# Assignment 4: DNS

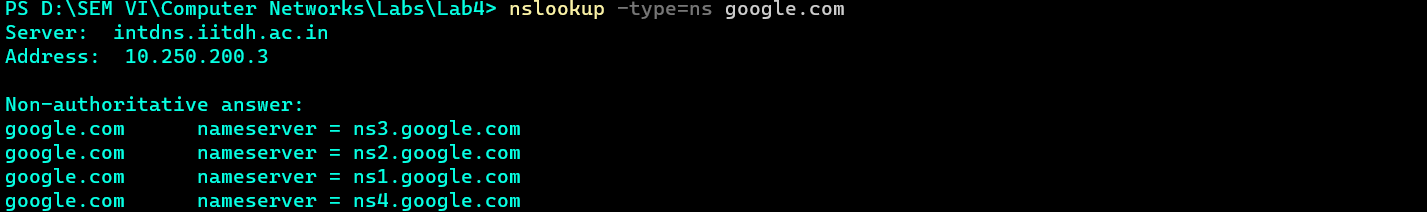
Hrishikesh Ravindra Karande 210010020

Part1:

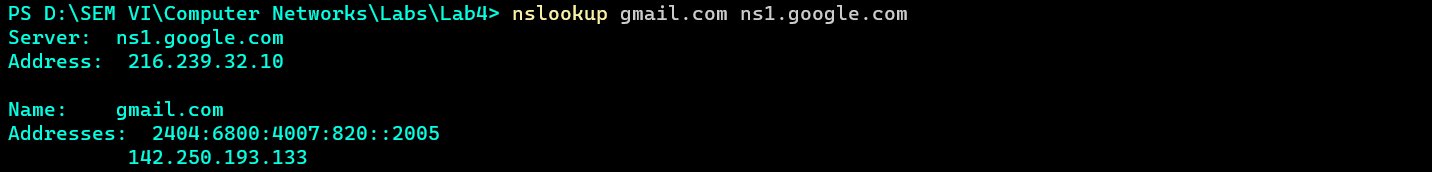
1. IP Address: 10.195.250.62



1. The servers for google.com can be found out using -ns option.

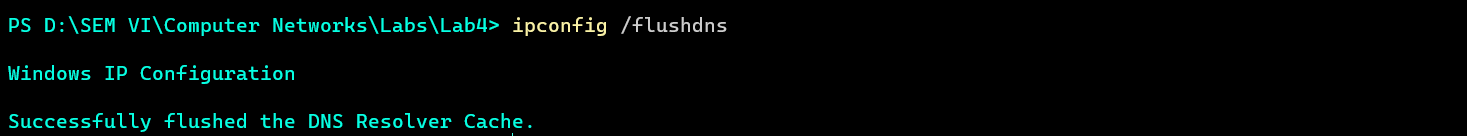


1. Queried server ns1.google.com instead of using server intdn.iitdh.ac.in obtained from Q2. The IP Address can be seen below.



