

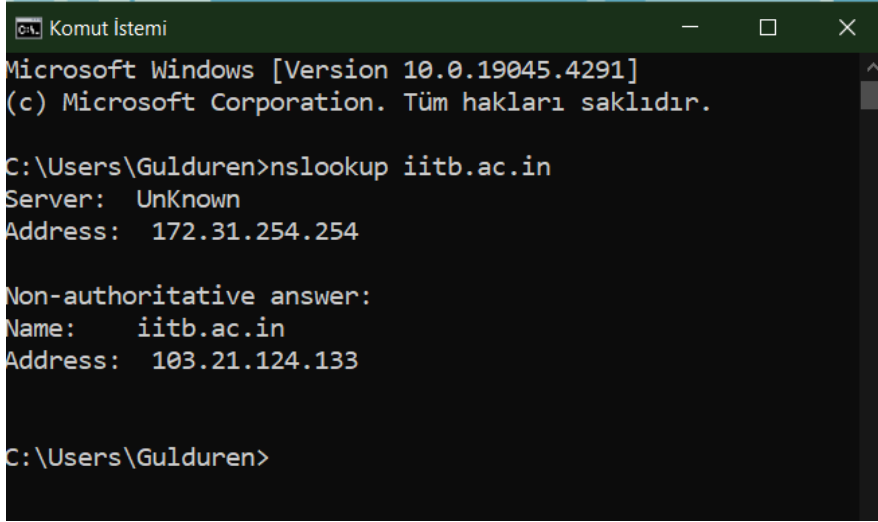
BİLGİSAYAR AĞLARI – TAKE HOME EXAM-III
DNS

DERYA NAİLİYE KIMIRTI - 21100011001

Yapılması gerekenler:

1. nslookup

- a. nslookup komutunu kullanarak iitb.ac.in sunucusuna ait IP adresini bulunuz. Ekran görüntüsü ile gösteriniz.**



```
Komut İstemi
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. Tüm hakları saklıdır.

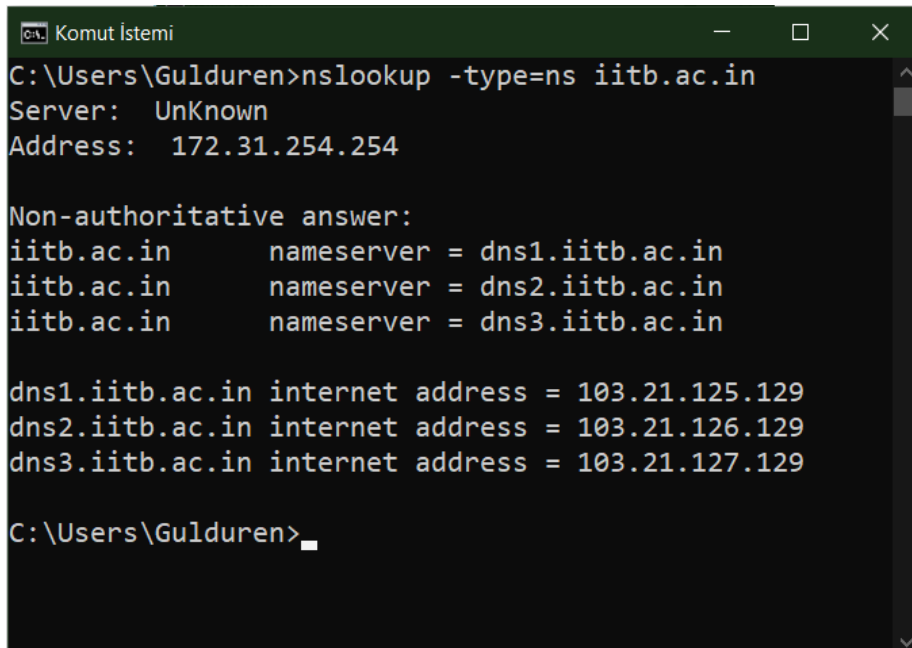
C:\Users\Gulduren>nslookup iitb.ac.in
Server: UnKnown
Address: 172.31.254.254

Non-authoritative answer:
Name: iitb.ac.in
Address: 103.21.124.133

C:\Users\Gulduren>
```

