CS315: Assignment-4

Name: Shahil Patel

Roll No.: 200010039

Part-1: nslookup

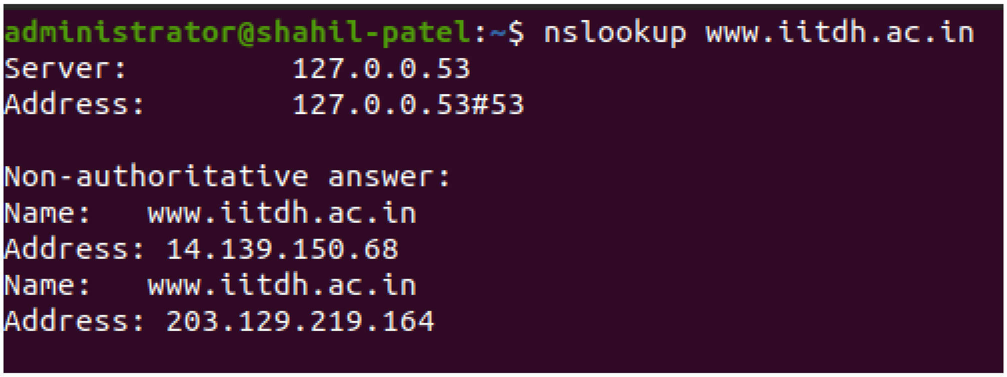
1. Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology Dharwad, India: www.iitdh.ac.in. What is the IP address of www.iitdh.ac.in

Ans: The command used to obtain the IP address of of www.iitdh.ac.in is: **nslookup www.iitdh.ac.in**

The IP address obtained of the web server for the Indian Institute of Technology, Dharwad is

a. **14.139.150.68**

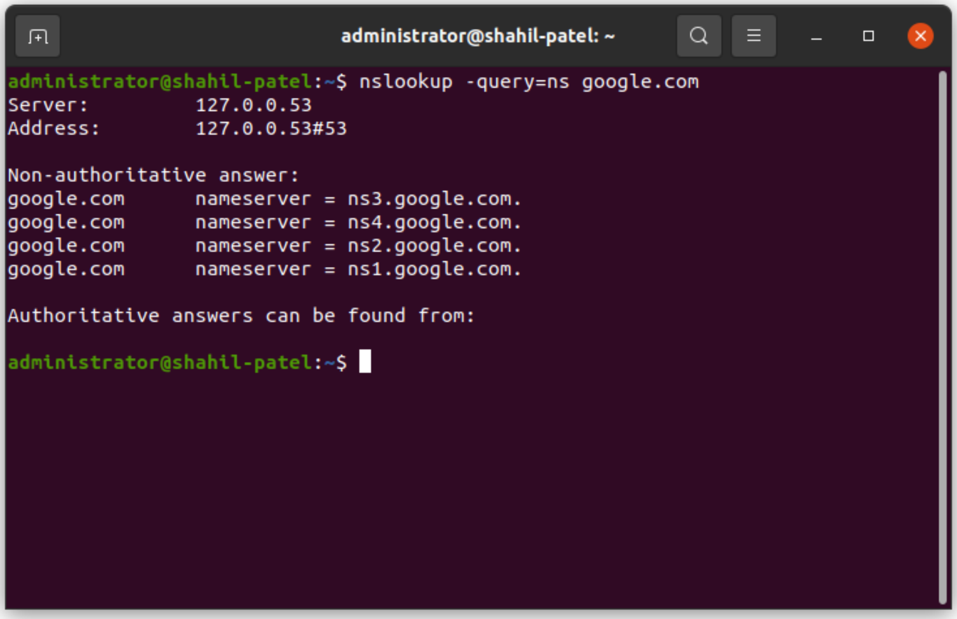
b. **203.129.219.164**



```
administrator@shahil-patel:~$ nslookup www.iitdh.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.iitdh.ac.in
Address: 14.139.150.68
Name:   www.iitdh.ac.in
Address: 203.129.219.164
```

2. Run *nslookup* to determine the DNS servers for google.com.

Ans: The DNS servers for google.com are: ***(ns4/ns3/ns2/ns1).google.com*** as shown in the figure.

