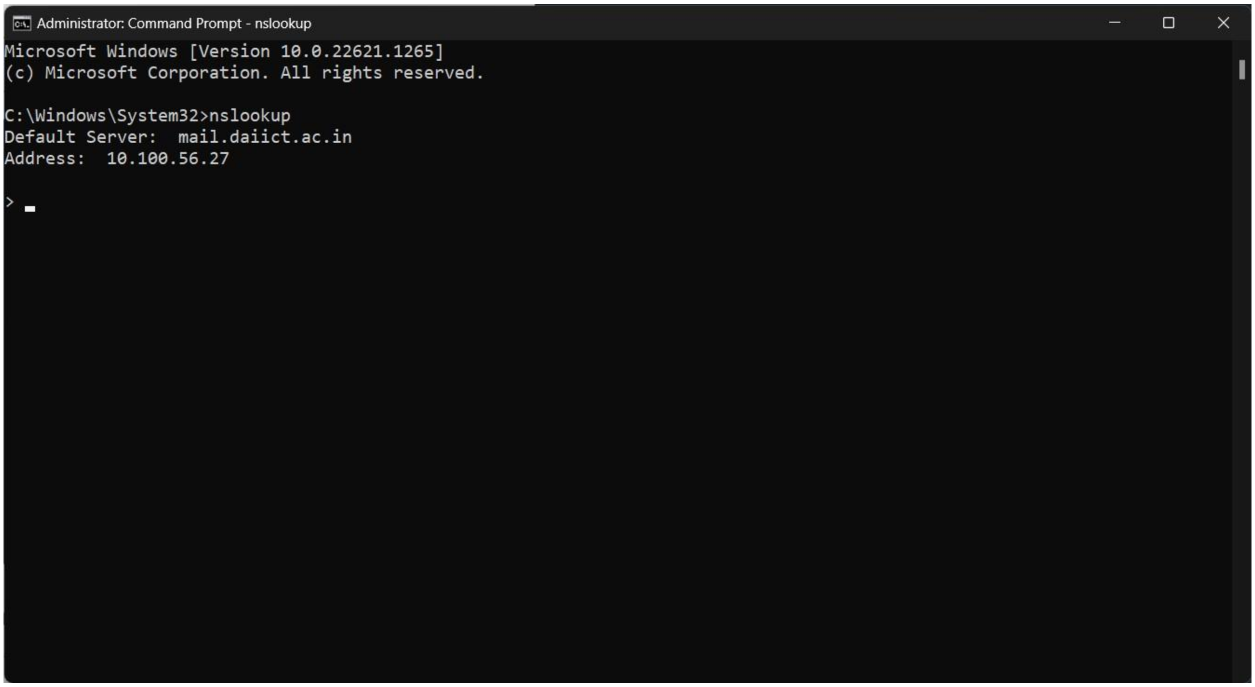
Khushi Mehta
202312125

Lab-4

2.3.1 Exercise 1

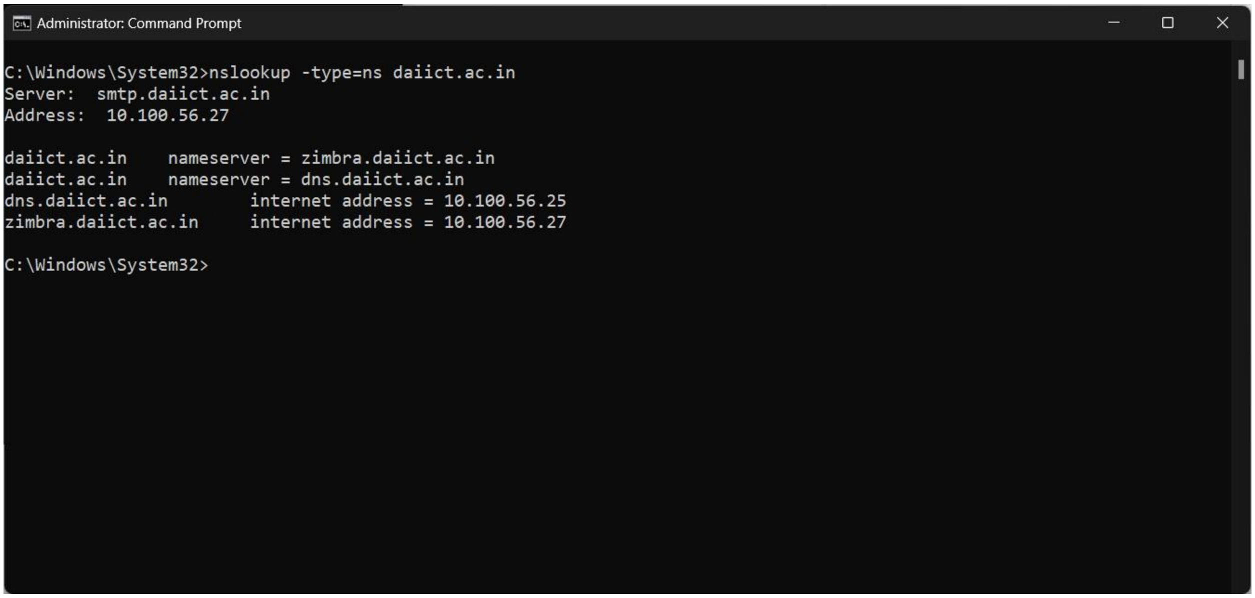
1. Run nslookup to obtain the IP address of daiict.ac.in server.



```
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup
Default Server:  mail.daiict.ac.in
Address:  10.100.56.27

> 
```

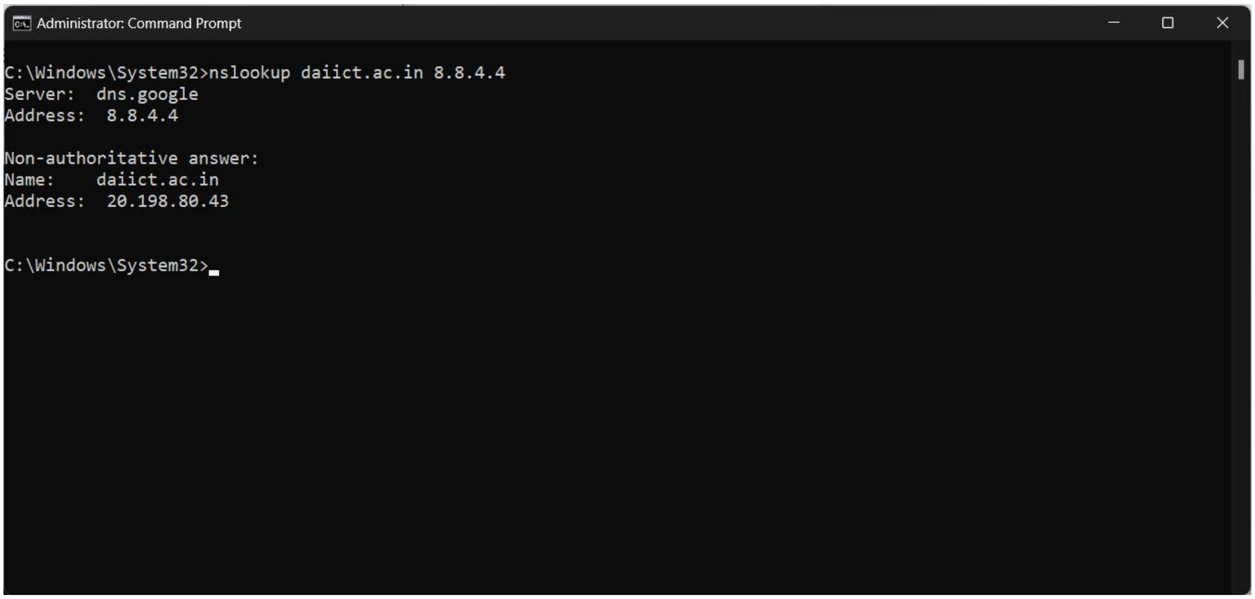
2. Run nslookup to determine the authoritative DNS servers for daiict.ac.in server.

Khushi Mehta
202312125



```
C:\Windows\System32>nslookup -type=ns daiict.ac.in
Server:  smtp.daiict.ac.in
Address:  10.100.56.27

daiict.ac.in    nameserver = zimbra.daiict.ac.in
daiict.ac.in    nameserver = dns.daiict.ac.in
dns.daiict.ac.in        internet address = 10.100.56.25
zimbra.daiict.ac.in     internet address = 10.100.56.27

C:\Windows\System32>
```

3. Run nslookup so that 8.8.4.4 is queried for the mail servers for google.com.

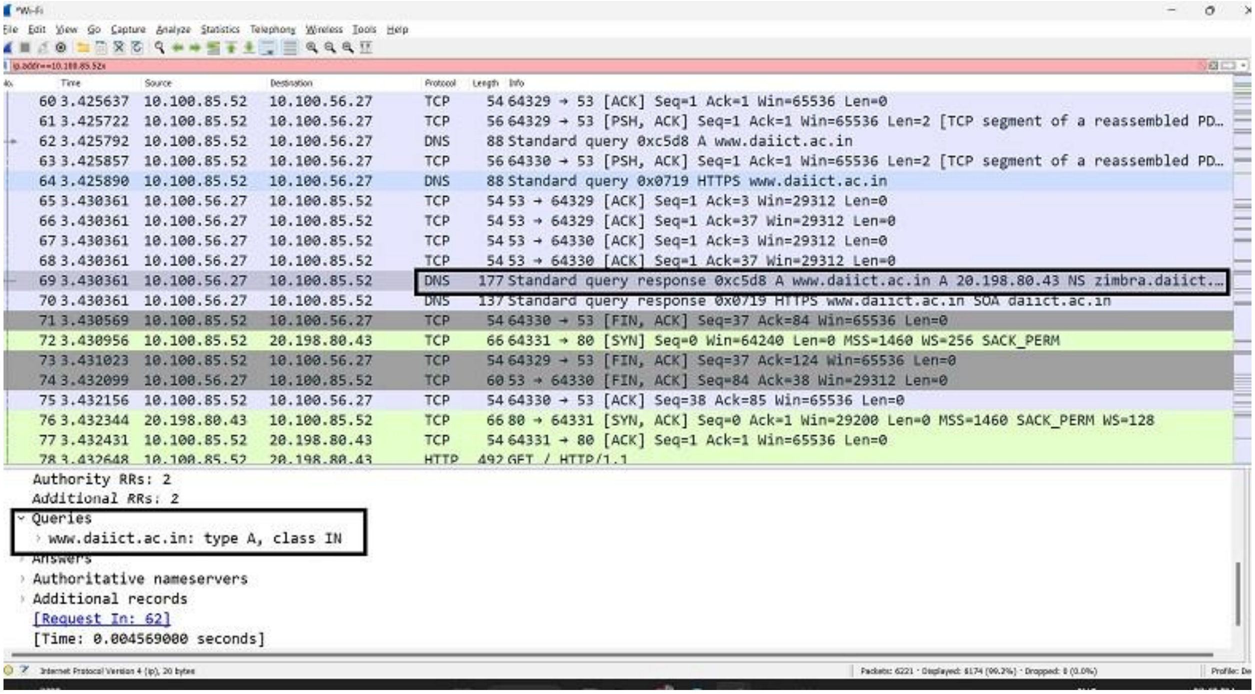


```
C:\Windows\System32>nslookup daiict.ac.in 8.8.4.4
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
Name:    daiict.ac.in
Address:  20.198.80.43


C:\Windows\System32>
```