- b. iitb.ac.in sunucusuna ait güvenilir (authorative) DNS sunucularını elde etmek için nslookup sorgusunu gerekli parametreler ile yeniden çalıştırınız. Kaç farklı güvenilir DNS sunucusundan bilgi aldınız? Bu sunucuların IP adresleri nelerdir? Ekran görüntüsü ile gösteriniz.**

Çıktıya göre, iitb.ac.in alan adına ait 3 adet isim sunucusu (nameserver) var: dns1.iitb.ac.in, dns2.iitb.ac.in ve dns3.iitb.ac.in. Bu isim sunucularının IP adresleri de verilmiştir.



```
Komut İstemi
C:\Users\Gulduren>nslookup -type=ns iitb.ac.in
Server: UnKnown
Address: 172.31.254.254

Non-authoritative answer:
iitb.ac.in nameserver = dns1.iitb.ac.in
iitb.ac.in nameserver = dns2.iitb.ac.in
iitb.ac.in nameserver = dns3.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:\Users\Gulduren>
```

2. Wireshark

- a. İstedığınız bir yöntemle bilgisayarınıza ait IP adresini bulunuz.
IPv4 Address başlığı altında bilgisayarımızın IP adresini bulabiliriz.

```
Seç Komut İstemi

C:\Users\Gulduren>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

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  . : erbakan.local
    Link-local IPv6 Address . . . . . : fe80::9489:2ab1:6df1:d777%18
    IPv4 Address. . . . . : 172.18.24.220
    Subnet Mask . . . . . : 255.255.128.0
    Default Gateway . . . . . : 172.18.0.1
```

- b. Bilgisayarımızdaki DNS önbellegini temizleyiniz.

```
Komut İstemi

C:\Users\Gulduren>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Gulduren>
```

- c. İsteddiğiniz bir internet tarayıcısını açarak önbellegini temizleyiniz.
d. Wireshark programını yönetici olarak çalıştırınız. Paket yakalama işlemini başlatınız.
e. İnternet tarayıcısında www.ietf.org adresini ziyaret ediniz. Paket yakalama işlemini durdurarak yakalanmış paketlerin bulunduğu dosyayı kaydediniz.
(Format: OgrNo_Odev3.pcapng) ①

- f. **Görüntüleme filtresi (display filter) ile bilgisayarınızın IP bilgisini içeren paketleri görüntüleyiniz.**

Filtreleme kısmına “ip.addr == [bilgisayarınızın IP adresi]” yazarak istenilen sonuçlara ulaştım.

