

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.

```
Wireshark - Packet 22213 - Wi-Fi

> Frame 22213: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{69DBA93A-EAD3-44DC-A60B-A349B8014BE8}, id 0
> Ethernet II, Src: IntelCor_15:59:1e (34:e1:2d:15:59:1e), Dst: NokiaSha_1e:36:b0 (dc:d9:ae:1e:36:b0)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 4.4.8.8
▼ User Datagram Protocol, Src Port: 57095, Dst Port: 53
  Source Port: 57095
  Destination Port: 53
  Length: 42
  Checksum: 0xcd88 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 48]
  > [Timestamps]
> Domain Name System (query)

0000  dc d9 ae 1e 36 b0 34 e1 2d 15 59 1e 08 00 45 00  ....6.4. .Y...E.
0010  00 1e 42 8d 00 00 00 11 00 00 c0 a8 01 09 04 04  .>B.....
0020  08 08 df 07 00 35 00 2a cd f8 70 46 01 00 00 01  ....5.* .pF....
0030  00 00 00 00 00 00 03 77 77 77 06 64 61 69 69 63  ....www.daiic
0040  74 02 61 63 02 69 6e 00 00 01 00 01          t.ac.in. ....
```

```
Wireshark - Packet 22235 - Wi-Fi

> Frame 22235: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{69DBA93A-EAD3-44DC-A60B-A349B8014BE8}, id 0
> Ethernet II, Src: NokiaSha_1e:36:b0 (dc:d9:ae:1e:36:b0), Dst: IntelCor_15:59:1e (34:e1:2d:15:59:1e)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.9
▼ User Datagram Protocol, Src Port: 53, Dst Port: 57095
  Source Port: 53
  Destination Port: 57095
  Length: 58
  Checksum: 0xdec2 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 47]
  > [Timestamps]
> Domain Name System (response)

0000  34 e1 2d 15 59 1e dc d9 ae 1e 36 b0 08 00 45 00  4...Y... .6...E.
0010  00 4e a3 e3 00 00 7a 11 ca fa 08 08 08 08 c0 a8  .N...Z. ....
0020  01 09 00 35 df 07 00 3a de c2 70 46 81 80 00 01  ...S... .pF....
0030  00 01 00 00 00 00 03 77 77 77 06 64 61 69 69 63  ....www.daiic
0040  74 02 61 63 02 69 6e 00 00 01 00 01 c0 0c 00 01  t.ac.in. ....
0050  00 01 00 00 54 5f 00 04 68 ee 6e 9f          ....T_...h-n-
```

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

The screenshot shows a Wireshark packet capture of a DNS query. The packet list on the left shows several packets, with packet 3443 selected. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol (Src Port: 56026, Dst Port: 53), and Domain Name System (query). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3727	22.407621	d8:32:e3:54:96:70	30:24:32:aa:9f:42	ARP	42	Who has 192.168.43.48? Tell 192.168.43.1
3728	22.407652	30:24:32:aa:9f:42	d8:32:e3:54:96:70	ARP	42	192.168.43.48 is at 30:24:32:aa:9f:42
3443	21.407662	192.168.43.48	192.168.43.1	DNS	76	Standard query 0x28ba A www.dailict.ac.in
3445	21.408514	192.168.43.48	192.168.43.1	DNS	76	Standard query 0x13e2 AAAA www.dailict.ac.in
3455	21.544243	192.168.43.1	192.168.43.48	DNS	92	Standard query response 0x28ba A www.dailict.ac.in A 104.238.110.159
3456	21.544743	192.168.43.1	192.168.43.48	DNS	143	Standard query response 0x13e2 AAAA www.dailict.ac.in SOA ns1.relianceada.com
3463	21.560104	192.168.43.48	192.168.43.1	DNS	89	Standard query 0x98f6 A nav.smartscreen.microsoft.com
3464	21.560615	192.168.43.48	192.168.43.1	DNS	89	Standard query 0x529a AAAA nav.smartscreen.microsoft.com
3471	21.604678	192.168.43.1	192.168.43.48	DNS	271	Standard query response 0x529a AAAA nav.smartscreen.microsoft.com CHAVE wd-prod-ss.traffic...
3472	21.605146	192.168.43.1	192.168.43.48	DNS	210	Standard query response 0x98f6 A nav.smartscreen.microsoft.com
4217	24.617799	192.168.43.48	192.168.43.1	DNS	69	Standard query 0xb865 A c.msn.com
4218	24.618689	192.168.43.48	192.168.43.1	DNS	69	Standard query 0xb85a AAAA c.msn.com
4224	24.627771	192.168.43.48	192.168.43.1	DNS	71	Standard query 0xd539 A ntp.msn.com
4225	24.628289	192.168.43.48	192.168.43.1	DNS	71	Standard query 0xe6c0 AAAA ntp.msn.com

