152120211104_Doğukan_Kıyıklık.docx

Yazar Doğukan Kıyıklık

Gönderim Tarihi: 02-Mar-2025 09:19PM (UTC+0300)
Gönderim Numarası: 2602847803
Dosya adı: 152120211104_Doğukan_Kıyıklık.docx (1.04M)
Kelime sayısı: 559
Karakter sayısı: 3298

Laboratuvar Raporu #2

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

(152116027)

Doğukan Kıyıklık

152120211104

Dr. Öğr. Üyesi İlker Özçelik

2024-2025

1 İçindekiler

2 Giriş

Bu laboratuvarda, DNS yapısı incelenmiştir. Laboratuvar kapsamında belirlenen sorulara verdiğim yanıtları, Wireshark uygulamasından elde edilen ekran görüntüleriyle ve terminal çıktılarıyla destekledim.

3 Laboratuvar Uygulaması

3.1 nslookup

3.1.1 1. Soru

Cevap: IPv4 adresleri = 188.114.97.2 ve 188.114.96.2

```
PS C:\Users\user> nslookup socratesdergi.com
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    socratesdergi.com
Addresses:  2a06:98c1:3121::2
          2a06:98c1:3120::2
          188.114.97.2
          188.114.96.2
```

3.1.2 2. Soru

Cevap: emily.ns.cloudflare.com ve dion.ns.cloudflare.com

```
PS C:\Users\user> nslookup
Default Server:  UnKnown
Address:  172.20.10.1

> set type=ns
> socratesdergi.com
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
socratesdergi.com       nameserver = emily.ns.cloudflare.com
socratesdergi.com       nameserver = dion.ns.cloudflare.com
```

3.1.3 3. Soru

Cevap: 2. soruda bulduğum DNS sunucularından birini gmail.com ile sorguladım ve mail sunucuları elde ettim. Ardından bu mail sunucularından birisinin IP adresini sorguladım ve 66.102.1.26 çıktısını aldım.

```
PS C:\Users\user> nslookup
Default Server:  UnKnown
Address:  172.20.10.1

> dion.ns.cloudflare.com
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    dion.ns.cloudflare.com
Addresses:  2a06:98c1:50::ac40:219c
          2803:f800:50::6ca2:c19c
          2606:4700:58::adf5:3b9c
          108.162.193.156
          172.64.33.156
          173.245.59.156

> set type=mx
> gmail.com
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
>
```

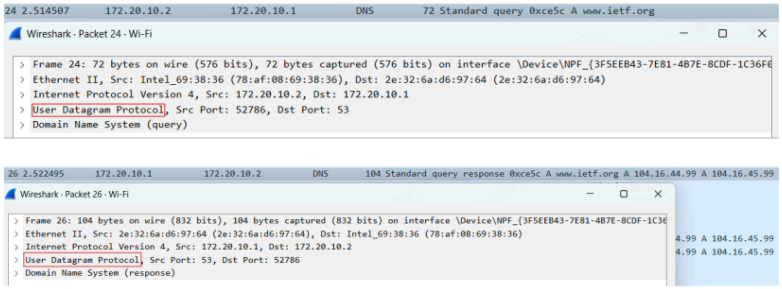
```
> set type=a
> gmail-smtp-in.l.google.com
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    gmail-smtp-in.l.google.com
Address:  66.102.1.26
```

3.2 İpconfig

3.3 Tracing DNS with Wireshark

3.3.1 4. Soru

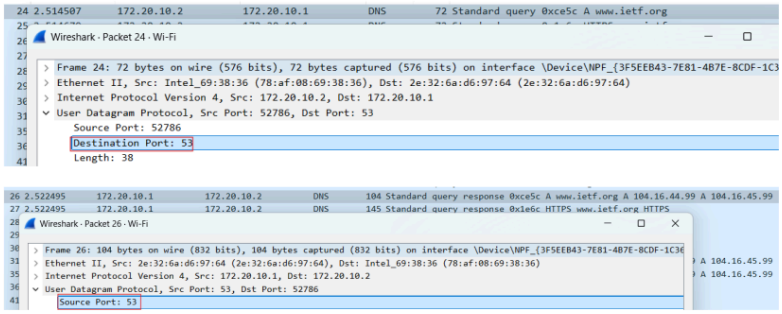
Cevap: Query ve Response Message incelendiğinde, bunların UDP ile gönderildiği gözükmektedir. Ekran görüntülerine örnek olması açısından iki adet paket koydum ancak diğer paketlerde de UDP bilgisi görülmektedir.



