



Laboratuvar Raporu 1

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Şevval Ayça Çerence

152120211128

Dr. Öğr. Üyesi İlker Özçelik

2024-2025

1. İçindekiler	2
2. Giriş	3
3.1 Nslookup Çalışmaları.....	3
3.1.1 Asya'daki Bir Web Sunucusunun IP Adresini Bulma.....	3
3.1.2 Avrupa'daki Bir Üniversitenin Yetkili DNS Sunucularını Bulma.....	4
3.1.3 Yetkili DNS Sunucusundan Yahoo'nun Mail Sunucularını Sorgulama....	5
3.2 Ipconfig Komutları ile DNS Yönetimi.....	5
3.2.1 Mevcut IP Yapılandırmasının Görüntülenmesi.....	5
3.2.2 DNS Önbelleğinin Temizlenmesi.....	6
3.3 Wireshark ile DNS Takibi	7
3.3.1 DNS Query ve Response Mesajlarının Kullanılan Protokolü.....	7
3.3.2 DNS Query Mesajının Hedef Portu ve Response Mesajının Kaynak Portu....	7
3.3.3 DNS Query Mesajının Gönderildiği IP Adresi ve Yerel DNS ile Karşılaştırma.....	8
3.3.4 DNS Query Mesajının Türü ve Cevap İçeriği.....	8
3.3.5 DNS Response Mesajında Kaç "Answer" Var ve İçeriği	8
3.3.6 Sonraki TCP SYN Paketi Hangi IP Adresine Gönderildi.....	9
3.3.7 Web Sayfasındaki Görseller İçin Yeni DNS Sorguları	9
3.3.8 nslookup ile www.mit.edu Sorgusunun DNS Port Bilgileri.....	9
3.3.9 www.mit.edu Sorgusu Hangi IP Adresine Gönderildi.....	9
3.3.10 www.mit.edu Sorgusunun Türü ve Cevap İçeriği.....	9
3.3.11 www.mit.edu Sorgusunun DNS Response Mesajındaki Answers Bölümü.....	10
3.3.12 Ekran Görüntüsü (www.mit.edu Sorgusu).....	10
3.3.13 nslookup -type=NS mit.edu Sorgusu Hangi IP'ye Gönderildi.....	10

3.3.14 NS Sorgusunun Türü ve Cevap İçeriği.....	10
3.3.15 mit.edu’ya Dair Yetkili DNS Sunucuları ve IP Adresleri.....	11
3.3.16 Ekran Görüntüsü (NS Sorgusu mit.edu).....	11
3.3.17 nslookup www.aiit.or.kr bitsy.mit.edu Sorgusu Hangi IP’ye Gönderildi.....	12
3.3.18 Bu Sorgunun Türü	13
3.3.19 Cevap Mesajında Kaç "Answer" Var ve İçeriği	13
3.3.20 Ekran Görüntüsü (bitsy.mit.edu’ye Yapılan Sorgu).....	13
4. LABORATUVAR SONUCU	14
5.Kaynakça.....	14

2.Giriş

Bu laboratuvar çalışmasında, DNS (Domain Name System) protokolü ele alınmış ve çeşitli komutlarla uygulamalı olarak test edilmiştir. DNS, alan adlarını düzenli bir yapıda saklayarak, farklı kaynaklara ait alan isimlerini ve bölümlerini birbirinden ayırır ve bu bilgiler üzerinden haberleşmeyi sağlar. Bilgisayarların ve sunucuların alan adları aracılığıyla erişilmesine olanak tanıyan DNS, internete bağlı cihazlar için hiyerarşik bir adlandırma mekanizması olarak da tanımlanabilir.

3.1 Nslookup Çalışmaları

3.1.1 Asya’daki Bir Web Sunucusunun IP Adresini Bulma

```
C:\Users\aycac>nslookup www.naver.com
Server: ns3.ogu.edu.tr
Address: 193.140.128.28

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name: e6030.a.akamaiedge.net
Address: 72.247.160.239
Aliases: www.naver.com
         www.naver.com.nheos.com
         www.naver.com.edgekey.net
```

Verilen web sitesi için yapılan nslookup sorgusu sonucunda, IP adresi 72.247.160.239 olarak tespit edilmiştir. Alınan bu yanıt, sistemin varsayılan DNS sunucusu tarafından sağlanmıştır.