Khushi Mehta
202312125

2.3.2 Exercise 2: DNS query from browser

1. Locate the DNS query and response messages. Are they sent over UDPor TCP?

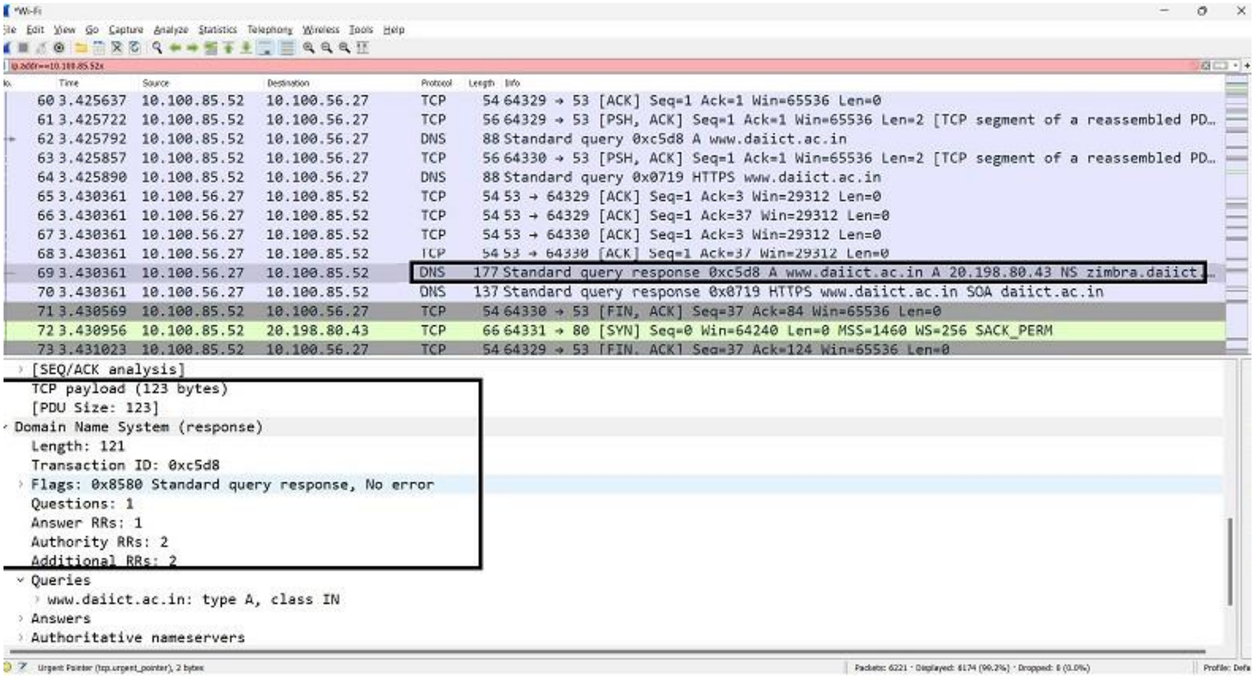

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.100.85.52
No. Time Source Destination Protocol Length Info

```
 60 3.425637 10.100.85.52  10.100.56.27  TCP   54 64329 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 61 3.425722 10.100.85.52  10.100.56.27  TCP   56 64329 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PD…
 62 3.425792 10.100.85.52  10.100.56.27  DNS   88 Standard query 0xc5d8 A www.daiict.ac.in
 63 3.425857 10.100.85.52  10.100.56.27  TCP   56 64330 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PD…
 64 3.425890 10.100.85.52  10.100.56.27  DNS   88 Standard query 0x0719 HTTPS www.daiict.ac.in
 65 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64329 [ACK] Seq=1 Ack=3 Win=29312 Len=0
 66 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64329 [ACK] Seq=1 Ack=37 Win=29312 Len=0
 67 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64330 [ACK] Seq=1 Ack=3 Win=29312 Len=0
 68 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64330 [ACK] Seq=1 Ack=37 Win=29312 Len=0
 69 3.430361 10.100.56.27  10.100.85.52  DNS  177 Standard query response 0xc5d8 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict…
 70 3.430361 10.100.56.27  10.100.85.52  DNS  137 Standard query response 0x0719 HTTPS www.daiict.ac.in SOA daiict.ac.in
 71 3.430569 10.100.85.52  10.100.56.27  TCP   54 64330 → 53 [FIN, ACK] Seq=37 Ack=84 Win=65536 Len=0
 72 3.430956 10.100.85.52  20.198.80.43  TCP   66 64331 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 73 3.431023 10.100.85.52  10.100.56.27  TCP   54 64329 → 53 [FIN, ACK] Seq=37 Ack=124 Win=65536 Len=0
 74 3.432099 10.100.56.27  10.100.85.52  TCP   60 53 → 64330 [FIN, ACK] Seq=84 Ack=38 Win=29312 Len=0
 75 3.432156 10.100.85.52  10.100.56.27  TCP   54 64330 → 53 [ACK] Seq=38 Ack=85 Win=65536 Len=0
 76 3.432344 20.198.80.43  10.100.85.52  TCP   66 80 → 64331 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 77 3.432431 10.100.85.52  20.198.80.43  TCP   54 64331 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 78 3.432648 10.100.85.52  20.198.80.43  HTTP 492 GET / HTTP/1.1
```

```
    Authority RRs: 2
    Additional RRs: 2
  ˅ Queries
    › www.daiict.ac.in: type A, class IN
  › Answers
  › Authoritative nameservers
  › Additional records
    [Request In: 62]
    [Time: 0.004569000 seconds]
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 6221 · Displayed: 6174 (99.2%) · Dropped: 0 (0.0%)
Profile: De

Response:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.100.85.52
No. Time Source Destination Protocol Length Info

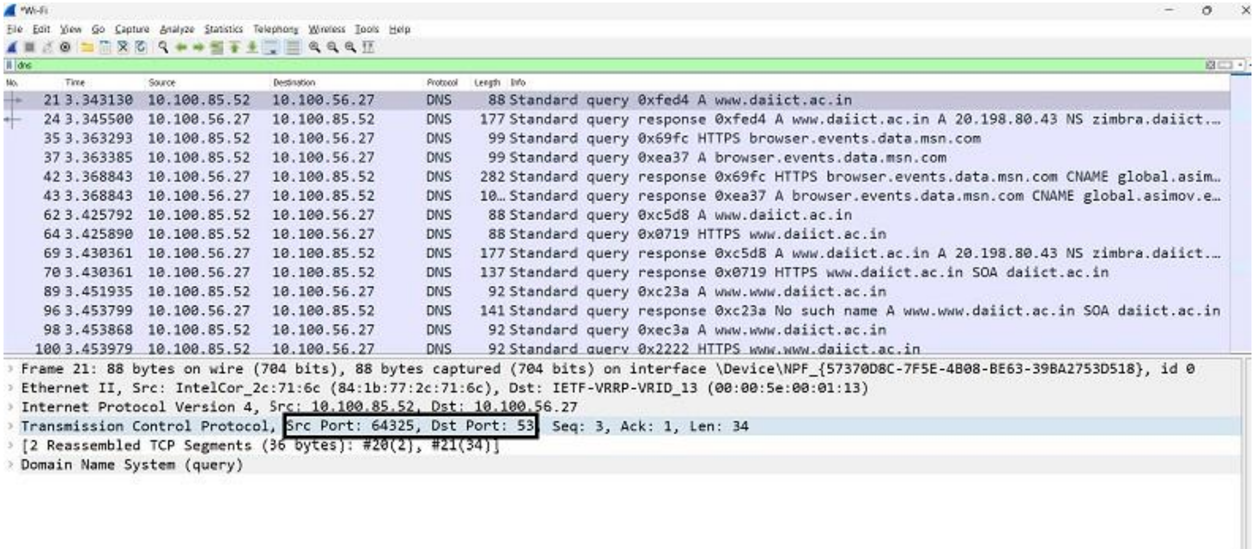
```
 60 3.425637 10.100.85.52  10.100.56.27  TCP   54 64329 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 61 3.425722 10.100.85.52  10.100.56.27  TCP   56 64329 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PD…
 62 3.425792 10.100.85.52  10.100.56.27  DNS   88 Standard query 0xc5d8 A www.daiict.ac.in
 63 3.425857 10.100.85.52  10.100.56.27  TCP   56 64330 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PD…
 64 3.425890 10.100.85.52  10.100.56.27  DNS   88 Standard query 0x0719 HTTPS www.daiict.ac.in
 65 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64329 [ACK] Seq=1 Ack=3 Win=29312 Len=0
 66 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64329 [ACK] Seq=1 Ack=37 Win=29312 Len=0
 67 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64330 [ACK] Seq=1 Ack=3 Win=29312 Len=0
 68 3.430361 10.100.56.27  10.100.85.52  TCP   54 53 → 64330 [ACK] Seq=1 Ack=37 Win=29312 Len=0
 69 3.430361 10.100.56.27  10.100.85.52  DNS  177 Standard query response 0xc5d8 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.…
 70 3.430361 10.100.56.27  10.100.85.52  DNS  137 Standard query response 0x0719 HTTPS www.daiict.ac.in SOA daiict.ac.in
 71 3.430569 10.100.85.52  10.100.56.27  TCP   54 64330 → 53 [FIN, ACK] Seq=37 Ack=84 Win=65536 Len=0
 72 3.430956 10.100.85.52  20.198.80.43  TCP   66 64331 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 73 3.431023 10.100.85.52  10.100.56.27  TCP   54 64329 → 53 [FIN, ACK] Seq=37 Ack=124 Win=65536 Len=0
```

```
  › [SEQ/ACK analysis]
    TCP payload (123 bytes)
    [PDU Size: 123]
˅ Domain Name System (response)
    Length: 121
    Transaction ID: 0xc5d8
  › Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ˅ Queries
    › www.daiict.ac.in: type A, class IN
  › Answers
  › Authoritative nameservers
```

Urgent Pointer (tcp.urgent_pointer), 2 bytes
Packets: 6221 · Displayed: 6174 (99.2%) · Dropped: 0 (0.0%)
Profile: Defa

Khushi Mehta
202312125

2. What is the destination port for the DNS query message? What is thesource port of DNS response message?

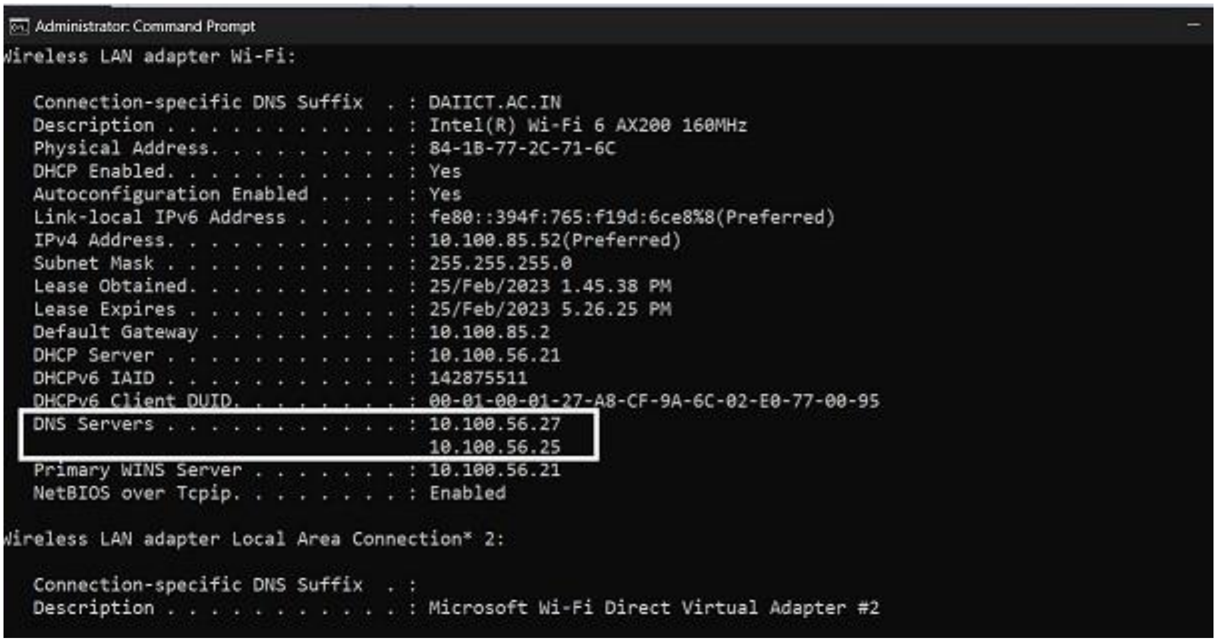


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time       Source         Destination    Protocol Length Info
   21 3.343130   10.100.85.52   10.100.56.27   DNS       88 Standard query 0xfed4 A www.daiict.ac.in
   24 3.345500   10.100.56.27   10.100.85.52   DNS      177 Standard query response 0xfed4 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.…
   35 3.363293   10.100.85.52   10.100.56.27   DNS       99 Standard query 0x69fc HTTPS browser.events.data.msn.com
   37 3.363385   10.100.85.52   10.100.56.27   DNS       99 Standard query 0xea37 A browser.events.data.msn.com
   42 3.368843   10.100.56.27   10.100.85.52   DNS      282 Standard query response 0x69fc HTTPS browser.events.data.msn.com CNAME global.asim…
   43 3.368843   10.100.56.27   10.100.85.52   DNS      10… Standard query response 0xea37 A browser.events.data.msn.com CNAME global.asimov.e…
   62 3.425792   10.100.85.52   10.100.56.27   DNS       88 Standard query 0xc5d8 A www.daiict.ac.in
   64 3.425890   10.100.85.52   10.100.56.27   DNS       88 Standard query 0x0719 HTTPS www.daiict.ac.in
   69 3.430361   10.100.56.27   10.100.85.52   DNS      177 Standard query response 0xc5d8 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.…
   70 3.430361   10.100.56.27   10.100.85.52   DNS      137 Standard query response 0x0719 HTTPS www.daiict.ac.in SOA daiict.ac.in
   89 3.451935   10.100.85.52   10.100.56.27   DNS       92 Standard query 0xc23a A www.www.daiict.ac.in
   96 3.453799   10.100.56.27   10.100.85.52   DNS      141 Standard query response 0xc23a No such name A www.www.daiict.ac.in SOA daiict.ac.in
   98 3.453868   10.100.85.52   10.100.56.27   DNS       92 Standard query 0xec3a A www.www.daiict.ac.in
  100 3.453979   10.100.85.52   10.100.56.27   DNS       92 Standard query 0x2222 HTTPS www.www.daiict.ac.in

> Frame 21: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{57370D8C-7F5E-4B08-BE63-39BA2753D518}, id 0
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 10.100.56.27
> Transmission Control Protocol, Src Port: 64325, Dst Port: 53, Seq: 3, Ack: 1, Len: 34
> [2 Reassembled TCP Segments (36 bytes): #20(2), #21(34)]
> Domain Name System (query)
```

3. To what IP address is the DNS query message sent? Use ipconfig todetermine the IP address of your local DNS server. Are these two IP addresses the same?