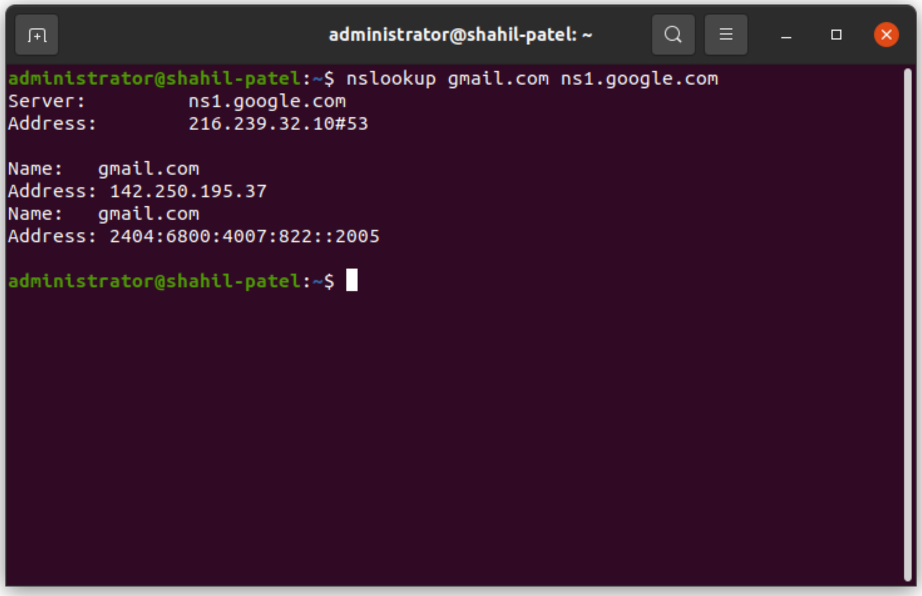


```
administrator@shahil-patel:~$ nslookup -query=ns google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns1.google.com.

Authoritative answers can be found from:

administrator@shahil-patel:~$ 
```

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for gmail.com. What is its IP address?

Ans: The command is: ***nslookup gmail.com ns1.google.com***

The IP address is: ***142.250.195.37***



```
administrator@shahil-patel:~$ nslookup gmail.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   gmail.com
Address: 142.250.195.37
Name:   gmail.com
Address: 2404:6800:4007:822::2005

administrator@shahil-patel:~$ 
```

Part-3: Tracing DNS with Wireshark

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Ans: The DNS query and response messages are sent over **UDP**.

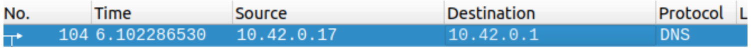
2. What is the destination port for the DNS query message? What is the source port of DNS response messages?

Ans: The Destination port for the DNS query message is: **53**

The Source port for the DNS response message is: **53**

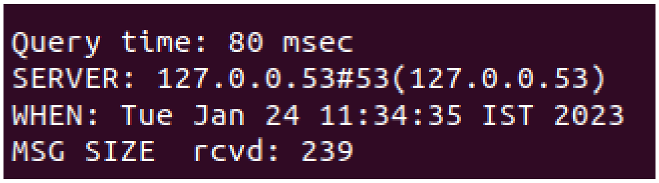
3. To what IP address is the DNS query message sent? Use *ipconfig(Windows)/dig(Linux)* to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans: The IP address to which the DNS query is sent is: **10.42.0.1**



No.	Time	Source	Destination	Protocol	L
104	6.102286530	10.42.0.17	10.42.0.1	DNS	

The IP address of local DNS server is: **127.0.0.53**

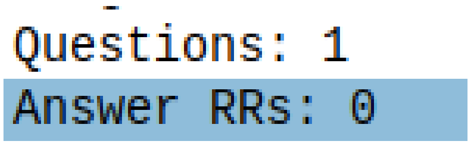


```
Query time: 80 msec
SERVER: 127.0.0.53#53(127.0.0.53)
WHEN: Tue Jan 24 11:34:35 IST 2023
MSG SIZE  rcvd: 239
```

