Laboratuvar Raporu 2

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Ferdi İslam Yılmaz

152120191055

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İçindekiler

2 Giriş

Bugünkü labaratuvar 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 adresleriini 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
```

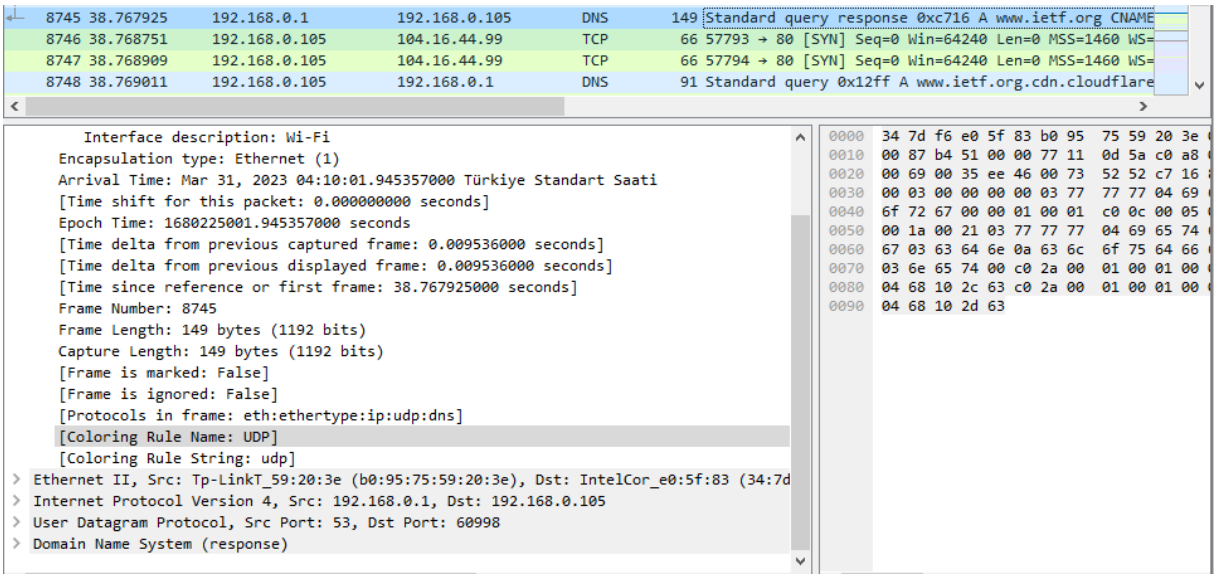
3.İkinci soruda elde ettiğimiz DNS sunucularından birini Yahoo! İçin sorguladığımızda 87.248.119.251 IP adresini elde ediyoruz.

```
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

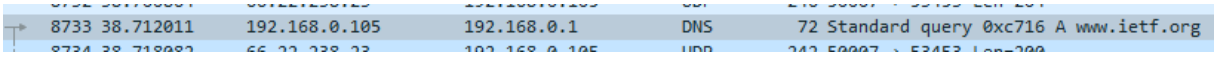
4. Alınan cevaba göre sorgumuz UDP üzerinden yapılmıştır.



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.



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.