Frame 3443: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: d8:32:e3:54:96:70 (30:24:32:aa:9f:42), Dst: d8:32:e3:54:96:70 (d8:32:e3:54:96:70)
Internet Protocol Version 4, Src: 192.168.43.48, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 56026, Dst Port: 53
Domain Name System (query)

```
0000 d8 32 e3 54 96 70 30 24 32 aa 9f 42 00 00 45 00 .2.T.p0$ 2..B..E.
0010 00 3e c6 b5 00 00 00 11 00 00 c0 a8 2b 30 c0 a8 .>.....00..
0020 2b 01 00 00 00 00 00 00 28 ba 01 00 00 01 +.....(.....
0030 00 00 00 00 00 00 03 77 77 06 64 61 69 69 63 .....w.dailic
0040 74 02 61 63 02 69 6e 00 00 01 00 01 t.ac.in. ....
```

The screenshot shows a Wireshark packet capture of a DNS response. The packet list on the left shows several packets, with packet 3455 selected. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol (Src Port: 53, Dst Port: 56026), and Domain Name System (response). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3727	22.407621	d8:32:e3:54:96:70	30:24:32:aa:9f:42	ARP	42	Who has 192.168.43.48? Tell 192.168.43.1
3728	22.407652	30:24:32:aa:9f:42	d8:32:e3:54:96:70	ARP	42	192.168.43.48 is at 30:24:32:aa:9f:42
3443	21.407662	192.168.43.48	192.168.43.1	DNS	76	Standard query 0x28ba A www.dailict.ac.in
3445	21.408514	192.168.43.48	192.168.43.1	DNS	76	Standard query 0x13e2 AAAA www.dailict.ac.in
3455	21.544243	192.168.43.1	192.168.43.48	DNS	92	Standard query response 0x28ba A www.dailict.ac.in A 104.238.110.159
3456	21.544743	192.168.43.1	192.168.43.48	DNS	143	Standard query response 0x13e2 AAAA www.dailict.ac.in SOA ns1.relianceada.com
3463	21.560104	192.168.43.48	192.168.43.1	DNS	89	Standard query 0x98f6 A nav.smartscreen.microsoft.com
3464	21.560615	192.168.43.48	192.168.43.1	DNS	89	Standard query 0x529a AAAA nav.smartscreen.microsoft.com
3471	21.604678	192.168.43.1	192.168.43.48	DNS	271	Standard query response 0x529a AAAA nav.smartscreen.microsoft.com CHAVE wd-prod-ss.traffic...
3472	21.605146	192.168.43.1	192.168.43.48	DNS	210	Standard query response 0x98f6 A nav.smartscreen.microsoft.com
4217	24.617799	192.168.43.48	192.168.43.1	DNS	69	Standard query 0xb865 A c.msn.com
4218	24.618689	192.168.43.48	192.168.43.1	DNS	69	Standard query 0xb85a AAAA c.msn.com
4224	24.627771	192.168.43.48	192.168.43.1	DNS	71	Standard query 0xd539 A ntp.msn.com
4225	24.628289	192.168.43.48	192.168.43.1	DNS	71	Standard query 0xe6c0 AAAA ntp.msn.com

Frame 3455: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Ethernet II, Src: d8:32:e3:54:96:70 (d8:32:e3:54:96:70), Dst: 30:24:32:aa:9f:42 (30:24:32:aa:9f:42)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.48
User Datagram Protocol, Src Port: 53, Dst Port: 56026
Domain Name System (response)

```
0000 30 24 32 aa 9f 42 d8 32 e3 54 96 70 00 00 45 00 0$2..B.2.T.p..E.
0010 00 4e 17 91 40 00 00 11 4b 8c c0 a8 2b 01 c0 a8 .N..B..K...t...
0020 2b 30 00 00 00 00 00 00 28 ba 01 00 00 01 +.....(.....
0030 00 01 00 00 00 00 03 77 77 06 64 61 69 69 63 .....w.dailic
0040 74 02 61 63 02 69 6e 00 00 01 00 01 c0 0c 00 01 t.ac.in. ....
0050 00 01 00 00 41 5d 00 04 68 ee 6e 9f ....A]..h.n..
```