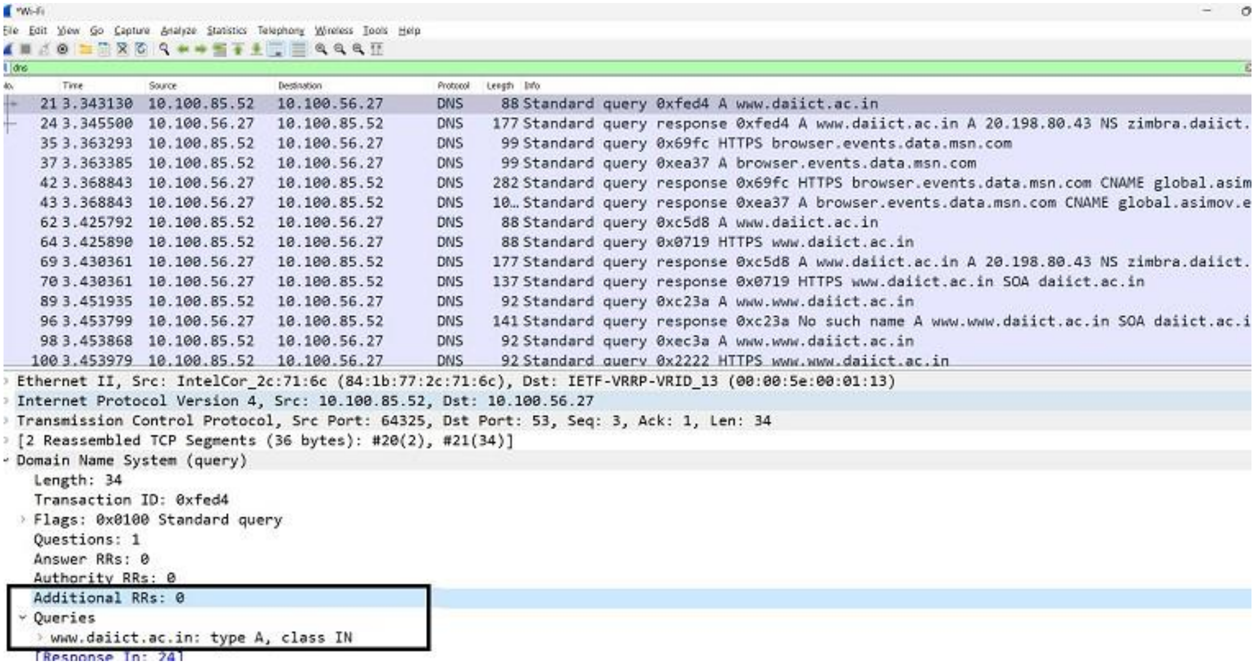
-> It is sen to 10.100.56.27 which is one of my dns server's address



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : DAIICT.AC.IN
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
   Physical Address. . . . . . . . . : 84-1B-77-2C-71-6C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::394f:765:f19d:6ce8%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.100.85.52(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 25/Feb/2023 1.45.38 PM
   Lease Expires . . . . . . . . . . : 25/Feb/2023 5.26.25 PM
   Default Gateway . . . . . . . . . : 10.100.85.2
   DHCP Server . . . . . . . . . . . : 10.100.56.21
   DHCPv6 IAID . . . . . . . . . . . : 142875511
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-A8-CF-9A-6C-02-E0-77-00-95
   DNS Servers . . . . . . . . . . . : 10.100.56.27
                                       10.100.56.25
   Primary WINS Server . . . . . . . : 10.100.56.21
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
```

4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Khushi Mehta
202312125

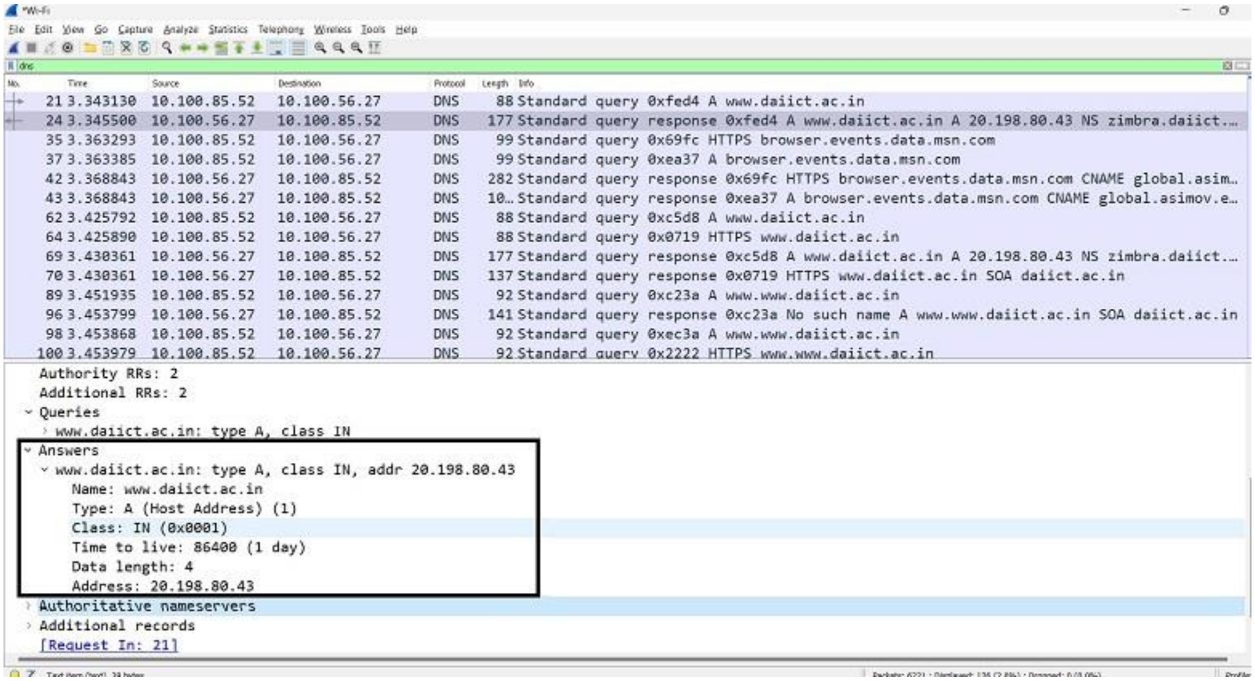

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time      Source        Destination   Protocol Length Info
  21 3.343130  10.100.85.52  10.100.56.27  DNS        88 Standard query 0xfed4 A www.daiict.ac.in
  24 3.345500  10.100.56.27  10.100.85.52  DNS       177 Standard query response 0xfed4 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.
  35 3.363293  10.100.85.52  10.100.56.27  DNS        99 Standard query 0x69fc HTTPS browser.events.data.msn.com
  37 3.363385  10.100.85.52  10.100.56.27  DNS        99 Standard query 0xea37 A browser.events.data.msn.com
  42 3.368843  10.100.56.27  10.100.85.52  DNS       282 Standard query response 0x69fc HTTPS browser.events.data.msn.com CNAME global.asim
  43 3.368843  10.100.56.27  10.100.85.52  DNS       10… Standard query response 0xea37 A browser.events.data.msn.com CNAME global.asimov.e
  62 3.425792  10.100.85.52  10.100.56.27  DNS        88 Standard query 0xc5d8 A www.daiict.ac.in
  64 3.425890  10.100.85.52  10.100.56.27  DNS        88 Standard query 0x0719 HTTPS www.daiict.ac.in
  69 3.430361  10.100.56.27  10.100.85.52  DNS       177 Standard query response 0xc5d8 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.
  70 3.430361  10.100.56.27  10.100.85.52  DNS       137 Standard query response 0x0719 HTTPS www.daiict.ac.in SOA daiict.ac.in
  89 3.451935  10.100.85.52  10.100.56.27  DNS        92 Standard query 0xc23a A www.www.daiict.ac.in
  96 3.453799  10.100.56.27  10.100.85.52  DNS       141 Standard query response 0xc23a No such name A www.www.daiict.ac.in SOA daiict.ac.i
  98 3.453868  10.100.85.52  10.100.56.27  DNS        92 Standard query 0xec3a A www.www.daiict.ac.in
 100 3.453979  10.100.85.52  10.100.56.27  DNS        92 Standard query 0x2222 HTTPS www.www.daiict.ac.in
```

```
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 10.100.56.27
> Transmission Control Protocol, Src Port: 64325, Dst Port: 53, Seq: 3, Ack: 1, Len: 34
> [2 Reassembled TCP Segments (36 bytes): #20(2), #21(34)]
v Domain Name System (query)
    Length: 34
    Transaction ID: 0xfed4
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.daiict.ac.in: type A, class IN
    [Response In: 24]
```

5. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

-> There were 1 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

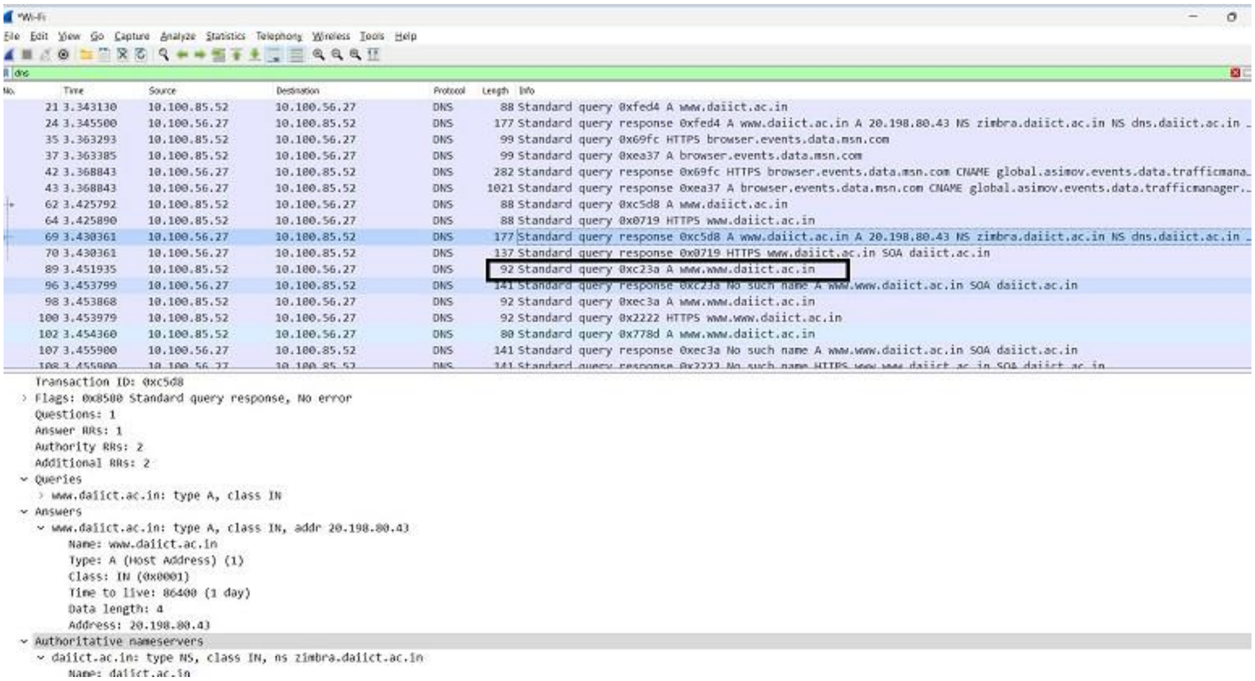
```
No.  Time      Source        Destination   Protocol Length Info
  21 3.343130  10.100.85.52  10.100.56.27  DNS        88 Standard query 0xfed4 A www.daiict.ac.in
  24 3.345500  10.100.56.27  10.100.85.52  DNS       177 Standard query response 0xfed4 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.…
  35 3.363293  10.100.85.52  10.100.56.27  DNS        99 Standard query 0x69fc HTTPS browser.events.data.msn.com
  37 3.363385  10.100.85.52  10.100.56.27  DNS        99 Standard query 0xea37 A browser.events.data.msn.com
  42 3.368843  10.100.56.27  10.100.85.52  DNS       282 Standard query response 0x69fc HTTPS browser.events.data.msn.com CNAME global.asim…
  43 3.368843  10.100.56.27  10.100.85.52  DNS       10… Standard query response 0xea37 A browser.events.data.msn.com CNAME global.asimov.e…
  62 3.425792  10.100.85.52  10.100.56.27  DNS        88 Standard query 0xc5d8 A www.daiict.ac.in
  64 3.425890  10.100.85.52  10.100.56.27  DNS        88 Standard query 0x0719 HTTPS www.daiict.ac.in
  69 3.430361  10.100.56.27  10.100.85.52  DNS       177 Standard query response 0xc5d8 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.…
  70 3.430361  10.100.56.27  10.100.85.52  DNS       137 Standard query response 0x0719 HTTPS www.daiict.ac.in SOA daiict.ac.in
  89 3.451935  10.100.85.52  10.100.56.27  DNS        92 Standard query 0xc23a A www.www.daiict.ac.in
  96 3.453799  10.100.56.27  10.100.85.52  DNS       141 Standard query response 0xc23a No such name A www.www.daiict.ac.in SOA daiict.ac.in
  98 3.453868  10.100.85.52  10.100.56.27  DNS        92 Standard query 0xec3a A www.www.daiict.ac.in
 100 3.453979  10.100.85.52  10.100.56.27  DNS        92 Standard query 0x2222 HTTPS www.www.daiict.ac.in
```

```
    Authority RRs: 2
    Additional RRs: 2
  v Queries
    > www.daiict.ac.in: type A, class IN
  v Answers
    v www.daiict.ac.in: type A, class IN, addr 20.198.80.43
        Name: www.daiict.ac.in
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 86400 (1 day)
        Data length: 4
        Address: 20.198.80.43
  > Authoritative nameservers
  > Additional records
    [Request In: 21]
```