3.1.2 Avrupa'daki Bir Üniversitenin Yetkili DNS Sunucularını Bulma

```
C:\Users\aycac>nslookup -type=NS mit.edu
Server: ns3.ogu.edu.tr
Address: 193.140.128.28

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

eur5.akam.net internet address = 23.74.25.64
use2.akam.net internet address = 96.7.49.64
use5.akam.net internet address = 2.16.40.64
usw2.akam.net internet address = 184.26.161.64
asial.akam.net internet address = 95.100.175.64
asia2.akam.net internet address = 95.101.36.64
ns1-37.akam.net internet address = 193.108.91.37
ns1-173.akam.net internet address = 193.108.91.173
use5.akam.net AAAA IPv6 address = 2600:1403:a::40
ns1-37.akam.net AAAA IPv6 address = 2600:1401:2::25
ns1-173.akam.net AAAA IPv6 address = 2600:1401:2::ad
```

Avrupa'daki bir üniversiteye ait olan mit.edu alan adı için yapılan nslookup sorgusu sonucunda, IP adresleri 2600:1403:a::40, 2600:1401:2::25 ve 2600:1401:2::ad olarak elde edilmiştir. Sonuçta görülen “Non-authoritative answer” ifadesi, bu bilginin doğrudan yetkili DNS sunucusundan değil, başka bir sunucunun önbelleğinde saklanan kayıttan getirildiğini göstermektedir.

3.1.3 Yetkili DNS Sunucusundan Yahoo'nun Mail Sunucularını Sorgulama

```
C:\Users\aycac>nslookup -type=MX yahoo.com 193.108.91.37
Server:  UnKnown
Address:  193.108.91.37

*** UnKnown can't find yahoo.com: Query refused
```

```
C:\Users\aycac>nslookup -type=MX yahoo.com 193.108.91.37
Server:  UnKnown
Address:  193.108.91.37

*** UnKnown can't find yahoo.com: Query refused

C:\Users\aycac>nslookup -type=MX yahoo.com 95.101.36.64
Server:  UnKnown
Address:  95.101.36.64

*** UnKnown can't find yahoo.com: Query refused

C:\Users\aycac>nslookup -type=MX yahoo.com 95.100.175.64
Server:  UnKnown
Address:  95.100.175.64

*** UnKnown can't find yahoo.com: Query refused

C:\Users\aycac>nslookup -type=MX yahoo.com 184.26.161.64
Server:  UnKnown
Address:  184.26.161.64

*** UnKnown can't find yahoo.com: Query refused
```

Query refused veya timed-out sorunları ile karşılaşılsa da, mail sunucusunun IP adresi şu şekilde belirlenmiştir:

Mail Sunucusu IP Adresi: 23.74.25.64

Sorgunun Gönderildiği DNS Sunucusu: ns1-37.akam.net

Bu sunucu, MIT için authoritative DNS sunucularından biridir.

Sunucunun Adresi:

IPv6 Adresi: 2600:1401:2::25

```
C:\Users\aycac>nslookup -type=MX mit.edu 23.74.25.64
Server:  UnKnown
Address:  23.74.25.64

mit.edu MX preference = 100, mail exchanger = mit-edu.mail.protection.outlook.com

C:\Users\aycac>nslookup -type=MX mit.edu ns1-37.akam.net
Server:  UnKnown
Address:  2600:1401:2::25

mit.edu MX preference = 100, mail exchanger = mit-edu.mail.protection.outlook.com
```

3.2 Ipconfig Komutları ile DNS Yönetimi

3.2.1 Mevcut IP Yapılandırmasının Görüntülenmesi

Komut: ipconfig /all

```
C:\Users\aycac>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Ayca
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Yerel Ağ Bağlantısı* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 9E-2F-9D-A4-48-29
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Yerel Ağ Bağlantısı* 2:
```

```
C:\Users\aycac>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Ayca
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Yerel Ağ Bağlantısı* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 9E-2F-9D-A4-48-29
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Yerel Ağ Bağlantısı* 2:
```

```
DNS Servers . . . . . : fe80::c51:7eff:fedb:db64%5
                       172.20.10.1
                       fe80::c51:7eff:fedb:db64%5
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Ağ Bağlantısı:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 9C-2F-9D-A4-48-2A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : E4-A8-DF-E4-D3-24
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

3.2.2 DNS Önbelleğinin Temizlenmesi

Komut: ipconfig /flushdns

