

**Laboratuvar Raporu 2**

**Eskişehir Osmangazi Üniversitesi**

**Bilgisayar Ağları**

**152116028**

**Ferdi İslam Yılmaz**

**152120191055**

**Dr. Öğr. Üyesi İlker Özçelik**

**2022-2023**

**İçindekiler**

[2 Giriş 3](#_Toc131137762)

[3 Laboratuvar Uygulaması 3](#_Toc131137763)

[3.1 nsconfig Komutu 3](#_Toc131137764)

[3.2 Tracing DNS with Wireshark 4](#_Toc131137765)

[4 Kaynakça 10](#_Toc131137766)

# 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.

# Laboratuvar Uygulaması

## nsconfig Komutu

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

metin içeren bir resim

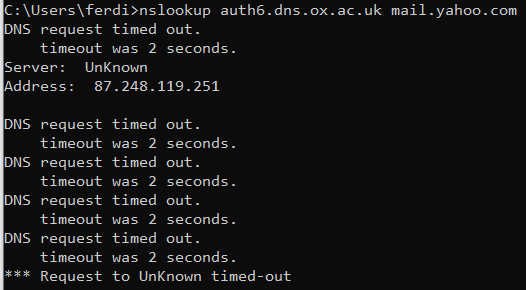
Açıklama otomatik olarak oluşturuldu

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.

metin içeren bir resim

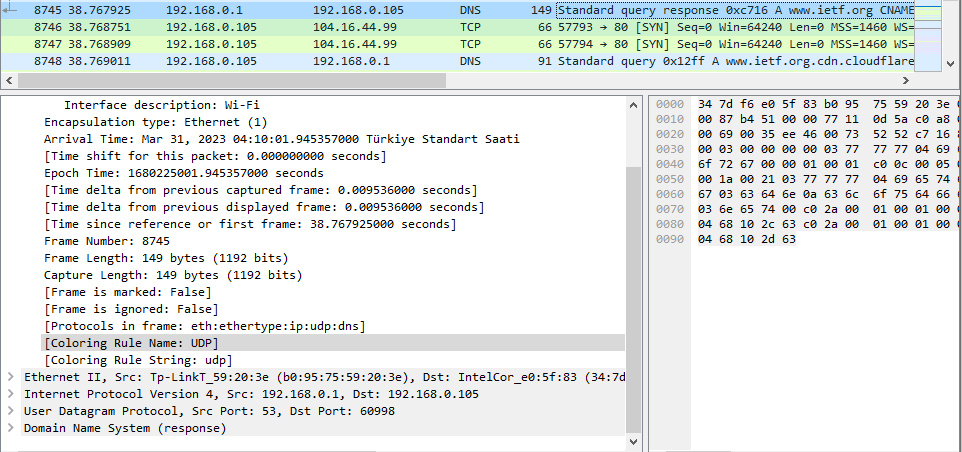
Açıklama otomatik olarak oluşturuldu

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



## 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.

metin içeren bir resim

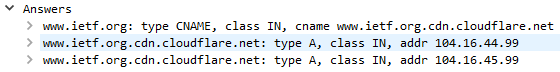
Açıklama otomatik olarak oluşturuldu

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

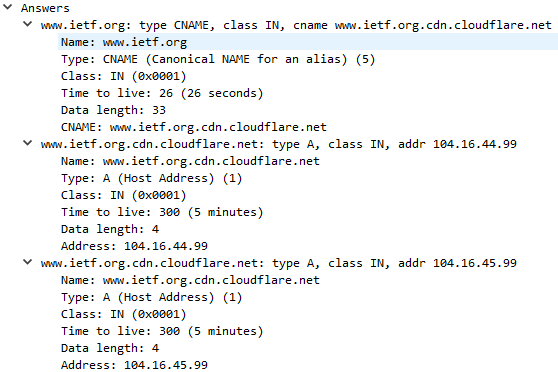


7. Kullandığımız DNS sorgusu type A. Sorgu mesajımızın içerdiği “cevaplar” ise alttaki ekran görüntüsündedir.

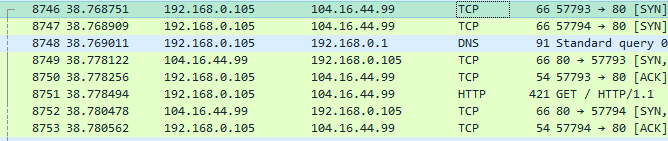




8. DNS yanıtını incelediğimizde bize 4 adet cevap sağlandığını görüyoruz. Cevaplar; Name, Type,Class,Time to Live Data length ve CNAME bilgilerini içeriyor.