Khushi Mehta
202312125

6. Consider the subsequent TCP SYN packet sent by your host. Does thedestination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

-> The first SYN packet was sent to 20.198.80.43 which corresponds to the first IP address provided in the DNS response message.



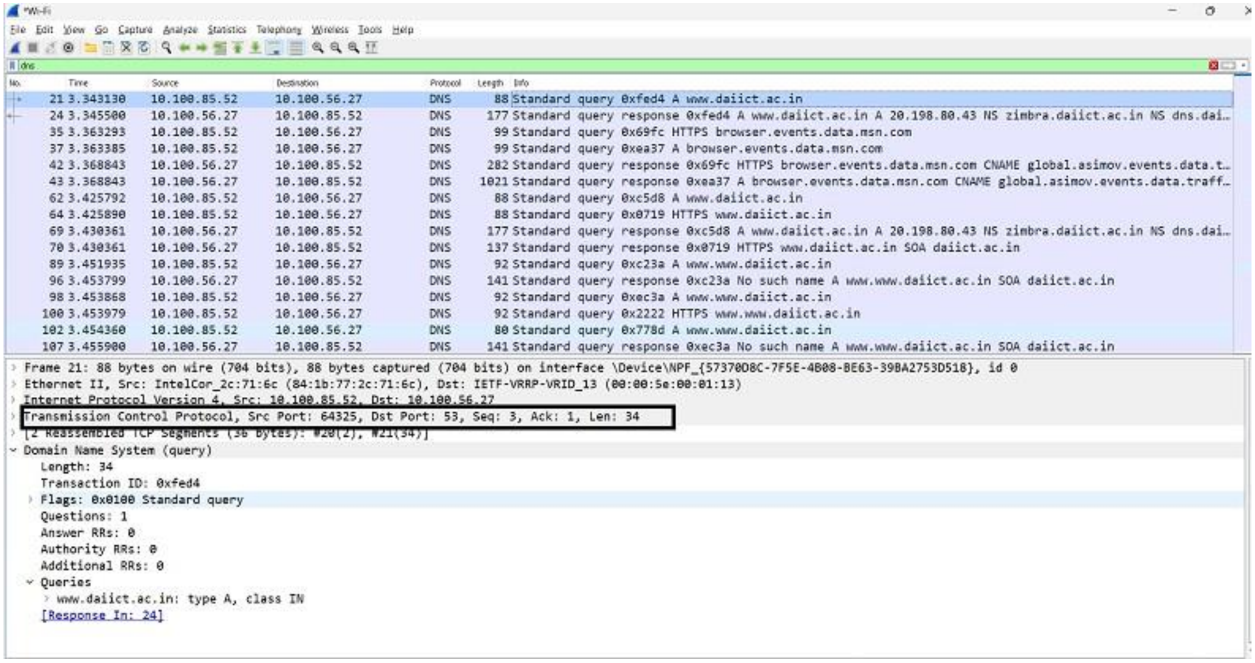
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time       Source         Destination    Protocol Length Info
   21 3.343130   10.100.85.52   10.100.56.27   DNS        88 Standard query 0xfed4 A www.daiict.ac.in
   24 3.345500   10.100.56.27   10.100.85.52   DNS       177 Standard query response 0xfed4 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.ac.in NS dns.daiict.ac.in …
   35 3.363293   10.100.85.52   10.100.56.27   DNS        99 Standard query 0x69fc HTTPS browser.events.data.msn.com
   37 3.363385   10.100.85.52   10.100.56.27   DNS        99 Standard query 0xea37 A browser.events.data.msn.com
   42 3.368843   10.100.56.27   10.100.85.52   DNS       282 Standard query response 0x69fc HTTPS browser.events.data.msn.com CNAME global.asimov.events.data.trafficmana…
   43 3.368843   10.100.56.27   10.100.85.52   DNS      1021 Standard query response 0xea37 A browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.…
   62 3.425792   10.100.85.52   10.100.56.27   DNS        88 Standard query 0xc5d8 A www.daiict.ac.in
   64 3.425890   10.100.85.52   10.100.56.27   DNS        88 Standard query 0x0719 HTTPS www.daiict.ac.in
   69 3.430361   10.100.56.27   10.100.85.52   DNS       177 Standard query response 0xc5d8 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.ac.in NS dns.daiict.ac.in …
   70 3.430361   10.100.56.27   10.100.85.52   DNS       137 Standard query response 0x0719 HTTPS www.daiict.ac.in SOA daiict.ac.in
   89 3.451935   10.100.85.52   10.100.56.27   DNS        92 Standard query 0xc23a A www.www.daiict.ac.in
   96 3.453799   10.100.56.27   10.100.85.52   DNS       141 Standard query response 0xc23a No such name A www.www.daiict.ac.in SOA daiict.ac.in
   98 3.453868   10.100.85.52   10.100.56.27   DNS        92 Standard query 0xec3a A www.www.daiict.ac.in
  100 3.453979   10.100.85.52   10.100.56.27   DNS        92 Standard query 0x2222 HTTPS www.www.daiict.ac.in
  102 3.454360   10.100.85.52   10.100.56.27   DNS        80 Standard query 0x778d A www.www.daiict.ac.in
  107 3.455900   10.100.56.27   10.100.85.52   DNS       141 Standard query response 0xec3a No such name A www.www.daiict.ac.in SOA daiict.ac.in
  108 3.455900   10.100.56.27   10.100.85.52   DNS       141 Standard query response 0x2222 No such name HTTPS www.www.daiict.ac.in SOA daiict.ac.in
```

```
    Transaction ID: 0xc5d8
  > Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ˅ Queries
    > www.daiict.ac.in: type A, class IN
  ˅ Answers
    ˅ www.daiict.ac.in: type A, class IN, addr 20.198.80.43
          Name: www.daiict.ac.in
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 86400 (1 day)
          Data length: 4
          Address: 20.198.80.43
  ˅ Authoritative nameservers
    ˅ daiict.ac.in: type NS, class IN, ns zimbra.daiict.ac.in
          Name: daiict.ac.in
```

7. This web page contains images. Before retrieving each image, doesyour host issue new DNS queries?

Khushi Mehta
202312125


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.   Time      Source         Destination    Protocol Length Info
   21 3.343130  10.100.85.52   10.100.56.27   DNS        88 Standard query 0xfed4 A www.daiict.ac.in
   24 3.345500  10.100.56.27   10.100.85.52   DNS       177 Standard query response 0xfed4 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.ac.in NS dns.dai…
   35 3.363293  10.100.85.52   10.100.56.27   DNS        99 Standard query 0x69fc HTTPS browser.events.data.msn.com
   37 3.363385  10.100.85.52   10.100.56.27   DNS        99 Standard query 0xea37 A browser.events.data.msn.com
   42 3.368843  10.100.56.27   10.100.85.52   DNS       282 Standard query response 0x69fc HTTPS browser.events.data.msn.com CNAME global.asimov.events.data.t…
   43 3.368843  10.100.56.27   10.100.85.52   DNS      1021 Standard query response 0xea37 A browser.events.data.msn.com CNAME global.asimov.events.data.traff…
   62 3.425792  10.100.85.52   10.100.56.27   DNS        88 Standard query 0xc5d8 A www.daiict.ac.in
   64 3.425890  10.100.85.52   10.100.56.27   DNS        88 Standard query 0x0719 HTTPS www.daiict.ac.in
   69 3.430361  10.100.56.27   10.100.85.52   DNS       177 Standard query response 0xc5d8 A www.daiict.ac.in A 20.198.80.43 NS zimbra.daiict.ac.in NS dns.dai…
   70 3.430361  10.100.56.27   10.100.85.52   DNS       137 Standard query response 0x0719 HTTPS www.daiict.ac.in SOA daiict.ac.in
   89 3.451935  10.100.85.52   10.100.56.27   DNS        92 Standard query 0xc23a A www.www.daiict.ac.in
   96 3.453799  10.100.56.27   10.100.85.52   DNS       141 Standard query response 0xc23a No such name A www.www.daiict.ac.in SOA daiict.ac.in
   98 3.453868  10.100.85.52   10.100.56.27   DNS        92 Standard query 0xec3a A www.www.daiict.ac.in
  100 3.453979  10.100.85.52   10.100.56.27   DNS        92 Standard query 0x2222 HTTPS www.www.daiict.ac.in
  102 3.454360  10.100.85.52   10.100.56.27   DNS        80 Standard query 0x778d A www.www.daiict.ac.in
  107 3.455900  10.100.56.27   10.100.85.52   DNS       141 Standard query response 0xec3a No such name A www.www.daiict.ac.in SOA daiict.ac.in
```

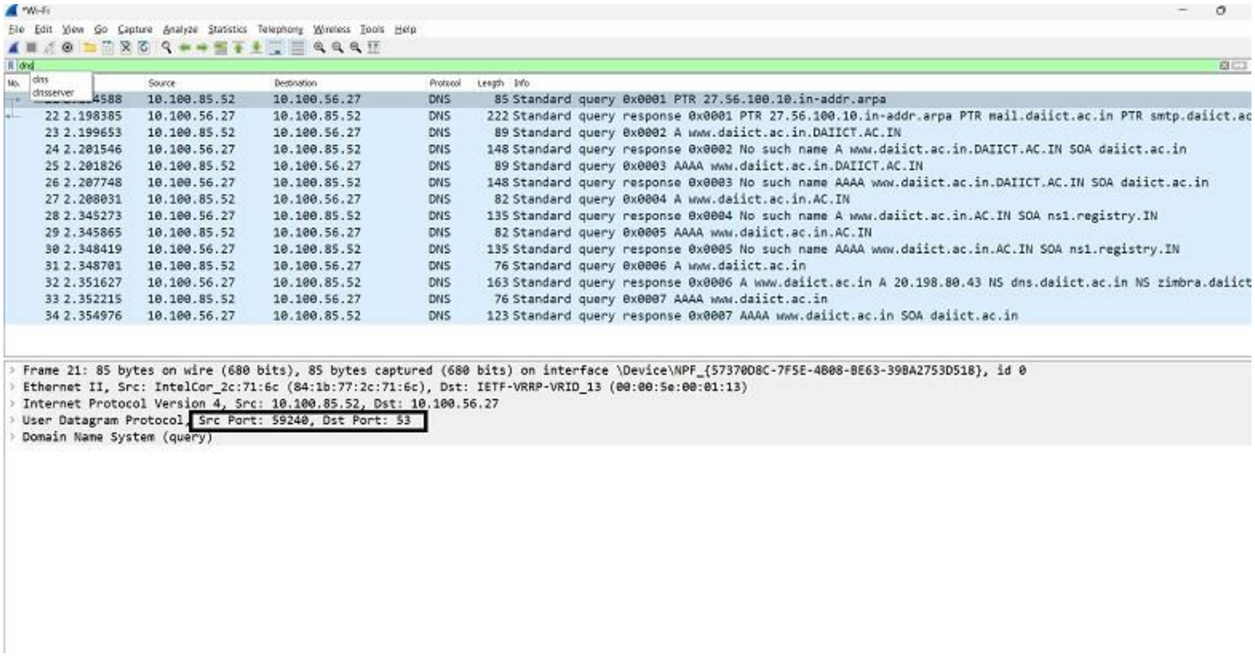
```
> Frame 21: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{57370D8C-7F5E-4B08-BE63-39BA2753D518}, id 0
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 10.100.56.27
> Transmission Control Protocol, Src Port: 64325, Dst Port: 53, Seq: 3, Ack: 1, Len: 34
> [2 Reassembled TCP Segments (36 bytes): #20(2), #21(34)]
v Domain Name System (query)
    Length: 34
    Transaction ID: 0xfed4
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.daiict.ac.in: type A, class IN
    [Response In: 24]
```

