Udaya Vijay Anand (uvijayanand)

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

```
C:\Users\Udaya Vijay Anand>nslookup www.aiit.or.kr 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  58.229.6.225
```

The IP Address of a Web Server in India: 58.229.6.225

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

```
C:\Users\Udaya Vijay Anand>nslookup ox.ac.uk 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    ox.ac.uk
Addresses:  151.101.194.216
          151.101.130.216
          151.101.2.216
          151.101.66.216
```

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?

```
C:\Users\Udaya Vijay Anand>nslookup
Default Server:  rdns2.wpi.edu
Address:  130.215.41.2

> set type=mx
> yahoo.com 151.101.130.216
Server:  [151.101.130.216]
Address:  151.101.130.216

Non-authoritative answer:
yahoo.com       MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
>
```

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

The responses are sent over UDP

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

```
Source Port: 53
Destination Port: 60097
Length: 276
Checksum: 0xcb89 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
UDP payload (268 bytes)
```

The destination port for the query message is 60097.

The source port of DNS response message is 53.

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

122	1.164631	130.215.217.103	130.215.41.1	DNS

The DNS query message is sent to 130.215.41.1 which is the IP address of my local DNS server

The IP address of my local IP address is as follows, and therefore they match

```
DNS Servers . . . . . . . . . . . : 130.215.41.2
                                    130.215.41.3
                                    130.215.41.1
```

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

The DNS query message is a type A query, as indicated by the "Type" field value of 1. This means that the client is requesting the IPv4 address for the hostname "catalog-public-service-prod06.ol.epicgames.com".

The query message does not contain any answers, as it is only a request for information. The server will respond with one or more answers if it has the requested information available.

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

There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address

```
Answers
    www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        Name: www.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
```

```
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.16.45.99
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.16.44.99
```

9. 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?

   The first SYN packet was sent to 104.16.44.99 which corresponds to the first IP address provided in the DNS message.

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

    No, the host does not issue new queries before retrieving each image.

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

The destination port of the DNS query is 53, and the source port of the DNS response is 53 as well.

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

The DNS query messages are sent to the Destination Address: 130.215.41.1, which as we can see from the ipconfig –all screenshots, is the default local DNS server.

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

The query is of type A, and it doesn't contain any answers.

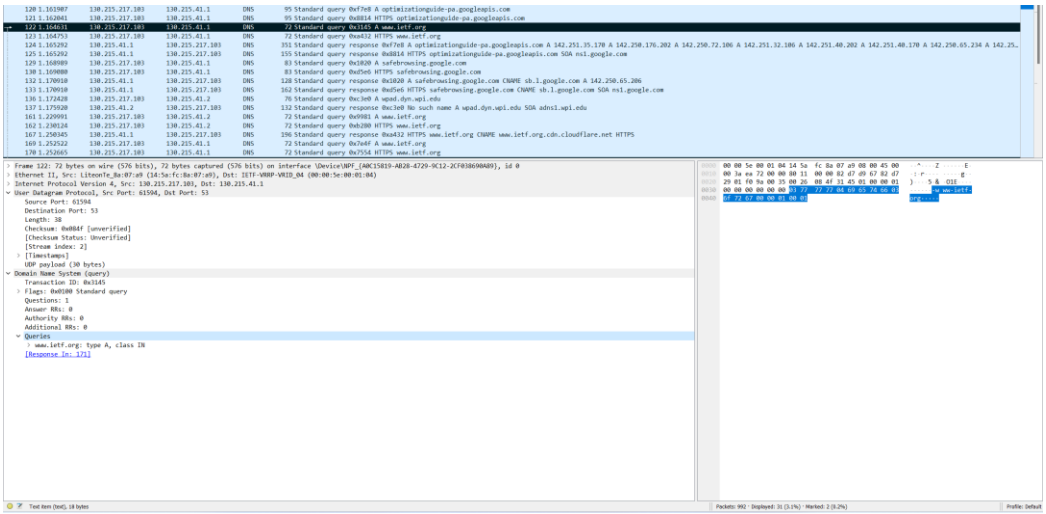
14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

The response

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

    Name: www.ietf.org.cdn.cloudflare.net

    Type: A (Host Address) (1)

    Class: IN (0x0001)

    Time to live: 300 (5 minutes)

    Data length: 4

    Address: 104.16.45.99
```

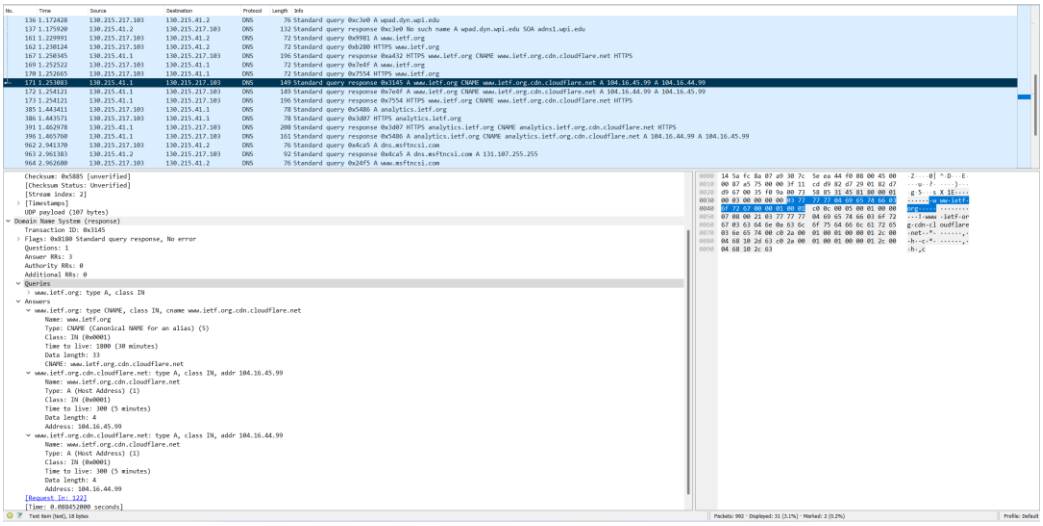
15. Provide a screenshot

Screenshot of Query



Udaya Vijay Anand (uvijayanand)

Screenshot of Response



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