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

```
Command Prompt
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) Wireless-AC 9560 160MHz
Physical Address. . . . . : 30-24-32-AA-9F-42
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2409:4041:e81:4bfe:7459:f67e:4a92:e280(Preferred)
Temporary IPv6 Address. . . . . : 2409:4041:e81:4bfe:391a:26cb:7071:e025(Preferred)
Link-local IPv6 Address . . . . . : fe80::7459:f67e:4a92:e280%9(Preferred)
IPv4 Address. . . . . : 192.168.43.48(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, October 3, 2020 8:46:49 AM
Lease Expires . . . . . : Saturday, October 3, 2020 4:24:34 PM
Default Gateway . . . . . : fe80::da32:e3ff:fe54:9670%9
                          192.168.43.1
DHCP Server . . . . . : 192.168.43.1
DHCPv6 IAID . . . . . : 53486642
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-D7-51-92-4C-ED-FB-2D-18-68
DNS Servers . . . . . : 192.168.43.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 
Description . . . . . : Bluetooth Device (Personal Area Network)
```

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

3.1.1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
3727	22.407621	d8:32:e3:54:96:70	30:24:32:aa:9f:42	ARP	42	Who has 192.168.43.48? Tell 192.168.43.1
3728	22.407652	30:24:32:aa:9f:42	d8:32:e3:54:96:70	ARP	42	192.168.43.48 is at 30:24:32:aa:9f:42
3443	21.487662	192.168.43.48	192.168.43.1	DNS	76	Standard query 0x28ba A www.daiict.ac.in
3445	21.488514	192.168.43.48	192.168.43.1	DNS	76	Standard query 0x13e2 AAAA www.daiict.ac.in
3455	21.544243	192.168.43.1	192.168.43.48	DNS	92	Standard query response 0x28ba A www.daiict.ac.in A 104.238.110.159
3456	21.544743	192.168.43.1	192.168.43.48	DNS	143	Standard query response 0x13e2 AAAA www.daiict.ac.in SOA ns1.relianceada.com
3463	21.560104	192.168.43.48	192.168.43.1	DNS	89	Standard query 0x98f6 A nav.smartscreen.microsoft.com
3464	21.560615	192.168.43.48	192.168.43.1	DNS	89	Standard query 0x529a AAAA nav.smartscreen.microsoft.com
3471	21.604678	192.168.43.1	192.168.43.48	DNS	271	Standard query response 0x529a AAAA nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficman...
3472	21.605146	192.168.43.1	192.168.43.48	DNS	210	Standard query response 0x98f6 A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficman...
4217	24.617799	192.168.43.48	192.168.43.1	DNS	69	Standard query 0x8d65 A c.msn.com
4218	24.618689	192.168.43.48	192.168.43.1	DNS	69	Standard query 0xb85a AAAA c.msn.com
4224	24.627771	192.168.43.48	192.168.43.1	DNS	71	Standard query 0xd539 A ntp.msn.com
4225	24.628289	192.168.43.48	192.168.43.1	DNS	71	Standard query 0xe6c0 AAAA ntp.msn.com

Destination Port: 53
Length: 42
Checksum: 0xd7bd [unverified]
[Checksum Status: Unverified]
[Stream index: 3]

Domain Name System (query)
[Response In: 3455]
Transaction ID: 0x28ba
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
> www.daiict.ac.in: type A, class IN

0000 d8 32 e3 54 96 70 30 24 32 aa 9f 42 08 00 45 00 .2.T.p0\$ 2..0..E.
0010 00 3e c6 b5 00 00 11 00 00 c0 a8 2b 30 c0 a8 .>.....+0..
0020 2b 01 00 00 00 00 00 00 00 00 00 00 00 00 01 +.....
0030 00 00 00 00 00 00 03 77 77 77 06 64 61 69 69 63w ww.daiic
0040 74 02 61 63 02 69 6e 00 00 01 00 01t.ac.in.

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

The screenshot shows a Wireshark capture of a network packet. The packet list on the left shows a DNS response packet (No. 3443) from 192.168.43.48 to 192.168.43.1. The packet details pane on the right shows the 'Domain Name System (response)' section. The 'Answers' section contains one entry: 'www.daiict.ac.in: type A, class IN, addr 104.238.110.159'. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

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

The screenshot shows a Wireshark capture of a network packet. The packet list on the left shows a SYN packet (No. 3457) from 192.168.43.48 to 104.238.110.159. The packet details pane on the right shows the 'Internet Protocol Version 4' section. The 'Destination' field is set to 104.238.110.159. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

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

3.2)

