Assignment 4

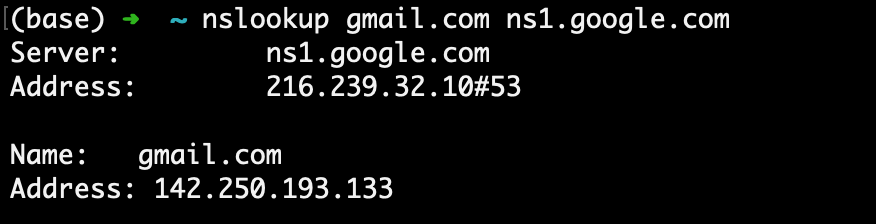
Om Deshmukh

210010033

Part 1:

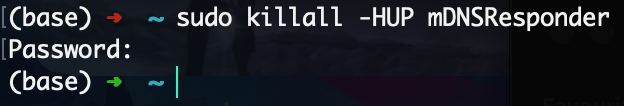
The ip address of [www.iitdh.ac.in](http://www.iitdh.ac.in) server is **10.195.250.62**

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

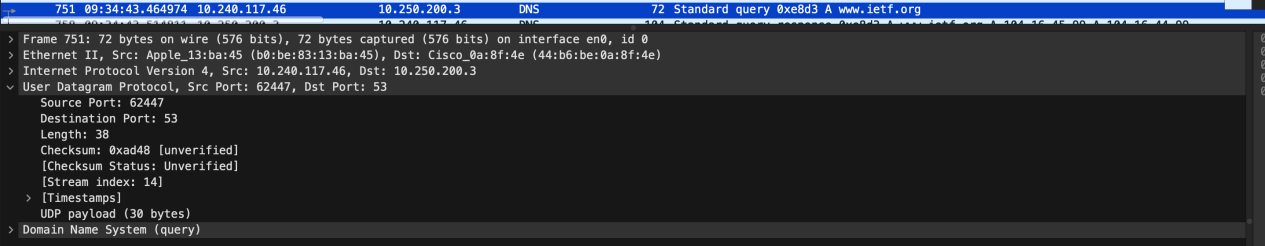


The ip for gmail.com is **142.250.193.133**

Part 2:



Part 3:

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

They follow the UDP stream.

The destination port for the DNS query message is **53**.

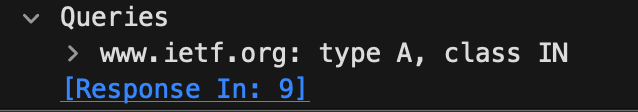
The source port of the DNS response message is **53**.

**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.

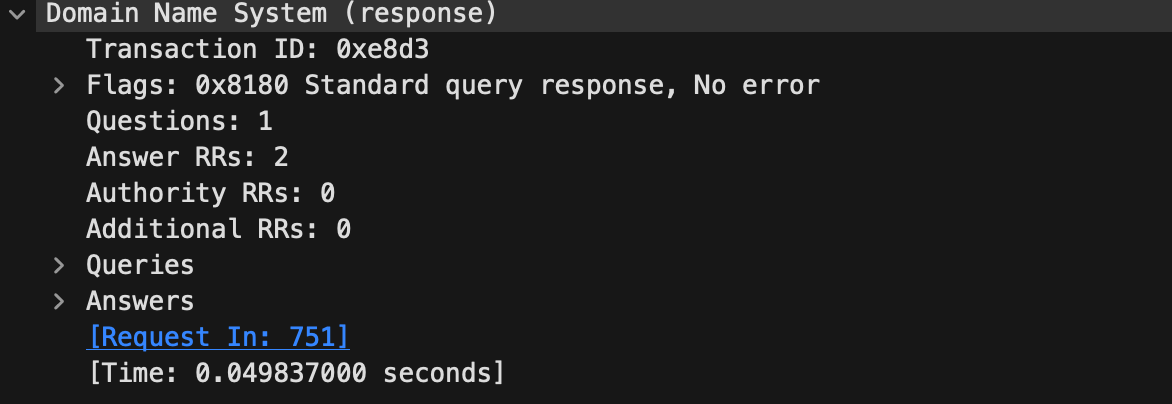
Yes, the two ip are same.