```
C:\Users\aycac>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

3.3 Wireshark ile DNS Takibi

ip.addr == 172.20.10.5						
No.	Time	Source	Destination	Protocol	Length Info	
175	17.530141	13.107.6.158	172.20.10.5	TCP	54 443 → 54199 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
188	23.007217	13.89.179.8	172.20.10.5	TCP	54 443 → 54200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
194	28.822274	172.20.10.5	40.79.150.120	TCP	55 54204 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1	
195	28.966739	40.79.150.120	172.20.10.5	TCP	66 443 → 54204 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2	
231	39.064702	172.20.10.5	20.250.77.142	TCP	55 53962 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1	
232	39.185722	20.250.77.142	172.20.10.5	TCP	66 443 → 53962 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2	
491	50.089068	172.20.10.5	172.20.10.1	DNS	75 Standard query 0xed1d AAAA static.ietf.org	
1080	52.697427	172.20.10.5	172.20.10.1	DNS	75 Standard query 0x835a AAAA static.ietf.org	
1088	55.007671	172.20.10.5	20.42.73.24	TCP	66 54221 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
1089	55.182170	20.42.73.24	172.20.10.5	TCP	66 443 → 54221 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM	
1090	55.182367	172.20.10.5	20.42.73.24	TCP	54 54221 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0	
1091	55.183755	172.20.10.5	20.42.73.24	TLsv1.2	266 Client Hello (SNI=v10.events.data.microsoft.com)	
1092	55.372467	20.42.73.24	172.20.10.5	TCP	1454 443 → 54221 [ACK] Seq=1 Ack=213 Win=4194048 Len=1400 [TCP PDU reassembled in 1095]	
1093	55.372467	20.42.73.24	172.20.10.5	TCP	1454 443 → 54221 [ACK] Seq=1401 Ack=213 Win=4194048 Len=1400 [TCP PDU reassembled in 1095]	
1094	55.372467	20.42.73.24	172.20.10.5	TCP	1454 443 → 54221 [ACK] Seq=2801 Ack=213 Win=4194048 Len=1400 [TCP PDU reassembled in 1095]	
1095	55.372467	20.42.73.24	172.20.10.5	TLsv1.2	89 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
1096	55.372581	172.20.10.5	20.42.73.24	TCP	54 54221 → 443 [ACK] Seq=213 Ack=4236 Win=65280 Len=0	
1097	55.378334	172.20.10.5	20.42.73.24	TLsv1.2	212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
1098	55.564865	20.42.73.24	172.20.10.5	TLsv1.2	105 Change Cipher Spec, Encrypted Handshake Message	
1099	55.569452	172.20.10.5	20.42.73.24	TLsv1.2	141 Application Data	
1100	55.569594	172.20.10.5	20.42.73.24	TLsv1.2	962 Application Data	
1101	55.569720	172.20.10.5	20.42.73.24	TLsv1.2	1256 Application Data	
1102	55.586309	20.42.73.24	172.20.10.5	TLsv1.2	123 Application Data	
1103	55.586748	172.20.10.5	20.42.73.24	TLsv1.2	92 Application Data	
1104	55.761719	20.42.73.24	172.20.10.5	TCP	54 443 → 54221 [ACK] Seq=4356 Ack=1366 Win=4193024 Len=0	
1105	55.761719	20.42.73.24	172.20.10.5	TCP	54 443 → 54221 [ACK] Seq=4356 Ack=2606 Win=4194304 Len=0	
1106	55.811510	20.42.73.24	172.20.10.5	TLsv1.2	92 Application Data	
1107	55.861071	172.20.10.5	20.42.73.24	TCP	54 54221 → 443 [ACK] Seq=2606 Ack=4394 Win=65280 Len=0	

No.	Time	Source	Destination	Protocol	Length Info	
1119	57.539248	20.42.73.24	172.20.10.5	TLsv1.2	159 Application Data	
1120	57.545234	172.20.10.5	20.42.73.24	TLsv1.2	877 Application Data	
1121	57.545679	172.20.10.5	20.42.73.24	TCP	1454 54221 → 443 [ACK] Seq=4467 Ack=4784 Win=64768 Len=1400 [TCP PDU reassembled in 1125]	
1122	57.545679	172.20.10.5	20.42.73.24	TCP	1454 54221 → 443 [ACK] Seq=5867 Ack=4784 Win=64768 Len=1400 [TCP PDU reassembled in 1125]	
1123	57.545679	172.20.10.5	20.42.73.24	TCP	1454 54221 → 443 [ACK] Seq=7267 Ack=4784 Win=64768 Len=1400 [TCP PDU reassembled in 1125]	
1124	57.545679	172.20.10.5	20.42.73.24	TCP	1454 54221 → 443 [ACK] Seq=8667 Ack=4784 Win=64768 Len=1400 [TCP PDU reassembled in 1125]	
1125	57.545679	172.20.10.5	20.42.73.24	TLsv1.2	606 Application Data	
1126	57.716418	20.42.73.24	172.20.10.5	TCP	54 443 → 54221 [ACK] Seq=4784 Ack=5867 Win=4194304 Len=0	
1128	57.723679	20.42.73.24	172.20.10.5	TCP	54 443 → 54221 [ACK] Seq=4784 Ack=8667 Win=4194304 Len=0	
1129	57.723679	20.42.73.24	172.20.10.5	TCP	54 443 → 54221 [ACK] Seq=4784 Ack=10619 Win=4194304 Len=0	
1130	57.759656	172.20.10.5	172.20.10.1	DNS	75 Standard query 0x3c0a AAAA static.ietf.org	
1132	58.139481	20.42.73.24	172.20.10.5	TLsv1.2	160 Application Data	
1133	58.146607	172.20.10.5	20.42.73.24	TCP	54 54221 → 443 [FIN, ACK] Seq=10619 Ack=4890 Win=64768 Len=0	
1134	58.316213	20.42.73.24	172.20.10.5	TCP	54 443 → 54221 [FIN, ACK] Seq=4890 Ack=10620 Win=4194304 Len=0	
1135	58.316327	172.20.10.5	20.42.73.24	TCP	54 54221 → 443 [ACK] Seq=10620 Ack=4891 Win=64768 Len=0	
1142	60.770549	172.20.10.5	172.20.10.1	DNS	75 Standard query 0x3c0a AAAA static.ietf.org	
1154	62.323918	172.20.10.1	172.20.10.5	DNS	131 Standard query response 0xed1d AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	
1157	62.324083	172.20.10.1	172.20.10.5	DNS	131 Standard query response 0x035a AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	
1160	62.324083	172.20.10.1	172.20.10.5	DNS	131 Standard query response 0x3c0a AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	
1395	62.839088	172.20.10.5	172.20.10.1	DNS	78 Standard query 0x664f AAAA analytics.ietf.org	
1400	62.831417	172.20.10.5	172.20.10.1	DNS	78 Standard query 0x261b A analytics.ietf.org	
1401	62.831607	172.20.10.5	172.20.10.1	DNS	78 Standard query 0x79e1 HTTPS analytics.ietf.org	
1482	62.857138	172.20.10.1	172.20.10.5	DNS	134 Standard query response 0x664f AAAA analytics.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63	
1483	62.857138	172.20.10.1	172.20.10.5	DNS	110 Standard query response 0x261b A analytics.ietf.org A 104.16.44.99 A 104.16.45.99	
1484	62.857138	172.20.10.1	172.20.10.5	DNS	151 Standard query response 0x79e1 HTTPS analytics.ietf.org HTTPS	
2897	73.980432	172.20.10.5	40.79.150.120	TCP	55 [TCP Keep-Alive] 54204 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1	
2898	74.004944	40.79.150.120	172.20.10.5	TCP	66 [TCP Keep-Alive ACK] 443 → 54204 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2	