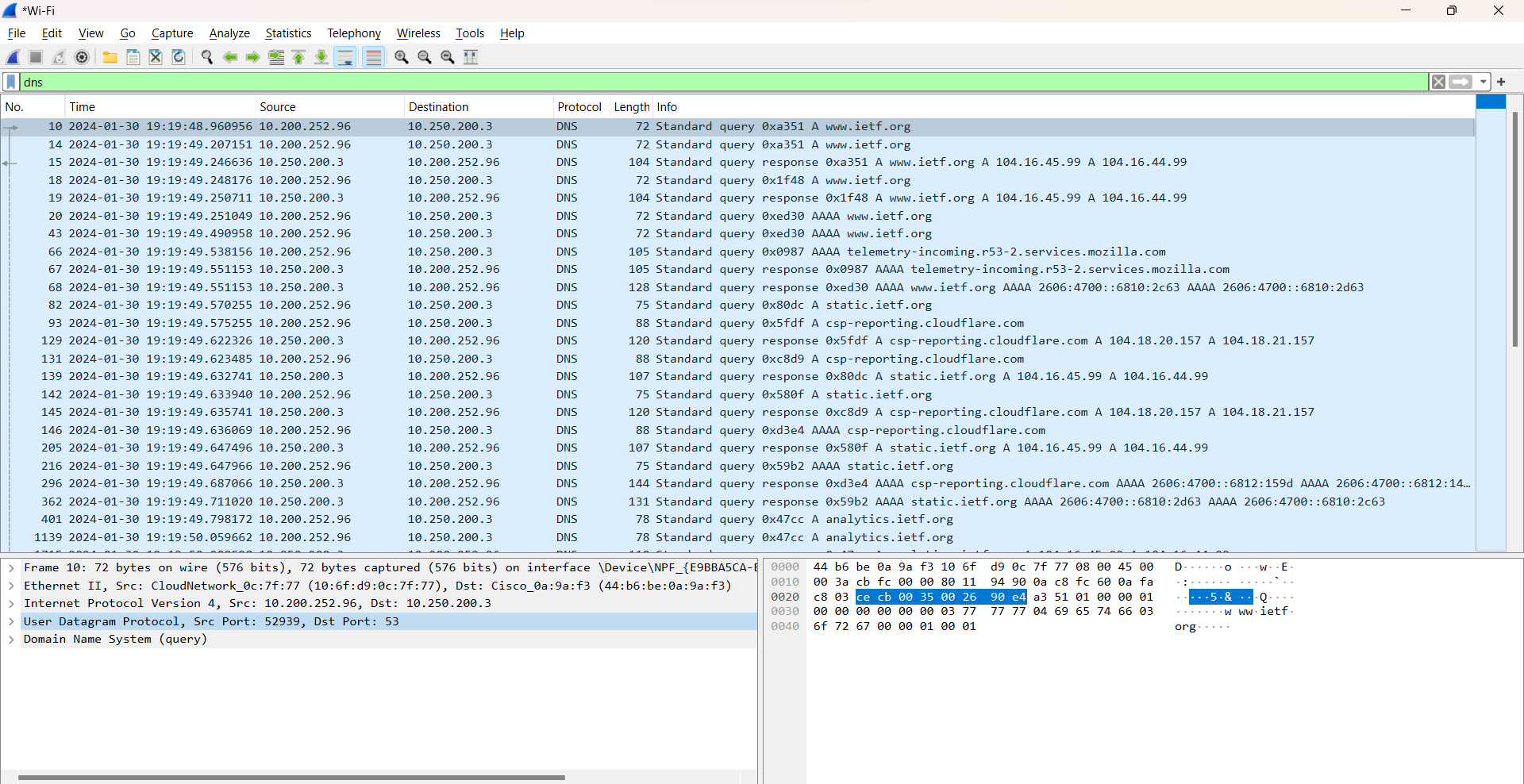
Part2

1. ipconfig /flushdns

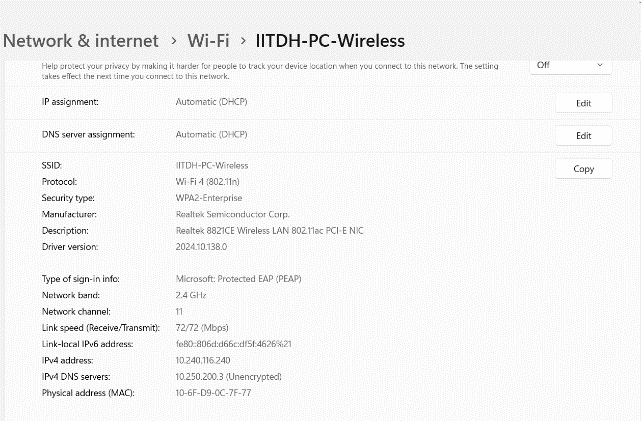


Part3

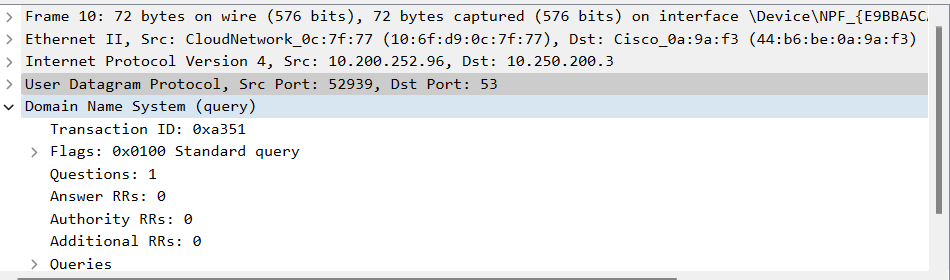
1. DNS Follows UDP protocol.



