



Laboratuvar Raporu 2

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Ferdi İslam Yılmaz

152120191055

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İindekiler

2	Giriş.....	3
3	Laboratuvar Uygulaması.....	3
3.1	nsconfig Komutu	3
3.2	Tracing DNS with Wireshark	4
4	Kaynaka.....	10

2 Giriş

Bugünkü laboratuvar dersimizde “nslookup” ve “ipconfig” komutlarını öğreneceğiz. Bu öğrendiğimiz komutları Wireshark uygulamasında deneyeceğiz ve pekiştireceğiz. **nslookup** komutu bir servisin IP/TCP adresinin bulunmasına yardımcı olur. **ipconfig** komutu ise bilgisayarın ağ bağlantı özelliklerini gösterir.

3 Laboratuvar Uygulaması

3.1 nsconfig Komutu

1. Asya'daki bir internet sitesinin adresini sorguladık ve serverın IP adresini 58.229.6.225 olarak buldu.

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

2. Oxford Üniversitesi'nin authoritative dns serverlarını bulduk öncelikle. Daha sonra bulduğumuz serverların da IP adreslerini bulmak için tekrar nslookup komutunu kullandık. Oxford Üniversitesi'nin dns serverlarından birisi olan auth6.dns.ox.ac.uk adresinin IP'si ise 185.24.221.32.

```
C:\Users\ferdi>nslookup -type=ns ox.ac.uk  
Server:  UnKnown  
Address: 192.168.0.1  
  
Non-authoritative answer:  
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk  
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk  
ox.ac.uk      nameserver = dns0.ox.ac.uk  
ox.ac.uk      nameserver = dns2.ox.ac.uk  
ox.ac.uk      nameserver = dns1.ox.ac.uk  
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk  
  
C:\Users\ferdi>nslookup auth6.dns.ox.ac.uk  
Server:  UnKnown  
Address: 192.168.0.1  
  
Non-authoritative answer:  
Name:      auth6.dns.ox.ac.uk  
Addresses: 2a02:2770:11:0:21a:4aff:febe:759b  
           185.24.221.32
```

3.İkinci soruda elde ettiğimiz DNS sunucularından birini Yahoo! İçin sorguladığımızda 87.248.119.251 IP adresini elde ediyoruz.

```
C:\Users\ferdi>nslookup auth6.dns.ox.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.119.251

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

3.2 Tracing DNS with Wireshark

4. Alınan cevaba göre sorgumuz UDP üzerinden yapılmıştır.

The image shows a Wireshark packet capture. The top pane displays a list of packets. Packet 8745 is a DNS Standard query response from 192.168.0.105 to 192.168.0.1. The packet details pane shows the following information:

- Interface description: Wi-Fi
- Encapsulation type: Ethernet (1)
- Arrival Time: Mar 31, 2023 04:10:01.945357000 Türkiye Standart Saati
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1680225001.945357000 seconds
- [Time delta from previous captured frame: 0.009536000 seconds]
- [Time delta from previous displayed frame: 0.009536000 seconds]
- [Time since reference or first frame: 38.767925000 seconds]
- Frame Number: 8745
- Frame Length: 149 bytes (1192 bits)
- Capture Length: 149 bytes (1192 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:udp:dns]
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]
- > Ethernet II, Src: Tp-LinkT_59:20:3e (b0:95:75:59:20:3e), Dst: IntelCor_e0:5f:83 (34:7d:83:5f:e0:5f)
- > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
- > User Datagram Protocol, Src Port: 53, Dst Port: 60998
- > Domain Name System (response)

The packet bytes pane shows the raw data of the packet, starting with 0000 34 7d f6 e0 5f 83 b0 95 75 59 20 3e.

5. Gönderdiğimiz sorgunun varış portu ve aldığımız cevabın kaynak portu aynıdır. Bu port ise 53tür.

```

▼ User Datagram Protocol, Src Port: 60998, Dst Port: 53
  Source Port: 60998
  Destination Port: 53
  Length: 38
  Checksum: 0x81f2 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  > [Timestamps]
  UDP payload (30 bytes)

```

6. Sorguyu 192.168.0.1 adresine gönderdik. İpconfig kullandığımda da IP adreslerinin aynı olduğunu gördüm.

8733	38.712011	192.168.0.105	192.168.0.1	DNS	72 Standard query 0xc716 A www.ietf.org
8734	38.712011	192.168.0.105	192.168.0.105	UDP	342 50007 0x5453 100-200

7. Kullandığımız DNS sorgusu type A. Sorgu mesajımızın içerdiği “cevaplar” ise alttaki ekran görüntüsündedir.

