



Laboratuvar Raporu 2

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Özlem Kayıkcı

152120191043

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İçindekiler

2	Giriş.....	3
3	Laboratuvar Uygulaması.....	3
3.1	Nslookup 1.bölüm	3
3.1.1.....		3
3.1.2.....		3
3.1.3.....		4
3.2	ipconfig 2.bölüm	4
3.3	tracing dns with wireshark 3.bölüm	5
3.3.1.....		6
3.3.2.....		6
3.3.3.....		6
3.3.4.....		6
3.3.5.....		6
3.3.6.....		6
3.3.7.....		7
3.3.8.....		7
3.3.9.....		7
3.3.10.....		8
3.3.11.....		8
3.3.12.....		8
3.3.13.....		8
3.3.14.....		8
3.3.15.....		8
3.3.16.....		9
3.3.17.....		9
3.3.18.....		9
3.3.19.....		10
3.3.20.....		10

2 Giriş

Bu laboratuvar kapsamında DNS (Domain Name System) işlenmiş ilgili komutlarla uygulamalar gerçekleştirilmiştir. DNS alan adlarını sistemli bir şekilde tutmak için hiyerarşiyi kullanarak herhangi bir kaynak için bölüm ve alan adlarını ayırmaya, isimlendirmeye ve aradaki iletişimi sağlamaya yarar. Bilgisayar adı ve sunucunun alan adına ulaşmamızı sağlayan DNS, ağa bağlı bir kaynak için hiyerarşik bir isimlendirme sistemi de denilebilir.

3 Laboratuvar Uygulaması

3.1 Nslookup 1.bölüm

3.1.1

```
C:\Users\ahmet>nslookup www.aiit.or.kr
Server:  MyRouter.Home
Address:  192.168.1.1

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

Föyde verilmiş olan web sitesini nslookup komutunu kullanarak IP adresi 58.229.6.225 olarak bulunmuştur. Gelen cevap yerel DNS sunucusundan gelmiş olup local server cevabı alabilmek adına birden fazla DNS sunucusuna bağlanmıştır.

3.1.2

```
C:\Users\ahmet>nslookup -type=NS mit.edu
Server:  MyRouter.Home
Address:  192.168.1.1

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

Avrupadaki bir üniversite olarak mit.edu sitesini kullanarak IP adresi 2a02:26f0:8c00:288::255e2a02:26f0:8c00:2aa::255e184.84.235.19 olarak bulunmuştur. Buradaki -type=NS komutu yetkili DNS'lerin host isimlerine ulaşmak için kullanılır. "Non-authoritative answer" dönütünün anlamı ise cevabın aranan DNS sunucusundan değil de başka bir server'ın önbelleğinden gelmiş olmasıdır.

