Name: Abhijit Paul

ID:1201

Lab: WireShark DNS

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

Ans: For Nanyang Technological University, one of its web server's ip is -> 13.107.213.37

```
abhijit@iit-Vostro-3670:~$ nslookup www.ntu.edu.sg
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.ntu.edu.sg  canonical name = ntusitefinity.azurefd.net.
ntusitefinity.azurefd.net       canonical name = star-azurefd-prod.trafficmanager.net.
star-azurefd-prod.trafficmanager.net    canonical name = dual.part-0009.t-0009.t-msedge.net.
dual.part-0009.t-0009.t-msedge.net      canonical name = part-0009.t-0009.t-msedge.net.
Name:   part-0009.t-0009.t-msedge.net
Address: 13.107.213.37
Name:   part-0009.t-0009.t-msedge.net
Address: 13.107.246.37
Name:   part-0009.t-0009.t-msedge.net
Address: 2620:1ec:bdf::37
Name:   part-0009.t-0009.t-msedge.net
Address: 2620:1ec:46::37
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

Ans: One of Oxford's DNS servers is dns0.ox.ac.uk

```
abhijit@iit-Vostro-3670:~$ nslookup -type=NS ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.

Authoritative answers can be found from:

abhijit@iit-Vostro-3670:~$
```

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Ans: We tried two approaches and none returned an answer.

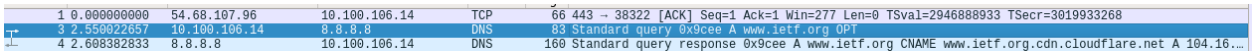
```
abhijit@iit-Vostro-3670:~$ nslookup -type=MX ox.ac.uk dns1.ox.ac.uk
Server:         dns1.ox.ac.uk
Address:        129.67.1.191#53

ox.ac.uk        mail exchanger = 9 in.hes.trendmicro.eu.
```

The following approach seems logical but none of the nameservers returned mail server.

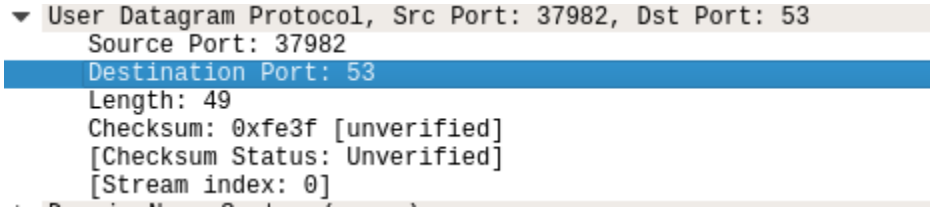
```
abhijit@iit-Vostro-3670:~$ nslookup -type=MX mail.yahoo.com dns0.ox.ac.uk
Server:         dns0.ox.ac.uk
Address:        129.67.1.190#53

