

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.ait.or.kr 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: www.ait.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”?

Udaya Vijay Anand (uvijayanand)

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)

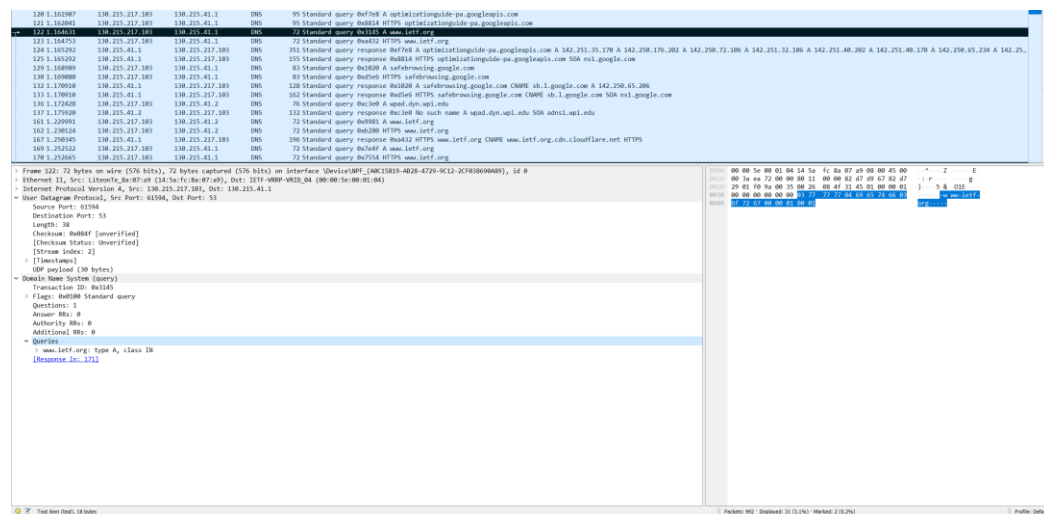
Time to live: 300 (5 minutes)

Data length: 4

Address: 104.16.45.99

15. Provide a screenshot

Screenshot of Query



Time	Source	Destination	Prot	Length	Info
136.177428	190.235.237.383	190.235.41.2	000	76	Standard query 6a3c00 A wpa2.dynapi.edu
137.179760	190.235.41.2	190.235.237.383	000	132	Standard query response 6a3c00 No such name A wpa2.dynapi.edu SOA sdhslapi.edu
163.122095	190.235.237.383	190.235.41.2	000	72	Standard query 6a08f0 A www.ietf.org
162.138034	190.235.237.383	190.235.41.2	000	72	Standard query 6a08f0 HTTPS www.ietf.org
167.136465	190.235.41.2	190.235.237.383	000	256	Standard query response 6a08f0 HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS
169.129522	190.235.237.383	190.235.41.2	000	72	Standard query 6a0ef0 A www.ietf.org
170.129540	190.235.237.383	190.235.41.2	000	72	Standard query 6a0ef0 HTTPS www.ietf.org
171.125363	190.235.41.2	190.235.237.383	000	160	Standard query response 6a0ef0 HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 184.16.45.99 A 184.16.44.99
172.125423	190.235.41.2	190.235.237.383	000	160	Standard query response 6a0ef0 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 184.16.44.99 A 184.16.45.99
173.125423	190.235.41.2	190.235.237.383	000	396	Standard query response 6a05fa HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 184.16.44.99 A 184.16.45.99
185.143441	190.235.237.383	190.235.41.2	000	78	Standard query 6a0480 A analytics.ietf.org
186.148372	190.235.237.383	190.235.41.2	000	78	Standard query 6a0480 HTTPS analytics.ietf.org
191.146278	190.235.41.2	190.235.237.383	000	208	Standard query response 6a0480 HTTPS analytics.ietf.org CNAME analytics.ietf.org.cdn.cloudflare.net HTTPS
190.140708	190.235.41.2	190.235.237.383	000	331	Standard query response 6a0480 A analytics.ietf.org CNAME analytics.ietf.org.cdn.cloudflare.net A 184.16.44.99 A 184.16.45.99
192.144178	190.235.237.383	190.235.41.2	000	78	Standard query 6a0d40 A dns.cloudflare.com
193.146183	190.235.237.383	190.235.237.383	000	92	Standard query response 6a0d40 A dns.cloudflare.com A 131.107.255.255
193.146183	190.235.237.383	190.235.41.2	000	78	Standard query 6a0d40 A www.cloudflare.com

