HACETTEPE UNIVERSITY

COMPUTER ENGINEERING DEPARTMENT

BBM 453 LAB EXPERIMENT 2
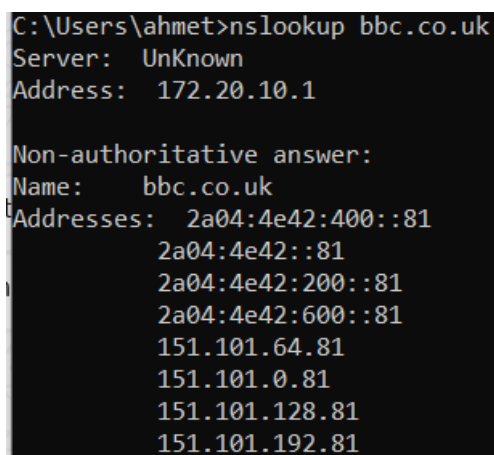
Group No: 41

Yiğit Emir İşıkçı: 2200356028

Ahmet Eren Akbaş: 21945757

Yiğit's IP Address: 10.225.62.14 (Q11-23)

Ahmet's IP Address: 172.20.10.1 (Q1-10)

1)nslookup

Q1) Run nslookup to obtain the IP address of a Web server in Europe. What is the IP address of that server?


```
C:\Users\ahmet>nslookup bbc.co.uk
Server:   UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:     bbc.co.uk
Addresses: 2a04:4e42:400::81
          2a04:4e42::81
          2a04:4e42:200::81
          2a04:4e42:600::81
          151.101.64.81
          151.101.0.81
          151.101.128.81
          151.101.192.81
```

There are multiple IP addresses that we can use for the web server of bbc.co.uk.

IPv6 Addresses:

2a04:4e42:200::81, 2a04:4e42:600::81, 2a04:4e42::81, 2a04:4e42:400::81

IPv4 Addresses:

151.101.64.81, 151.101.128.81, 151.101.192.81, 151.101.0.81

Q2) Run nslookup to determine the authoritative DNS servers for a university in United States.

```
C:\Users\ahmet>nslookup -type=NS www.asu.edu
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
www.asu.edu      canonical name = pantheon-systems.map.fastly.net

fastly.net
        primary name server = ns1.fastly.net
        responsible mail addr = hostmaster.fastly.com
        serial  = 2017052201
        refresh = 3600 (1 hour)
        retry   = 600 (10 mins)
        expire  = 604800 (7 days)
        default TTL = 30 (30 secs)
```

The authorititative DNS server for Arizona State University is **ns1.fastly.net**.