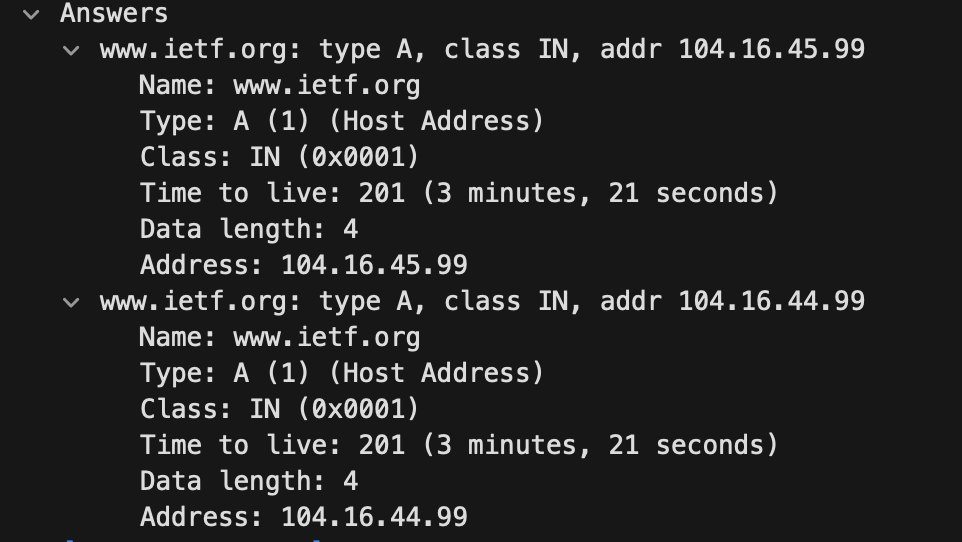
Screenshot 2024-01-31 at 10.44.39 AM



The type of the DNS message query is type A**.**

No, the query message does not contain any answers.



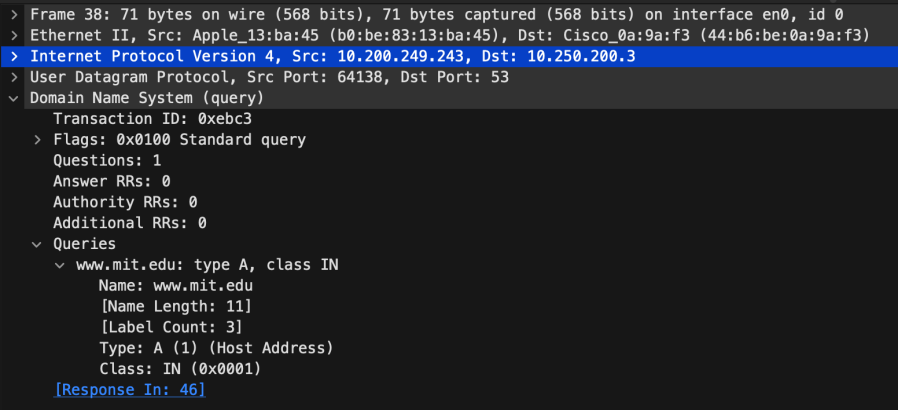
2 answers are provided in the DNS response message.

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.](http://www.ietf.org.)

The destination IP address of the SYN packet corresponds to the ip address of [www.ietf.org](http://www.ietf.org) which was mentioned in the answers of the query response message.

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:**



Destination port of query message: 53

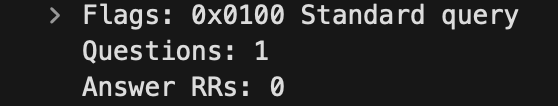
Source port of response message: 53

Both have ip address: **10.250.200.3**

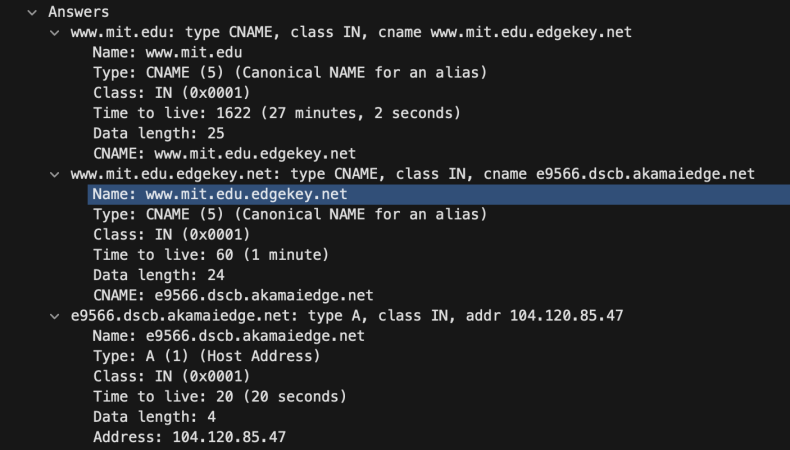
**Yes**, both of them have the same ip.