3.1.3

```
C:\Users\ahmet>nslookup -type=NS upt.ro
Server: MyRouter.Home
Address: 192.168.1.1

Non-authoritative answer:
upt.ro nameserver = ns1.upt.ro
upt.ro nameserver = nsh.upt.ro
upt.ro nameserver = ns2.upt.ro
upt.ro nameserver = ns3.upt.ro
upt.ro nameserver = ns.upt.ro

C:\Users\ahmet>nslookup mail.yahoo.com ns1.upt.ro
Server: ns1.upt.ro
Address: 193.226.8.202

*** ns1.upt.ro can't find mail.yahoo.com: Query refused

C:\Users\ahmet>nslookup mail.yahoo.com nsh.upt.ro
Server: UnKnown
Address: 82.78.244.241

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

C:\Users\ahmet>nslookup mail.yahoo.com ns2.upt.ro
Server: UnKnown
Address: 89.238.245.202

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

C:\Users\ahmet>nslookup mail.yahoo.com ns3.upt.ro
Server: UnKnown
Address: 92.87.208.67

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

C:\Users\ahmet>nslookup mail.yahoo.com ns.upt.ro
Server: ns.upt.ro
Address: 193.226.8.201

*** ns.upt.ro can't find mail.yahoo.com: Query refused

PS C:\Users\ahmet> nslookup www.ait.or.kr
Server: MyRouter.Home
Address: 192.168.1.1

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

PS C:\Users\ahmet> nslookup -type=NS mit.edu
Server: MyRouter.Home
Address: 192.168.1.1

Non-authoritative answer:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = use5.akam.net
PS C:\Users\ahmet> nslookup mail.yahoo.com aur5.akam.net
*** Can't find server address for 'aur5.akam.net':
Server: MyRouter.Home
Address: 192.168.1.1

Non-authoritative answer:
Name: edge.gycpi.b.yahoodns.net
Addresses: 2a00:1288:80:807::1
2a00:1288:80:807::2
87.248.119.251
87.248.119.252
Aliases: mail.yahoo.com

PS C:\Users\ahmet> nslookup mail.yahoo.com bitsy.edu.tr
*** Can't find server address for 'bitsy.edu.tr':
Server: MyRouter.Home
Address: 192.168.1.1

Non-authoritative answer:
Name: edge.gycpi.b.yahoodns.net
Addresses: 2a00:1288:80:807::1
2a00:1288:80:807::2
87.248.119.251
87.248.119.252
Aliases: mail.yahoo.com

C:\Users\ahmet>nslookup mail.yahoo.com bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.0.72.3

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

C:\Users\ahmet>_

PS C:\Users\ahmet> nslookup mail.yahoo.com aur5.akam.net
*** Can't find server address for 'aur5.akam.net':
Server: MyRouter.Home
Address: 192.168.1.1

Non-authoritative answer:
Name: edge.gycpi.b.yahoodns.net
Addresses: 2a00:1288:80:807::1
2a00:1288:80:807::2
87.248.119.251
87.248.119.252
Aliases: mail.yahoo.com
```

Query refused ya da timed-out sorunları alınmasına karşılık mail sunucusunun IP adresi 18.0.72.3 olarak belirlenmiştir. Burada beklenen hostun adı mail.yahoo.com ve IP adresinin cevap olarak gelmesidir. Beklenen yanıt başka bir komut sisteminde işe yaramıştır.

3.2 ipconfig 2.bölüm

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

İstenilen uygulama gerçekleştirilmiştir ve önbellek temizlenmiştir.

3.3 tracing dns with wireshark 3.bölüm

ip.addr == 192.168.43.103							
No.	Time	Source	Destination	Protocol	Length	Info	
46	22:48:58,050204	20.189.173.5	192.168.43.103	TCP	66	443 → 58614 [ACK] Seq=1 Ack=2 Win=2047 Len=0 SLE=1 SRE=	
47	22:49:06,250927	192.168.43.103	104.18.21.157	TCP	55	[TCP Keep-Alive] 58598 → 443 [ACK] Seq=1 Ack=1 Win=252 L	
48	22:49:06,310143	104.18.21.157	192.168.43.103	TCP	66	[TCP Keep-Alive ACK] 443 → 58598 [ACK] Seq=1 Ack=2 Win=1	
49	22:49:06,534197	192.168.43.103	104.83.4.50	TCP	55	[TCP Keep-Alive] 58609 → 443 [ACK] Seq=1 Ack=1 Win=253 L	
50	22:49:06,631565	104.83.4.50	192.168.43.103	TCP	54	443 → 58609 [RST] Seq=1 Win=0 Len=0	
51	22:49:10,340647	192.168.43.103	192.168.43.1	DNS	72	Standard query 0x3fb8 A www.ietf.org	
52	22:49:10,341798	192.168.43.103	192.168.43.1	DNS	72	Standard query 0xf666 HTTPS www.ietf.org	
53	22:49:10,363150	192.168.43.103	192.168.43.1	DNS	72	Standard query 0x44fb A www.ietf.org	
54	22:49:10,405892	192.168.43.103	192.168.43.1	DNS	78	Standard query 0x12d8 A analytics.ietf.org	
55	22:49:10,407588	192.168.43.103	192.168.43.1	DNS	78	Standard query 0xa171 HTTPS analytics.ietf.org	
56	22:49:10,476055	192.168.43.1	192.168.43.103	DNS	149	Standard query response 0x3fb8 A www.ietf.org CNAME www	
57	22:49:10,476129	192.168.43.103	20.189.173.5	TCP	54	58614 → 443 [FIN, ACK] Seq=2 Ack=1 Win=252 Len=0	
58	22:49:10,476648	192.168.43.103	204.79.197.219	TCP	54	58611 → 443 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0	
59	22:49:10,476756	192.168.43.103	204.79.197.219	TCP	54	58612 → 443 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0	
Frame 51: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{B2607407-1B85-4DD5-BC71-915DC00AF9A8}, id							
Ethernet II, Src: IntelCor_d7:85:ac (5c:87:9c:d7:85:ac), Dst: XiaomiCo_fc:23:5c (20:f4:78:fc:23:5c)							
Internet Protocol Version 4, Src: 192.168.43.103, Dst: 192.168.43.1							
User Datagram Protocol, Src Port: 61080, Dst Port: 53							
Domain Name System (query)							
Transaction ID: 0x3fb8							
Flags: 0x0100 Standard query							
Questions: 1							
Answer RRs: 0							
Authority RRs: 0							
Additional RRs: 0							
Queries							
www.ietf.org: type A, class IN							
Name: www.ietf.org							
[Name Length: 12]							
[Label Count: 3]							
Type: A (Host Address) (1)							
Class: IN (0x0001)							
[Response In: 56]							