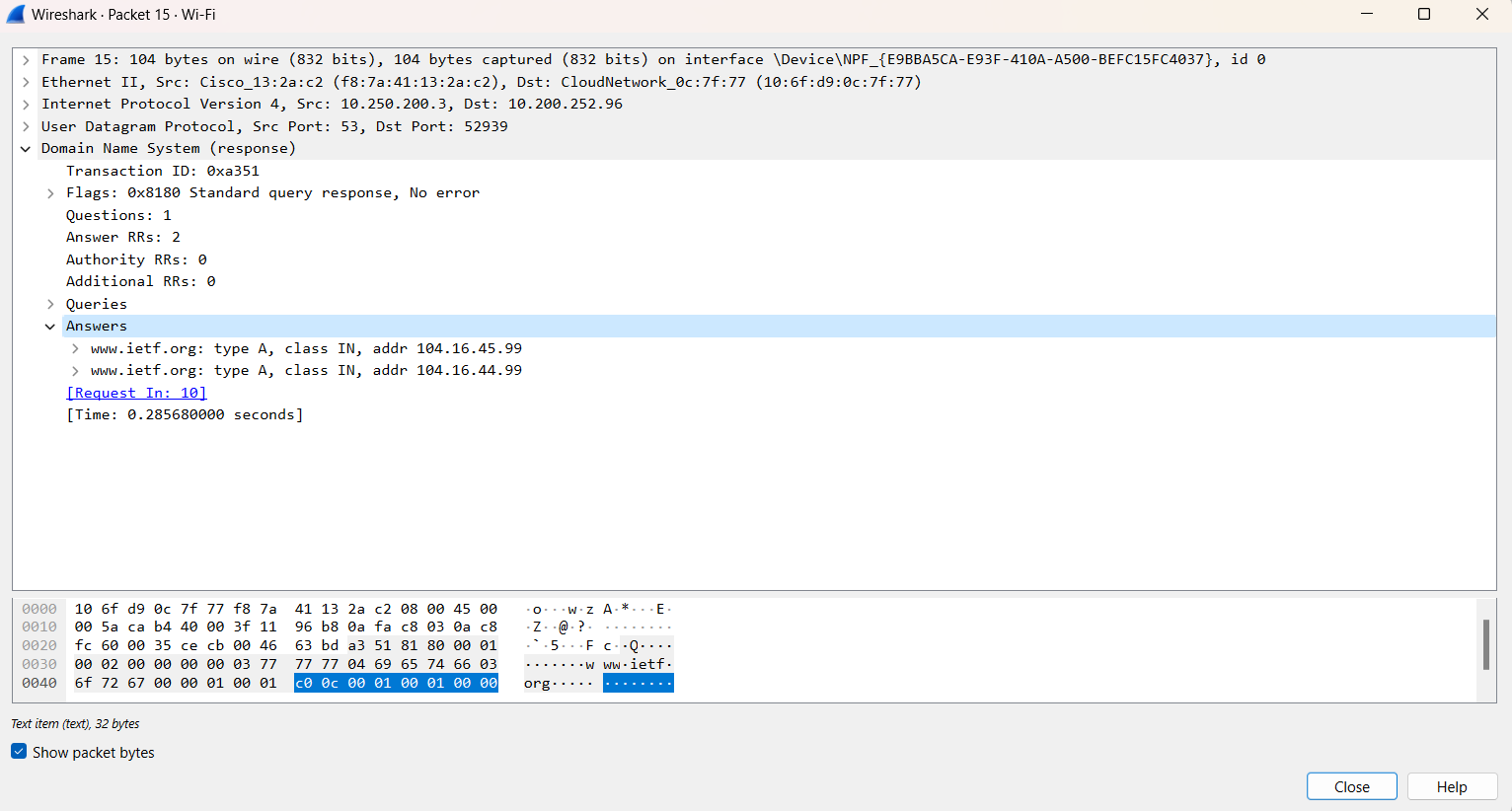
1. The source for DNS Query Message and destination for DNS response message is **port 53.**
2. The highlighted IPv4 address matches the destination address obtained by checking the wifi settings on local computer.



