# 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
```

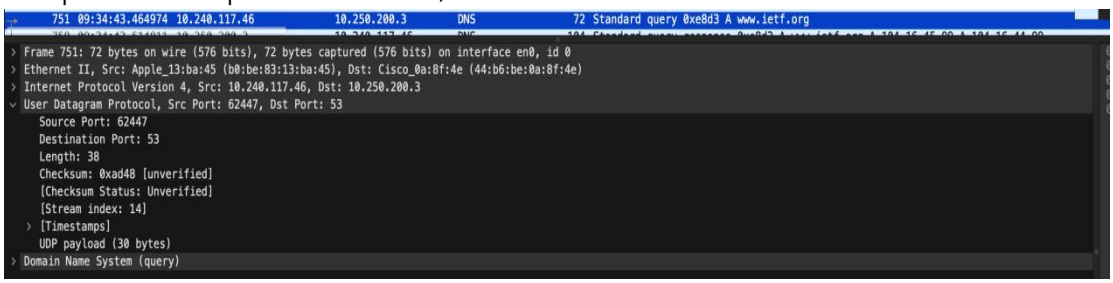
The ip for gmail.com is 142.250.193.133

## Part 2:

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

## Part 3:

1. The packet are packet no. 751, 752 .

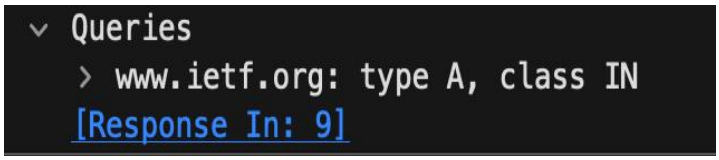



They follow the UDP stream.

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

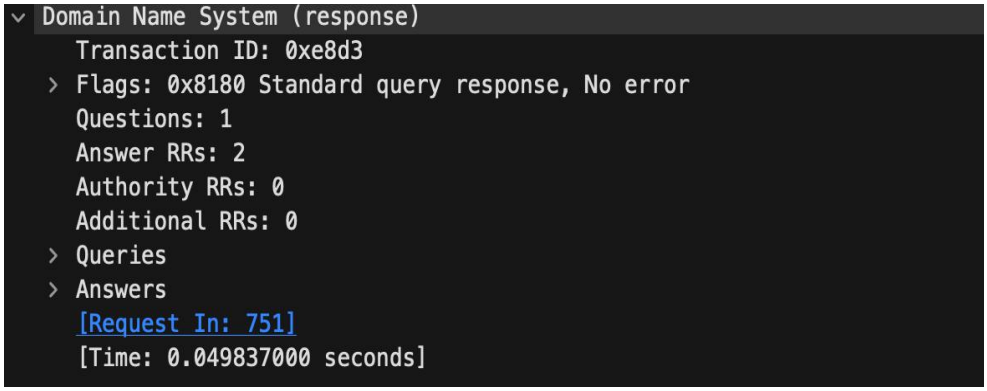
3.
10.240.200.3 is the ip to which the DNS query message was sent to.
10.250.200.3 is the ip of the DNS server.
Yes, the two ip are same.


4.

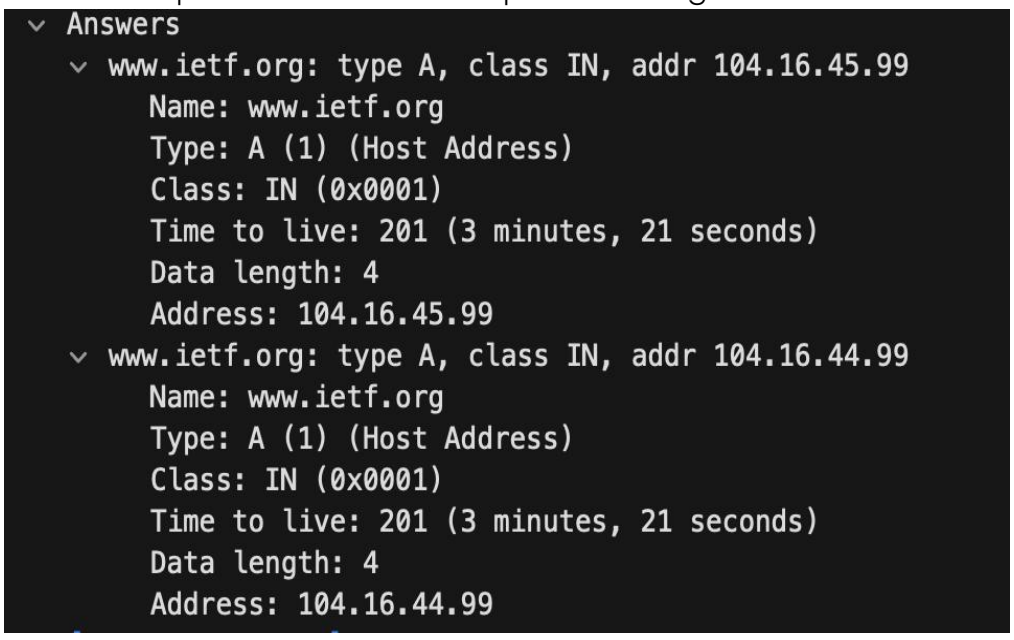



The type of the DNS message query is type A.