56	22:49:10,476055	192.168.43.1	192.168.43.103	DNS	149	Standard query response 0x3fb8 A www.ietf.org CNAME www.ietf.
57	22:49:10,476129	192.168.43.103	20.189.173.5	TCP	54	58614 → 443 [FIN, ACK] Seq=2 Ack=1 Win=252 Len=0
58	22:49:10,476648	192.168.43.103	204.79.197.219	TCP	54	58611 → 443 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
59	22:49:10,476756	192.168.43.103	204.79.197.219	TCP	54	58612 → 443 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
Frame 56: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{B2607407-1B85-4DD5-BC71-915DC00AF9A8}, id						
Ethernet II, Src: XiaomiCo_fc:23:5c (20:f4:78:fc:23:5c), Dst: IntelCor_d7:85:ac (5c:87:9c:d7:85:ac)						
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.103						
User Datagram Protocol, Src Port: 53, Dst Port: 61080						
Domain Name System (response)						
Transaction ID: 0x3fb8						
Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 3						
Authority RRs: 0						
Additional RRs: 0						
Queries						
www.ietf.org: type A, class IN						
Name: www.ietf.org						
[Name Length: 12]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Answers						
[Request In: 51]						
[Time: 0.135408000 seconds]						

3.3.1

Query ve response mesajları UDP protokolü üzerinden gönderilmiştir.

3.3.2

Destination ve source port numarası query ve response mesajları için 53 olarak belirlenmiştir.

3.3.3

192.168.43.1 adresine gönderilmiştir ve aynıdır, bu adres yerel DNS serverlarındandır,

3.3.4

Standart query olduğundan hiçbir cevap taşımamaktadır.

3.3.5

```
Class: IN (0x0001)
▼ 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: 222 (3 minutes, 42 seconds)
    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
\[Request In: 51\]
[Time: 0.135408000 seconds]
```

Host adres olarak 2 , CNAME olarak 1 toplamda 3 cevap alınmıştır. host adresleri ortak olarak name, type , class, TTL, data length ve address bulunmaktadır.

3.3.6

DNS response adreslerinden biri olarak 104.16.44.99 TCP SYN packet'in destinasyon adresiyle eşleşmemektedir.

```

C:\Users\ahmet>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : complex.upt.ro

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::2a6f:494a:6c54:49ec%9
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Yerel Ağ Bağlantısı* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Yerel Ağ Bağlantısı* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ca2:4503:e404:6798%15
    IPv4 Address. . . . . : 192.168.43.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.43.1

C:\Users\ahmet>

```

No.	Time	Source	Destination	Protocol	Length	Info
8	23:22:37,693192	192.168.43.103	52.111.243.2	TLSv1.2	89	Application Data
9	23:22:37,896489	52.111.243.2	192.168.43.103	TCP	54	443 → 58624 [ACK] Seq=1 Ack=36 Win=16386 Len=0
12	23:22:39,288347	192.168.43.103	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
13	23:22:39,434106	192.168.43.1	192.168.43.103	DNS	140	Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa
14	23:22:39,441572	192.168.43.103	192.168.43.1	DNS	71	Standard query 0x0002 A www.mit.edu
15	23:22:39,640015	192.168.43.1	192.168.43.103	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.m