1. The DNS Query is Type A Standard Query and contains 0 answers.



1. Two answers is provided. Contents of answers are: Name, Type, Class, Time To Live(TTL) and Address.



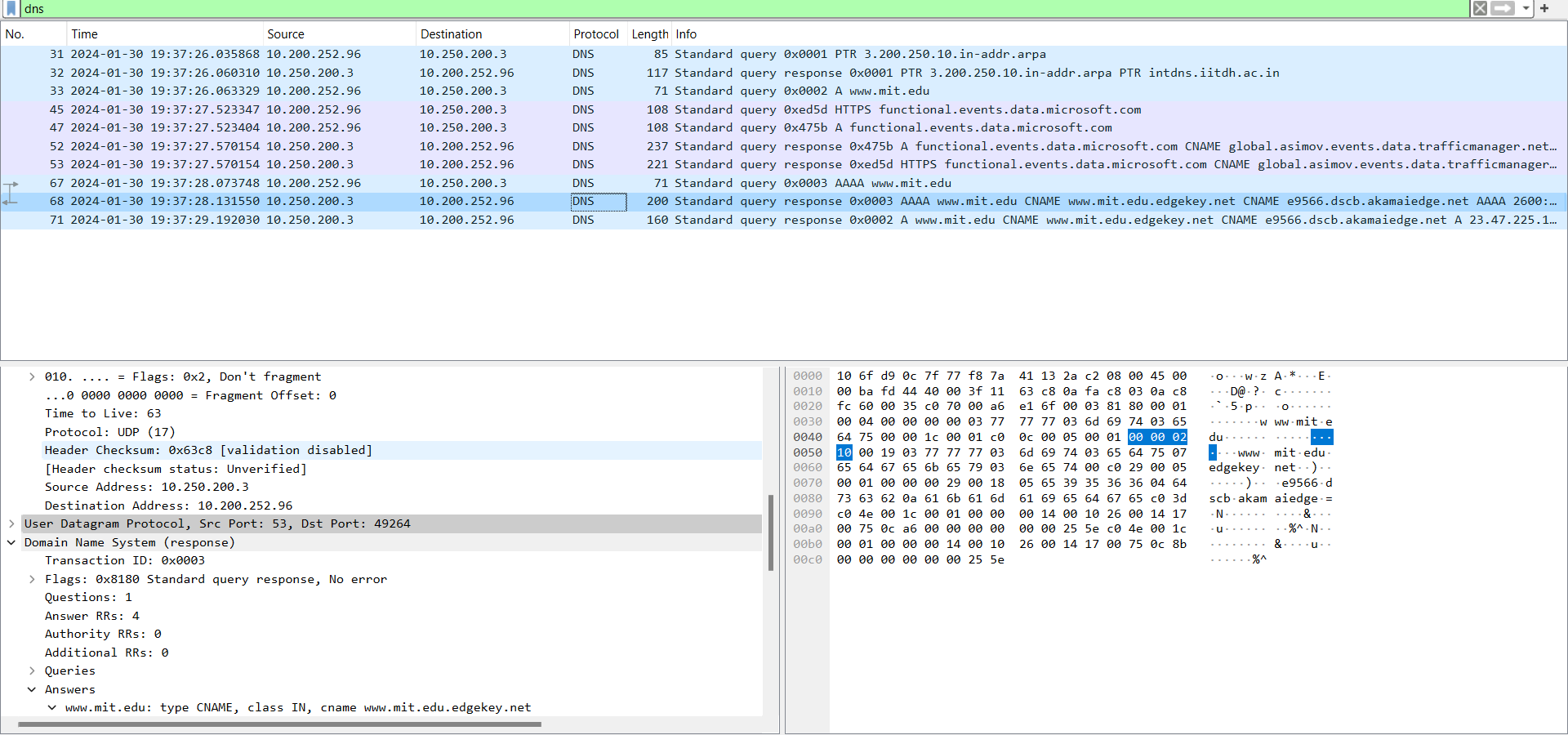
1. The Destination IP address on first TCP-SYN packet 10.240.116.240 corresponds to first DNS response message.
2. No, the images are all loaded from www.ietf.org, so no additional DNS queries are necessary to fetch the request of objects.

Part4

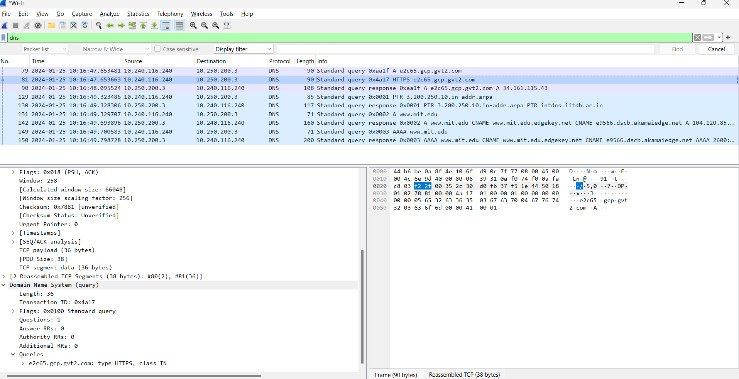
1.