21100011001_Odev3.pcapng						
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım						
ip.addr == 172.18.24.220						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.192115	172.18.24.220	172.31.254.254	DNS	79	Standard query 0x68bf A play.googleapis.com
3	0.196150	172.31.254.254	172.18.24.220	DNS	335	Standard query response 0x68bf A play.googleapis.com A 1
4	0.196591	172.18.24.220	142.251.141.42	TCP	66	52047 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
5	0.222343	142.251.141.42	172.18.24.220	TCP	66	443 → 52047 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
6	0.222444	172.18.24.220	142.251.141.42	TCP	54	52047 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
7	0.226822	172.18.24.220	142.251.141.42	TLSv1.2	244	Client Hello (SNI=play.googleapis.com)
8	0.246393	142.251.141.42	172.18.24.220	TCP	56	443 → 52047 [ACK] Seq=1 Ack=191 Win=1148160 Len=0
9	0.289425	142.251.141.42	172.18.24.220	TLSv1.2	1434	Server Hello
10	0.289425	142.251.141.42	172.18.24.220	TCP	1434	443 → 52047 [PSH, ACK] Seq=1381 Ack=191 Win=66816 Len=1
11	0.289425	142.251.141.42	172.18.24.220	TCP	1434	443 → 52047 [ACK] Seq=2761 Ack=191 Win=66816 Len=1380 [1
12	0.289425	142.251.141.42	172.18.24.220	TLSv1.2	505	Certificate, Server Key Exchange, Server Hello Done
13	0.289519	172.18.24.220	142.251.141.42	TCP	54	52047 → 443 [ACK] Seq=191 Ack=4592 Win=66048 Len=0
14	0.293879	172.18.24.220	142.251.141.42	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Hand
15	0.322276	142.251.141.42	172.18.24.220	TLSv1.2	349	New Session Ticket, Change Cipher Spec, Encrypted Hand
16	0.335497	172.18.24.220	142.251.141.42	TLSv1.2	587	Application Data
17	0.335652	172.18.24.220	142.251.141.42	TLSv1.2	1698	Application Data
18	0.364412	142.251.141.42	172.18.24.220	TCP	56	443 → 52047 [ACK] Seq=4887 Ack=2197 Win=70656 Len=0
19	0.367673	142.251.141.42	172.18.24.220	TCP	56	443 → 52047 [ACK] Seq=4887 Ack=2461 Win=73472 Len=0
20	0.417726	142.251.141.42	172.18.24.220	TLSv1.2	723	Application Data
21	0.417885	142.251.141.42	172.18.24.220	TLSv1.2	88	Application Data
22	0.417931	172.18.24.220	142.251.141.42	TCP	54	52047 → 443 [ACK] Seq=2461 Ack=5590 Win=65024 Len=0
23	0.765112	172.18.24.220	108.177.127.188	TCP	55	51957 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
26	0.825307	108.177.127.188	172.18.24.220	TCP	66	5228 → 51957 [ACK] Seq=1 Ack=2 Win=289 Len=0 SLE=1 SRE=2
29	1.851135	172.18.24.220	172.18.159.180	TCP	66	52045 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
34	3.842175	172.18.24.220	173.194.76.100	TCP	55	52041 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment
35	3.905825	173.194.76.100	172.18.24.220	TCP	66	443 → 52041 [ACK] Seq=1 Ack=2 Win=300 Len=0 SLE=1 SRE=2
36	3.971500	172.18.24.220	142.250.187.142	TCP	55	52042 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment
37	3.997730	142.250.187.142	172.18.24.220	TCP	66	443 → 52042 [ACK] Seq=1 Ack=2 Win=300 Len=0 SLE=1 SRE=2
38	4.269411	172.18.24.220	108.177.15.84	TCP	55	52040 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment
39	4.330585	108.177.15.84	172.18.24.220	TCP	66	443 → 52040 [ACK] Seq=1 Ack=2 Win=311 Len=0 SLE=1 SRE=2
41	4.842389	172.18.24.220	172.31.254.254	DNS	74	Standard query 0x2dc7 A www.google.com
42	4.842585	172.18.24.220	172.31.254.254	DNS	74	Standard query 0x99bd HTTPS www.google.com
43	4.851945	172.31.254.254	172.18.24.220	DNS	90	Standard query response 0x2dc7 A www.google.com A 172.21
44	4.851945	172.31.254.254	172.18.24.220	DNS	99	Standard query response 0x99bd HTTPS www.google.com HTTP
45	4.853720	172.18.24.220	172.217.169.164	QUIC	1292	Initial, DCID=acd317b19a3ac965, PKN: 1, CRYPTO

SORULAR

1. **DNS sorgu (query) ve cevap (response) mesajlarını bulunuz. Bu mesajlar TCP veya UDP protokollerinden hangisi ile gönderilmiştir?**

Yakaladığım paketlerden sonra filtrelemeye dns yazarak dns sorgu ve cevap mesajlarını buldum.

İncelediğimde “Internet Protocol Version 4” başlığı altında “Protocol” başlığında mesajın gönderilirken “UDP” ile gönderildiği bilgisine ulaştım.