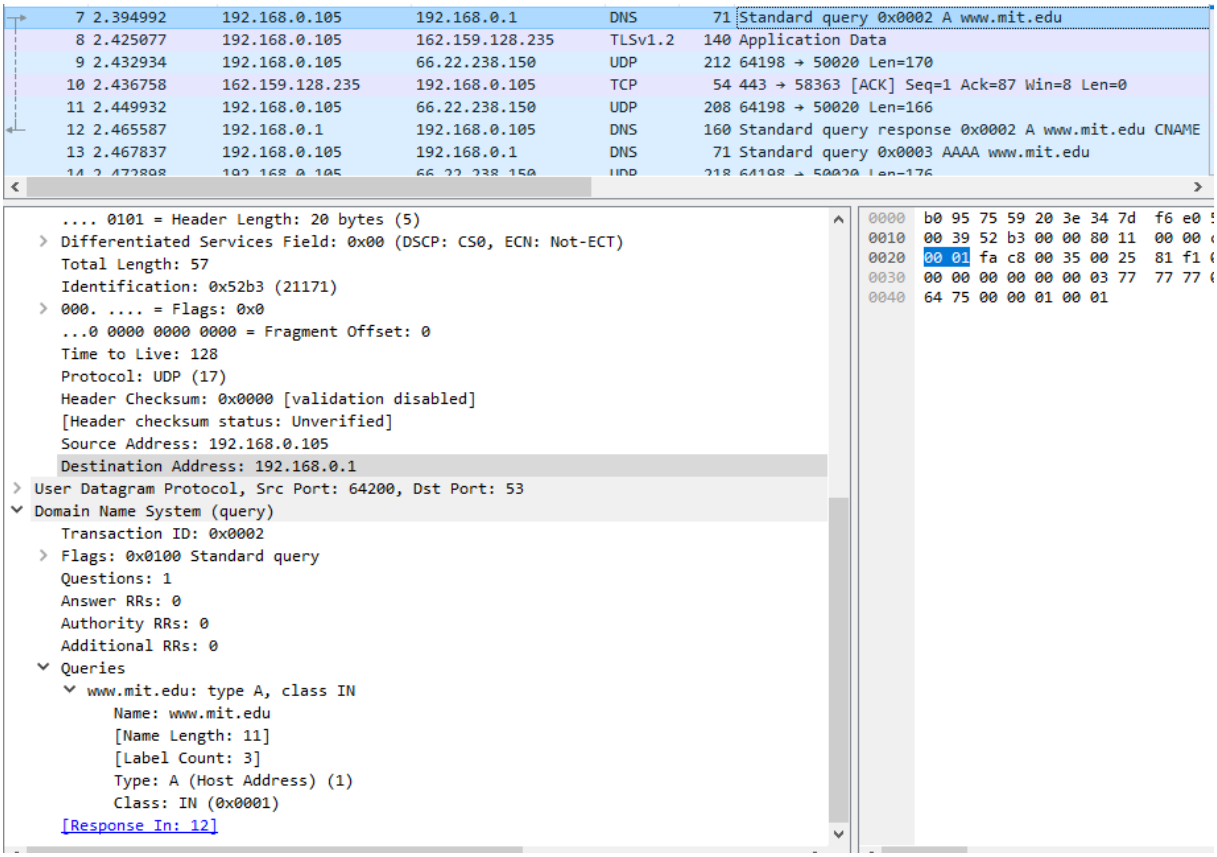
```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 26 (26 seconds)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: 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.



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
```

