Assignment 4
Om Deshmukh
210010033

Part 1:

1.
The ip address of www.iitdh.ac.in server is 10.195.250.62

2.
DNS servers for google.com include ns1.google.com, ns2.google.com, ns3.google.com, ns4.google.com.

3.

```
(base) ➜  ~ nslookup gmail.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   gmail.com
Address: 142.250.193.133
```
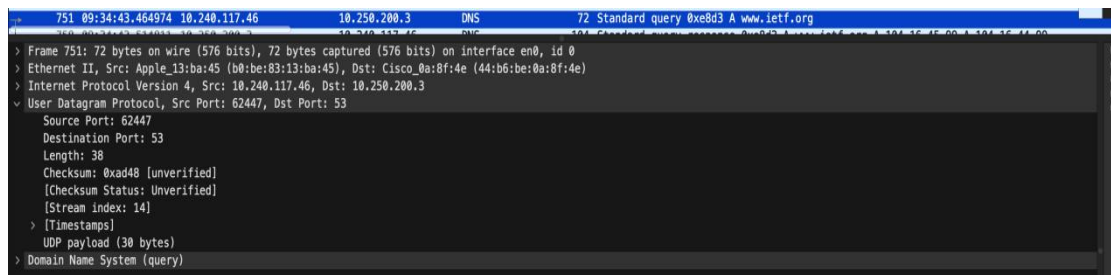
The ip for gmail.com is 142.250.193.133

Part 2:

```
(base) ➜  ~ sudo killall -HUP mDNSResponder
Password:
(base) ➜  ~ |
```

This clears all the web cache.

Part 3:

```
   751 09:34:43.464974 10.240.117.46          10.250.200.3      DNS        72 Standard query 0xe8d3 A www.ietf.org
> Frame 751: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
> Ethernet II, Src: Apple_13:ba:45 (b0:be:83:13:ba:45), Dst: Cisco_0a:8f:4e (44:b6:be:0a:8f:4e)
> Internet Protocol Version 4, Src: 10.240.117.46, Dst: 10.250.200.3
v User Datagram Protocol, Src Port: 62447, Dst Port: 53
    Source Port: 62447
    Destination Port: 53
    Length: 38
    Checksum: 0xad48 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 14]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

1. The packet are packet no. 751, 752 .
They follow the UDP stream.

2.
The destination port for the DNS query message is **53**.
The source port of the DNS response message is **53**.

3.
10.250.200.3 is the ip to which the DNS query message was sent to.
 10.250.200.3 is the ip of the DNS server.
Yes, the two ip are same.

```
   8 10:42:59.427107 10.200.129.150          10.250.200.3      DNS        72 Standard query 0xee98 A www.ietf.org
```

4.

```
v Queries
  > www.ietf.org: type A, class IN
  [Response In: 9]
```

The type of the DNS message query is type A.
 No, the query message does not contain any answers.

5.

```
v Domain Name System (response)
    Transaction ID: 0xe8d3
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 751]
    [Time: 0.049837000 seconds]
```

```
v Answers
  v www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 201 (3 minutes, 21 seconds)
      Data length: 4
      Address: 104.16.45.99
  v www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 201 (3 minutes, 21 seconds)
      Data length: 4
      Address: 104.16.44.99
```

2 answers are provided in the DNS response message.
The two answers contained the name of the website, the type of host, the class, the time to live of the packet sent, the data length and the ip of www.ietf.org.

6.

```
759 09:34:43.516543 10.240.117.46        104.16.45.99        TCP        78 58963 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2751211108 TSecr=0
760 09:34:43.516671 10.240.117.46        104.16.45.99        TCP        78 58964 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4014118796 TSecr=0
```

The destination IP address of the SYN packet corresponds to the ip address of www.ietf.org which was mentioned in the answers of the query response message.

7.
Since the destination ip remains the same in all the request query messages, we can say that all the images came from the same source, hence we can say that the host did **not** issue any new DNS queries.

Part 4.1:

```
> Frame 38: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
> Ethernet II, Src: Apple_13:ba:45 (b0:be:83:13:ba:45), Dst: Cisco_0a:9a:f3 (44:b6:be:0a:9a:f3)
> Internet Protocol Version 4, Src: 10.200.249.243, Dst: 10.250.200.3
> User Datagram Protocol, Src Port: 64138, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xebc3
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 46]
```

1.
Destination port of query message: 53
Source port of response message: 53

2.
Both have ip address: 10.250.200.3
Yes, both of them have the same ip.

3. Query message is of type A
No answers in the query message.

```
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
```

4. 3 answers are provided to the response message.They contain various information such as name, type, class, TLL, data length and CNAME of the DNS servers.

5.

Part 4.2:

1.   The DNS query message was sent to 10.250.200.3.
Yes, it matches with that of the local DNS server.

2.   The DNS query message has type A. No, it does not
contain any answers.

3.   The DNS response provides 8 answers each of which has
an MIT nameservers: usw2.akam.net , eur5.akam.net,
asia2.akam.net, ns1-173.akam.net, use2.akam.net,
asia1.akam.net, use5.akam.net and ns1-37.akam.net

4.

```
  ˅ mit.edu: type NS, class IN, ns use2.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 1775 (29 minutes, 35 seconds)
      Data length: 7
      Name Server: use2.akam.net
  ˅ mit.edu: type NS, class IN, ns asia1.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 1775 (29 minutes, 35 seconds)
      Data length: 8
      Name Server: asia1.akam.net
  ˅ mit.edu: type NS, class IN, ns use5.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 1775 (29 minutes, 35 seconds)
      Data length: 7
      Name Server: use5.akam.net
  ˅ mit.edu: type NS, class IN, ns ns1-37.akam.net
      Name: mit.edu
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 1775 (29 minutes, 35 seconds)
      Data length: 9
      Name Server: ns1-37.akam.net
  [Request In: 1]
```

Part 4.3

1. The DNS query message was sent to 216.239.36.10. No,it is
    not same to the address of the local DNS server.

2. The DNS query message has Type **A. No**, the query does
    not contain any answers.

3. Only 1 answer is provided in the DNS response query. The
    answer contains DNS server's name, Type, class, TTL,
    Data length and IP address.

4.

```
> Frame 9: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: Apple_13:ba:45 (b0:be:83:13:ba:45)
> Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.200.129.150
> User Datagram Protocol, Src Port: 53, Dst Port: 55528
v Domain Name System (response)
    Transaction ID: 0x2f30
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v ns3.google.com: type A, class IN, addr 216.239.36.10
        Name: ns3.google.com
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 21569 (5 hours, 59 minutes, 29 seconds)
        Data length: 4
        Address: 216.239.36.10
    [Request In: 8]
    [Time: 0.012114000 seconds]
```