

Computer Networks Lab, Assignment 4

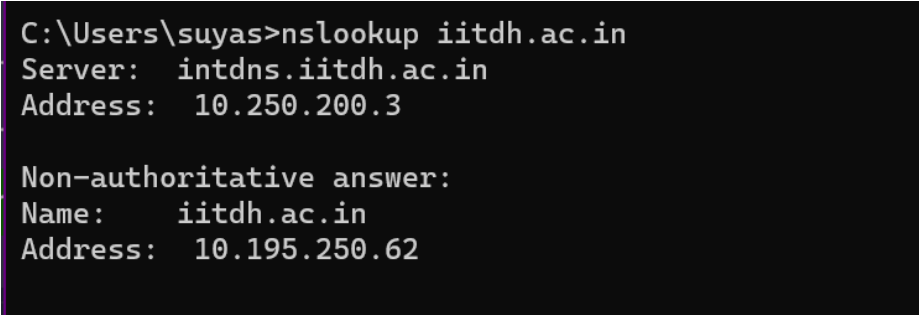
Suyash Gaurav

210010054

1 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`?

IP of iitdh: 10.195.250.62



```
C:\Users\suyas>nslookup iitdh.ac.in
Server:   intdns.iitdh.ac.in
Address:  10.250.200.3

Non-authoritative answer:
Name:     iitdh.ac.in
Address:  10.195.250.62
```

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

Got 4 DNS servers for `google.com`. Screenshot attached.

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for `gmail.com`.

```
C:\Users\suyas>nslookup -type=NS google.com
Server:   intdns.iitdh.ac.in
Address:  10.250.200.3

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

Figure 1: Q2.google.com DNS servers

What is its IP address?

`nslookup gmail.com ns1.google.com`. Using `ns1.google.com` nameserver, IP address of `gmail.com` is `142.250.193.133`

```
C:\Users\suyas>nslookup gmail.com ns1.google.com
Server:   ns1.google.com
Address:  216.239.32.10

Name:     gmail.com
Addresses: 2404:6800:4007:820::2005
          142.250.193.133
```

Figure 2: Q3. gmail.com

2 Part - 2: The DNS cache on your computer

ipconfig /flushdns

3 Part - 3 Tracing DNS with Wireshark

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

They are sent over UDP(User Datagram Protocol).

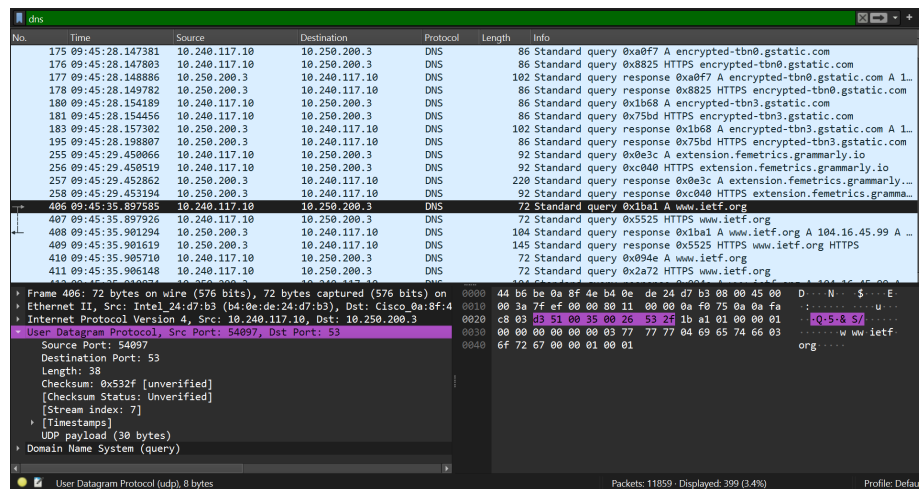


Figure 3: Q1. DNS query and response messages

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

Destination Port: 53 Source Port: 54097

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?

The DNS query message is sent to 10.250.200.3, Yes my local DNS server is same as this.