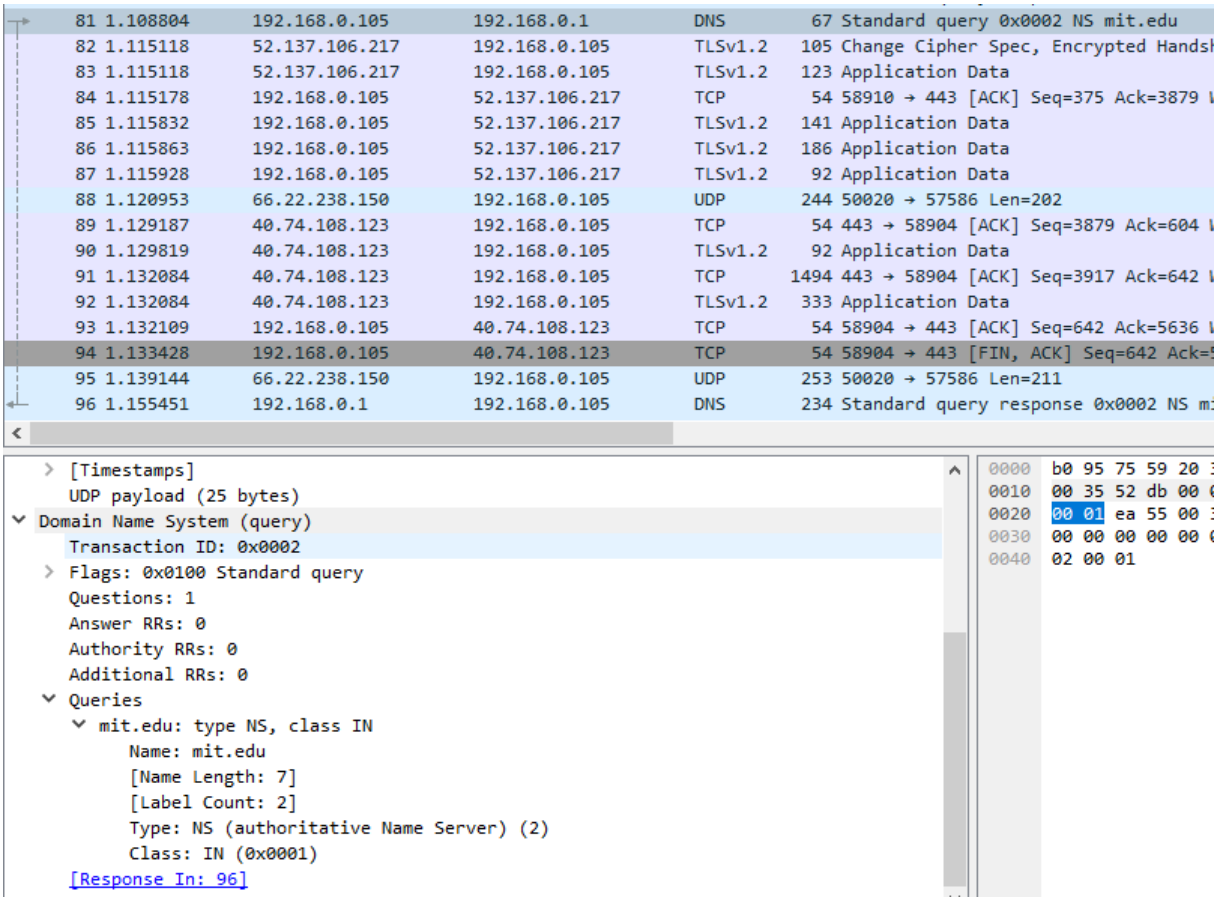
13. Sorgumuz a tipi bir sorgudur. DNS sorgumuzda herhangi bir cevap da bulunmamaktadır.

```
▾ 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.

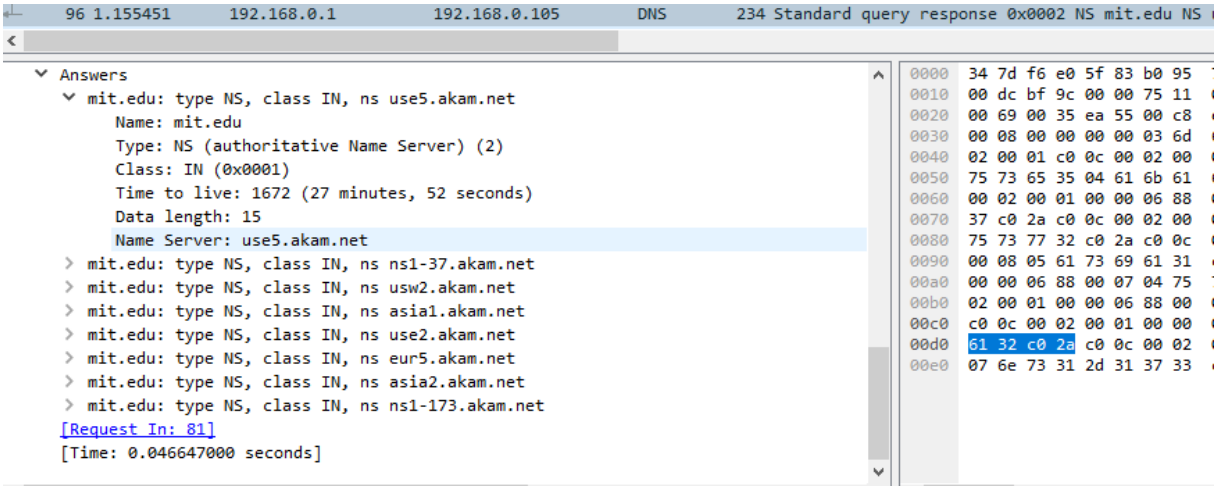
```
▾ Answers
  ▸ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  ▸ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  ▾ e9566.dscb.akamaiedge.net: type A, class IN, addr 92.122.34.235
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (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 serberımız ile aynıdır.