21100011001_Odev3.pcapng

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

dns

No.	Time	Info
2	0.192115	79 Standard query 0x68bf A play.googleapis.com
3	0.196150	335 Standard query response 0x68bf A play.google
41	4.842389	74 Standard query 0x2dc7 A www.google.com
42	4.842585	74 Standard query 0x99bd HTTPS www.google.com
43	4.851945	90 Standard query response 0x2dc7 A www.google
44	4.851945	99 Standard query response 0x99bd HTTPS www.goc
52	4.906686	85 Standard query 0xf6d5 A lh4.googleusercontent
53	4.906938	85 Standard query 0x9b9c HTTPS lh4.googleusercon
55	4.926058	130 Standard query response 0xf6d5 A lh4.google
78	5.019322	171 Standard query response 0x9b9c HTTPS lh4.goc
257	5.203590	85 Standard query 0x1ec8 A lh3.googleusercontent
258	5.203869	85 Standard query 0x81c1 HTTPS lh3.googleusercon
263	5.208199	130 Standard query response 0x1ec8 A lh3.google
264	5.208199	171 Standard query response 0x81c1 HTTPS lh3.goc
272	5.216039	75 Standard query 0x2ed6 A www.gstatic.com
273	5.216189	75 Standard query 0x81e6 HTTPS www.gstatic.com
281	5.218695	91 Standard query response 0x2ed6 A www.gstatic
282	5.218695	132 Standard query response 0x81e6 HTTPS www.gst
443	5.399893	75 Standard query 0xe06f A apis.google.com
444	5.400198	75 Standard query 0xbffb HTTPS apis.google.com
445	5.420382	112 Standard query response 0xe06f A apis.google
447	5.440141	96 Standard query response 0xbffb HTTPS apis.goc
495	6.406168	75 Standard query 0x25a5 A play.google.com
496	6.406625	75 Standard query 0xf6b29 HTTPS play.google.com
497	6.412232	91 Standard query response 0x25a5 A play.google
498	6.412232	125 Standard query response 0xf6b29 HTTPS play.g
554	7.149141	95 Standard query 0xefd8 A optimizationguide-pe
555	7.149359	95 Standard query 0xc5c5 HTTPS optimizationguic
556	7.151331	72 Standard query 0x586e A www.ietf.org
557	7.151625	72 Standard query 0x745d HTTPS www.ietf.org
558	7.151711	351 Standard query response 0xefd8 A optimizatio
559	7.151711	152 Standard query response 0xc5c5 HTTPS optimiz
561	7.154545	78 Standard query 0x9cfe A www.googleapis.com
562	7.154780	78 Standard query 0x093c HTTPS www.googleleap
563	7.157865	334 Standard query response 0x9cfe A www.google

Wireshark - Paket 556 - 21100011001_Odev3.pcapng

Frame 556: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface

Ethernet II, Src: Intel_13:37:56 (38:87:d5:13:37:56), Dst: JuniperNetwo_4c:8

Internet Protocol Version 4, Src: 172.18.24.220, Dst: 172.31.254.254

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 58

Identification: 0xd0d1 (53457)

000. ... = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 172.18.24.220

Destination Address: 172.31.254.254

User Datagram Protocol, Src Port: 49875, Dst Port: 53

Source Port: 49875

Destination Port: 53

Length: 38

Checksum: 0x7044 [unverified]

[Checksum Status: Unverified]

[Stream index: 26]

[Timestamps]

UDP payload (30 bytes)

Domain Name System (query)