4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Ans: Type of the DNS query is: **A**

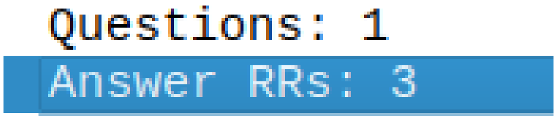
The query message has **0** answers.



```
Questions: 1
Answer RRs: 0
```

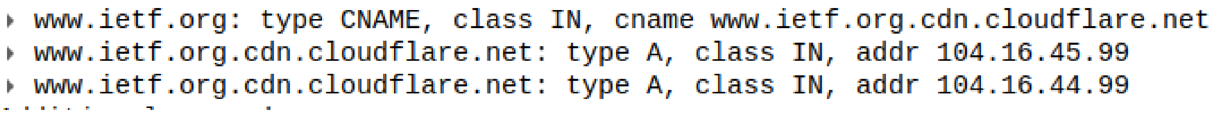
5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Ans: There are **3** answers.



```
Questions: 1
Answer RRs: 3
```

The first answer contains ***CNAME*** which is alias of the Domain Name, while next two answers contains the *IP address of the Doman Name*.



```
▸ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
```

6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans: **Yes**, the DNS response message contains the IP address to which the TCP SYN packet was sent.

7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

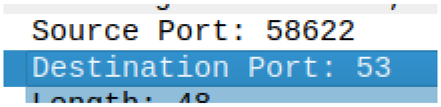
Ans: No, The host doesn't issue new DNS queries.

Part-4: Wireshark and nslookup

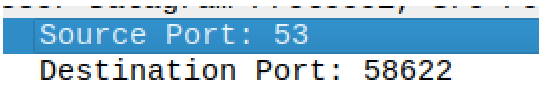
1. What is the destination port for the DNS query message? What is the source port of DNS response messages?

Ans: The destination port for the DNS query message is: **53**

The source port of DNS response messages is: **53**



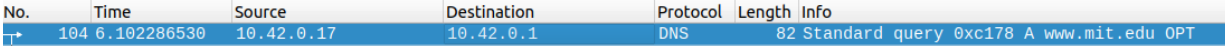
```
Source Port: 58622
Destination Port: 53
Length: 48
```



```
Source Port: 53
Destination Port: 58622
```

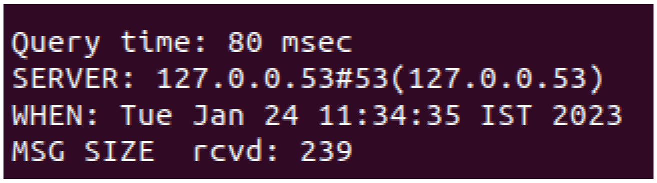
2. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans: The IP address where the DNS query message is sent is: **10.42.0.1.**



```
No.   Time          Source      Destination  Protocol  Length  Info
  104 6.102286530   10.42.0.17  10.42.0.1    DNS           82  Standard query 0xc178 A www.mit.edu OPT
```

IP address of local DNS server: **127.0.0.53**



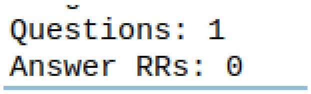
```
Query time: 80 msec
SERVER: 127.0.0.53#53(127.0.0.53)
WHEN: Tue Jan 24 11:34:35 IST 2023
MSG SIZE  rcvd: 239
```

No, For my system the IP address of the destination for the DNS query message and IP address of my local DNS server is not same.

3. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans: The type of DNS query is: **A**

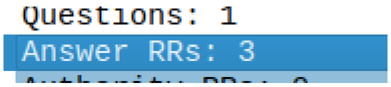
There are **0** answers:



```
Questions: 1
Answer RRs: 0
```

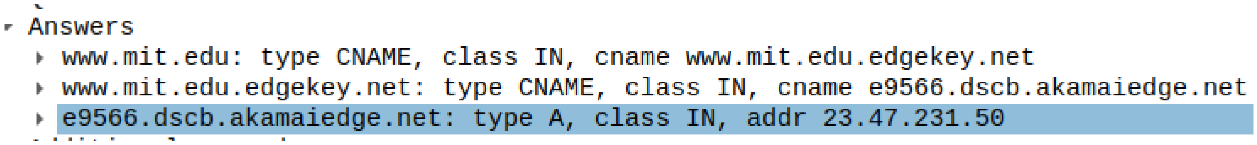
4. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans: There are **3** answers:



```
Questions: 1
Answer RRs: 3
```

The first and second answers contains ***CNAME*** which is alias of the Domain Name, while the third answer contains the *IP address of the Doman Name*.

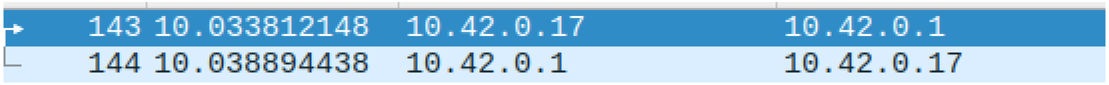


```
▾ Answers
  ▸ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  ▸ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  ▸ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.47.231.50
```

5. Screenshots have been attached below answers of each questions

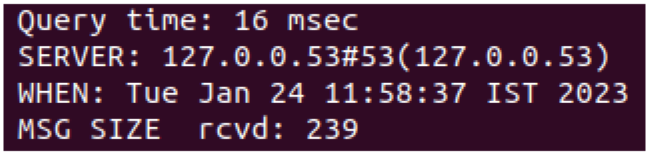
6. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans: IP address to which the DNS query message was sent is: **10.42.0.1**



```
143 10.033812148   10.42.0.17             10.42.0.1
144 10.038894438   10.42.0.1              10.42.0.17
```

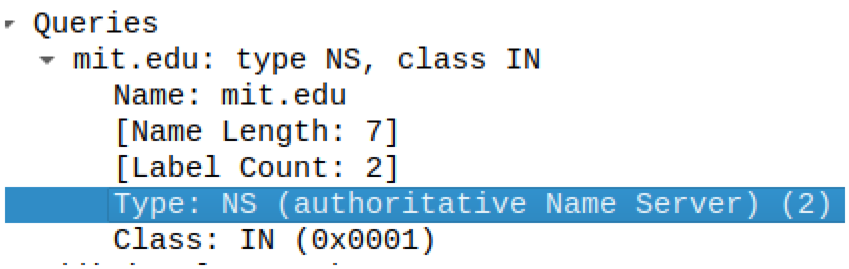
IP address of local DNS server is: **127.0.0.53**



```
Query time: 16 msec
SERVER: 127.0.0.53#53(127.0.0.53)
WHEN: Tue Jan 24 11:58:37 IST 2023
MSG SIZE  rcvd: 239
```

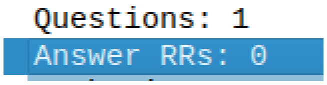
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans: Type of DNS query is: **NS**



```
▾ Queries
  ▾ mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
```

There are **0** answers:



```
Questions: 1
Answer RRs: 0
```

8. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

Ans: The MIT nameservers provided by the response message are:

a. ***ns1-37.akam.net***

b. ***ns1-173-akam.net***

c. ***usw2.akam.net***

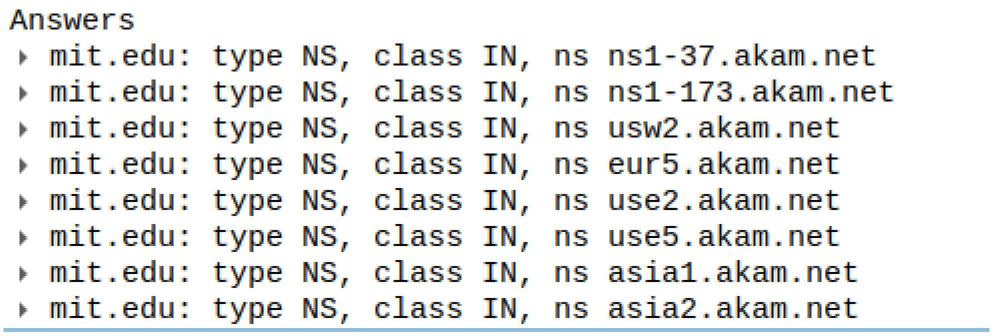
d. ***eur5.akam.net***

e. ***use2.akam.net***

f. ***use5.akam.net***

g. ***asia1.akam.net***

h. ***asia2.akam.net***



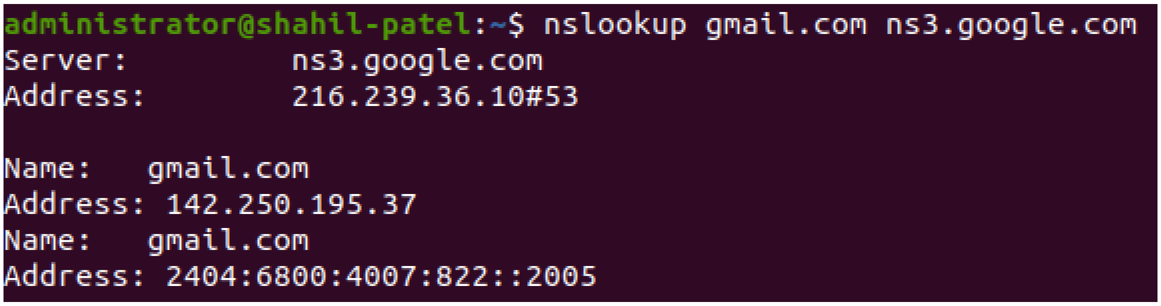
```
Answers
▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
▸ mit.edu: type NS, class IN, ns usw2.akam.net
▸ mit.edu: type NS, class IN, ns eur5.akam.net
▸ mit.edu: type NS, class IN, ns use2.akam.net
▸ mit.edu: type NS, class IN, ns use5.akam.net
▸ mit.edu: type NS, class IN, ns asia1.akam.net
▸ mit.edu: type NS, class IN, ns asia2.akam.net
```

No, the response ***doesn't provide IP address***.

9. The screenshots have been attached below each anwer.

10. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Ans: The DNS message is sent to the IP address: **216.239.36.10**

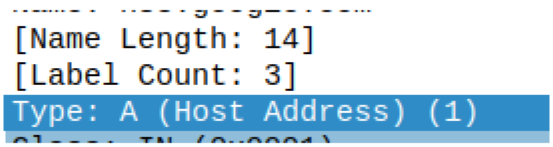


```
administrator@shahil-patel:~$ nslookup gmail.com ns3.google.com
Server:         ns3.google.com
Address:        216.239.36.10#53

Name:   gmail.com
Address: 142.250.195.37
Name:   gmail.com
Address: 2404:6800:4007:822::2005
```

No, the IP address doesn't match the IP address of our Local DNS Server because the request is sent to the *ns3.google.com*

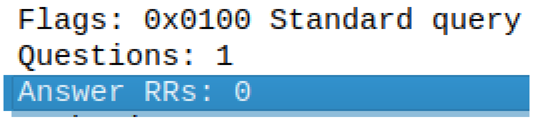
11. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Ans: The type of DNS query is: **A**



```
[Name Length: 14]
[Label Count: 3]
Type: A (Host Address) (1)
```

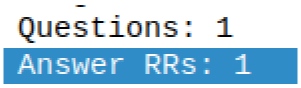
There are **0** answers:



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

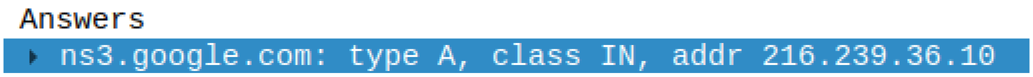
12. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

Ans: There is **1** answer



```
Questions: 1
Answer RRs: 1
```

The answer contain the IP address of *ns3.google.com* which is ***216.239.36.10***



```
Answers
  ▸ ns3.google.com: type A, class IN, addr 216.239.36.10
```

13. The screenshots have been attached with answers of each question.