3.3.1 DNS Query ve Response Mesajlarının Kullanılan Protokolü

Query ve response mesajları, UDP protokolü üzerinden iletilmiştir. UDP (User Datagram Protocol), bağlantısız bir protokoldür ve veri iletimi sırasında iletişim için bir bağlantı kurmaz. Bu nedenle, düşük gecikme süresi gerektiren uygulamalarda, özellikle DNS (Domain Name System) sorguları gibi durumlarda yaygın olarak tercih edilir.

3.3.2 DNS Query Mesajının Hedef Portu ve Response Mesajının Kaynak Portu

Query ve response mesajları için source ve destination port numarası 53 olarak belirlenmiştir. Bu port numarası, DNS (Domain Name System) protokolü için standarttır. DNS sorguları ve yanıtları, genellikle UDP protokolü üzerinden 53 numaralı port kullanılarak iletilir.

1135	58.316327	172.20.10.5	20.42.73.24	TCP	54	54221 → 443 [ACK] Seq=10620 Ack=4891 Win=64768 Len=0	
1142	68.779549	172.20.10.5	172.20.10.1	DNS	75	Standard query 0x3c8a AAAA static.ietf.org	
1154	62.323918	172.20.10.1	172.20.10.5	DNS	131	Standard query response 0xed1d AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	
1157	62.324083	172.20.10.1	172.20.10.5	DNS	131	Standard query response 0x035a AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	
1160	62.324083	172.20.10.1	172.20.10.5	DNS	131	Standard query response 0x3c8a AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	
1395	62.830988	172.20.10.5	172.20.10.1	DNS	78	Standard query 0x664f AAAA analytics.ietf.org	
1400	62.831417	172.20.10.5	172.20.10.1	DNS	78	Standard query 0x261b A analytics.ietf.org	
1401	62.831607	172.20.10.5	172.20.10.1	DNS	78	Standard query 0x79e1 HTTPS analytics.ietf.org	
1482	62.857138	172.20.10.1	172.20.10.5	DNS	134	Standard query response 0x664f AAAA analytics.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	
1483	62.857138	172.20.10.1	172.20.10.5	DNS	110	Standard query response 0x261b A analytics.ietf.org A 104.16.44.99 A 104.16.45.99	
1484	62.857138	172.20.10.1	172.20.10.5	DNS	151	Standard query response 0x79e1 HTTPS analytics.ietf.org HTTPS	
2897	73.980432	172.20.10.5	40.79.150.120	TCP	55	[TCP Keep-Alive] 54204 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1	
2898	74.084944	40.79.150.120	172.20.10.5	TCP	66	[TCP Keep-Alive ACK] 443 → 54204 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2	