```

▼ Queries
  > www.ietf.org: type A, class IN
  .

▼ Answers
  > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
  > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

```

8. DNS yanıtını incelediğimizde bize 4 adet cevap sağlandığını görüyoruz. Cevaplar; Name, Type, Class, Time to Live Data length ve CNAME bilgilerini içeriyor.

```

▼ 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: 26 (26 seconds)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  ▼ 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
  ▼ 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

```

9. Bizim gönderdiğimiz TCP SYN paketimizi incelediğimizde varış adresini önceki DNS yanıt mesajının doğruladığını görüyoruz.

8746	38.768751	192.168.0.105	104.16.44.99	TCP	66 57793 → 80 [SYN]
8747	38.768909	192.168.0.105	104.16.44.99	TCP	66 57794 → 80 [SYN]
8748	38.769011	192.168.0.105	192.168.0.1	DNS	91 Standard query 0
8749	38.778122	104.16.44.99	192.168.0.105	TCP	66 80 → 57793 [SYN,
8750	38.778256	192.168.0.105	104.16.44.99	TCP	54 57793 → 80 [ACK]
8751	38.778494	192.168.0.105	104.16.44.99	HTTP	421 GET / HTTP/1.1
8752	38.780478	104.16.44.99	192.168.0.105	TCP	66 80 → 57794 [SYN,
8753	38.780562	192.168.0.105	104.16.44.99	TCP	54 57794 → 80 [ACK]

10. Evet sitede resimler var. Ama benim sunucum resimler için herhangi bir DNS sorgusu oluşturmamış.

11. DNS sorgu mesajının varış portu 53 aynı zamanda DNS yanıt mesajının kaynak portu da 53.

7 2.394992 192.168.0.105 192.168.0.1 DNS 71 Standard query 0x0002 A www.mit.edu

8 2.425077 192.168.0.105 162.159.128.235 TLSv1.2 140 Application Data

9 2.432934 192.168.0.105 66.22.238.150 UDP 212 64198 → 50020 Len=170

10 2.436758 162.159.128.235 192.168.0.105 TCP 54 443 → 58363 [ACK] Seq=1 Ack=87 Win=8 Len=0

11 2.449932 192.168.0.105 66.22.238.150 UDP 208 64198 → 50020 Len=166

12 2.465587 192.168.0.1 192.168.0.105 DNS 160 Standard query response 0x0002 A www.mit.edu CNAME

13 2.467837 192.168.0.105 192.168.0.1 DNS 71 Standard query 0x0003 AAAA www.mit.edu

14 2.472808 192.168.0.105 66.22.238.150 UDP 218 64198 → 50020 Len=176

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 57

Identification: 0x52b3 (21171)

> 000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.105

Destination Address: 192.168.0.1

> User Datagram Protocol, Src Port: 64200, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ www.mit.edu: type A, class IN

Name: www.mit.edu

[Name Length: 11]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 12]

0000 b0 95 75 59 20 3e 34 7d f6 e0 :

0010 00 39 52 b3 00 00 80 11 00 00 :

0020 00 01 fa c8 00 35 00 25 81 f1 :

0030 00 00 00 00 00 00 03 77 77 77 :

0040 64 75 00 00 01 00 01

12. DNS sorgu mesajı 192.168.0.1 adresine gönderilmiş ve bu adres benim yerel sunucumun adresi ile aynı.

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::e144:df25:1775:a437%5
IPv4 Address. . . . . : 192.168.0.105
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
```

13. Sorgumuz a tipi bir sorgudur. DNS sorgumuzda herhangi bir cevap da bulunmamaktadır.

```
▼ Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 12]
```

14. DNS yanıt mesajımızda 3 adet cevap bulunmaktadır. İçerdiği bilgiler aşağıdaki ekran görüntüsünde mevcuttur.

```
▼ Answers
  > www.mit.edu: type CNAME, class IN, 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 92.122.34.235
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 4
    Address: 92.122.34.235
```

16. DNS sorgu mesajımız 192.168.0.1 numaralı IP adresine gönderilmiştir. Bu IP adresi bizim yerel DNS serberimiz ile aynıdır.