```
486 09:45:35.897585 10.240.117.10 10.250.200.3 DNS 72 Standard query 0x1ba1 A www.ietf.org

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
Physical Address. . . . . : B4-0E-DE-24-D7-B3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
IPv4 Address. . . . . : 10.240.117.10(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Lease Obtained. . . . . : 25 January 2024 08:38:32
Lease Expires . . . . . : 25 January 2024 10:59:50
Default Gateway . . . . . : 10.240.116.2
DHCP Server . . . . . : 10.240.116.1
DNS Servers . . . . . : 10.250.200.3
NetBIOS over Tcpip. . . . . : Enabled
```

Figure 4: Q3. local DNS

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

It is showing ”Type” of DNS query is type A. But query message does not contain ”answers”.

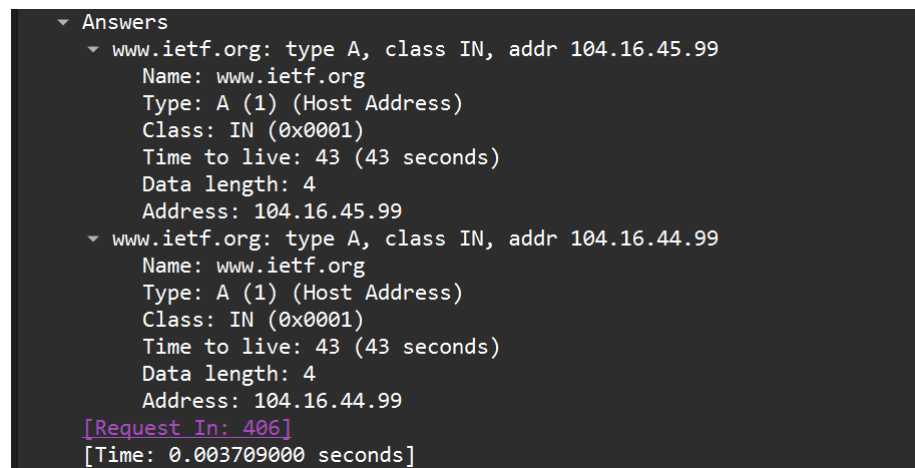
```
▼ Queries
  ► www.ietf.org: type A, class IN
    [Response In: 408]
```

Figure 5: Q4. DNS query message

5. Examine the DNS response message. How

many “answers” are provided? What do each of these answers contain?

In DNS response message, 2 “answers” are provided. It contain two address corresponding to Name: www.ietf.org

A screenshot of a network packet capture tool showing the 'Answers' section of a DNS response. It lists two A records for the domain www.ietf.org. The first record has an IP address of 104.16.45.99 and the second has 104.16.44.99. Both records show a TTL of 43 seconds and a data length of 4 bytes. At the bottom, it indicates the request ID was 406 and the response time was 0.003709000 seconds.

```
▼ Answers
  ▼ 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: 43 (43 seconds)
    Data length: 4
    Address: 104.16.45.99
  ▼ 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: 43 (43 seconds)
    Data length: 4
    Address: 104.16.44.99
  [Request In: 406]
  [Time: 0.003709000 seconds]
```

Figure 6: Q5. DNS response message “answers”

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?

Yes, the destination IP address of the SYN packet correspond to any of the IP addresses are provided in the DNS response message.

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

No, before retrieving each image, my host does not

issue new DNS queries.

4 Part - 4 Wireshark and nslookup

4.1 1: Answer the following questions:

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

Destination port for the DNS query message is 53. And source port of DNS response messages are also 53.

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

The IP address of DNS message is sent is 10.250.200.3, Yes, this IP is my default local DNS server.

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

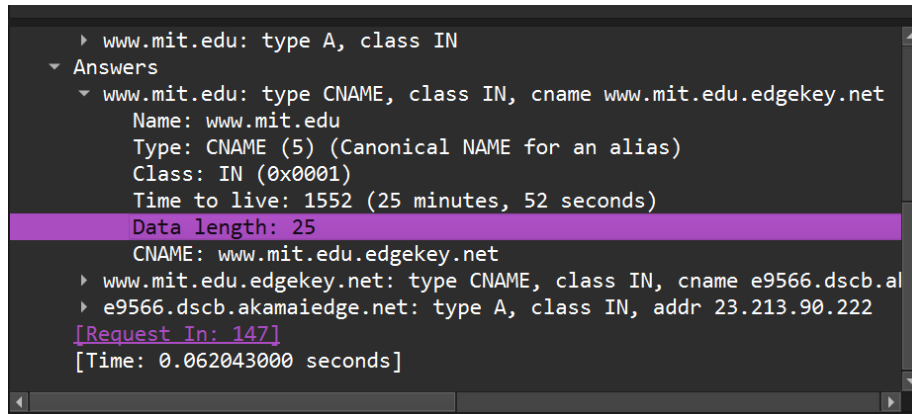
The "Type" of DNS query is standard "queries". No the query does not contain any answers.

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

I got 3 answers. Each answers contain name of host, type, class IN, cname, time to live, data length. They

are as: www.mit.edu: **type** CNAME, class IN, **cname** www.mit.edu.edgekey.net

5. Provide a screenshot.



