

```
Administrator: Komut İstemi
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Windows\System32>nslookup iitb.ac.in
Server: Tenda.Home
Address: 192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name: iitb.ac.in
Address: 103.21.124.133

C:\Windows\System32>nslookup -type=ns iitb.ac.in
Server: Tenda.Home
Address: 192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
iitb.ac.in nameserver = dns1.iitb.ac.in
iitb.ac.in nameserver = dns3.iitb.ac.in
iitb.ac.in nameserver = dns2.iitb.ac.in

dns1.iitb.ac.in internet address = 103.21.125.129
dns2.iitb.ac.in internet address = 103.21.126.129
dns3.iitb.ac.in internet address = 103.21.127.129

C:\Windows\System32>
```

1.a. iitb.ac.in IP adresi

nslookup iitb.ac.in komutu ile yapılan sorgu sonucunda sunucunun IP adresi:

- 103.21.124.133

1.b. Güvenilir (authoritative) DNS sunucuları

nslookup -type=ns iitb.ac.in komutu sonucunda 3 farklı güvenilir DNS sunucusu tespit edilmiştir:

DNS Sunucusu	IP Adresi
dns1.iitb.ac.in	103.21.125.129
dns2.iitb.ac.in	103.21.126.129
dns3.iitb.ac.in	103.21.127.129

No.	Time	Source	Destination	Protocol	Length	Info
39	0.126977	172.18.19.42	172.31.254.254	DNS	84	Standard query 0xf55a A ecn.dev.virtualearth.net
40	0.127353	172.18.19.42	172.31.254.254	DNS	84	Standard query 0xf055 HTTPS ecn.dev.virtualearth.net
79	0.188028	172.31.254.254	172.18.19.42	DNS	234	Standard query response 0xf055 HTTPS ecn.dev.virtualearth.net CNAME ssl2.tiles.virtualearth.net.edgekey.net CNAME e4113.dscd.akamai-
87	0.207472	172.31.254.254	172.18.19.42	DNS	186	Standard query response 0xf55a A ecn.dev.virtualearth.net CNAME ssl2.tiles.virtualearth.net.edgekey.net CNAME e4113.dscd.akamai-
112	5.402452	172.18.19.42	172.31.254.254	DNS	72	Standard query 0x11f1 A www.ietf.org
813	5.418736	172.18.19.42	172.31.254.254	DNS	72	Standard query 0x11f1 A www.ietf.org
814	5.418784	172.18.19.42	172.31.254.254	DNS	72	Standard query 0x2b51 HTTPS www.ietf.org
831	5.441737	172.18.19.42	172.31.254.254	DNS	72	Standard query 0x8e7b A www.ietf.org
832	5.442075	172.18.19.42	172.31.254.254	DNS	72	Standard query 0x8a2a HTTPS www.ietf.org
858	5.590072	172.31.254.254	172.18.19.42	DNS	104	Standard query response 0x11f1 A www.ietf.org A 104.16.45.99 A 104.16.44.99
859	5.590072	172.31.254.254	172.18.19.42	DNS	104	Standard query response 0x8e7b A www.ietf.org A 104.16.45.99 A 104.16.44.99
860	5.590072	172.31.254.254	172.18.19.42	DNS	145	Standard query response 0x2b51 HTTPS www.ietf.org
873	5.592063	172.18.19.42	172.31.254.254	DNS	72	Standard query 0xf934 A www.ietf.org
874	5.592722	172.18.19.42	172.31.254.254	DNS	94	Standard query 0x4228 A nav-edge.smartscreen.microsoft.com
875	5.592954	172.18.19.42	172.31.254.254	DNS	94	Standard query 0xb0ae HTTPS nav-edge.smartscreen.microsoft.com
884	5.606284	172.18.19.42	172.31.254.254	DNS	78	Standard query 0xc908 A edge.microsoft.com
885	5.606519	172.18.19.42	172.31.254.254	DNS	78	Standard query 0xa6ba HTTPS edge.microsoft.com
920	5.622119	172.31.254.254	172.18.19.42	DNS	104	Standard query response 0x8e7b A www.ietf.org A 104.16.45.99 A 104.16.44.99
921	5.622119	172.31.254.254	172.18.19.42	DNS	145	Standard query response 0x8a2a HTTPS www.ietf.org
922	5.622119	172.31.254.254	172.18.19.42	DNS	104	Standard query response 0xf934 A www.ietf.org A 104.16.45.99 A 104.16.44.99

2 -> Display filter ile bilgisayarımın IP bilgisini içeren paketler.

Wireshark - Paket 39 · d1.pcapng

Frame 39: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{D2...}

Ethernet II, Src: 20:ac:84:a1:5c:c3 (20:ac:84:a1:5c:c3), Dst: JuniperNetwo_4c:85:00 (14:b3:a1:4c:85:00)

Internet Protocol Version 4, Src: 172.18.19.42, Dst: 172.31.254.254

User Datagram Protocol, Src Port: 56772, Dst Port: 53

Source Port: 56772

Destination Port: 53

Length: 50

Checksum: 0x8320 [unverified]

[Checksum Status: Unverified]

[Stream index: 6]

[Stream Packet Number: 1]

[Timestamps]

UDP payload (42 bytes)

Domain Name System (query)

0000 14 b3 a1 4c 85 00 20 ac 84 a1 5c c3 08 00 45 00 ...L... ..E..