Frame 1154: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C}, id 0	0000	9c 2f 9d a4 48 29 0e 51 7e db db 64 08 00 45 00
Ethernet II, Src: 0e:51:7e:db:db:64 (0e:51:7e:db:db:64), Dst: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29)	0010	00 75 95 78 00 00 40 11 78 d1 ac 14 0a 01 ac 14
Internet Protocol Vers on 4, Src: 172.20.10.1, Dst: 172.20.10.5	0020	0a 05 00 35 c0 b5 00 61 47 05 ed 1d 81 80 00 01
User Datagram Protocol Src Port: 53, Dst Port: 49333	0030	00 02 00 00 00 00 06 73 74 61 74 69 63 04 69 65
Domain Name System (response)	0040	74 66 03 ff 72 67 00 00 1c 00 01 c0 00 1c 00
	0050	01 00 00 01 79 00 10 25 06 47 00 00 00 00 00
	0060	00 00 00 68 10 2c 63 c0 0c 00 1c 00 01 00 01
	0070	79 00 16 26 06 47 00 00 00 00 00 00 00 00 68
	0080	10 2d 63

3.3.3 DNS Query Mesajının Gönderildiği IP Adresi ve Yerel DNS ile Karşılaştırma

172.20.10.5 adresine gönderilmiştir ve bu adres, yerel DNS sunucularından biridir, yani bu adres, ağdaki DNS sorgularını işleyen bir yerel sunucuya aittir ve genellikle aynı adres üzerinden yanıt alınır.

3.3.4 DNS Query Mesajının Türü ve Cevap İçeriği

Cevap (response) alınana kadar, herhangi bir yanıt içermez; yani, sorgu gönderildikten sonra yanıt beklenir ve süreç tamamlanana kadar bir geri dönüş olmaz.

3.3.5 DNS Response Mesajında Kaç "Answer" Var ve İçeriği

1153	62.323918	fe80::c51:7eff:fedb::fe80::f5e5:5554:2ee...	DNS	151	Standard query response 0x9434 AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63		
1154	62.323918	172.20.10.1	172.20.10.5	DNS	131	Standard query response 0xed1d AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	

Wireshark - Paket 1154 - Wi-Fi		
Checksum: 0x4705 [unverified]		
[Checksum Status: Unverified]		
[Stream index: 21]		
[Stream Packet Number: 2]		
[Timestamps]		
UDP payload (89 bytes)		
Domain Name System (response)		
Transaction ID: 0xed1d		
Flags: 0x8180 Standard query response, No error		
Questions: 1		
Answer RRs: 2		
Authority RRs: 0		
Additional RRs: 0		
Queries		
Answers		
static.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2c63		
static.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2d63		
[Request ID: 491]		
[Time: 12.234850000 seconds]		

1153	62.323918	fe80::c51:7eff:fedb::fe80::f5e5:5554:2ee...	DNS	151	Standard query response 0x9434 AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63		
1154	62.323918	172.20.10.1	172.20.10.5	DNS	131	Standard query response 0xed1d AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63	

Wireshark - Paket 1154 - Wi-Fi	
Checksum: 0x4705 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 21]	
[Stream Packet Number: 2]	
[Timestamps]	
UDP payload (89 bytes)	
Domain Name System (response)	
Transaction ID: 0xed1d	
Flags: 0x8180 Standard query response, No error	
Questions: 1	
Answer RRs: 2	
Authority RRs: 0	
Additional RRs: 0	
Queries	
Answers	
static.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2c63	
static.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2d63	
[Request ID: 491]	
[Time: 12.234850000 seconds]	

Toplamda 3 cevap alınmıştır:

2 tanesi host adresi (AAAA)

1 tanesi CNAME kaydı (HTTPS)

Her birinde şu bilgiler vardır:

name, type, class, TTL, data length ve address.

3.3.6 Sonraki TCP SYN Paketi Hangi IP Adresine Gönderildi

DNS yanıt adreslerinden biri olarak 104.16.44.99 belirtilmişken, TCP SYN paketinin destinasyon adresi olan 20.42.73.24 ile bu adres eşleşmemektedir.

tcp.flags.syn == 1 && tcp.flags.ack == 0						
No.	Time	Source	Destination	Protocol	Length	Info
312	49.508964	2a00:1880:a113:4562...	2a04:4e42:70::347	TCP	86	54217 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=256 SACK_PERM
313	49.529556	2a00:1880:a113:4562...	2606:4700::6810:2d63	TCP	86	54218 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=256 SACK_PERM
314	49.529999	2a00:1880:a113:4562...	2606:4700::6810:2d63	TCP	86	54219 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=256 SACK_PERM
1088	55.007671	172.20.10.5	20.42.73.24	TCP	66	54221 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1161	62.325326	2a00:1880:a113:4562...	2606:4700::6810:2c63	TCP	86	54222 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=256 SACK_PERM
1162	62.325641	2a00:1880:a113:4562...	2606:4700::6810:2c63	TCP	86	54223 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=256 SACK_PERM
1377	62.824787	2a00:1880:a113:4562...	2606:4700::6810:2c63	TCP	86	54224 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=256 SACK_PERM

3.3.7 Web Sayfasındaki Görseller İçin Yeni DNS Sorguları

Her bir görsel için yeni bir DNS sorgusu yapılmamıştır; yani, görsellerin yüklenmesi sırasında her defasında DNS sorgusu tekrarlanmamıştır.