81	1.108804	192.168.0.105	192.168.0.1	DNS	67 Standard query 0x0002 NS mit.edu
82	1.115118	52.137.106.217	192.168.0.105	TLSv1.2	105 Change Cipher Spec, Encrypted Handsh
83	1.115118	52.137.106.217	192.168.0.105	TLSv1.2	123 Application Data
84	1.115178	192.168.0.105	52.137.106.217	TCP	54 58910 → 443 [ACK] Seq=375 Ack=3879
85	1.115832	192.168.0.105	52.137.106.217	TLSv1.2	141 Application Data
86	1.115863	192.168.0.105	52.137.106.217	TLSv1.2	186 Application Data
87	1.115928	192.168.0.105	52.137.106.217	TLSv1.2	92 Application Data
88	1.120953	66.22.238.150	192.168.0.105	UDP	244 50020 → 57586 Len=202
89	1.129187	40.74.108.123	192.168.0.105	TCP	54 443 → 58904 [ACK] Seq=3879 Ack=604
90	1.129819	40.74.108.123	192.168.0.105	TLSv1.2	92 Application Data
91	1.132084	40.74.108.123	192.168.0.105	TCP	1494 443 → 58904 [ACK] Seq=3917 Ack=642
92	1.132084	40.74.108.123	192.168.0.105	TLSv1.2	333 Application Data
93	1.132109	192.168.0.105	40.74.108.123	TCP	54 58904 → 443 [ACK] Seq=642 Ack=5636
94	1.133428	192.168.0.105	40.74.108.123	TCP	54 58904 → 443 [FIN, ACK] Seq=642 Ack=
95	1.139144	66.22.238.150	192.168.0.105	UDP	253 50020 → 57586 Len=211
96	1.155451	192.168.0.1	192.168.0.105	DNS	234 Standard query response 0x0002 NS m:

> [Timestamps]
UDP payload (25 bytes)
▼ Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
mit.edu: type NS, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
[\[Response In: 96\]](#)

0000 b0 95 75 59 20
0010 00 35 52 db 00
0020 00 01 ea 55 00
0030 00 00 00 00 00
0040 02 00 01

17. DNS sorgu mesajımızı incelediğimizde “ns” türünde bir sorgu kullanıldığını görüyoruz. Üstteki ekran görüntüsünde de görüldüğü üzere bu sorgu hiç cevap içermiyor.

18. DNS yanıt mesajını incelediğimizde 8 adet nameserver sağlandığı görülüyor. Ama bu nameserverlar IP adreslerini bize göstermiyor.

96	1.155451	192.168.0.1	192.168.0.105	DNS	234 Standard query response 0x0002 NS mit.edu NS
----	----------	-------------	---------------	-----	--

▼ Answers
mit.edu: type NS, class IN, ns use5.akam.net
Name: mit.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1672 (27 minutes, 52 seconds)
Data length: 15
Name Server: use5.akam.net
> mit.edu: type NS, class IN, ns ns1-37.akam.net
> mit.edu: type NS, class IN, ns usw2.akam.net
> mit.edu: type NS, class IN, ns asia1.akam.net
> mit.edu: type NS, class IN, ns use2.akam.net
> mit.edu: type NS, class IN, ns eur5.akam.net
> mit.edu: type NS, class IN, ns asia2.akam.net
> mit.edu: type NS, class IN, ns ns1-173.akam.net
[\[Request In: 81\]](#)
[Time: 0.046647000 seconds]

0000 34 7d f6 e0 5f 83 b0 95
0010 00 dc bf 9c 00 00 75 11
0020 00 69 00 35 ea 55 00 c8
0030 00 08 00 00 00 00 03 6d
0040 02 00 01 c0 0c 00 02 00
0050 75 73 65 35 04 61 6b 61
0060 00 02 00 01 00 00 06 88
0070 37 c0 2a c0 0c 00 02 00
0080 75 73 77 32 c0 2a c0 0c
0090 00 08 05 61 73 69 61 31
00a0 00 00 06 88 00 07 04 75
00b0 02 00 01 00 00 06 88 00
00c0 c0 0c 00 02 00 01 00 00
00d0 61 32 c0 2a c0 0c 00 02
00e0 07 6e 73 31 2d 31 37 33

20. DNS sorgu mesajımız 192.168.0.1 numaralı IP adresine gönderildi. BU IP adresi bizim yerel DNS serverımızinkine ile aynı.