** server can't find mail.yahoo.com: REFUSED
```

INFO: ifconfig
Ifconfig -a : To see all host-related information.
Linux does not have any DNS caching enabled by default. On Linux, **there is no OS-level DNS caching unless a caching service such as Systemd-Resolved, DNSMasq, or Nscd is installed and running**

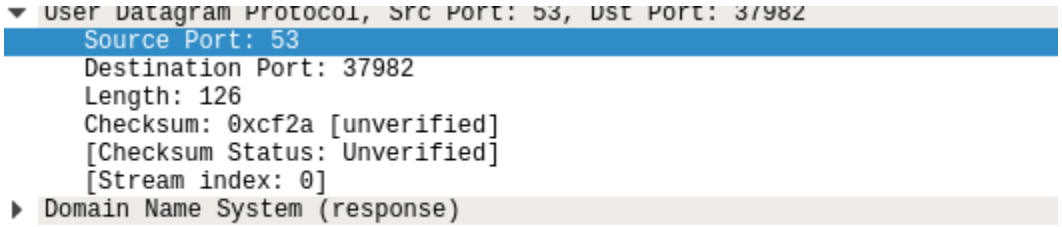
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
   Ans: They are sent over UDP.



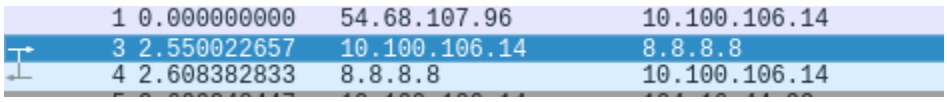
5. What is the destination port for the DNS query message? What is the source port of DNS response messages?
   Ans: Destination port is 53.



5.1 What is the Source port of DNS response message?
   Ans: Port 53



6. To what IP address is the DNS query message sent?
   Ans: 8.8.8.8



6.1 Use ipconfig to determine the IP address of your local DNS server.
   Ans: Its not possible to use Ifconfig to see DNS information so instead, we use nslookup.

So the ip address of our local DNS server is = 127.0.0.53

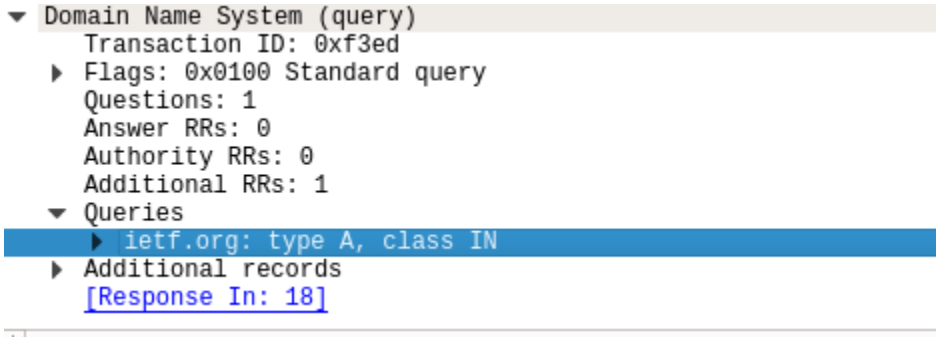
```
abhijit@iit-Vostro-3670:~$ nslookup iit.du.ac.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   iit.du.ac.bd
Address: 103.221.253.162
```

6.3 Are these two IP addresses the same?

Ans: No, the local IP address and the google's DNS is address that was used, are not same.

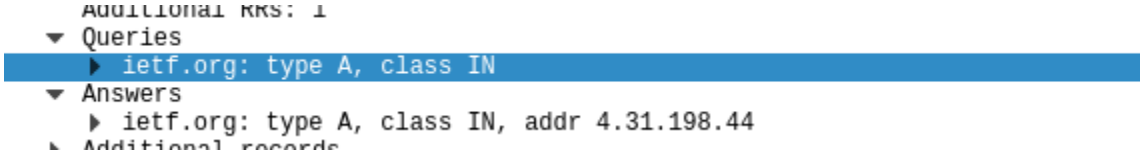
7. What "Type" of DNS query is it?

   Ans: Type A



7.1 Does the query message contain any "answers"?

Ans: No, the response message contains an answer. The query message does not.



8. How many "answers" are provided?

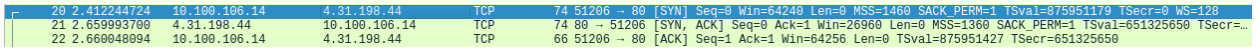
   Ans: 1

8.1 What do each of these answers contain?

Ans: Ip address.

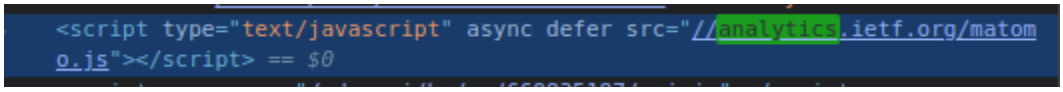
9. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

   Ans: Yes, The ip address was: 4.31.198.44



10. Before retrieving each image, does your host issue new DNS queries?

    Ans: No. There were only 4 DNS queries. The first two was to get the ip of the site and the last two were to get another site thats used by it - analytics.ierf.org



Using inspect element, we are sure that the images were hosted locally. So there is no need for DNS queries to pull them.

11. What is the destination port for the DNS query message?

Ans: Port 53

```
▼ User Datagram Protocol, Src Port: 42303, Dst Port: 53
    Source Port: 42303
    Destination Port: 53
    Length: 60
    Checksum: 0xfb05 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
```

11.1 What is the source port of a DNS response message?

Ans: port 53

```
▼ User Datagram Protocol, Src Port: 53, Dst Port: 42303
    Source Port: 53
    Destination Port: 42303
    Length: 112
    Checksum: 0x02e7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
▼ Domain Name System (response)
```

12. To what IP address is the DNS query message sent?

Ans: 8.8.8.8

```
  5 0.796095433   8.8.8.8          10.100.106.14
282 4.649742965   10.100.106.14    8.8.8.8
283 4.790547398   8.8.8.8          10.100.106.14
```

12.1 Is this the IP address of your default local DNS server?

Ans: 127.0.0.53

```
abhijit@iit-Vostro-3670:~/Desktop$ cat /etc/resolv.conf | grep "nameserver"
nameserver 127.0.0.53
```

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

Ans: Type A. No.

```
  5 0.796095433   8.8.8.8          10.100.106.14    DNS    151 Standard query response 0x4ebd AAAA api.snapcraft.io SOA
282 4.649742965   10.100.106.14    8.8.8.8          DNS     94 Standard query 0xe610 A www.mit.edu.edgekey.net OPT
283 4.790547398   8.8.8.8          10.100.106.14    DNS    146 Standard query response 0xe610 A www.mit.edu.edgekey.net
```

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

Ans: 2 Answers. One is CNAME for the hostname and the other is ip address.