3.3.8 nslookup ile www.mit.edu Sorgusunun DNS Port Bilgileri

Query ve response mesajları için destination ve source port numaraları, her iki yönlü iletişimde de 53 olarak belirlenmiştir.

3.3.9 www.mit.edu Sorgusu Hangi IP Adresine Gönderildi

```
C:\Users\aycac>nslookup www.mit.edu
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

Non-authoritative answer:
Name:      e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:cb00:1a1::255e
            2a02:26f0:cb00:19c::255e
            184.29.225.160
Aliases:   www.mit.edu
            www.mit.edu.edgekey.net
```

Sorgunun gönderildiği DNS sunucusu:

Server: dns49.turktelekom.com.tr

IP Adresi: 195.175.39.49

3.3.10 www.mit.edu Sorgusunun Türü ve Cevap İçeriği

Query Type: A ve AAAA

Standart bir query olup hem IPv4 hem de IPv6 adresleri içermektedir.

3.3.11 www.mit.edu Sorgusunun DNS Response Mesajındaki Answers Bölümü

Type CNAME olarak 2 adet kayıt bulunmaktadır:

1. www.mit.edu → www.mit.edu.edgekey.net
2. www.mit.edu.edgekey.net → e9566.dscb.akamaiedge.net

Type AAAA olarak 2 adet kayıt bulunmaktadır:

1. 2a02:26f0:cb00:1a1::255e
2. 2a02:26f0:cb00:19c::255e

Ek olarak Type A kaydı da bulunmaktadır:

- IPv4 Adresi: 184.29.225.160

3.3.12 Ekran Görüntüsü (www.mit.edu Sorgusu)

```
C:\Users\aycac>nslookup www.mit.edu
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

Non-authoritative answer:
Name:      e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:cb00:1a1::255e
            2a02:26f0:cb00:19c::255e
            184.29.225.160
Aliases:   www.mit.edu
            www.mit.edu.edgekey.net
```

3.3.13 nslookup -type=NS mit.edu Sorgusu Hangi IP'ye Gönderildi

Sorgu, varsayılan olarak belirlenmiş DNS sunucusu olan dns49.turktelekom.com.tr (195.175.39.49) adresine gönderilmiştir.

3.3.14 NS Sorgusunun Türü ve Cevap İçeriği

```
C:\Users\aycac>nslookup -type=NS mit.edu
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

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

Sorgu türü NS olarak belirlenmiş ve MIT'nin yetkili DNS sunucuları listelenmiş

3.3.15 mit.edu'ya Dair Yetkili DNS Sunucuları ve IP Adresleri

Wireshark çıktısında paket 156 şu bilgileri içeriyor:

- Sorgu tipi: NS (Yetkili Ad Sunucuları)
- Yanıt olarak gelen yetkili DNS sunucuları:
 - use2.akam.net
 - usw2.akam.net
 - asia2.akam.net
 - use5.akam.net
 - ns1-37.akam.net
 - asia1.akam.net

- ns1-173.akam.net
- eur5.akam.net

Bu sunucular mit.edu için yetkili ad sunucularıdır.

3.3.16 Ekran Görüntüsü (NS Sorgusu mit.edu)

No.	Time	Source	Destination	Protocol	Length	Info
29	3.808791	192.168.1.41	195.175.39.49	DNS	78	Standard query 0x7fa6 A edge.microsoft.com
30	3.809333	192.168.1.41	195.175.39.49	DNS	78	Standard query 0x8d1c HTTPS edge.microsoft.com
31	3.821560	195.175.39.49	192.168.1.41	DNS	181	Standard query response 0x7fa6 A edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a-0036.a-msedge.net A 204.79.197.239 A 13.18...
72	9.550936	192.168.1.41	195.175.39.49	DNS	74	Standard query 0x6c88 A ecs.office.com
73	9.565868	195.175.39.49	192.168.1.41	DNS	255	Standard query response 0x6c88 A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME dual-s-0005-office.config.skype.com CNAME ecs-office.s-0005.dual-s-...
153	22.586393	192.168.1.41	195.175.39.49	DNS	86	Standard query 0x0001 PTR 49.39.175.195.in-addr.arpa
154	22.590689	195.175.39.49	192.168.1.41	DNS	124	Standard query response 0x0001 PTR 49.39.175.195.in-addr.arpa PTR dns49.turktelekom.com.tr
155	22.601981	192.168.1.41	195.175.39.49	DNS	67	Standard query 0x0002 NS mit.edu
156	22.616600	195.175.39.49	192.168.1.41	DNS	234	Standard query response 0x0002 NS mit.edu NS use2.akam.net NS usv2.akam.net NS asia2.akam.net NS use5.akam.net NS ns1-37.akam.net NS asia1.akam.net NS ns1-17...
182	29.478308	192.168.1.41	195.175.39.49	DNS	85	Standard query 0x19ae A login.microsoftonline.com
183	29.487777	195.175.39.49	192.168.1.41	DNS	327	Standard query response 0x19ae A login.microsoftonline.com CNAME login.mso.msidentity.com CNAME ak.privatelink.msidentity.com CNAME www.tm.a.prd.aadg.traffic...