Q3) Run nslookup so that one of the DNS servers of Google is queried for the mail servers for Yahoo! mail. What is its IP address?

```
C:\Users\ahmet>nslookup 8.8.8.8 www.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.100.216

DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

We used 8.8.8.8 as the DNS Server of Google. The IP Address it resolved for Yahoo! İs **87.248.100.216**.

2) ipconfig – Tracing DNS with Wireshark

Q4) Locate the DNS query and response messages. Are they sent over UDP or TCP?

DNS Query:
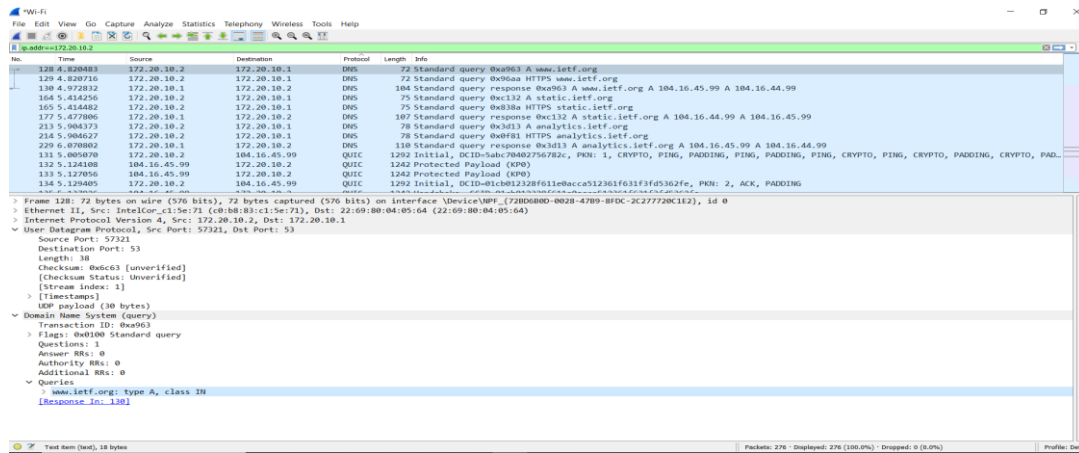
DNS Response:
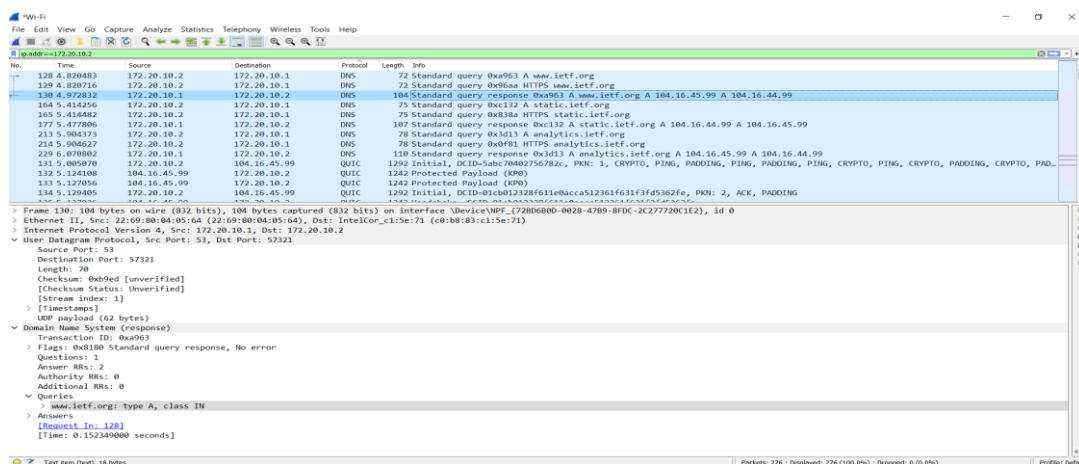
They are sent over UDP.

Q5) What is the destination port for the DNS query message? What is the source port of DNS response message?

As we can see from the screenshots in Q4,

Destination port of the DNS query message is **53**.

Source port of the DNS response messsage is **53**.

Q6) 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?

The DNS Query is sent to **172.20.10.1**. Yes as we can see the ipconfig screenshot that is provided above these two IP addresses are the **same**.

Q7) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
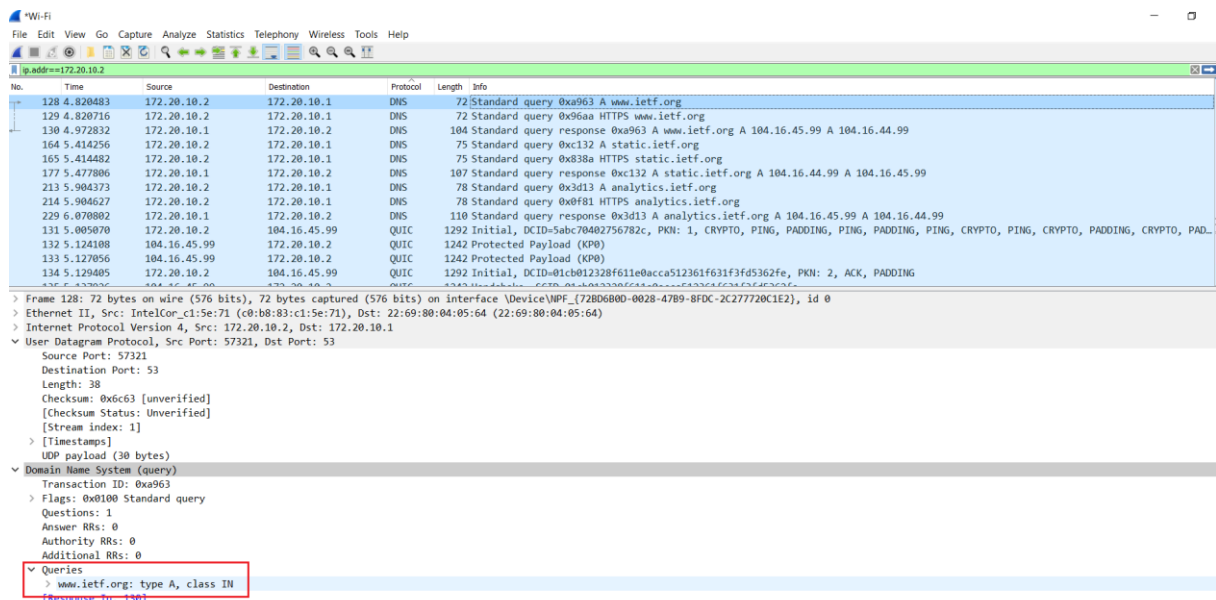
It is a type A Standart Query. No, it doesn't contain any answer.

Q8) Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

There were 2 answers. They contain 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 A, class IN, addr 104.16.45.99
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 377 (6 minutes, 17 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 (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 377 (6 minutes, 17 seconds)
        Data length: 4
        Address: 104.16.44.99
```