No, the query message does not contain any answers.

5.




2 answers are provided in the DNS response message.



The two answers contaied 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.

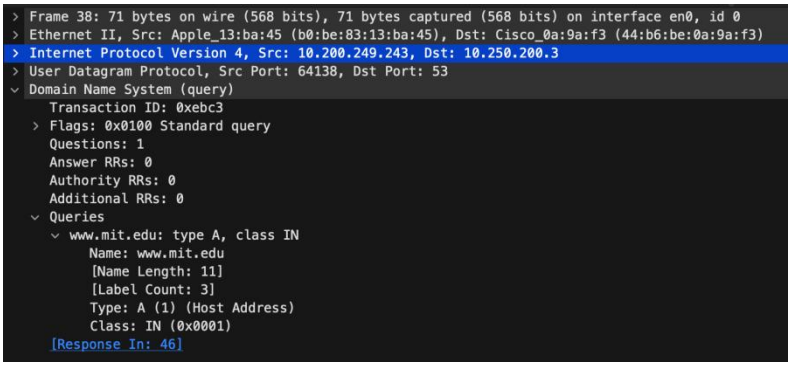
6.


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:



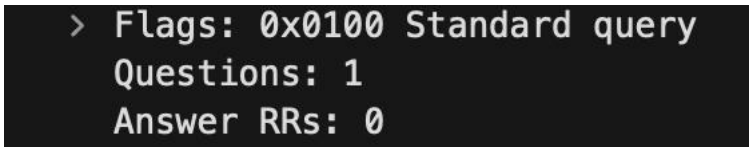

1.

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

2.

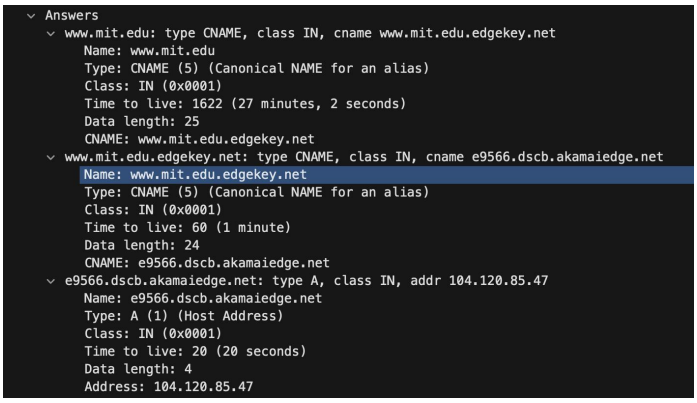
Both have ip address: 10.250.200.3
Yes, both of them have the same ip.

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



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.