3.3.2 5. Soru

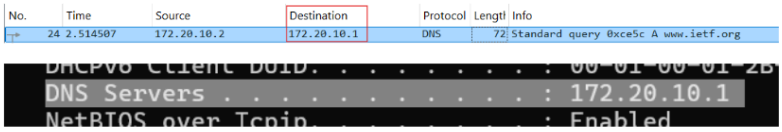
Cevap: Query mesajını ve response mesajını detaylı incelersek Destination Port ve source port numaralarının 53 olduğu gözükmektedir.

Response mesajını



3.3.3 6. Soru

Cevap: Query mesajının destination IP adresine baktığımızda bunun 172.20.10.1 olduğu görülmektedir. Terminalden DNS sunucumun adresine baktığımızda ise bununda Query mesajının destination IP adresi ile aynı olduğu görülmektedir.



3.3.4 7. Soru

Cevap: Query mesajına baktığımızda bunun A tipinde olduğu gözükmektedir. Bu bir istek olduğundan herhangi bir cevap döndürülmemiştir.

```
Domain Name System (query)
    Transaction ID: 0xce5c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > www.ietf.org: type A, class IN
```

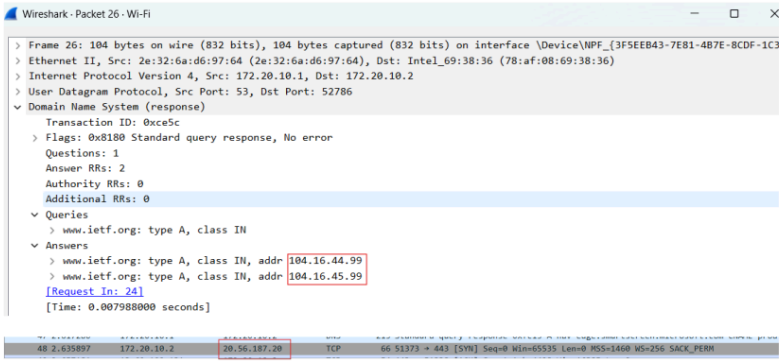
3.3.5 8. Soru

Cevap: Query response mesajı çin 2 adet cevap gözükmektedir. Bunların içeriği aşağıdaki ekran görüntüsünden gözlemlenebilir.

```
Answers
  www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 231 (3 minutes, 51 seconds)
      Data length: 4
      Address: 104.16.44.99
  www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 231 (3 minutes, 51 seconds)
      Data length: 4
      Address: 104.16.45.99
```

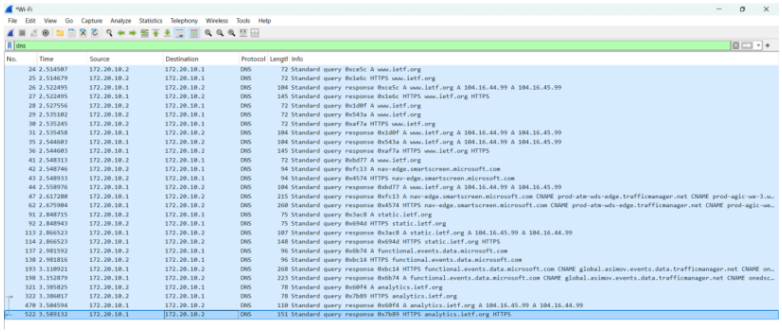
3.3.6 9. Soru

Cevap:Query response mesajından dönen cevaplardaki IP adresleri ile SYN paketinin destination IP adresi aynı değildir.



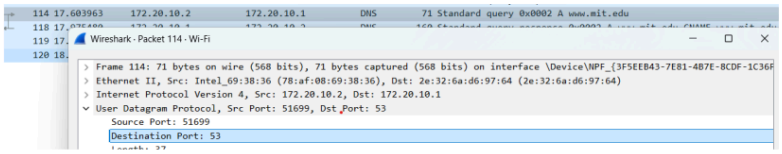
3.3.7 10. Soru

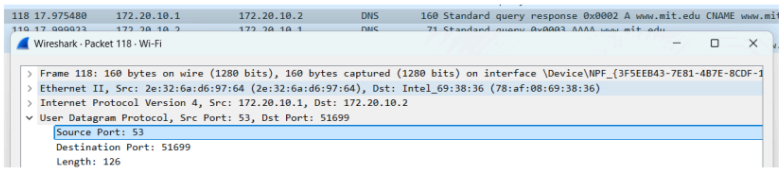
Cevap: Böyle bir paket gözlemlenmemiştir.