28	1.946464	192.168.0.105	192.168.0.1	DNS	73	Standard query 0x5879 A bitsy.mit.edu	
29	1.964980	192.168.0.1	192.168.0.105	DNS	89	Standard query response 0x5879 A bitsy.mit.edu A 18	
30	1.967479	192.168.0.105	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa	
31	2.015605	192.168.0.105	162.159.128.235	TLSv1.2	140	Application Data	
32	2.022909	192.168.0.105	66.22.238.150	UDP	211	52133 → 50020 Len=169	
33	2.024793	162.159.128.235	192.168.0.105	TCP	54	443 → 58363 [ACK] Seq=1 Ack=87 Win=8 Len=0	
34	2.039945	192.168.0.105	66.22.238.150	UDP	230	52133 → 50020 Len=188	
35	2.067934	192.168.0.105	66.22.238.150	UDP	233	52133 → 50020 Len=191	
36	2.083932	192.168.0.105	66.22.238.150	UDP	244	52133 → 50020 Len=202	

[Timestamps]		0000	b0 95 75 59 20 3e 34 7d f6 e0 5f 83
UDP payload (31 bytes)		0010	00 3b 53 05 00 00 80 11 00 00 c0 a8
Domain Name System (query)		0020	00 01 ce 76 00 35 00 27 81 f3 58 79
Transaction ID: 0x5879		0030	00 00 00 00 00 00 05 62 69 74 73 79
Flags: 0x0100 Standard query		0040	03 65 64 75 00 00 01 00 01
Questions: 1			
Answer RRs: 0			
Authority RRs: 0			
Additional RRs: 0			
Queries			
bitsy.mit.edu: type A, class IN			
Name: bitsy.mit.edu			
[Name Length: 13]			
[Label Count: 3]			
Type: A (Host Address) (1)			
Class: IN (0x0001)			
[Response In: 29]			

21. DNS sorgu mesajını incelediğimizde “a” türünde bir sorgu olduğunu görüyoruz(üstteki ekran fotoğrafında) ama herhangi bir cevap içermiyor.

22. DNS yanıt mesajını incelediğimizde bir tane cevap alındığını görüyoruz. Bu cevapta Name, Type, Class, Time to Live, Data length bilgilerini ve IP adresini içerdiğini görüyoruz.

29	1.964980	192.168.0.1	192.168.0.105	DNS	89	Standard query response 0x5879 A bitsy.mit.edu A	
30	1.967479	192.168.0.105	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa	
31	2.015605	192.168.0.105	162.159.128.235	TLSv1.2	140	Application Data	
32	2.022909	192.168.0.105	66.22.238.150	UDP	211	52133 → 50020 Len=169	
33	2.024793	162.159.128.235	192.168.0.105	TCP	54	443 → 58363 [ACK] Seq=1 Ack=87 Win=8 Len=0	
34	2.039945	192.168.0.105	66.22.238.150	UDP	230	52133 → 50020 Len=188	
35	2.067934	192.168.0.105	66.22.238.150	UDP	233	52133 → 50020 Len=191	
36	2.083932	192.168.0.105	66.22.238.150	UDP	244	52133 → 50020 Len=202	

Queries		0000	34 7d f6 e0 5f 83 b0 95 75 5
bitsy.mit.edu: type A, class IN		0010	00 4b a2 d7 00 00 77 11 1f 1
Name: bitsy.mit.edu		0020	00 69 00 35 ce 76 00 37 f4 f
[Name Length: 13]		0030	00 01 00 00 00 00 05 62 69 7
[Label Count: 3]		0040	03 65 64 75 00 00 01 00 01 c
Type: A (Host Address) (1)		0050	00 00 11 00 04 12 00 48 03
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: 17 (17 seconds)			
Data length: 4			
Address: 18.0.72.3			

4 Kaynakça

<https://www.baeldung.com/cs/dns-authoritative-server-ip>