```
▶ Queries
▼ Answers
  ▶ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  ▶ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.120.75.121
▶ Additional records
```

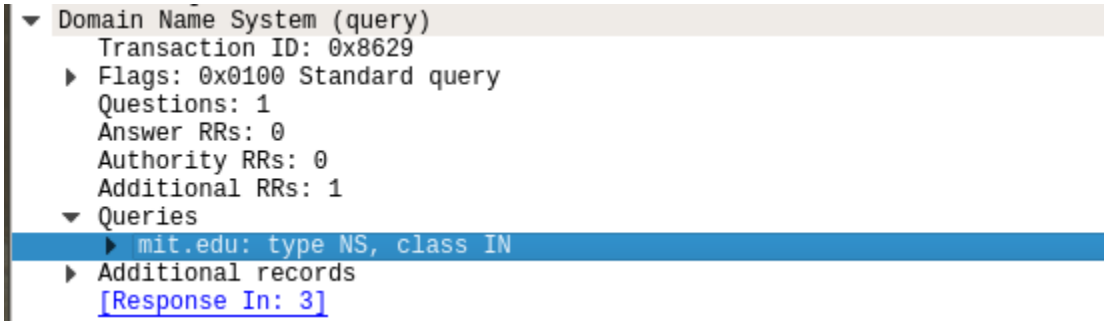
In detail, it contains:

```
▼ Answers
  ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▶ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.120.75.121
```

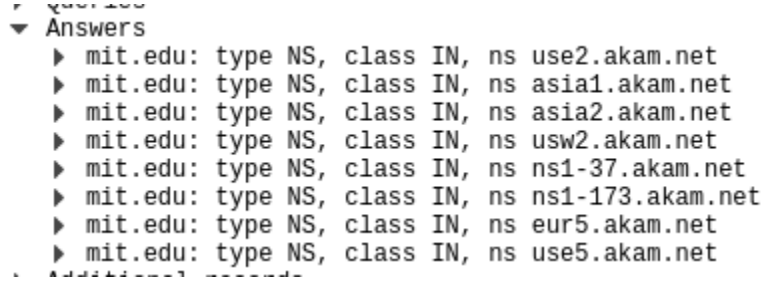
15. Screenshots have been provided already.
16. To what IP address is the DNS query message sent?
    Ans: It was naturally sent to the Local DNS server . This local server by itself or by looking through higher level DNS servers satisfied our DNS queries.
    Ans: Yes, it's the ip address of my local DNS server.

```
abhijit@iit-Vostro-3670:~/Desktop$ nslookup -type=NS mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = usw2.akam.net.
```

17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contains any "answers"?
    Ans: Type NS. No answers.



18. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
    Ans: No, it does not provide ip of any nameserver.



19. Screenshots have already been provided.
    NOTE: In the next task, the given links were not working.

```
abhijit@iit-Vostro-3670:~/Desktop$ nslookup www.aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached
```

    So instead, we used this:

```
abhijit@iit-Vostro-3670:~/Desktop$ nslookup mit.edu use5.akam.net
Server:         use5.akam.net
Address:        2.16.40.64#53

Name:   mit.edu
Address: 23.15.106.234
Name:   mit.edu
Address: 2600:1413:b000:194::255e
Name:   mit.edu
Address: 2600:1413:b000:199::255e
```

20. To what IP address is the DNS query message sent?

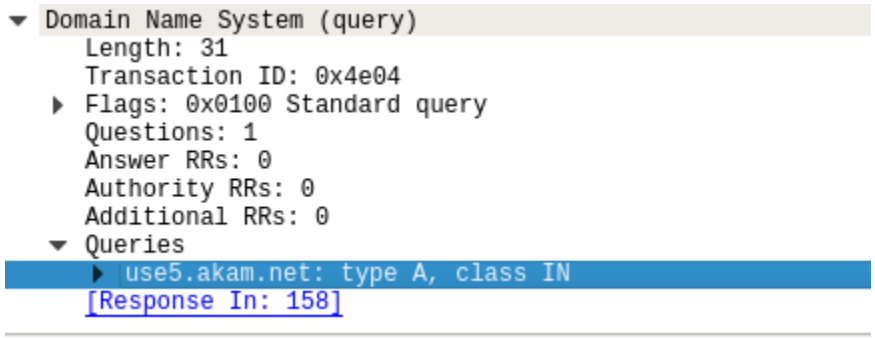
    Ans: 2.16.40.64, the ip address of

20.1 Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

    Ans: It's naturally not a local DNS server. It's the ip of user5.akam.net

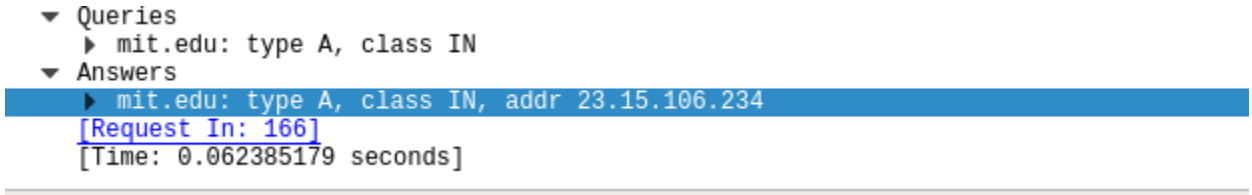
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

    Ans: Type A. No Answers.



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

    Ans: 1. Only the ip address.



23. Screenshots have been provided.