3.3.8 11. Soru

Cevap: Query mesajının destination port'u 53; Query response mesajının source port'u 53'dür.



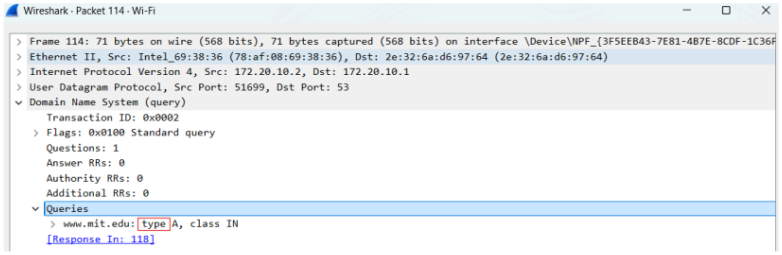


3.3.9 12. Soru

Cevap: Evet IP adresi benim DNS sunucumun IP'si ile aynı.

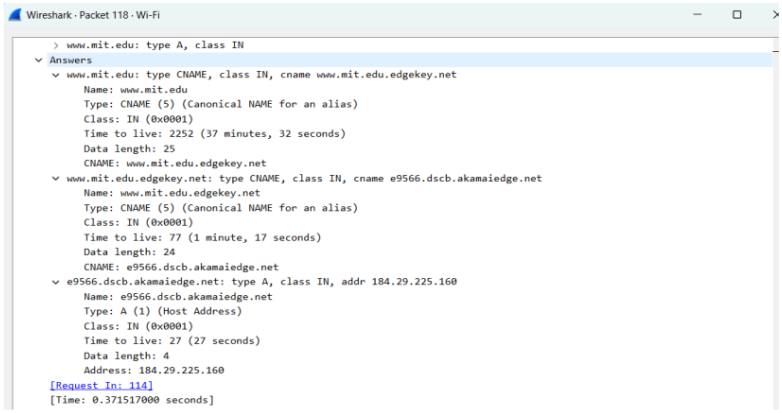
3.3.10 13. Soru

Cevap: A tipidir. Bu bir istek olduğundan herhangi bir mesaj içermemektedir.



3.3.11 14. Soru

Cevap: 3 adet cevap görülmektedir. Cevapların içeriği aşağıdaki ekran görüntüsünde görülebilir.

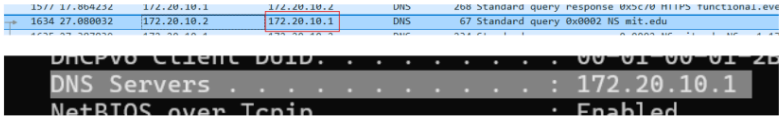


3.3.12 15. Soru

Cevap: Gerekli ekran görüntüleri her bir sorunun altında verilmiştir.

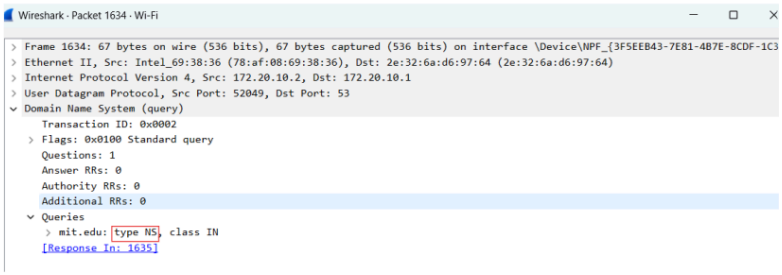
3.3.13 16. Soru

Cevap: Ekran görüntülerinden de görüldüğü üzere IP adresleri aynıdır.



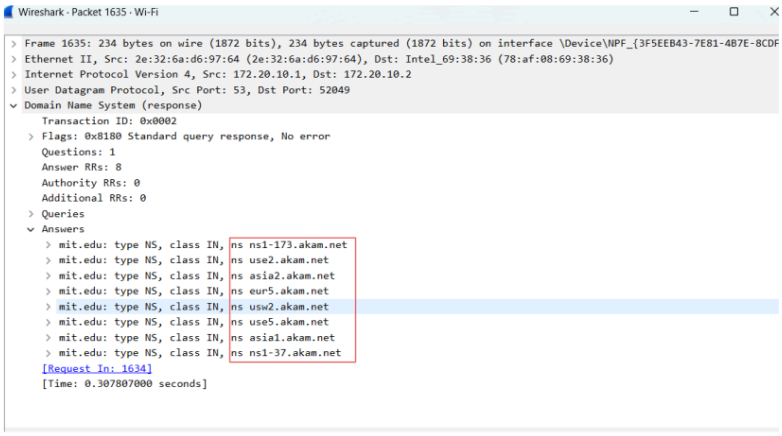
3.3.14 17. Soru

Cevap: Sorgu mesajının tipi NS'dir. Herhangi bir cevap görüntülenememektedir.