1. The Destination port for DNS = 53

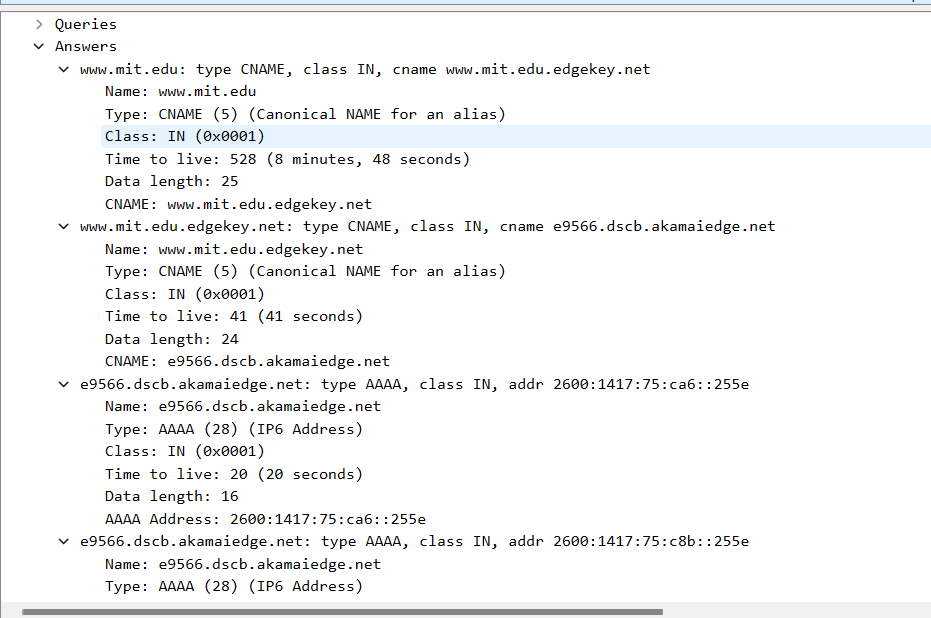
Query port for DNS Response=53



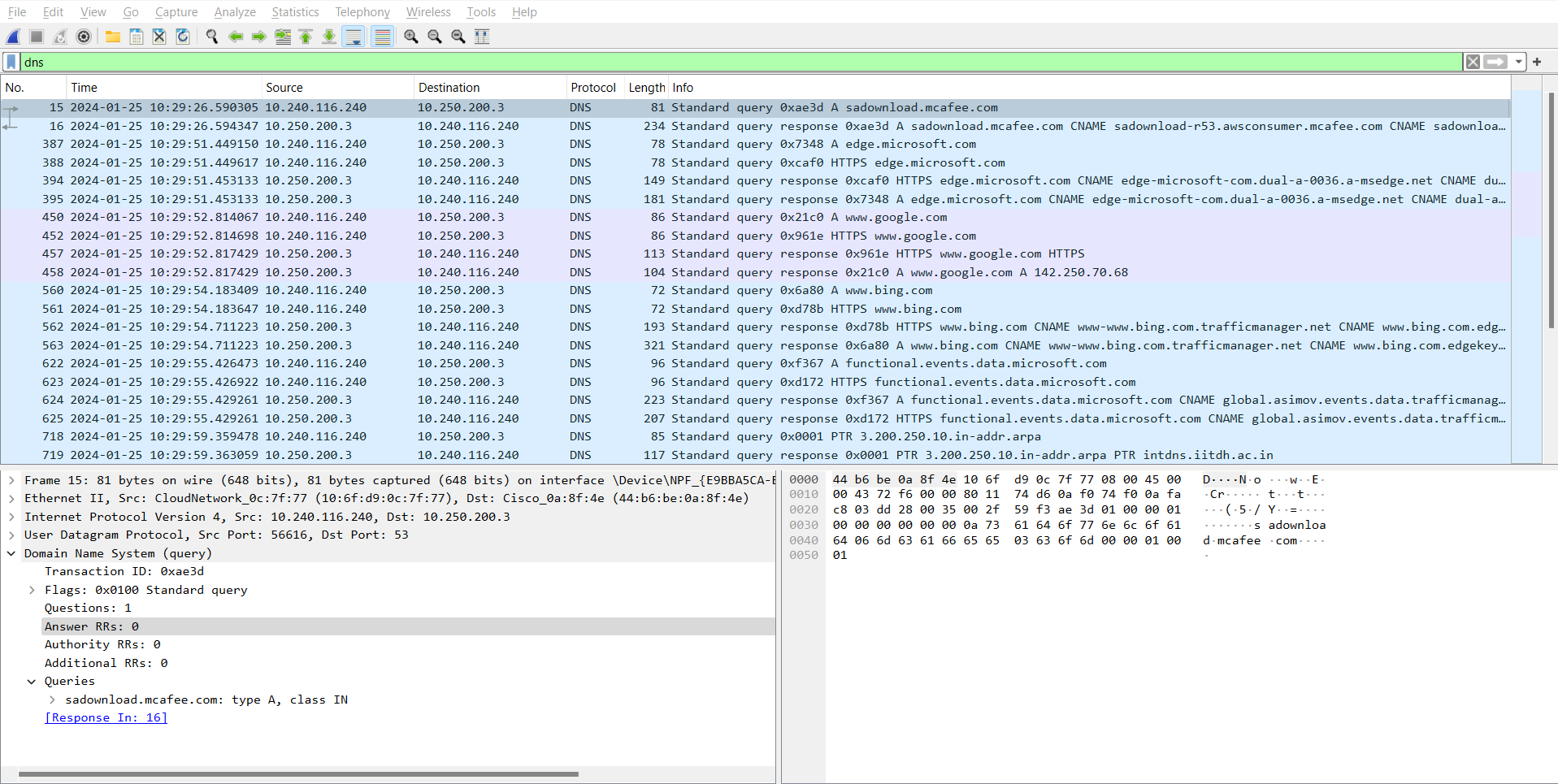
1. Destination IP is 10.250.200.3 ,Yes this is the IP of my default local DNS server.
2. Destination Port for DNS Query Message: 10.240.200.3
3. This is Type A Query and the Query message contains no answers.