Q9) 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?

```
211 5.889971      172.20.10.2        104.16.44.99      TCP       66 52949 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

130 4.972832      172.20.10.1        172.20.10.2       DNS       104 Standard query response 0xa963 A www.ietf.org A 104.16.45.99 A 104.16.44.99
```

Yes, the IP address 104.16.44.99 corresponds to an IP address provided in the DNS response message.

Q10) This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No it doesn't.

Q11) What is the destination port for the DNS query message? What is the source port of DNS response message?

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

Q12) To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

DNS query sent to IP address 193.140.216.203. Yes, it is same as my local DNS server.

Q13) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The type of the DNS query is "AAAA". But it does not contain any "answers"

Q14) Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

There are four answers provided in the DNS response.

Interpretation

The first two answers are CNAME records, indicating that www.mit.edu does not have a direct A (IPv4) or AAAA (IPv6) record but instead points to another domain name (www.mit.edu.edgekey.net), which in turn points to e9566.dscb.akamaiedge.net.

The last two answers are AAAA records, providing IPv6 addresses for e9566.dscb.akamaiedge.net. This is where the actual content for www.mit.edu is likely hosted.

Q15) Provide a screenshot

We have provided necessary screenshots.

Q16) To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

DNS query message sent to IP address 193.140.216.203 which is same as my default local DNS server.

Q17) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The type of the DNS query is "NS". But it does not contain any "Answers".

Q18) Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

1)Name Servers (NS Records):

ns1-173.akam.net, asia1.akam.net, ns1-37.akam.net, asia2.akam.net, eur5.akam.net, use2.akam.net, use5.akam.net, usw2.akam.net

2)Additional Records (IP Addresses):

2.1)A Records (IPv4 Addresses):

use2.akam.net: 96.7.49.64

ns1-37.akam.net: 193.108.91.37

ns1-173.akam.net: 193.108.91.173

asia1.akam.net: 95.100.175.64

eur5.akam.net: 23.74.25.64

2.2) AAAA Records (IPv6 Addresses):

ns1-37.akam.net: 2600:1401:2::25

use5.akam.net: 2600:1403:a::40

So, yes. Response also provide IP addresses of MIT name servers.

Q19) Provide a screenshot

We have provided necessary screenshots.

Q20) 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?

DNS query message sent to IP address 193.140.216.203 which is same as my local DNS server again.

Q21) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The type of the DNS query is "A". Again, it does not contain answers.

Q22) Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

There are 1 answer in DNS response message. It contains the IP address of the www.aiit.or.kr.

Q23) Provide a screenshot

We have provided necessary screenshots.