> Frame 14: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF{...}	0000	20 f4 78 fc 23 5c 5c 87 9c d7 85 ac
> Ethernet II, Src: IntelCor_d7:85:ac (5c:87:9c:d7:85:ac), Dst: XiaomiCo_fc:23:5c (20:f4:78:23:5c:20)	0010	00 39 6a 29 00 00 80 11 00 00 c0 a8
> Internet Protocol Version 4, Src: 192.168.43.103, Dst: 192.168.43.1	0020	2b 01 c5 6f 00 35 00 25 d7 ef 00 02
> User Datagram Protocol, Src Port: 50543, Dst Port: 53	0030	00 00 00 00 00 00 03 77 77 77 03 6d
> Domain Name System (query)	0040	64 75 00 00 01 00 01


```

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: 15]

```

3.3.7

Hayır, her image için ayrı ve yeni bir DNS query 'ye rastlanılmamıştır.

3.3.8

Destination ve source port numarası query ve response mesajları için 53 olarak belirlenmiştir.

3.3.9

192.168.43.103 adresine gönderilmiştir bu adres local DNS serverlarından biridir.

3.3.10

Query type A olarak belirlenmiştir ve standart bir query olduğundan hiçbir cevap içermemektedir.

3.3.11

Type cname olarak 2 adet ve type AAAA olarak 2 adet cevap alınmıştır ve name ,type,class ,TTL, data length , cname/ AAAA adresleri bulunmaktadır.

```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:cb00:19c::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:cb00:19c::255e
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:cb00:1a1::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:cb00:1a1::255e
[Request In: 16]
[Time: 0.189763000 seconds]
```

3.3.12

İstenilen görüntüler ilgili sorulara eklenmiştir.

3.3.13

Default olarak belirlenmiş DNS server olarak 192.168.43.1 adresine gönderilmiştir.

3.3.14

DNS server Type olarak NS olduğu görülmüştür.Herhangi bir cevap barındırmamaktadır.

3.3.15

3.3.16 de eklenmiş olan ekran görüntüsünde 8 nameserver'a rastlanılmıştır ancak beklendiği gibi IP adreslerine buradan ulaşamamaktadır.

3.3.16

Wi-Fi

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

ip.addr==192.168.43.103

No.	Time	Source	Destination	Protocol	Length	Info
1	23:35:45,600823	192.168.43.103	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
2	23:35:45,608043	192.168.43.1	192.168.43.103	DNS	85	Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa
3	23:35:45,615267	192.168.43.103	192.168.43.1	DNS	67	Standard query 0x0002 NS mit.edu
4	23:35:45,712163	192.168.43.1	192.168.43.103	DNS	234	Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS asia1.akam.net

> Frame 4: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{B2607407-1885-4DD5-BC71-915DC00AF9A8}, id 0000 5c 8:

> Ethernet II, Src: XiaomiCo_fc:23:5c (20:f4:78:fc:23:5c), Dst: IntelCor_d7:85:ac (5c:87:9c:d7:85:ac) 0010 00 d:

> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.103 0020 2b 6:

> User Datagram Protocol, Src Port: 53, Dst Port: 55124 0030 00 0:

> Domain Name System (response) 0040 02 0:

Transaction ID: 0x0002 0050 75 7:

> Flags: 0x8180 Standard query response, No error 0060 00 0:

Questions: 1 0070 c0 2:

Answer RRs: 8 0080 73 3:

Authority RRs: 0 0090 07 0:

Additional RRs: 0 00a0 01 0:

> Queries 00b0 00 0:

> mit.edu: type NS, class IN 00c0 37 c:

> Answers 00d0 61 7:

> mit.edu: type NS, class IN, ns usw2.akam.net 00e0 08 0:

> 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 use5.akam.net

> mit.edu: type NS, class IN, ns eur5.akam.net

> mit.edu: type NS, class IN, ns ns1-37.akam.net

> mit.edu: type NS, class IN, ns asia2.akam.net

> mit.edu: type NS, class IN, ns use2.akam.net

[Request In: 3]