0010 00 46 d8 d3 00 00 80 11 f7 78 ac 12 13 2a ac 1f ..F.....x...*

0020 fe fe dd c4 00 35 00 32 83 20 f5 5a 01 00 00 015.2...Z....

0030 00 00 00 00 00 00 03 65 63 6e 03 64 65 76 0c 76e.cn.dev.v

0040 69 72 74 75 61 6c 65 61 72 74 68 03 6e 65 74 00 irtualea rth net.

0050 00 01 00 01

No.: 39 · Time: 0.126977 · Source: 172.18.19.42 · Destination: 172.31.254.254 · Protocol: DNS · Length: 84 · Info: Standard query 0xf55a A ecn.dev.virtualearth.net

☒ Paket baytlarını göster Layout: Vertical (Stacked)

Kapat Yardım

2.a — DNS Mesajı Hangi Protokolle Gönderildi?

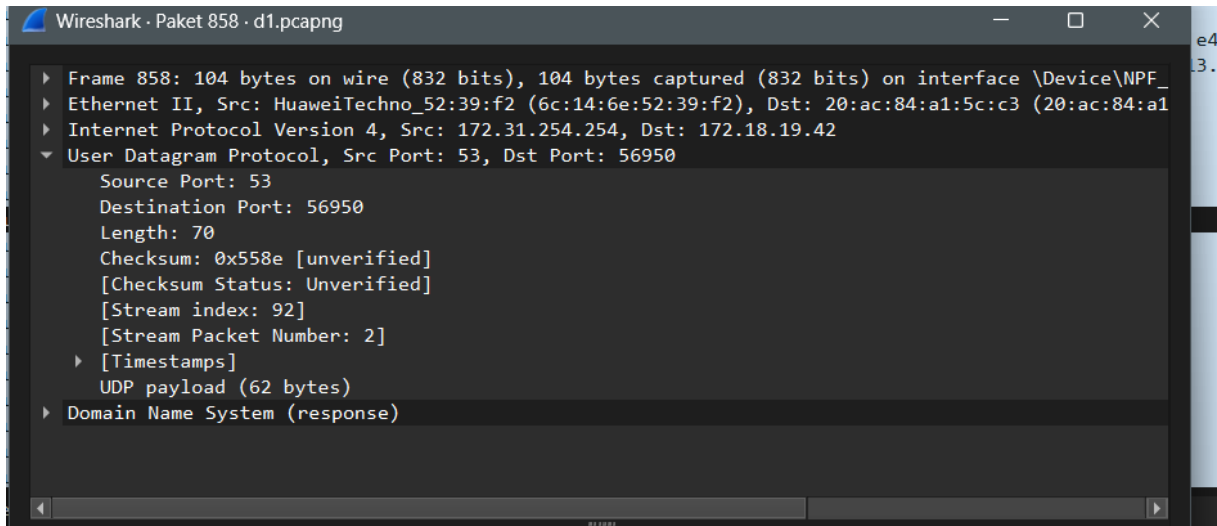
UDP (User Datagram Protocol)

2.b — DNS Sorgu Mesajının Port Numarası

- Source Port: 56772**
(Bu, bilgisayarının rastgele oluşturduğu bağlantı portu)
- Destination Port: 53**
(Bu da DNS sunucusunun standart portu)

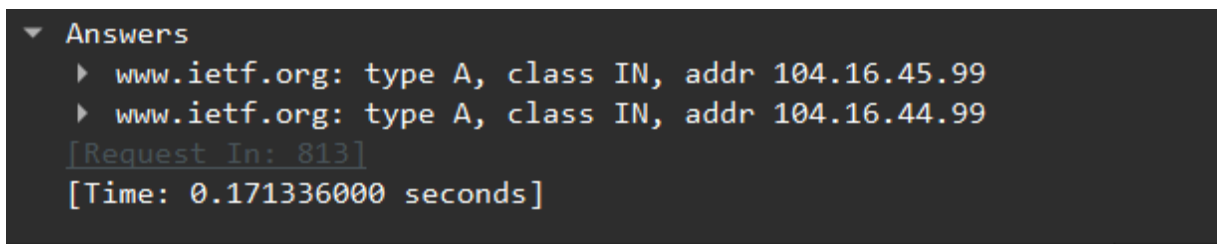
Yani DNS sorgu mesajı portları:

Kaynak portu: 56772, Hedef portu: 53



2.c – DNS CEVAP PORTLARI

- **Source Port: 53 → Bu DNS sunucusu**
- **Destination Port: 56950 → Bu benim bilgisayarım**



2.d. DNS Sorgusu Cevap İçeriyor mu?

Evet. Aşağıdaki IP adresleri dönmüştür:

- **104.16.45.99**
 - **104.16.44.99**
-

2.e. Kaç tane cevap (answer) var? Bu cevapların her birinin içeriği nedir?

```
Answers:  
▼ 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: 260 (4 minutes, 20 seconds)  
  Data length: 4  
  Address: 104.16.45.99  
▼ 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: 260 (4 minutes, 20 seconds)  
  Data length: 4  
  Address: 104.16.44.99  
[Request: Tcp: 812]
```

Toplam 2 adet cevap bulunmaktadır. İçerikleri ekran görüntüsünde verilmiştir.