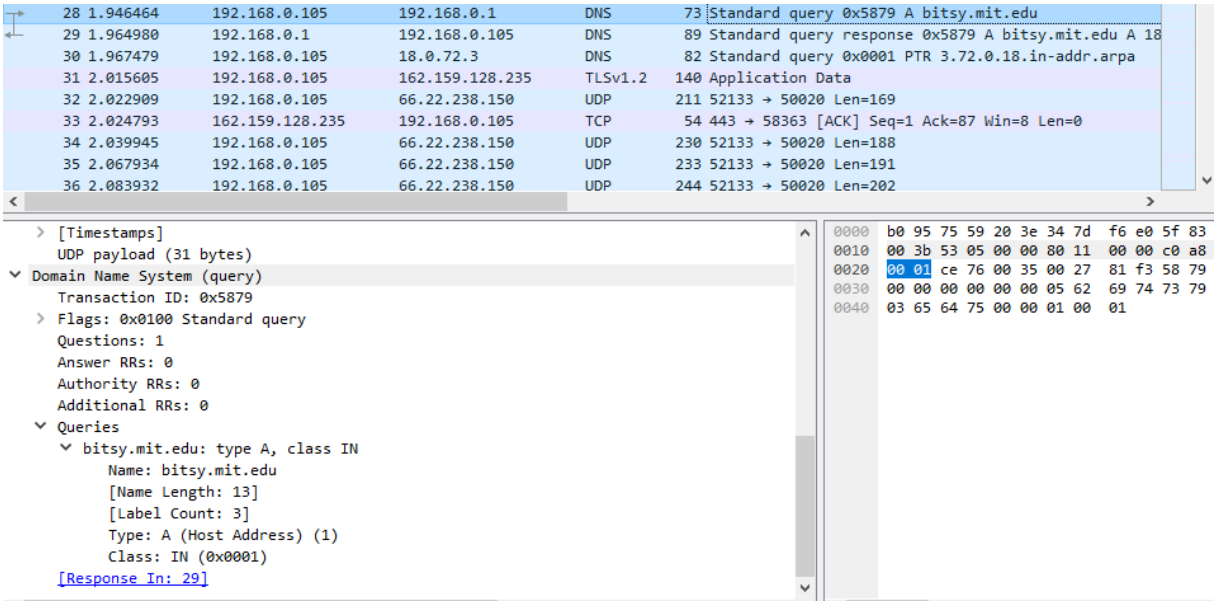


17. DNS sorgu mesajımızı incelediğimizde “ns” türünde bir sorgu kullanıldığını görüyoruz. Üstteki ekran görüntüsünde de görüldüğü üzere bu sorgu hiç cevap içermiyor.

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

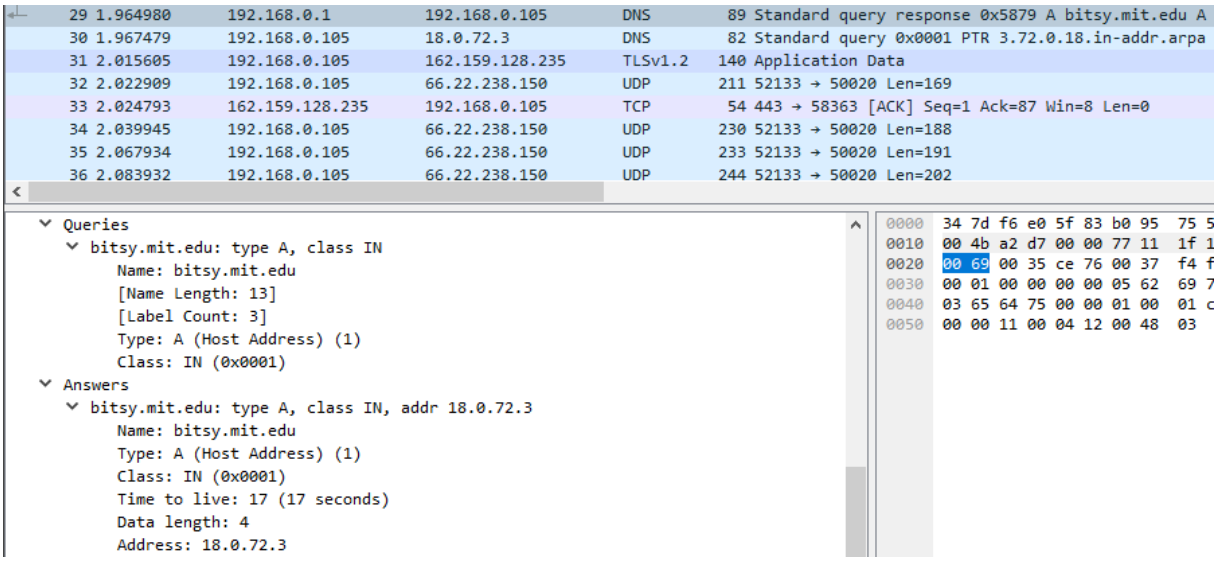


20. DNS sorgu mesajımız 192.168.0.1 numaralı IP adresine gönderildi. BU IP adresi bizim yerel DNS serverımızınki ile aynı.



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.



4 Kaynakça

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