1. Query message is of type A

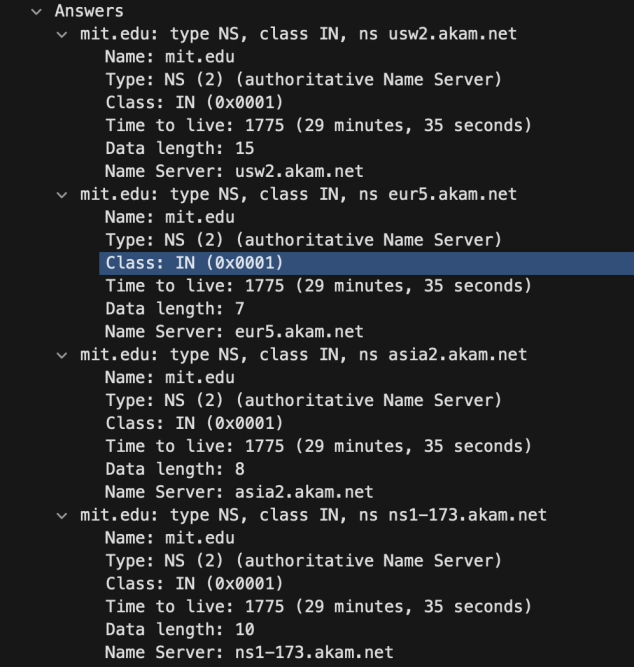
No answers in the query message.

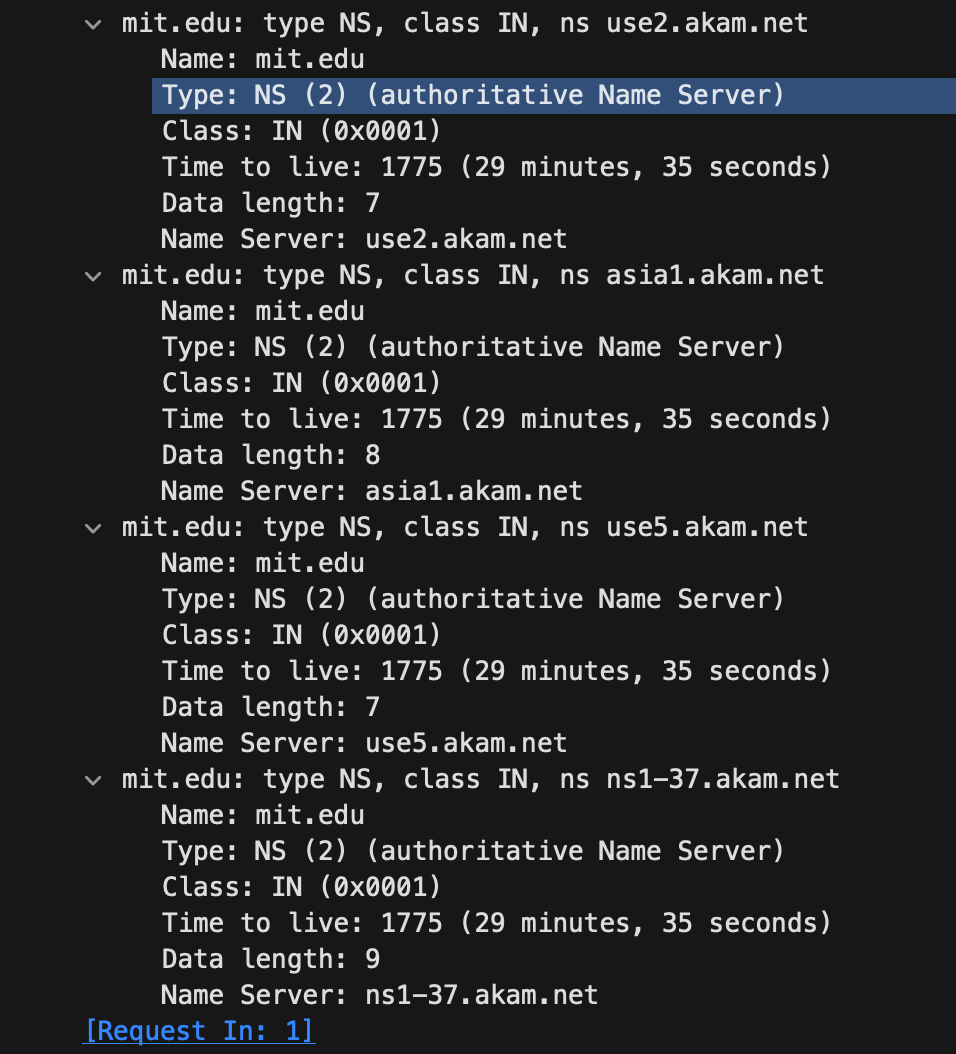


1. 3 answers are provided to the response message.They contain various information such as name, type, class, TLL, data length and CNAME of the DNS servers.



**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**

****

**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. 