Checksum: 8b585 [verified]	
Checksum: Source [verified]	
[Source Index: 2]	
[Timestamp]	
[OS payload (COB bytes)]	
Domain Name System (Response)	
Transaction ID: 6a0450	
Flags: 0x0000 Standard query response, No error	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Queries:	
www.ietf.org: type A, class IN	
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 (Internet)	
Time to live: 10800 (30 minutes)	
Data length: 33	
CNAME: www.ietf.org.cdn.cloudflare.net	
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 184.16.44.99	
Name: www.ietf.org.cdn.cloudflare.net	
Type: A (host address) (1)	
Class: IN (Internet)	
Time to live: 3600 (15 minutes)	
Data length: 4	
Address: 184.16.44.99	
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 184.16.44.99	
Name: www.ietf.org.cdn.cloudflare.net	
Type: A (host address) (1)	
Class: IN (Internet)	
Time to live: 3600 (15 minutes)	
Data length: 4	
Address: 184.16.44.99	
[Request ID: 122]	
[Time: 0.00452000 seconds]	

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

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

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

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.

```
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
```

Udaya Vijay Anand (uvijayanand)

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

The screenshot displays a Wireshark packet capture of a DNS response. The packet list on the left shows a standard query response from 193.108.91.173 to 10.0.0.1. The packet details pane shows the DNS response structure with questions and answers. The packet bytes pane shows the raw data. The packet list pane shows the packet number, time, source, destination, and protocol.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
60	0.000000	193.108.91.173	10.0.0.1	DNS	76	Standard query response 0x70a2 A www.mftncsl.com
70	0.000000	193.108.91.173	10.0.0.1	DNS	185	Standard query response 0x70a2 A www.mftncsl.com
85	0.000000	193.108.91.173	10.0.0.1	DNS	85	Standard query response 0x0001 PTR 2.41.215.130.in-addr.arpa
112	0.000000	193.108.91.173	10.0.0.1	DNS	112	Standard query response 0x0001 PTR 2.41.215.130.in-addr.arpa
79	0.000000	193.108.91.173	10.0.0.1	DNS	79	Standard query response 0x0002 NS mit.edu.dyn.wpi.edu
139	0.000000	193.108.91.173	10.0.0.1	DNS	139	Standard query response 0x0002 NS mit.edu.dyn.wpi.edu
75	0.000000	193.108.91.173	10.0.0.1	DNS	75	Standard query response 0x0003 NS mit.edu.wpi.edu
131	0.000000	193.108.91.173	10.0.0.1	DNS	131	Standard query response 0x0003 NS mit.edu.wpi.edu
67	0.000000	193.108.91.173	10.0.0.1	DNS	67	Standard query response 0x0004 NS mit.edu
446	0.000000	193.108.91.173	10.0.0.1	DNS	446	Standard query response 0x0004 NS mit.edu

Packet Details:

Transaction ID: 0x0004
Flags: 0x0180 Standard query response, No error
Questions: 1
Answer RRs: 8
Authority RRs: 0
Additional RRs: 11
Queries

Answers:

- mit.edu: type NS, class IN, ns asia2.akam.net
- mit.edu: type NS, class IN, ns ns1-173.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]

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?

```
class: IN (0x0001)
  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
```