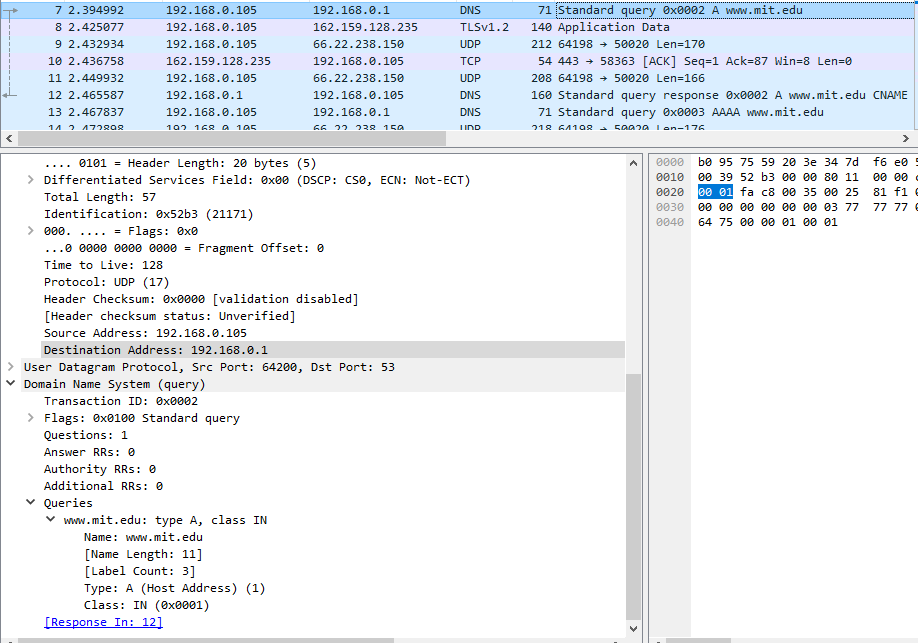


9. Bizim gönderdiğimiz TCP SYN paketimizi incelediğimizde varış adresini önceki DNS yanıt mesajının doğruladığını görüyoruz.

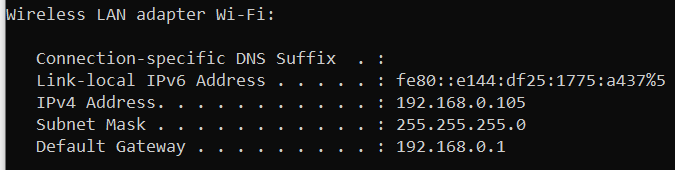


10. Evet sitede resimler var. Ama benim sunucum resimler için herhangi bir DNS sorgusu oluşturmamış.

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.



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

metin içeren bir resim

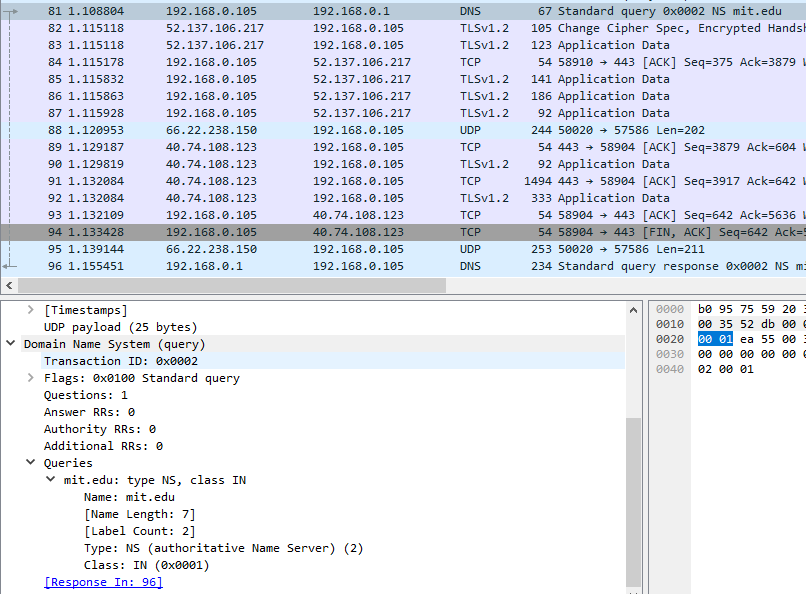
Açıklama otomatik olarak oluşturuldu

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

metin, mektup, harf içeren bir resim

Açıklama otomatik olarak oluşturuldu

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



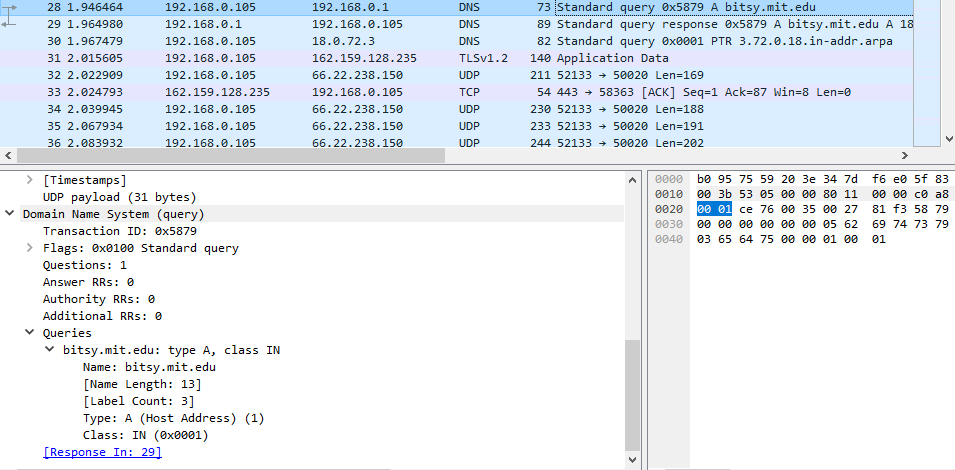
17. DNS sorgu mesajımızı incelediğimizde “ns” türünde bir sorgu kullanıldığını görüyoruz. Üstteki ekran görüntüsünde de görüldüğü üzere bu sorgu hiç cevap içermiyor.

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

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

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.

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

# Kaynakça

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