Khushi Mehta
202312125

2.3.3 Exercise 3: DNS query using nslookup

1. What is the destination port for the DNS query message? What is thesource port of DNS response message?

-> The destination port of the DNS query is 53 and the source port of the DNS response is 59240.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver
No.
Source
Destination
Protocol
Length
Info

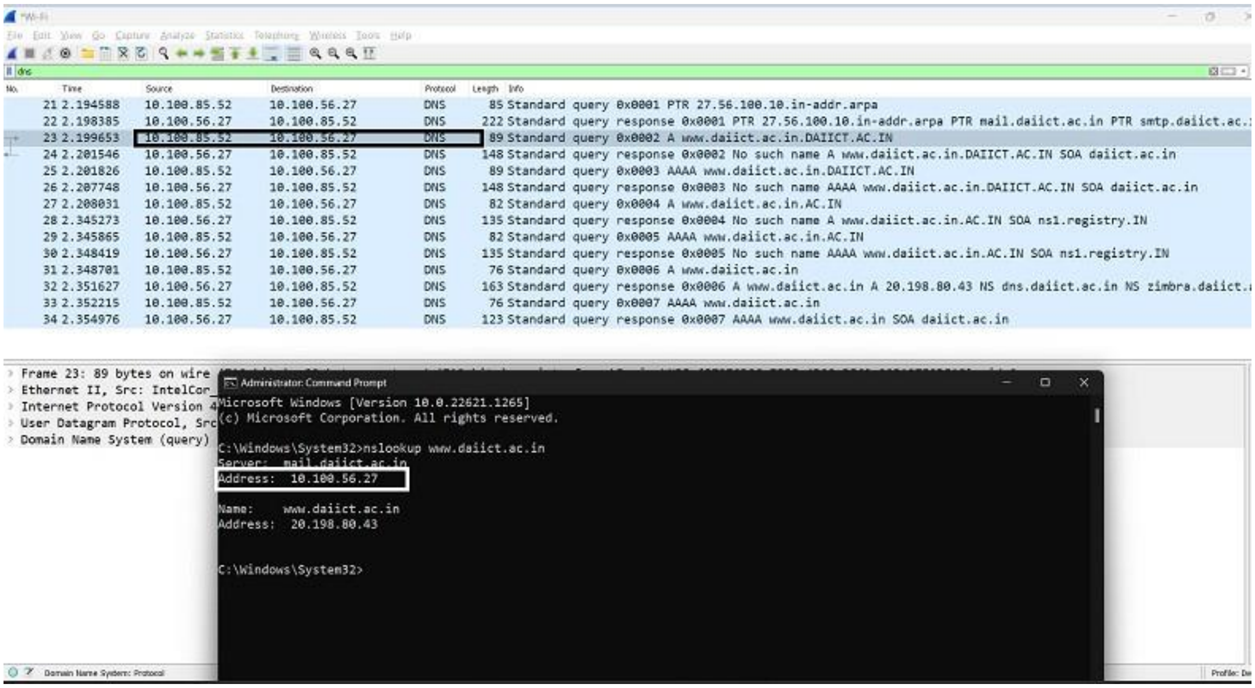
```
      4588  10.100.85.52   10.100.56.27   DNS    85 Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
   22 2.198385  10.100.56.27   10.100.85.52   DNS   222 Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PTR mail.daiict.ac.in PTR smtp.daiict.ac
   23 2.199653  10.100.85.52   10.100.56.27   DNS    89 Standard query 0x0002 A www.daiict.ac.in.DAIICT.AC.IN
   24 2.201546  10.100.56.27   10.100.85.52   DNS   148 Standard query response 0x0002 No such name A www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
   25 2.201826  10.100.85.52   10.100.56.27   DNS    89 Standard query 0x0003 AAAA www.daiict.ac.in.DAIICT.AC.IN
   26 2.207748  10.100.56.27   10.100.85.52   DNS   148 Standard query response 0x0003 No such name AAAA www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
   27 2.208031  10.100.85.52   10.100.56.27   DNS    82 Standard query 0x0004 A www.daiict.ac.in.AC.IN
   28 2.345273  10.100.56.27   10.100.85.52   DNS   135 Standard query response 0x0004 No such name A www.daiict.ac.in.AC.IN SOA ns1.registry.IN
   29 2.345865  10.100.85.52   10.100.56.27   DNS    82 Standard query 0x0005 AAAA www.daiict.ac.in.AC.IN
   30 2.348419  10.100.56.27   10.100.85.52   DNS   135 Standard query response 0x0005 No such name AAAA www.daiict.ac.in.AC.IN SOA ns1.registry.IN
   31 2.348701  10.100.85.52   10.100.56.27   DNS    76 Standard query 0x0006 A www.daiict.ac.in
   32 2.351627  10.100.56.27   10.100.85.52   DNS   163 Standard query response 0x0006 A www.daiict.ac.in A 20.198.80.43 NS dns.daiict.ac.in NS zimbra.daiict
   33 2.352215  10.100.85.52   10.100.56.27   DNS    76 Standard query 0x0007 AAAA www.daiict.ac.in
   34 2.354976  10.100.56.27   10.100.85.52   DNS   123 Standard query response 0x0007 AAAA www.daiict.ac.in SOA daiict.ac.in
```

```
> Frame 21: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{57370D8C-7F5E-4B08-BE63-39BA2753D518}, id 0
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 10.100.56.27
> User Datagram Protocol, Src Port: 59240, Dst Port: 53
> Domain Name System (query)
```

2. To what IP address is the DNS query message sent? Is this the IPaddress of your default local DNS server?

-> Yes. The ip address is of the default local DNS server.

Khushi Mehta
202312125

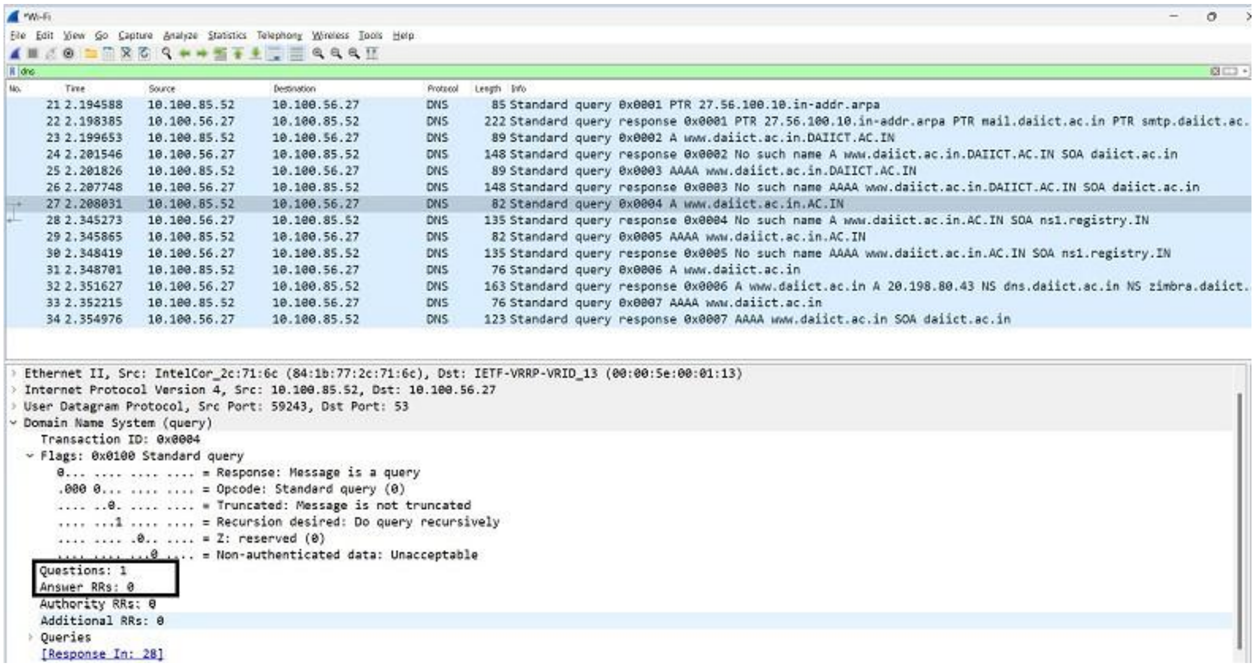

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Domain Name System: Protocol
Profile: De
Administrator: Command Prompt

```
No.   Time        Source         Destination    Protocol Length Info
   21 2.194588    10.100.85.52   10.100.56.27   DNS        85 Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
   22 2.198385    10.100.56.27   10.100.85.52   DNS       222 Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PTR mail.daiict.ac.in PTR smtp.daiict.ac.:
   23 2.199653    10.100.85.52   10.100.56.27   DNS        89 Standard query 0x0002 A www.daiict.ac.in.DAIICT.AC.IN
   24 2.201546    10.100.56.27   10.100.85.52   DNS       148 Standard query response 0x0002 No such name A www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
   25 2.201826    10.100.85.52   10.100.56.27   DNS        89 Standard query 0x0003 AAAA www.daiict.ac.in.DAIICT.AC.IN
   26 2.207748    10.100.56.27   10.100.85.52   DNS       148 Standard query response 0x0003 No such name AAAA www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
   27 2.208031    10.100.85.52   10.100.56.27   DNS        82 Standard query 0x0004 A www.daiict.ac.in.AC.IN
   28 2.345273    10.100.56.27   10.100.85.52   DNS       135 Standard query response 0x0004 No such name A www.daiict.ac.in.AC.IN SOA ns1.registry.IN
   29 2.345865    10.100.85.52   10.100.56.27   DNS        82 Standard query 0x0005 AAAA www.daiict.ac.in.AC.IN
   30 2.348419    10.100.56.27   10.100.85.52   DNS       135 Standard query response 0x0005 No such name AAAA www.daiict.ac.in.AC.IN SOA ns1.registry.IN
   31 2.348701    10.100.85.52   10.100.56.27   DNS        76 Standard query 0x0006 A www.daiict.ac.in
   32 2.351627    10.100.56.27   10.100.85.52   DNS       163 Standard query response 0x0006 A www.daiict.ac.in A 20.198.80.43 NS dns.daiict.ac.in NS zimbra.daiict.a
   33 2.352215    10.100.85.52   10.100.56.27   DNS        76 Standard query 0x0007 AAAA www.daiict.ac.in
   34 2.354976    10.100.56.27   10.100.85.52   DNS       123 Standard query response 0x0007 AAAA www.daiict.ac.in SOA daiict.ac.in
```

```
> Frame 23: 89 bytes on wire
> Ethernet II, Src: IntelCor_
> Internet Protocol Version 4
> User Datagram Protocol, Src
> Domain Name System (query)
```

```
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup www.daiict.ac.in
Server:  mail.daiict.ac.in
Address:  10.100.56.27

Name:    www.daiict.ac.in
Address:  20.198.80.43


C:\Windows\System32>
```

3. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

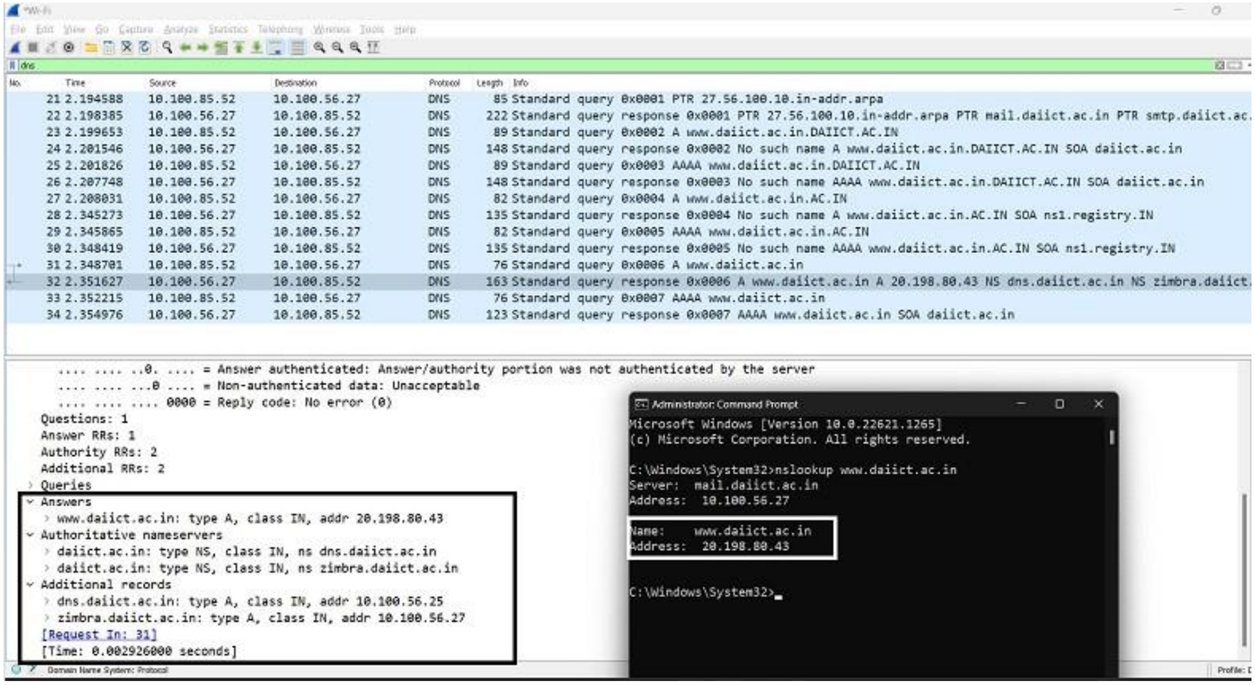

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time        Source         Destination    Protocol Length Info
   21 2.194588    10.100.85.52   10.100.56.27   DNS        85 Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
   22 2.198385    10.100.56.27   10.100.85.52   DNS       222 Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PTR mail.daiict.ac.in PTR smtp.daiict.ac.
   23 2.199653    10.100.85.52   10.100.56.27   DNS        89 Standard query 0x0002 A www.daiict.ac.in.DAIICT.AC.IN
   24 2.201546    10.100.56.27   10.100.85.52   DNS       148 Standard query response 0x0002 No such name A www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
   25 2.201826    10.100.85.52   10.100.56.27   DNS        89 Standard query 0x0003 AAAA www.daiict.ac.in.DAIICT.AC.IN
   26 2.207748    10.100.56.27   10.100.85.52   DNS       148 Standard query response 0x0003 No such name AAAA www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
   27 2.208031    10.100.85.52   10.100.56.27   DNS        82 Standard query 0x0004 A www.daiict.ac.in.AC.IN
   28 2.345273    10.100.56.27   10.100.85.52   DNS       135 Standard query response 0x0004 No such name A www.daiict.ac.in.AC.IN SOA ns1.registry.IN
   29 2.345865    10.100.85.52   10.100.56.27   DNS        82 Standard query 0x0005 AAAA www.daiict.ac.in.AC.IN
   30 2.348419    10.100.56.27   10.100.85.52   DNS       135 Standard query response 0x0005 No such name AAAA www.daiict.ac.in.AC.IN SOA ns1.registry.IN
   31 2.348701    10.100.85.52   10.100.56.27   DNS        76 Standard query 0x0006 A www.daiict.ac.in
   32 2.351627    10.100.56.27   10.100.85.52   DNS       163 Standard query response 0x0006 A www.daiict.ac.in A 20.198.80.43 NS dns.daiict.ac.in NS zimbra.daiict.
   33 2.352215    10.100.85.52   10.100.56.27   DNS        76 Standard query 0x0007 AAAA www.daiict.ac.in
   34 2.354976    10.100.56.27   10.100.85.52   DNS       123 Standard query response 0x0007 AAAA www.daiict.ac.in SOA daiict.ac.in
```

```
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 10.100.56.27
> User Datagram Protocol, Src Port: 59243, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 28]
```

4. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

Khushi Mehta
202312125


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time      Source         Destination    Protocol Length Info
  21 2.194588  10.100.85.52   10.100.56.27   DNS       85 Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
  22 2.198385  10.100.56.27   10.100.85.52   DNS      222 Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PTR mail.daiict.ac.in PTR smtp.daiict.ac.
  23 2.199653  10.100.85.52   10.100.56.27   DNS       89 Standard query 0x0002 A www.daiict.ac.in.DAIICT.AC.IN
  24 2.201546  10.100.56.27   10.100.85.52   DNS      148 Standard query response 0x0002 No such name A www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
  25 2.201826  10.100.85.52   10.100.56.27   DNS       89 Standard query 0x0003 AAAA www.daiict.ac.in.DAIICT.AC.IN
  26 2.207748  10.100.56.27   10.100.85.52   DNS      148 Standard query response 0x0003 No such name AAAA www.daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
  27 2.208031  10.100.85.52   10.100.56.27   DNS       82 Standard query 0x0004 A www.daiict.ac.in.AC.IN
  28 2.345273  10.100.56.27   10.100.85.52   DNS      135 Standard query response 0x0004 No such name A www.daiict.ac.in.AC.IN SOA ns1.registry.IN
  29 2.345865  10.100.85.52   10.100.56.27   DNS       82 Standard query 0x0005 AAAA www.daiict.ac.in.AC.IN
  30 2.348419  10.100.56.27   10.100.85.52   DNS      135 Standard query response 0x0005 No such name AAAA www.daiict.ac.in.AC.IN SOA ns1.registry.IN
  31 2.348701  10.100.85.52   10.100.56.27   DNS       76 Standard query 0x0006 A www.daiict.ac.in
  32 2.351627  10.100.56.27   10.100.85.52   DNS      163 Standard query response 0x0006 A www.daiict.ac.in A 20.198.80.43 NS dns.daiict.ac.in NS zimbra.daiict.
  33 2.352215  10.100.85.52   10.100.56.27   DNS       76 Standard query 0x0007 AAAA www.daiict.ac.in
  34 2.354976  10.100.56.27   10.100.85.52   DNS      123 Standard query response 0x0007 AAAA www.daiict.ac.in SOA daiict.ac.in
```

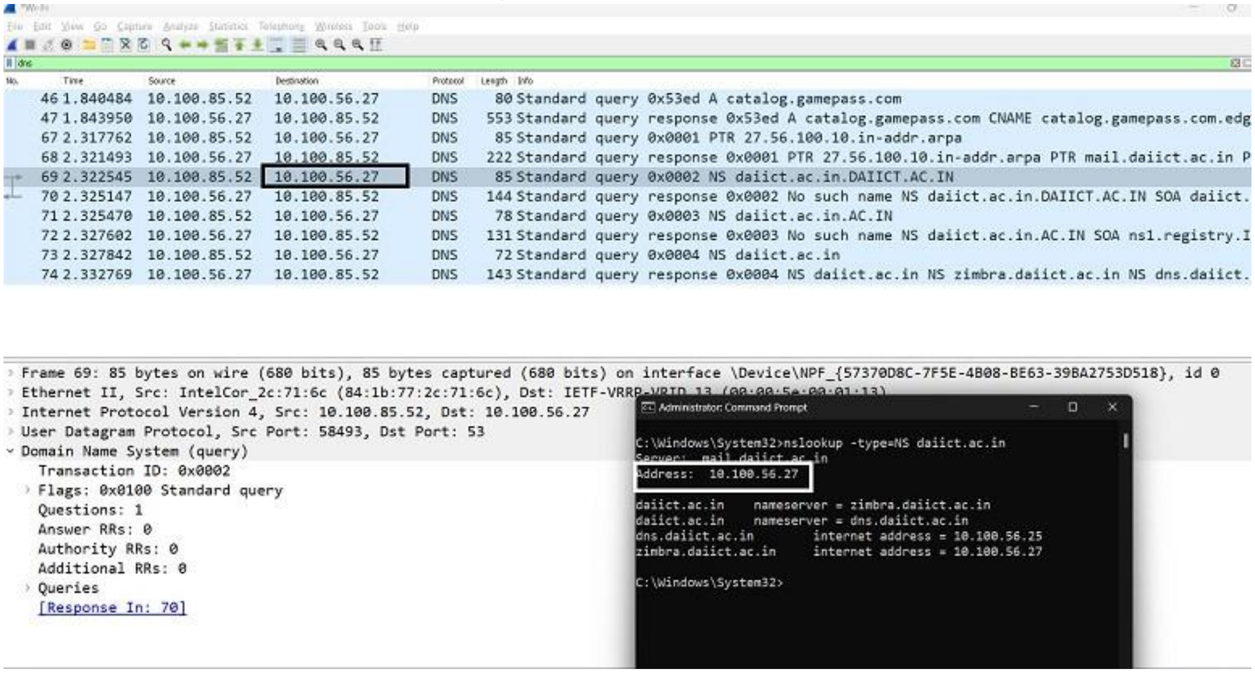
```
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 2
  Additional RRs: 2
> Queries
v Answers
  > www.daiict.ac.in: type A, class IN, addr 20.198.80.43
v Authoritative nameservers
  > daiict.ac.in: type NS, class IN, ns dns.daiict.ac.in
  > daiict.ac.in: type NS, class IN, ns zimbra.daiict.ac.in
v Additional records
  > dns.daiict.ac.in: type A, class IN, addr 10.100.56.25
  > zimbra.daiict.ac.in: type A, class IN, addr 10.100.56.27
  [Request In: 31]
  [Time: 0.002926000 seconds]
```

```
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup www.daiict.ac.in
Server:  mail.daiict.ac.in
Address:  10.100.56.27

Name:    www.daiict.ac.in
Address:  20.198.80.43

C:\Windows\System32>
```