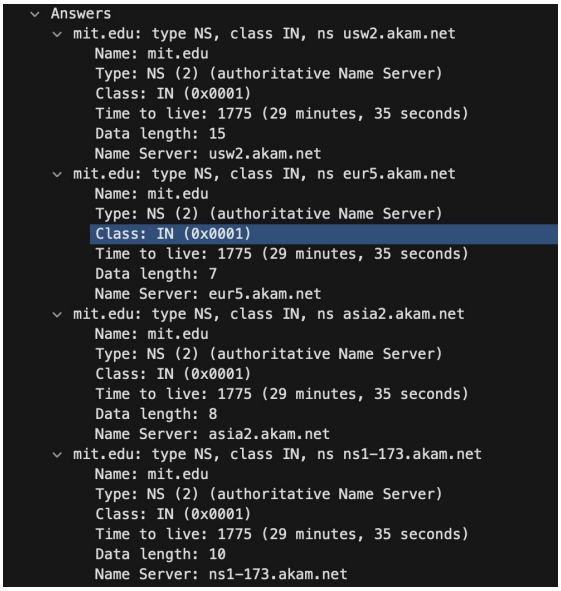

## Part 4.2:

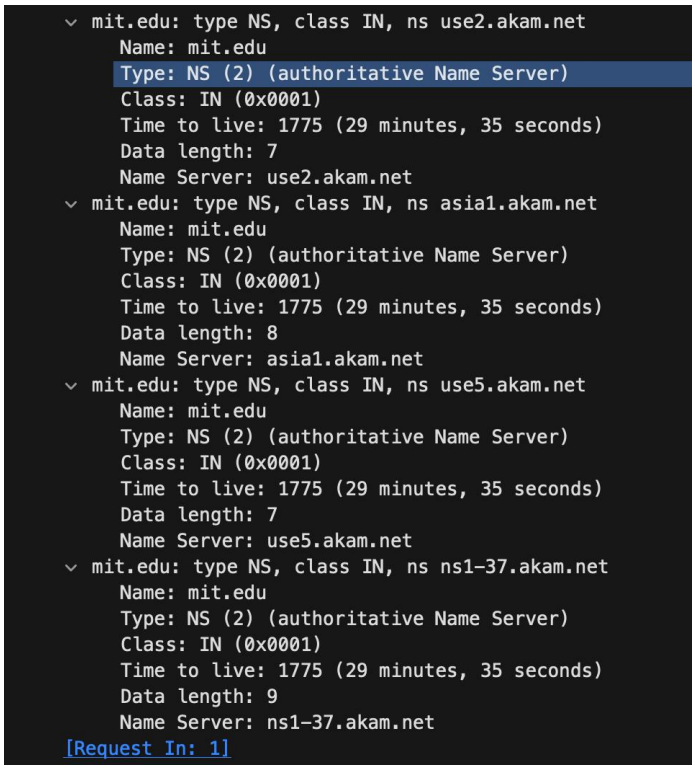
1. The DNS query message was sent to 10.250.200.3. Yes, it matches with that of the local DNS server.

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 nameserver: 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.





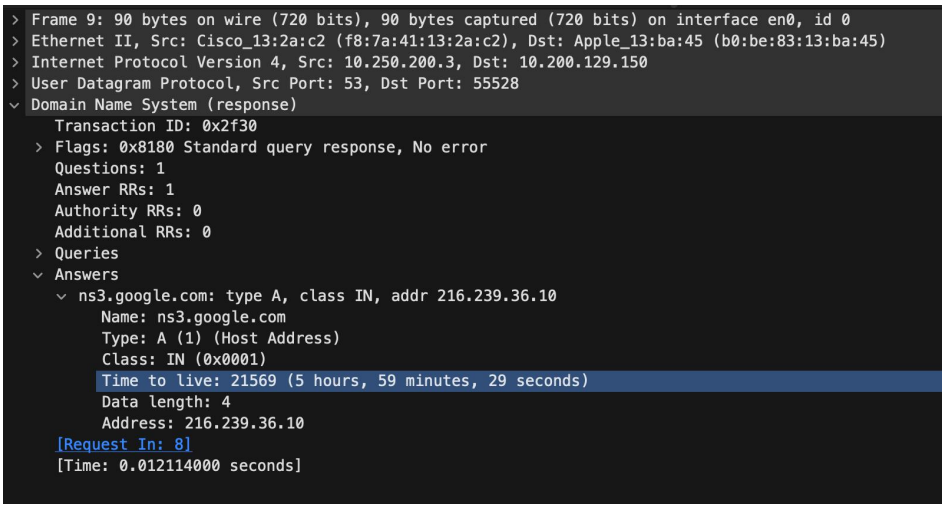

## Part 4.3

1. The DNS query message was sent to 10.250.200.3. Yes it is same to the address of the 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
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
Answers
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]