1) Destination Port for DNS Query : 53

No.	Time	Source	Destination	Protocol	Length	Info
1172	4.598440	192.168.43.119	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
1173	4.599657	192.168.43.1	192.168.43.119	DNS	85	Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa
1174	4.602359	192.168.43.119	192.168.43.1	DNS	76	Standard query 0x0002 A www.daiict.ac.in
1175	4.603547	192.168.43.1	192.168.43.119	DNS	92	Standard query response 0x0002 A www.daiict.ac.in A 104.238.110.159
1177	4.611637	192.168.43.119	192.168.43.1	DNS	76	Standard query 0x0003 AAAA www.daiict.ac.in
1178	4.613210	192.168.43.1	192.168.43.119	DNS	76	Standard query response 0x0003 AAAA www.daiict.ac.in

> Frame 1174: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{BF9054D7-661E-47B7-ADE5-50DDC93A1E9B}, id 0
> Ethernet II, Src: c6:d2:90:e1:ef:05 (c6:d2:90:e1:ef:05), Dst: 3e:46:88:e7:0e:4c (3e:46:88:e7:0e:4c)
> Internet Protocol Version 4, Src: 192.168.43.119, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 64663, Dst Port: 53
Source Port: 64663
Destination Port: 53
Length: 42
Checksum: 0x9810 [unverified]
[Checksum Status: Unverified]
[Stream index: 7]
> [Timestamps]
> Domain Name System (query)

Source Port for DNS message/response: 53

Source Port: 53

Destination Port: 64663

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

1174	4.602359	192.168.43.119	192.168.43.1	DNS	76	Standard query 0x0002 A www.daiict.ac.in
------	----------	----------------	--------------	-----	----	--

DNS servers: 192.168.43.1,
2405:205:c90d:b973::9d

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

```
Queries
  www.daiict.ac.in: type A, class IN
    Name: www.daiict.ac.in
    [Name Length: 16]
    [Label Count: 4]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 1175]
```

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

▼ 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

▼ 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)

[\[Response In: 5610\]](#)