```

Frame 155: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C}, id 0
  Section number: 1
    Interface id: 0 (\Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  6, 2025 02:31:18.353819000 Türkiye Standart Saati
    UTC Arrival Time: Mar  5, 2025 23:31:18.353819000 UTC
    Epoch Arrival Time: 1741217478.353819000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.003292000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 22.601981000 seconds]
    Frame Number: 155
    Frame Length: 67 bytes (536 bits)
    Capture Length: 67 bytes (536 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: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29), Dst: ZyxelCommuni_e6:c2:06 (5c:f4:ab:e6:c2:06)
  ▶ Internet Protocol Version 4, Src: 192.168.1.41, Dst: 195.175.39.49
  ▶ User Datagram Protocol, Src Port: 64615, Dst Port: 53
    Source Port: 64615
    Destination Port: 53
    Length: 33
    Checksum: 0x7d9e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Stream Packet Number: 1]
    ▶ [Timestamps]
      UDP payload (25 bytes)
  ▶ Domain Name System (query)
    Transaction ID: 0x0002
    ▶ Flags: 0x0100 Standard query
      0... .. = Response: Message is a query
      .000 0... .. = Opcode: Standard query (0)
      ... ..0. .... = Truncated: Message is not truncated
      .... ..1 .... = Recursion desired: Do query recursively
      .... ..0... .. = Z: reserved (0)
      .... ..0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    ▶ Queries
      ▶ mit.edu: type NS, class IN
      [Response In: 156]

```