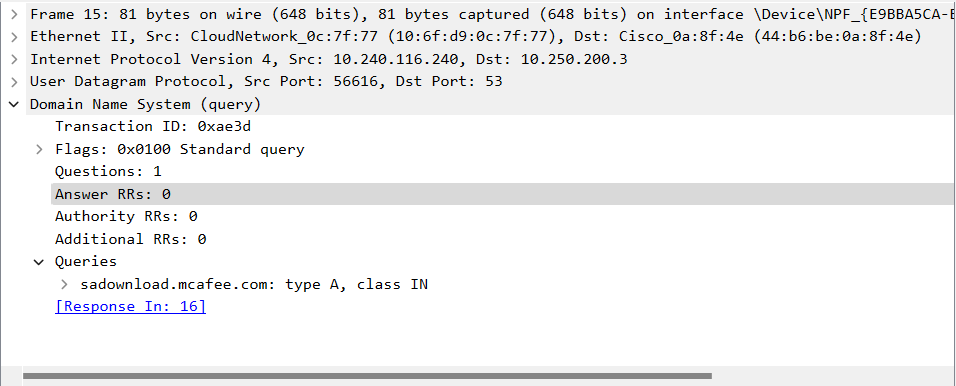


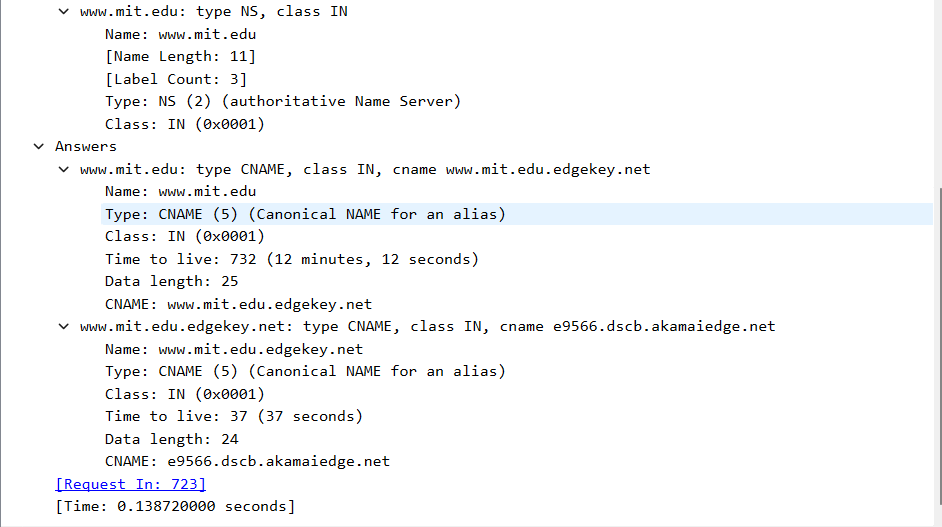
1. There are four answers two are Canonical and two are type A which is attached in screenshot below. Each contains name,type,class,TTL,Data Length and CNAME/AAAA Address as per the Type of packet.