Transaction ID: 0x586e

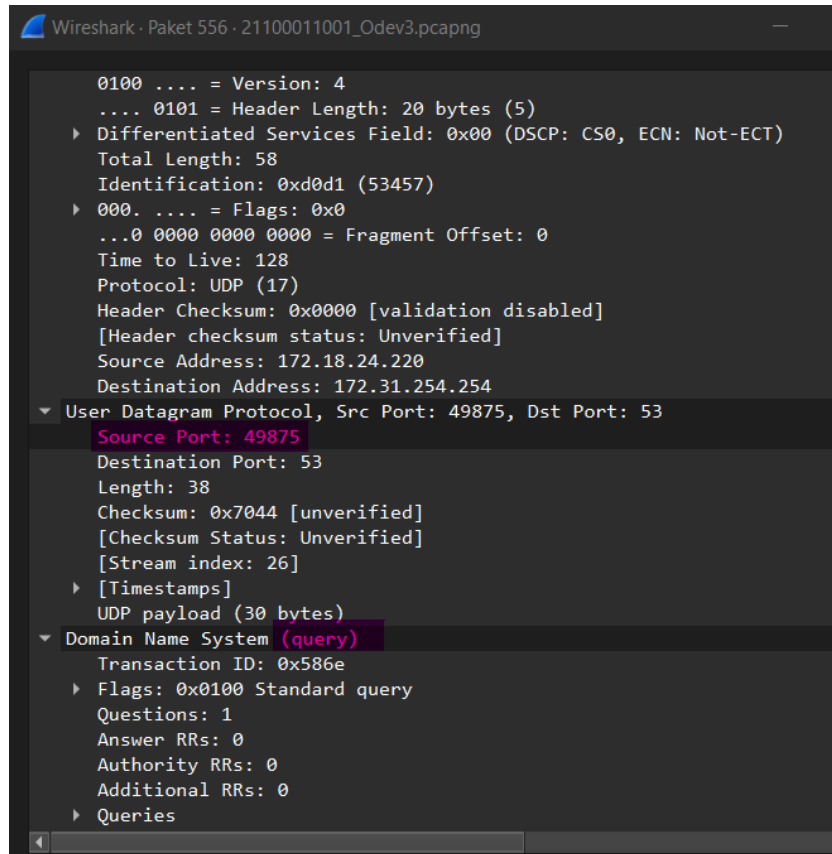
Flags: 0x0100 Standard query

Questions: 1

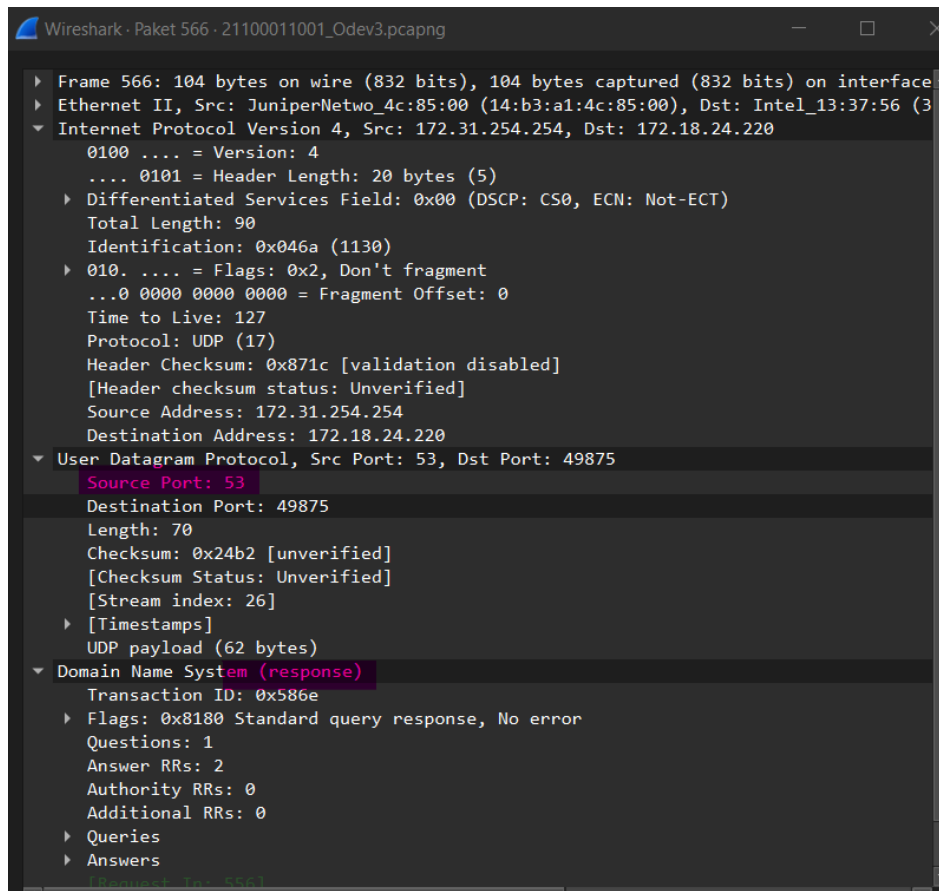
0000 14 b3 a1 4c 85 00 38 87 d5 13 37 56 08 00 45 00 ...L..8...7V..E.