3.3.15 18. Soru

Cevap: Ekran görüntülerinde görünen isim sunucularını döndürmüştür. Ancak IP adresleri gözükmemektedir.

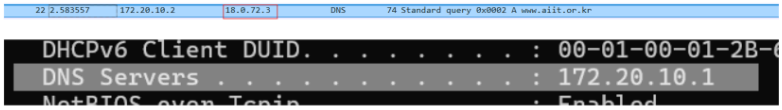


3.3.16 19. Soru

Cevap: Gerekli ekran görüntüleri her bir sorunun altında verilmiştir.

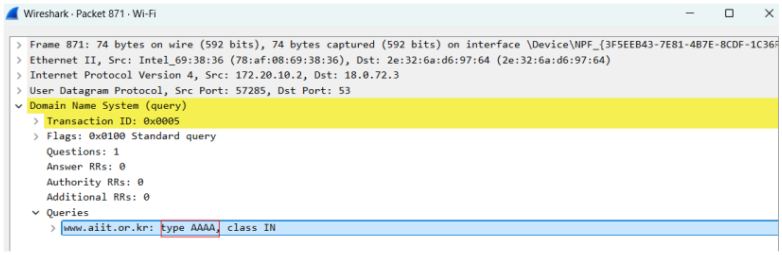
3.3.17 20. Soru

Cevap: Hayır benim DNS suncuum ile aynı IP adresine sahip değil. Bu IP adresi "bitsy.mit.edu" ya karşılık gelmektedir. Çünkü DNS sunucusu olarka bunu belirledik.



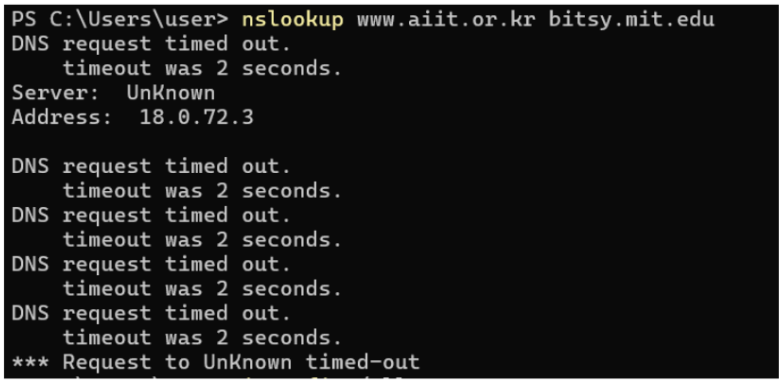
3.3.18 21. Soru

Cevap: Sorgu tipi AAAA olark gözükmektedir ve herhangi bri cevap içermemektedir.



3.3.19 22. Soru

Cevap: Ben herhangi bri cevap paketi yakalayamadım. Çünkü aşağıdaki ekran görüntüsünden de görüleceği üzere zaman aşımına uğradığından herhangi bir cevap döndürememiştir.



3.3.20 23. Soru

Cevap: Gerekli ekran görüntüleri her bir sorunun altında verilmiştir.

4 Kaynakça

152120211104_Doğukan_Kıyıklık.docx

ORİJİNALLİK RAPORU

%32 EN	%8	%4	%30
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	Submitted to University of Liverpool Öğrenci Ödevi	%13
2	Submitted to University of Sydney Öğrenci Ödevi	%6
3	Submitted to Eskisehir Osmangazi University Öğrenci Ödevi	%4
4	Submitted to Montana State University, Bozeman Öğrenci Ödevi	%3
5	www.coursehero.com İnternet Kaynağı	%3
6	Submitted to Anglia Ruskin University Öğrenci Ödevi	%2
7	eduscol.education.fr İnternet Kaynağı	%1

Alıntıları çıkart	Kapat	Exclude assignment template	üzerinde
Bibliyografyayı Çıkart	Kapat	Eşleşmeleri çıkar	Kapat