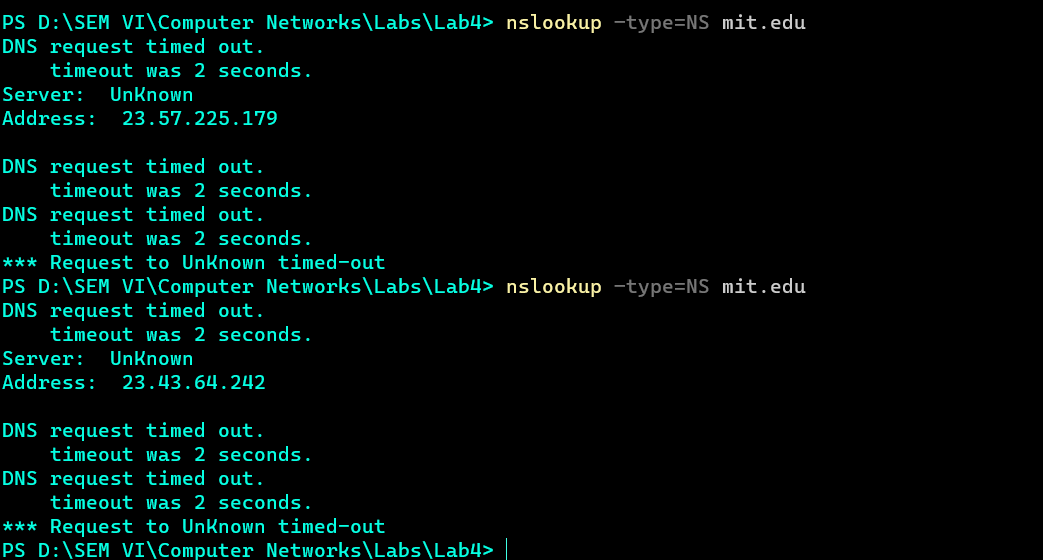


2.

1. The DNS Query message is sent to 10.250.200.3, same as my local server address.
2. The type of query is A. There are no answers in query message.

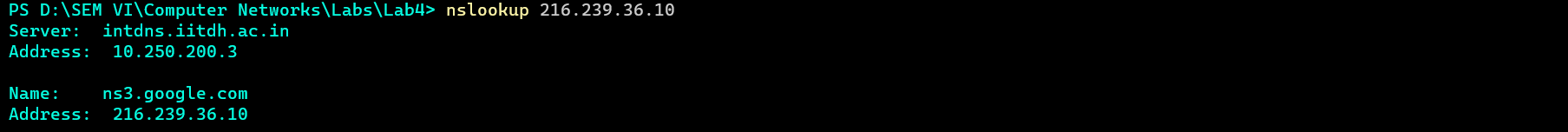


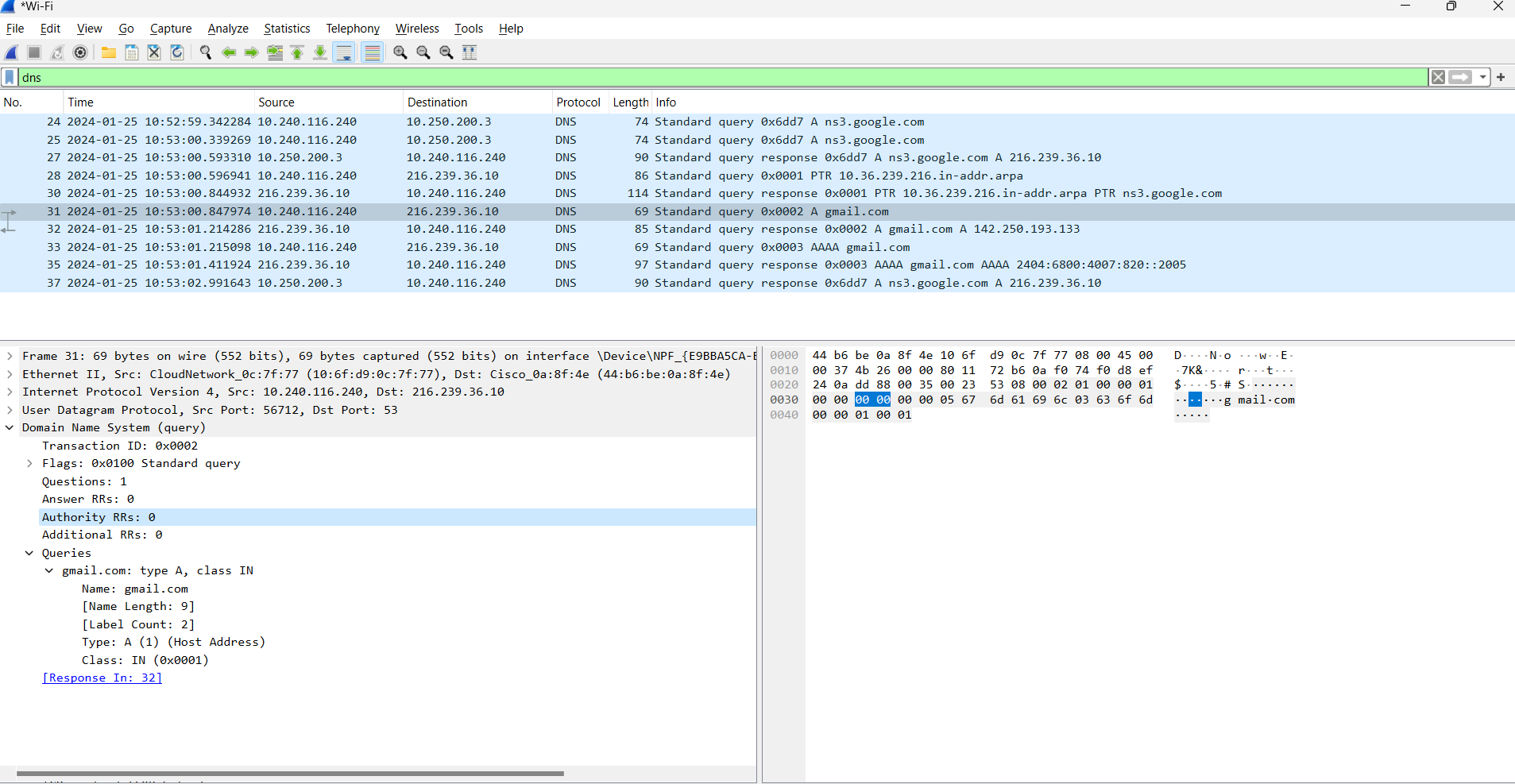
1. I could not find any MIT nameservers here, to verify this I have attached the screenshots also.