No.: 556 - Time: 7.151331 - Source: 172.18.24.220 - Destination: 1...col DNS - Length: 72 - Info: Standard query 0x586e A www.ietf.org

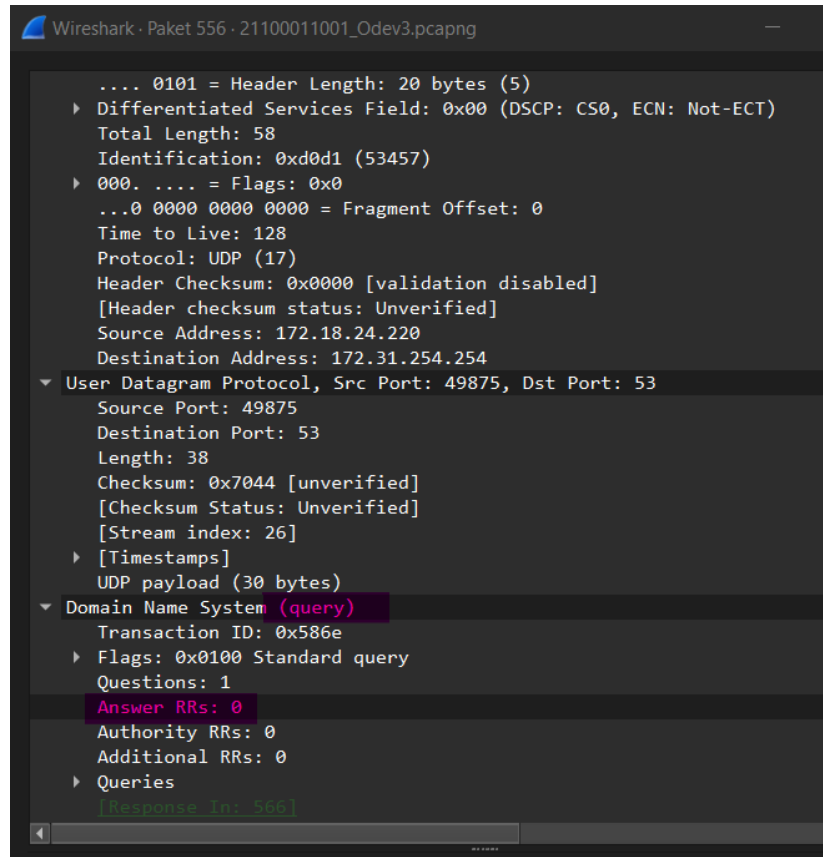
2. DNS sorgu mesajının port numarası nedir? →Paket-556 için → 49875