2.3.4 Exercise 4: Finding name servers

1. To what IP address is the DNS query message sent? Is this the IPaddress of your default local DNS server?

-> Yes. The IP address is ssame if my default local DNs server


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

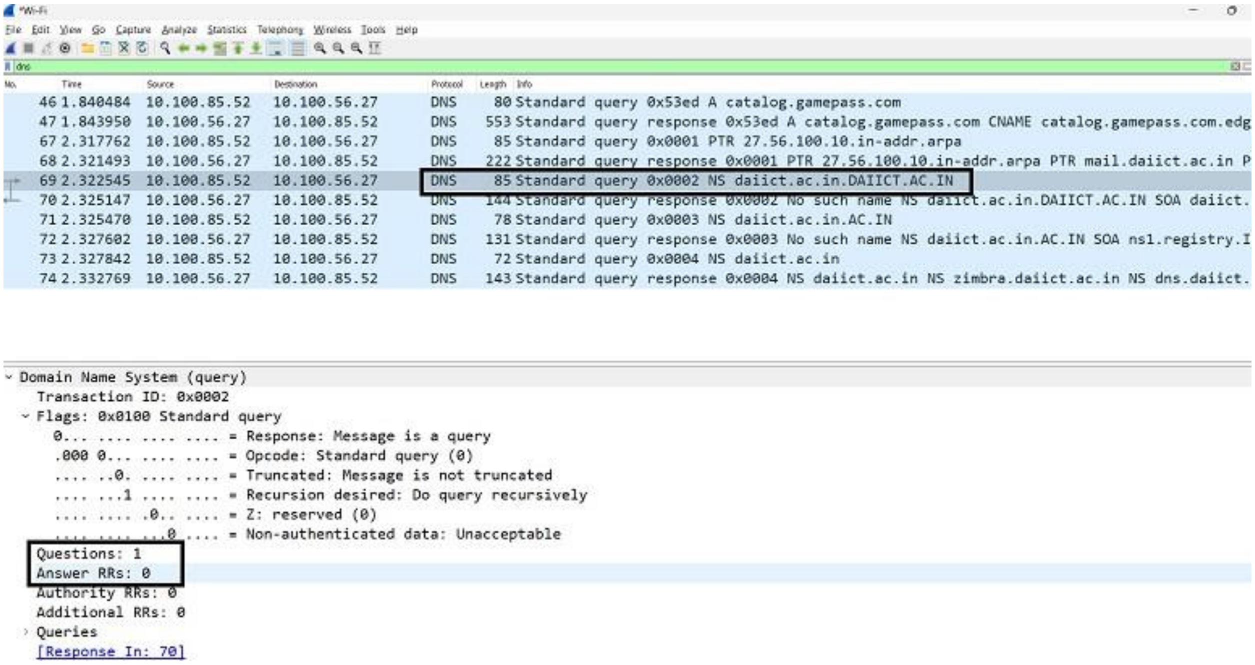
```
No.  Time      Source         Destination    Protocol Length Info
  46 1.840484  10.100.85.52   10.100.56.27   DNS       80 Standard query 0x53ed A catalog.gamepass.com
  47 1.843950  10.100.56.27   10.100.85.52   DNS      553 Standard query response 0x53ed A catalog.gamepass.com CNAME catalog.gamepass.com.edg
  67 2.317762  10.100.85.52   10.100.56.27   DNS       85 Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
  68 2.321493  10.100.56.27   10.100.85.52   DNS      222 Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PTR mail.daiict.ac.in P
  69 2.322545  10.100.85.52   10.100.56.27   DNS       85 Standard query 0x0002 NS daiict.ac.in.DAIICT.AC.IN
  70 2.325147  10.100.56.27   10.100.85.52   DNS      144 Standard query response 0x0002 No such name NS daiict.ac.in.DAIICT.AC.IN SOA daiict.
  71 2.325470  10.100.85.52   10.100.56.27   DNS       78 Standard query 0x0003 NS daiict.ac.in.AC.IN
  72 2.327602  10.100.56.27   10.100.85.52   DNS      131 Standard query response 0x0003 No such name NS daiict.ac.in.AC.IN SOA ns1.registry.I
  73 2.327842  10.100.85.52   10.100.56.27   DNS       72 Standard query 0x0004 NS daiict.ac.in
  74 2.332769  10.100.56.27   10.100.85.52   DNS      143 Standard query response 0x0004 NS daiict.ac.in NS zimbra.daiict.ac.in NS dns.daiict.
```

```
> Frame 69: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{57370D8C-7F5E-4B08-BE63-39BA2753D518}, id 0
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 10.100.56.27
> User Datagram Protocol, Src Port: 58493, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 70]
```

```
C:\Windows\System32>nslookup -type=NS daiict.ac.in
Server:  mail.daiict.ac.in
Address:  10.100.56.27

daiict.ac.in    nameserver = zimbra.daiict.ac.in
daiict.ac.in    nameserver = dns.daiict.ac.in
dns.daiict.ac.in        internet address = 10.100.56.25
zimbra.daiict.ac.in     internet address = 10.100.56.27

C:\Windows\System32>
```

Khushi Mehta
202312125

2. Examine the DNS query message. What “Type” of DNS query is it?
Does the query message contain any “answers”?

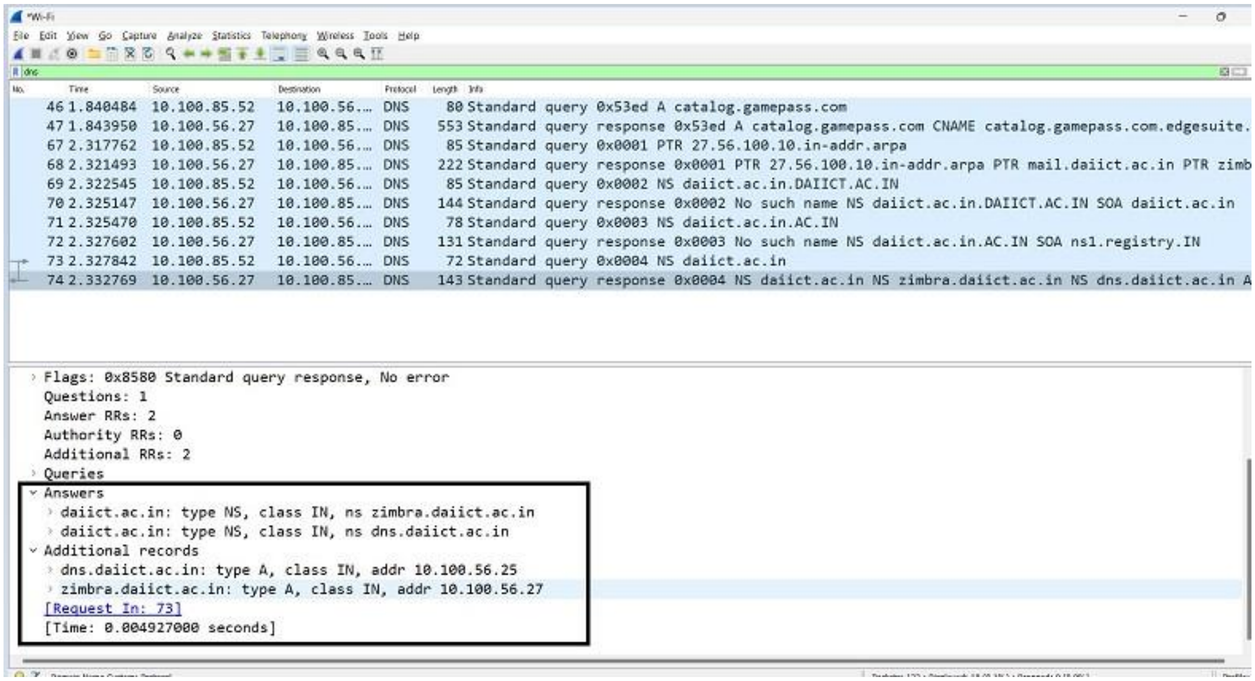

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time      Source        Destination   Protocol Length Info
  46 1.840484  10.100.85.52  10.100.56.27  DNS       80 Standard query 0x53ed A catalog.gamepass.com
  47 1.843950  10.100.56.27  10.100.85.52  DNS      553 Standard query response 0x53ed A catalog.gamepass.com CNAME catalog.gamepass.com.edg
  67 2.317762  10.100.85.52  10.100.56.27  DNS       85 Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
  68 2.321493  10.100.56.27  10.100.85.52  DNS      222 Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PTR mail.daiict.ac.in P
  69 2.322545  10.100.85.52  10.100.56.27  DNS       85 Standard query 0x0002 NS daiict.ac.in.DAIICT.AC.IN
  70 2.325147  10.100.56.27  10.100.85.52  DNS      144 Standard query response 0x0002 No such name NS daiict.ac.in.DAIICT.AC.IN SOA daiict.
  71 2.325470  10.100.85.52  10.100.56.27  DNS       78 Standard query 0x0003 NS daiict.ac.in.AC.IN
  72 2.327602  10.100.56.27  10.100.85.52  DNS      131 Standard query response 0x0003 No such name NS daiict.ac.in.AC.IN SOA ns1.registry.I
  73 2.327842  10.100.85.52  10.100.56.27  DNS       72 Standard query 0x0004 NS daiict.ac.in
  74 2.332769  10.100.56.27  10.100.85.52  DNS      143 Standard query response 0x0004 NS daiict.ac.in NS zimbra.daiict.ac.in NS dns.daiict.
```

```
⌄ Domain Name System (query)
    Transaction ID: 0x0002
  ⌄ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  › Queries
    [Response In: 70]
```

3. Examine the DNS response message. What daiict name servers doesthe response message provide?

-> The nameservers are dns,zimbra. We can find their IP addresses if we expand the Additional records field


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time      Source        Destination  Protocol Length Info
  46 1.840484  10.100.85.52  10.100.56.…  DNS       80 Standard query 0x53ed A catalog.gamepass.com
  47 1.843950  10.100.56.27  10.100.85.…  DNS      553 Standard query response 0x53ed A catalog.gamepass.com CNAME catalog.gamepass.com.edgesuite.
  67 2.317762  10.100.85.52  10.100.56.…  DNS       85 Standard query 0x0001 PTR 27.56.100.10.in-addr.arpa
  68 2.321493  10.100.56.27  10.100.85.…  DNS      222 Standard query response 0x0001 PTR 27.56.100.10.in-addr.arpa PTR mail.daiict.ac.in PTR zimb
  69 2.322545  10.100.85.52  10.100.56.…  DNS       85 Standard query 0x0002 NS daiict.ac.in.DAIICT.AC.IN
  70 2.325147  10.100.56.27  10.100.85.…  DNS      144 Standard query response 0x0002 No such name NS daiict.ac.in.DAIICT.AC.IN SOA daiict.ac.in
  71 2.325470  10.100.85.52  10.100.56.…  DNS       78 Standard query 0x0003 NS daiict.ac.in.AC.IN
  72 2.327602  10.100.56.27  10.100.85.…  DNS      131 Standard query response 0x0003 No such name NS daiict.ac.in.AC.IN SOA ns1.registry.IN
  73 2.327842  10.100.85.52  10.100.56.…  DNS       72 Standard query 0x0004 NS daiict.ac.in
  74 2.332769  10.100.56.27  10.100.85.…  DNS      143 Standard query response 0x0004 NS daiict.ac.in NS zimbra.daiict.ac.in NS dns.daiict.ac.in A
```

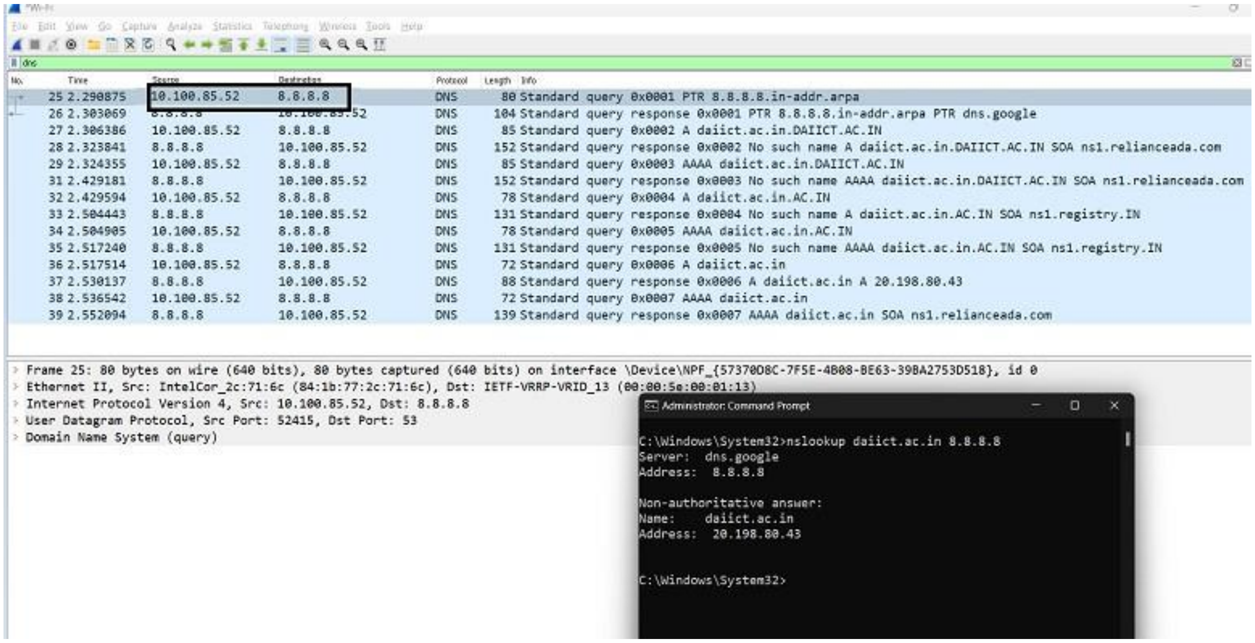
```
  › Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 2
  › Queries
  ⌄ Answers
    › daiict.ac.in: type NS, class IN, ns zimbra.daiict.ac.in
    › daiict.ac.in: type NS, class IN, ns dns.daiict.ac.in
  ⌄ Additional records
    › dns.daiict.ac.in: type A, class IN, addr 10.100.56.25
    › zimbra.daiict.ac.in: type A, class IN, addr 10.100.56.27
    [Request In: 73]
    [Time: 0.004927000 seconds]
```

Khushi Mehta
202312125

2.3.5 Exercise 5: DNS query to specific DNS server

1. To what IP address is the DNS query message sent? Is this the IPaddress of your default local DNS server? If not, what does the IP address correspond to?