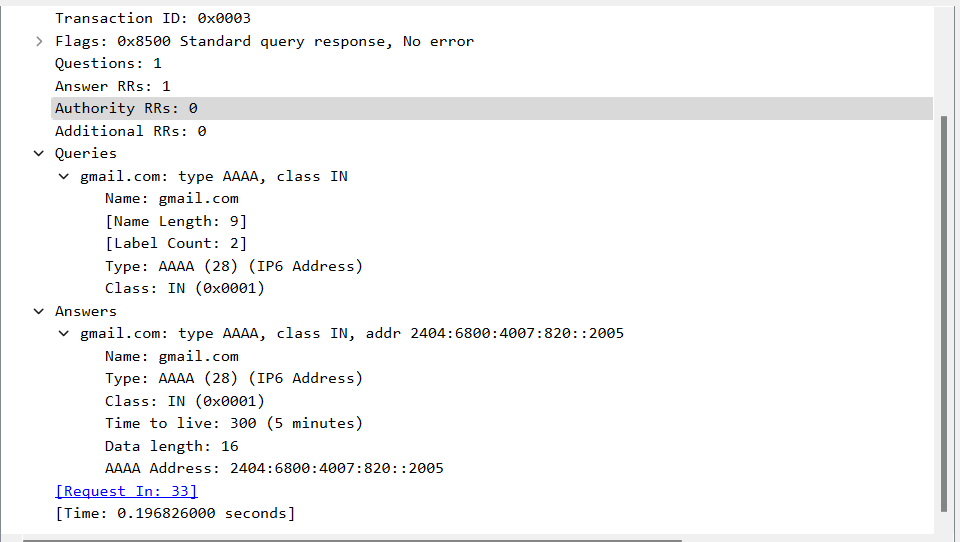
3.

1. Destination IP Address = 216.239.36.10 This is not the IP Address of my default DNS nameserver. This is because we have queried for specific DNS server given in question. After using nslookup to look for server name using this ip we get the server name as ns3.google.com itself this verifies our onservation.





1. Type is Type A Query and it contains no answers.
2. There is one answer with the following fields(Name,Type,Class,TTL,Data, AAAA Address) as per the screenshot below.



I have attached screenshots for questions separately so the questions which ask to add screenshots I have no written(not repeated the screenshots.)

Notes:

1)The DNS Query Answeres indicates the Hops that are taken.

2) SYN, ACK and SYN,ACK  
**TCP message types**

| **Message** | **Description** |
| --- | --- |
| Syn | Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices. |
| ACK | Helps to confirm to the other side that it has received the SYN. |
| SYN-ACK | SYN message from local device and ACK of the earlier packet. |
| FIN | Used to terminate a connection. |