3. DNS cevap mesajının port numarası nedir? →Paket-566 için → 53



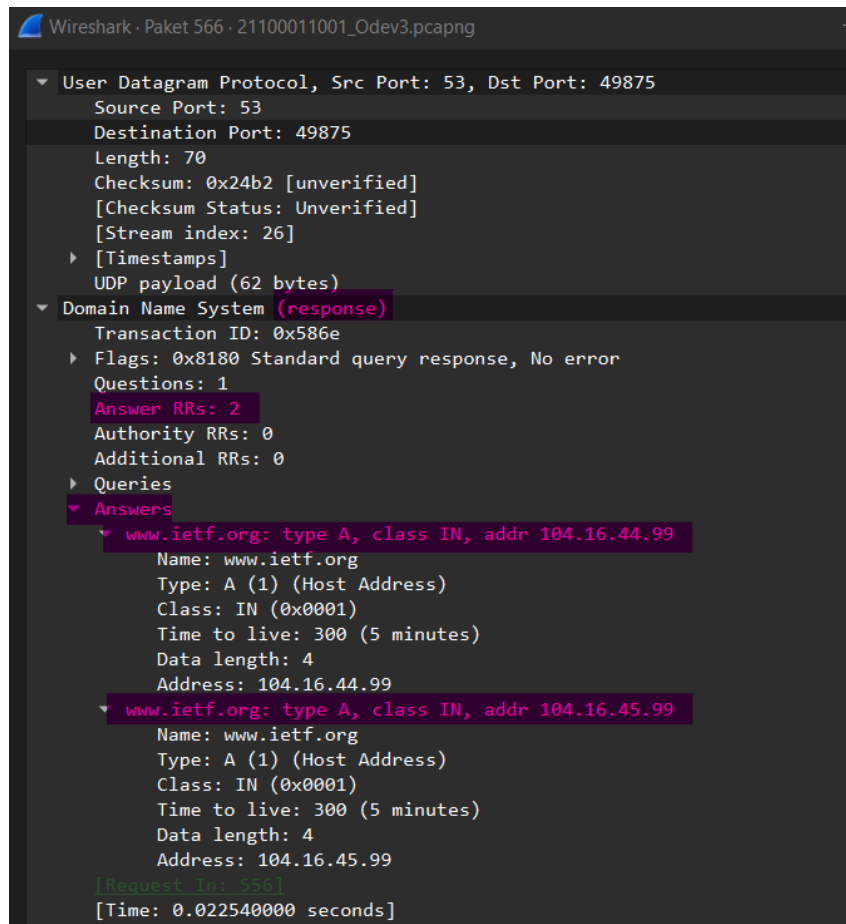
4. DNS sorgu mesajını inceleyiniz. Bu sorgu mesajı herhangi bir cevap (answer) içermekte midir? İçeriyorsa bu cevabın içeriği nedir? → Paket-556 için → İçermemektedir.



```
Wireshark · Paket 556 · 21100011001_Odev3.pcapng

... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0xd0d1 (53457)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.18.24.220
    Destination Address: 172.31.254.254
  ▾ User Datagram Protocol, Src Port: 49875, Dst Port: 53
    Source Port: 49875
    Destination Port: 53
    Length: 38
    Checksum: 0x7044 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 26]
    ▸ [Timestamps]
    UDP payload (30 bytes)
  ▾ Domain Name System (query)
    Transaction ID: 0x586e
    ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    ▸ Queries
      [Response In: 566]
```

5. DNS cevap mesajını inceleyiniz. Kaç tane cevap (answer) içermektedir? Bu cevapların her birinin içeriği nedir? → Paket-566 için → 2 tane



```
Wireshark · Paket 566 · 21100011001_Odev3.pcapng

  ▾ User Datagram Protocol, Src Port: 53, Dst Port: 49875
    Source Port: 53
    Destination Port: 49875
    Length: 70
    Checksum: 0x24b2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 26]
    ▸ [Timestamps]
    UDP payload (62 bytes)
  ▾ Domain Name System (response)
    Transaction ID: 0x586e
    ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
    ▸ Queries
  ▾ 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: 300 (5 minutes)
      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: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
    [Request In: 556]
    [Time: 0.022540000 seconds]
```