```
C:\Users\Udaya Vijay Anand>nslookup -type=NS mit.edu
Server:  rdns2.wpi.edu
Address:  130.215.41.2
```

The DNS query message was sent to 130.215.41.2, which is my default DNS server.

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

It's a type NS DNS query that doesn't contain any answers.

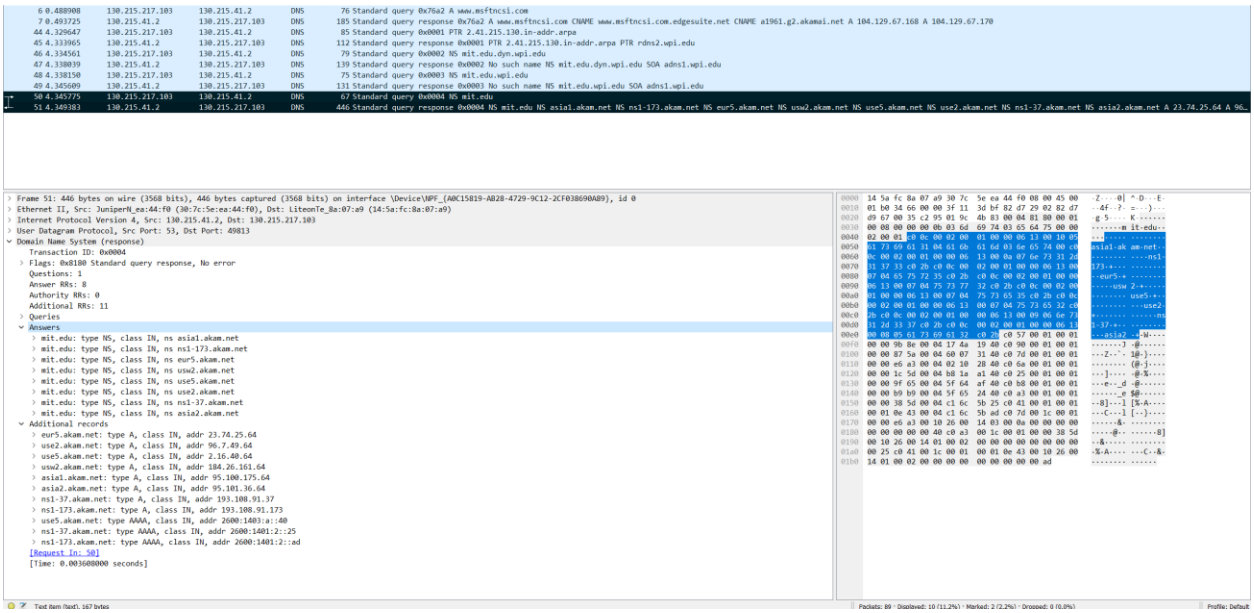
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

The nameservers are bitsy, strawb and W20ns. We can find their IP addresses if we expand the Additional Records field in Wireshark, as seen below.

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

```
        mit.edu: type NS, class IN, ns use5.akam.net
        mit.edu: type NS, class IN, ns use2.akam.net
        mit.edu: type NS, class IN, ns ns1-37.akam.net
        mit.edu: type NS, class IN, ns asia2.akam.net
    Additional records
        eur5.akam.net: type A, class IN, addr 23.74.25.64
        use2.akam.net: type A, class IN, addr 96.7.49.64
        use5.akam.net: type A, class IN, addr 2.16.40.64
        usw2.akam.net: type A, class IN, addr 184.26.161.64
        asia1.akam.net: type A, class IN, addr 95.100.175.64
        asia2.akam.net: type A, class IN, addr 95.101.36.64
        ns1-37.akam.net: type A, class IN, addr 193.108.91.37
        ns1-173.akam.net: type A, class IN, addr 193.108.91.173
        use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
        ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
        ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    [Request In: 50]
    [Time: 0.003608000 seconds]
```

19. Provide a screenshot



20. 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?

```
▾ Answers
  ▾ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
        Name: bitsy.mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 4
        Address: 18.0.72.3
    [Request In: 40]
```

This query is sent to 18.0.72.32, which corresponds to bitsy.mit.edu

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

It's a standard type A query that doesn't contain any answers

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

```
    Answers
www.aiit.or.kr: type A, class IN, addr 58.229.6.225
    Name: www.aiit.or.kr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 4
    Address: 58.229.6.225
```

Udaya Vijay Anand (uvijayanand)

23. Provide a screenshot