[Time: 0.096896000 seconds]

> Answers

> mit.edu: type NS, class IN, ns usw2.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 15

Name Server: usw2.akam.net

> mit.edu: type NS, class IN, ns asia1.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 8

Name Server: asia1.akam.net

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

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 10

Name Server: ns1-173.akam.net

> 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: 1800 (30 minutes)

Data length: 7

Name Server: use5.akam.net

> mit.edu: type NS, class IN, ns eur5.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 7

Name Server: eur5.akam.net

> mit.edu: type NS, class IN, ns ns1-37.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 9

Name Server: ns1-37.akam.net

> mit.edu: type NS, class IN, ns asia2.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 8

Name Server: asia2.akam.net

> mit.edu: type NS, class IN, ns use2.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 7

Name Server: use2.akam.net

[Request In: 3]

[Time: 0.096896000 seconds]

3.3.17

18.0.72.3 adresine gönderilmiştir. mit.edu adresinin nameserver'larından yani response cevaplarından birinin IP adresine denk düşmektedir.

3.3.18

Standart bir query(A) olduğundan hiçbir cevap içermemektedir.

3.3.19

Response mesajın koredeki web sitesinin incelemesi olarak bir mesaj beklenmekle birlikte, aldığımız timed-out ve query refused hataları sebebiyle ekrandaki 3.3.20 'de bulunan çıktıdaki gibi görülmektedir.

3.3.20

No.	Time	Source	Destination	Protocol	Length	Info
6	23:45:06,373423	192.168.43.103	192.168.43.1	DNS	73	Standard query 0x3f20 A bitsy.mit.edu
7	23:45:06,644932	192.168.43.103	192.168.43.1	DNS	73	Standard query 0x3f20 A bitsy.mit.edu
8	23:45:06,649395	192.168.43.1	192.168.43.103	DNS	89	Standard query response 0x3f20 A bitsy.mit.edu A 18.0.72.3
9	23:45:06,650328	192.168.43.1	192.168.43.103	DNS	89	Standard query response 0x3f20 A bitsy.mit.edu A 18.0.72.3
10	23:45:06,659488	192.168.43.103	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
11	23:45:08,672587	192.168.43.103	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
12	23:45:10,682770	192.168.43.103	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
13	23:45:12,698623	192.168.43.103	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
16	23:45:14,714303	192.168.43.103	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
17	23:45:18,339089	192.168.43.103	34.83.124.54	TCP	55	58594 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
18	23:45:18,697737	34.83.124.54	192.168.43.103	TCP	66	443 → 58594 [ACK] Seq=1 Ack=2 Win=222 Len=0 SLE=1 SRE=2
19	23:45:26,952605	192.168.43.103	74.125.143.188	TCP	55	[TCP Keep-Alive] 58591 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
20	23:45:27,195689	74.125.143.188	192.168.43.103	TCP	66	[TCP Keep-Alive ACK] 5228 → 58591 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2

> Frame 9: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{B2607407-1885-4DD5-BC71-915DC00AF9A8}, id 0

> Ethernet II, Src: XiaomiCo_fc:23:5c (20:f4:78:fc:23:5c), Dst: IntelCor_d7:85:ac (5c:87:9c:d7:85:ac)

> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.103

> User Datagram Protocol, Src Port: 53, Dst Port: 63372

> Domain Name System (response)

> Transaction ID: 0x3f20

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

> bitsy.mit.edu: type A, class IN, addr 18.0.72.3

[Retransmitted response. Original response in: 8]

[Retransmission: True]

0000 5c 87 9c d7 85 ac 20

0010 00 4b c0 25 40 00 40

0020 2b 67 00 35 f7 8c 00

0030 00 01 00 00 00 00 05

0040 03 65 64 75 00 00 01

0050 00 07 08 00 04 12 00

Bu bölümde DNS protokolünü wireshark uygulaması aracılığıyla takip edilmiştir. Uygulama sonucunda odaklanmamız gereken sorgu ve cevap çiftlerinin sondaki çiftler olduğunu gözlemledik. DNS query ve response mesajlarını incelerken tip, içerik, dönüt, IP adresleri, UDP protokolü ve port numarası öğrenilmiştir.