```

  ▶ www.mit.edu: type A, class IN
  ▼ Answers
    ▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 1552 (25 minutes, 52 seconds)
      Data length: 25
      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 23.213.90.222
  [Request In: 147]
  [Time: 0.062043000 seconds]
```

Figure 7: Q5. DNS response message answers

4.2 2: Now repeat the previous experiment, but instead issue the command: `nslookup -type=NS mit.edu`

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

The IP address of DNS message is sent is 10.250.200.3, Yes, this IP is my default local DNS server.

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

The “Type” of DNS query is NS “queries”. No the query does not contain any answers.

3. Examine the DNS response message. What MIT nameservers does the response message pro-

vide? Does this response message also provide the IP addresses of the MIT timeservers?

MIT nameservers response message provided as **mit.edu**. It provides addr as 23.198.105.5

4. Provide a screenshot.

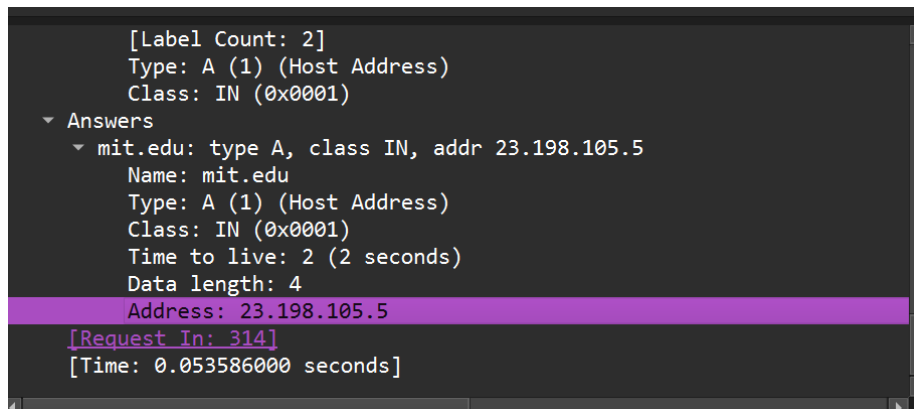


Figure 8: Q4. DNS response message answers

4.3 3: Now repeat the previous experiment, but instead issue the command: `nslookup gmail.com ns3.google.com`

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

The IP address of DNS message is sent to is 216.239.36.10, No, this IP is not my default local DNS server. This IP addresses to ns3.google.com

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

The “Type” of DNS query is standard “queries”. No

the query does not contain any answers.

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

It does provide one answer. It contains the following:
ns3.google.com: type A, class IN, addr 216.239.36.10
along with data-length and time to live.

4. Provide a screenshot.

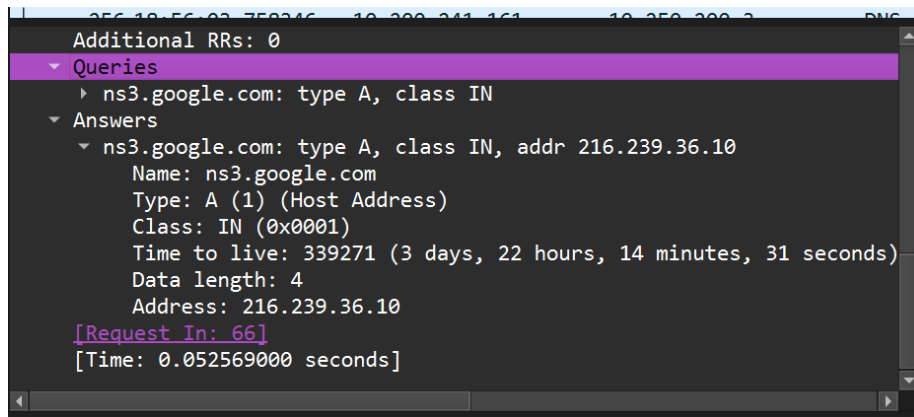


Figure 9: Q4. DNS response message answers ns3.google.com