-> Query was sent to IP 8.8.8.8



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

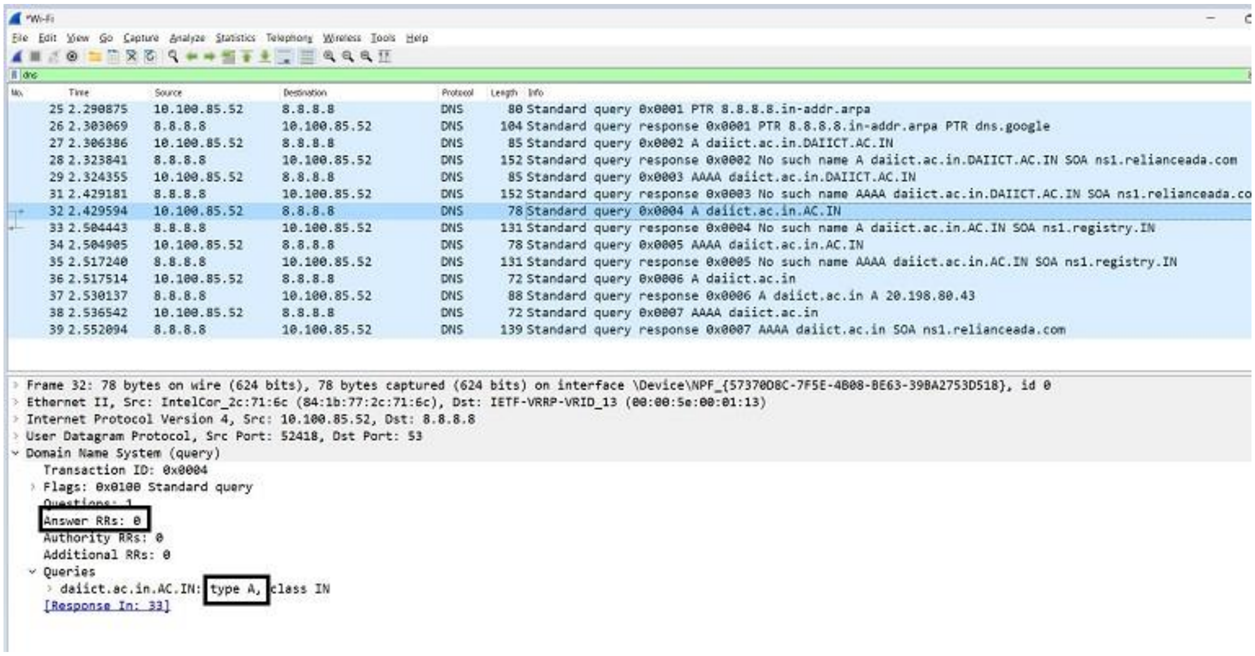
```
No.   Time       Source         Destination    Protocol Length Info
   25 2.290875   10.100.85.52   8.8.8.8        DNS       80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
   26 2.303069   8.8.8.8        10.100.85.52   DNS      104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
   27 2.306386   10.100.85.52   8.8.8.8        DNS       85 Standard query 0x0002 A daiict.ac.in.DAIICT.AC.IN
   28 2.323841   8.8.8.8        10.100.85.52   DNS      152 Standard query response 0x0002 No such name A daiict.ac.in.DAIICT.AC.IN SOA ns1.relianceada.com
   29 2.324355   10.100.85.52   8.8.8.8        DNS       85 Standard query 0x0003 AAAA daiict.ac.in.DAIICT.AC.IN
   31 2.429181   8.8.8.8        10.100.85.52   DNS      152 Standard query response 0x0003 No such name AAAA daiict.ac.in.DAIICT.AC.IN SOA ns1.relianceada.com
   32 2.429594   10.100.85.52   8.8.8.8        DNS       78 Standard query 0x0004 A daiict.ac.in.AC.IN
   33 2.504443   8.8.8.8        10.100.85.52   DNS      131 Standard query response 0x0004 No such name A daiict.ac.in.AC.IN SOA ns1.registry.IN
   34 2.504905   10.100.85.52   8.8.8.8        DNS       78 Standard query 0x0005 AAAA daiict.ac.in.AC.IN
   35 2.517240   8.8.8.8        10.100.85.52   DNS      131 Standard query response 0x0005 No such name AAAA daiict.ac.in.AC.IN SOA ns1.registry.IN
   36 2.517514   10.100.85.52   8.8.8.8        DNS       72 Standard query 0x0006 A daiict.ac.in
   37 2.530137   8.8.8.8        10.100.85.52   DNS       88 Standard query response 0x0006 A daiict.ac.in A 20.198.80.43
   38 2.536542   10.100.85.52   8.8.8.8        DNS       72 Standard query 0x0007 AAAA daiict.ac.in
   39 2.552094   8.8.8.8        10.100.85.52   DNS      139 Standard query response 0x0007 AAAA daiict.ac.in SOA ns1.relianceada.com
```

```
> Frame 25: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{57370D8C-7F5E-4B08-BE63-39BA2753D518}, id 0
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52415, Dst Port: 53
> Domain Name System (query)
```

```
C:\Windows\System32>nslookup daiict.ac.in 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    daiict.ac.in
Address:  20.198.80.43


C:\Windows\System32>
```

2. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Khushi Mehta
202312125

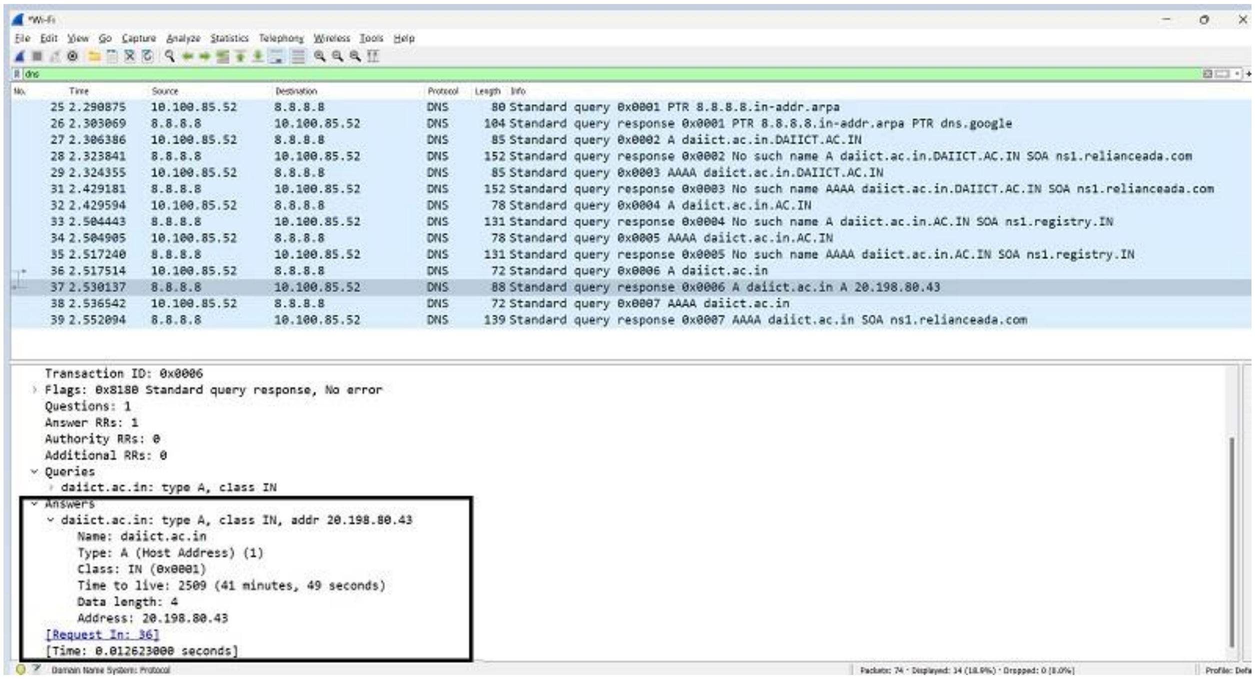

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time        Source          Destination     Protocol  Length  Info
  25 2.290875    10.100.85.52    8.8.8.8         DNS       80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
  26 2.303069    8.8.8.8         10.100.85.52    DNS      104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
  27 2.306386    10.100.85.52    8.8.8.8         DNS       85 Standard query 0x0002 A daiict.ac.in.DAIICT.AC.IN
  28 2.323841    8.8.8.8         10.100.85.52    DNS      152 Standard query response 0x0002 No such name A daiict.ac.in.DAIICT.AC.IN SOA ns1.relianceada.com
  29 2.324355    10.100.85.52    8.8.8.8         DNS       85 Standard query 0x0003 AAAA daiict.ac.in.DAIICT.AC.IN
  31 2.429181    8.8.8.8         10.100.85.52    DNS      152 Standard query response 0x0003 No such name AAAA daiict.ac.in.DAIICT.AC.IN SOA ns1.relianceada.co
  32 2.429594    10.100.85.52    8.8.8.8         DNS       78 Standard query 0x0004 A daiict.ac.in.AC.IN
  33 2.504443    8.8.8.8         10.100.85.52    DNS      131 Standard query response 0x0004 No such name A daiict.ac.in.AC.IN SOA ns1.registry.IN
  34 2.504905    10.100.85.52    8.8.8.8         DNS       78 Standard query 0x0005 AAAA daiict.ac.in.AC.IN
  35 2.517240    8.8.8.8         10.100.85.52    DNS      131 Standard query response 0x0005 No such name AAAA daiict.ac.in.AC.IN SOA ns1.registry.IN
  36 2.517514    10.100.85.52    8.8.8.8         DNS       72 Standard query 0x0006 A daiict.ac.in
  37 2.530137    8.8.8.8         10.100.85.52    DNS       88 Standard query response 0x0006 A daiict.ac.in A 20.198.80.43
  38 2.536542    10.100.85.52    8.8.8.8         DNS       72 Standard query 0x0007 AAAA daiict.ac.in
  39 2.552094    8.8.8.8         10.100.85.52    DNS      139 Standard query response 0x0007 AAAA daiict.ac.in SOA ns1.relianceada.com
```

```
> Frame 32: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{57370D8C-7F5E-4B08-8E63-39BA2753D518}, id 0
> Ethernet II, Src: IntelCor_2c:71:6c (84:1b:77:2c:71:6c), Dst: IETF-VRRP-VRID_13 (00:00:5e:00:01:13)
> Internet Protocol Version 4, Src: 10.100.85.52, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52418, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > daiict.ac.in.AC.IN: type A, class IN
    [Response In: 33]
```

3. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

->The response DNS message contains type 'A' only 1 answer containing the name of the host, the type of address, the class, the IP address


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time        Source          Destination     Protocol  Length  Info
  25 2.290875    10.100.85.52    8.8.8.8         DNS       80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
  26 2.303069    8.8.8.8         10.100.85.52    DNS      104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
  27 2.306386    10.100.85.52    8.8.8.8         DNS       85 Standard query 0x0002 A daiict.ac.in.DAIICT.AC.IN
  28 2.323841    8.8.8.8         10.100.85.52    DNS      152 Standard query response 0x0002 No such name A daiict.ac.in.DAIICT.AC.IN SOA ns1.relianceada.com
  29 2.324355    10.100.85.52    8.8.8.8         DNS       85 Standard query 0x0003 AAAA daiict.ac.in.DAIICT.AC.IN
  31 2.429181    8.8.8.8         10.100.85.52    DNS      152 Standard query response 0x0003 No such name AAAA daiict.ac.in.DAIICT.AC.IN SOA ns1.relianceada.com
  32 2.429594    10.100.85.52    8.8.8.8         DNS       78 Standard query 0x0004 A daiict.ac.in.AC.IN
  33 2.504443    8.8.8.8         10.100.85.52    DNS      131 Standard query response 0x0004 No such name A daiict.ac.in.AC.IN SOA ns1.registry.IN
  34 2.504905    10.100.85.52    8.8.8.8         DNS       78 Standard query 0x0005 AAAA daiict.ac.in.AC.IN
  35 2.517240    8.8.8.8         10.100.85.52    DNS      131 Standard query response 0x0005 No such name AAAA daiict.ac.in.AC.IN SOA ns1.registry.IN
  36 2.517514    10.100.85.52    8.8.8.8         DNS       72 Standard query 0x0006 A daiict.ac.in
  37 2.530137    8.8.8.8         10.100.85.52    DNS       88 Standard query response 0x0006 A daiict.ac.in A 20.198.80.43
  38 2.536542    10.100.85.52    8.8.8.8         DNS       72 Standard query 0x0007 AAAA daiict.ac.in
  39 2.552094    8.8.8.8         10.100.85.52    DNS      139 Standard query response 0x0007 AAAA daiict.ac.in SOA ns1.relianceada.com
```

```
    Transaction ID: 0x0006
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > daiict.ac.in: type A, class IN
  v Answers
    v daiict.ac.in: type A, class IN, addr 20.198.80.43
        Name: daiict.ac.in
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 2509 (41 minutes, 49 seconds)
        Data length: 4
        Address: 20.198.80.43
    [Request In: 36]
    [Time: 0.012623000 seconds]
```

Domain Name System: Protocol
Packets: 74 · Displayed: 14 (18.9%) · Dropped: 0 (0.0%)
Profile: Defa