▼ 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
```

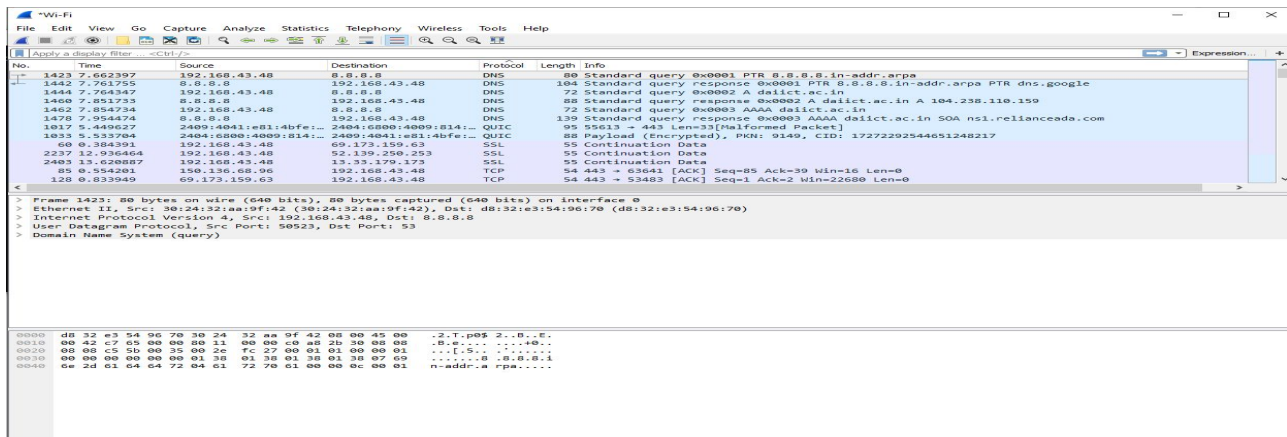
[\[Request In: 8454\]](#)

[Time: 0.031992000 seconds]

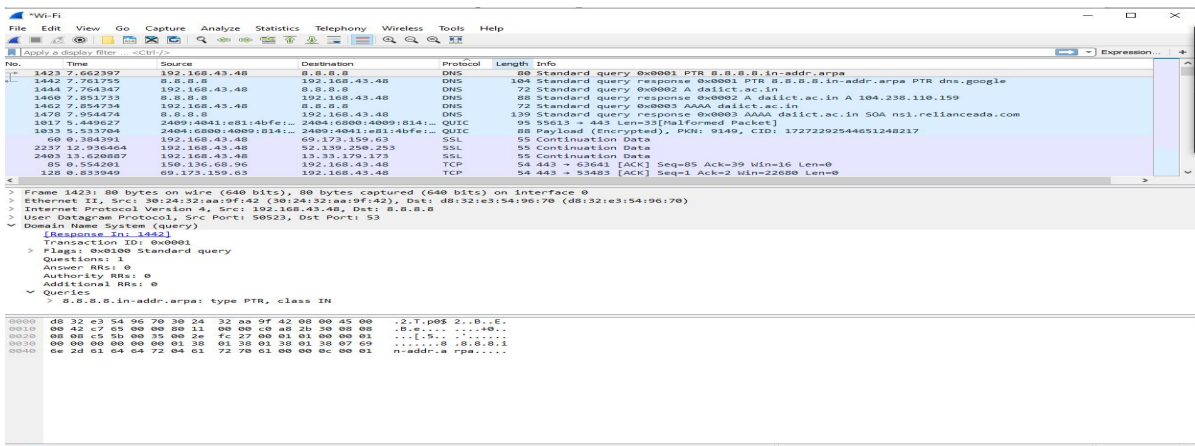
We obtained 6 name servers as can be seen in the above screenshot.

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.

The image shows a Wireshark packet capture window titled "Wi-Fi". The main pane displays a list of network packets. Packet 1460 is selected, showing a DNS response from 192.168.43.48 to 8.8.8.8. The packet details pane shows the "Domain Name System (response)" section, indicating a successful query for "daiict.ac.in" with an answer of 104.238.110.159. The packet bytes pane shows the raw data of the packet, including the IP header, UDP header, and DNS message structure.

No.	Time	Source	Destination	Protocol	Length	Info
1423	7.662397	192.168.43.48	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.in-addr.arpa
1442	7.761755	8.8.8.8	192.168.43.48	DNS	104	Standard query response 0x0001 PTR 8.8.8.in-addr.arpa PTR dns.google
1444	7.764347	192.168.43.48	8.8.8.8	DNS	72	Standard query 0x0002 A daiict.ac.in
1460	7.851733	8.8.8.8	192.168.43.48	DNS	88	Standard query response 0x0002 A daiict.ac.in A 104.238.110.159
1462	7.854734	192.168.43.48	8.8.8.8	DNS	72	Standard query 0x0003 AAAA daiict.ac.in
1478	7.954474	8.8.8.8	192.168.43.48	DNS	139	Standard query response 0x0003 AAAA daiict.ac.in SOA ns1.relianceada.com
1617	5.449627	2409:4041:e81:4bfe::...	2404:6800:4009:814::...	QUIC	95	55613 → 443 Len=33[Malformed Packet]
1033	5.533704	2404:6800:4009:814::...	2409:4041:e81:4bfe::...	QUIC	88	Payload (Encrypted), PKN: 9149, CID: 17272292544651248217
60	0.384391	192.168.43.48	69.173.159.63	SSL	55	Continuation Data
2237	12.936464	192.168.43.48	52.139.250.253	SSL	55	Continuation Data
2403	13.620887	192.168.43.48	13.33.179.173	SSL	55	Continuation Data
85	0.554201	150.136.68.96	192.168.43.48	TCP	54	443 → 63641 [ACK] Seq=85 Ack=39 Win=16 Len=0
128	0.833949	69.173.159.63	192.168.43.48	TCP	54	443 → 53483 [ACK] Seq=1 Ack=2 Win=22680 Len=0

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.43.48
User Datagram Protocol, Src Port: 53, Dst Port: 50524
Domain Name System (response)
[Request In: 1444]
[Time: 0.087386000 seconds]
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
daiict.ac.in: type A, class IN
Answers
daiict.ac.in: type A, class IN, addr 104.238.110.159

0000 30 24 32 aa 9f 42 d8 32 e3 54 96 70 08 00 45 28 052..8.2 .T.p..E(
0010 00 4a d1 99 00 00 73 11 79 f9 08 08 08 08 c0 a6 .J...5. y.....
0020 2b 30 00 35 c5 5c 00 36 bb 6c 00 02 81 80 00 01 +0.5.\.6 .l.....
0030 00 01 00 00 00 00 06 64 61 69 69 63 74 02 61 63d aiict.ac
0040 02 69 6e 00 00 01 00 01 c0 0c 00 01 00 01 00 00 .in.....
0050 52 74 00 04 68 ee 6e 9f 8t..h.n

Frame (frame), 88 bytes | Packets: 2577 · Displayed: 2577 (100.0%) | Profile: Default