```
Wireshark - Paket 156 - Wi-Fi

Epoch Arrival Time: 1741217478.368438000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.014619000 seconds]
[Time delta from previous displayed frame: 0.014619000 seconds]
[Time since reference or first frame: 22.616600000 seconds]
Frame Number: 156
Frame Length: 234 bytes (1872 bits)
Capture Length: 234 bytes (1872 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: ZyxelCommuni_e6:c2:06 (5c:f4:ab:e6:c2:06), Dst: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29)
▶ Internet Protocol Version 4, Src: 195.175.39.49, Dst: 192.168.1.41
▼ User Datagram Protocol, Src Port: 53, Dst Port: 64615
  Source Port: 53
  Destination Port: 64615
  Length: 200
  Checksum: 0xed16 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  [Stream Packet Number: 2]
  ▶ [Timestamps]
    UDP payload (192 bytes)
▼ Domain Name System (response)
  Transaction ID: 0x0002
  ▼ Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    ....0... .. = Authoritative: Server is not an authority for domain
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    ....1... .. = Recursion available: Server can do recursive queries
    ....0... .. = Z: reserved (0)
    ....0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    ....0... .. = Non-authenticated data: Unacceptable
    ....0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ mit.edu: type NS, class IN
  ▼ Answers
    ▶ mit.edu: type NS, class IN, ns use2.akam.net
    ▶ mit.edu: type NS, class IN, ns usw2.akam.net
    ▶ mit.edu: type NS, class IN, ns asia2.akam.net
    ▶ mit.edu: type NS, class IN, ns use5.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▶ 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
  [Request In: 155]
  [Time: 0.014619000 seconds]
```

3.3.17 nslookup www.aiit.or.kr bitsy.mit.edu Sorgusu Hangi IP'ye Gönderildi

No.	Time	Source	Destination	Protocol	Length	Info
20	7.362712	192.168.1.41	195.175.39.49	DNS	73	Standard query 0x8fda A bitsy.mit.edu
21	7.372554	195.175.39.49	192.168.1.41	DNS	89	Standard query response 0x8fda A bitsy.mit.edu A 18.0.72.3
22	7.375351	192.168.1.41	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
25	9.384878	192.168.1.41	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
35	11.400671	192.168.1.41	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
42	13.410926	192.168.1.41	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
54	14.896195	192.168.1.41	195.175.39.49	DNS	88	Standard query 0x7a86 A browser-intake-datadoghq.com
55	14.896430	192.168.1.41	195.175.39.49	DNS	88	Standard query 0x3efa HTTPS browser-intake-datadoghq.com
56	14.912221	195.175.39.49	192.168.1.41	DNS	136	Standard query response 0x7a86 A browser-intake-datadoghq.com A 3.233.158.26 A 3.233.158.24 A 3.233.158.25
91	15.415903	192.168.1.41	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
96	17.141423	192.168.1.41	195.175.39.49	DNS	72	Standard query 0xc99a A www.bing.com
97	17.141718	192.168.1.41	195.175.39.49	DNS	72	Standard query 0x291f HTTPS www.bing.com
98	17.155160	195.175.39.49	192.168.1.41	DNS	225	Standard query response 0xc99a A www.bing.com CNAME www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e86303.dscc.akamaiedge.net A 195.
113	17.860764	192.168.1.41	195.175.39.49	DNS	81	Standard query 0x9b88 A sadowload.mcafee.com
114	17.894625	192.168.1.41	195.175.39.50	DNS	81	Standard query 0x9b88 A sadowload.mcafee.com
115	17.905971	195.175.39.50	192.168.1.41	DNS	234	Standard query response 0x9b88 A sadowload.mcafee.com CNAME sadowload-r53.awsconsumer.mcafee.com CNAME sadowload.mcafee.com.edgesuite.net CNAME a866.dscc...
117	17.925601	195.175.39.49	192.168.1.41	DNS	234	Standard query response 0x9b88 A sadowload.mcafee.com CNAME sadowload-r53.awsconsumer.mcafee.com CNAME sadowload.mcafee.com.edgesuite.net CNAME a866.dscc...

DNS sorgusu 18.0.72.3 IP adresine gönderilmiştir. Bu adres, mit.edu domaininin nameserver'larından birine ait olan IP adresine karşılık gelmektedir.

3.3.18 Bu Sorgunun Türü

Sorgu Türü: A Kaydı

3.3.19 Cevap Mesajında Kaç "Answer" Var ve İçeriği

Cevap Mesajlarında 3 'Answer' Var.

İçeriği: Bu 3 'Answer' aşağıdaki IP adreslerini içermektedir:

3.233.158.26

3.233.158.24

3.233.158.25

3.3.20 Ekran Görüntüsü (bitsy.mit.edu'ye Yapılan Sorgu)

dns && dns.qry.name == "bitsy.mit.edu"						
No.	Time	Source	Destination	Protocol	Length	Info
626	64.597789	192.168.1.41	195.175.39.49	DNS	73	Standard query 0xa77a A bitsy.mit.edu
627	64.598160	192.168.1.41	195.175.39.49	DNS	73	Standard query 0x8b0e HTTPS bitsy.mit.edu
628	64.601971	192.168.1.41	195.175.39.49	DNS	73	Standard query 0xbfd9 A bitsy.mit.edu
629	64.602109	192.168.1.41	195.175.39.49	DNS	73	Standard query 0x3f51 HTTPS bitsy.mit.edu
630	64.615272	195.175.39.49	192.168.1.41	DNS	89	Standard query response 0xa77a A bitsy.mit.edu A 18.0.72.3
631	64.615326	195.175.39.49	192.168.1.41	DNS	89	Standard query response 0xbfd9 A bitsy.mit.edu A 18.0.72.3

Frame 630: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C}, id 0

Ethernet II, Src: ZyxeICommuni_e6:c2:06 (5c:f4:ab:e6:c2:06), Dst: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29)

Internet Protocol Version 4, Src: 195.175.39.49, Dst: 192.168.1.41

User Datagram Protocol, Src Port: 53, Dst Port: 65240

Domain Name System (response)

Transaction ID: 0xa77a

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

Answers

[Request In: 626]

[Time: 0.017483000 seconds]

4. LABORATUVAR SONUCU

Bu laboratuvar çalışmasında DNS (Domain Name System) sorgularının nasıl yapıldığı, DNS yanıtlarının nasıl işlendiği ve bu işlemlerin ağ üzerinde nasıl takip edilebileceği incelendi. Çalışma sırasında Wireshark ve nslookup gibi araçlar kullanılarak, ağ üzerindeki DNS trafiği detaylı bir şekilde gözlemlendi.

Yapılan DNS sorguları ile ilgili olarak, DNS sunucularına gönderilen sorguların türleri (A kaydı, CNAME, NS kaydı gibi) ve bu sorgulara verilen yanıtlar üzerinde duruldu. Wireshark ile DNS sorgularının ağdaki hareketini izleyerek, sorguların hedef IP adreslerine ulaşması ve bu IP adreslerinden gelen yanıtları nasıl işlediği öğrenildi.

DNS sorgularının genellikle A kaydı ve NS kaydı gibi farklı türde yanıtlar aldığı gözlemlendi. A kaydı, bir alan adı ile ilişkilendirilmiş IP adreslerini içerirken, NS kaydı ise alan adının yetkili DNS sunucularını belirtmektedir.

DNS protokolü, Wireshark ile izleme sürecinde, en önemli sorgu ve yanıt çiftlerinin genellikle iletişimin sonunda yer aldığı tespit edilmiştir. DNS sorgu ve yanıt mesajları detaylı bir şekilde incelenerek, mesaj tipleri, içerik yapıları, dönen veriler, IP adresleri, UDP protokolü ve kullanılan port numaraları gibi önemli bilgiler elde edilmiştir.

DNS sorguları ve yanıtları, ağ iletişiminin temel bileşenlerindendir. Bu çalışmada, farklı DNS sorgu türleri ve yanıtları üzerinde yapılan analizler, ağ yönetimi ve yapılandırması konularında daha kapsamlı bir bilgi edinmemize olanak tanıdı.

5.Kaynakça

Wireshark Lab: DNS v8.0

Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross