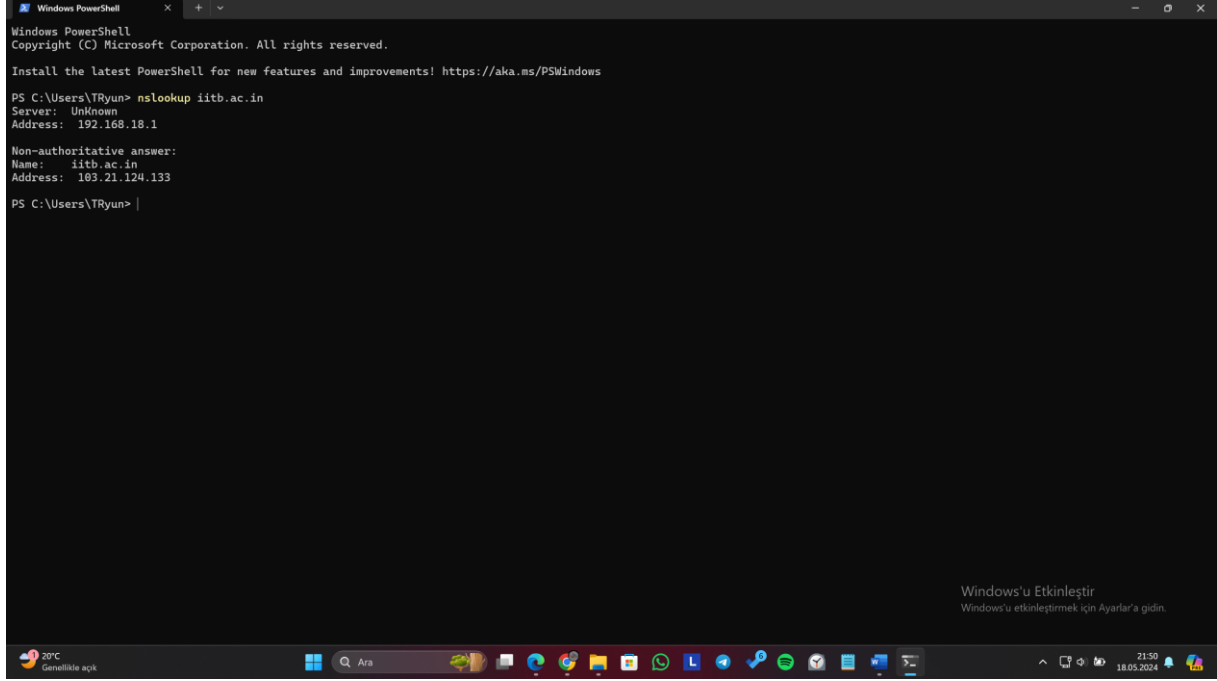


Yunus Emre Ay / 211000110016

① nslookup

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



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\TRYun> nslookup iitb.ac.in
Server:      Unknown
Address:     192.168.18.1

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

PS C:\Users\TRYun> |
```

Windows'u Etkinleştir
Windows'u etkinleştirmek için Ayarlar'a gidin.

20°C
Genelinde eğil

Ara

21:59
18.05.2024

- “iitb.ac.in” sunucusu IP adresi “103.21.124.133” tür.

b. iitb.ac.in sunucusuna ait güvenilir (authoritative) 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.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\TRYun> nslookup -type=ns iitb.ac.in
Server: Unknown
Address: 192.168.18.1

Non-authoritative answer:
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in
PS C:\Users\TRYun> nslookup dns2.iitb.ac.in
Server: Unknown
Address: 192.168.18.1

Non-authoritative answer:
Name:   dns2.iitb.ac.in
Address: 103.21.126.129

PS C:\Users\TRYun> nslookup dns1.iitb.ac.in
Server: Unknown
Address: 192.168.18.1

Non-authoritative answer:
Name:   dns1.iitb.ac.in
Address: 103.21.125.129

PS C:\Users\TRYun> nslookup dns3.iitb.ac.in
Server: Unknown
Address: 192.168.18.1

Non-authoritative answer:
Name:   dns3.iitb.ac.in
Address: 103.21.127.129

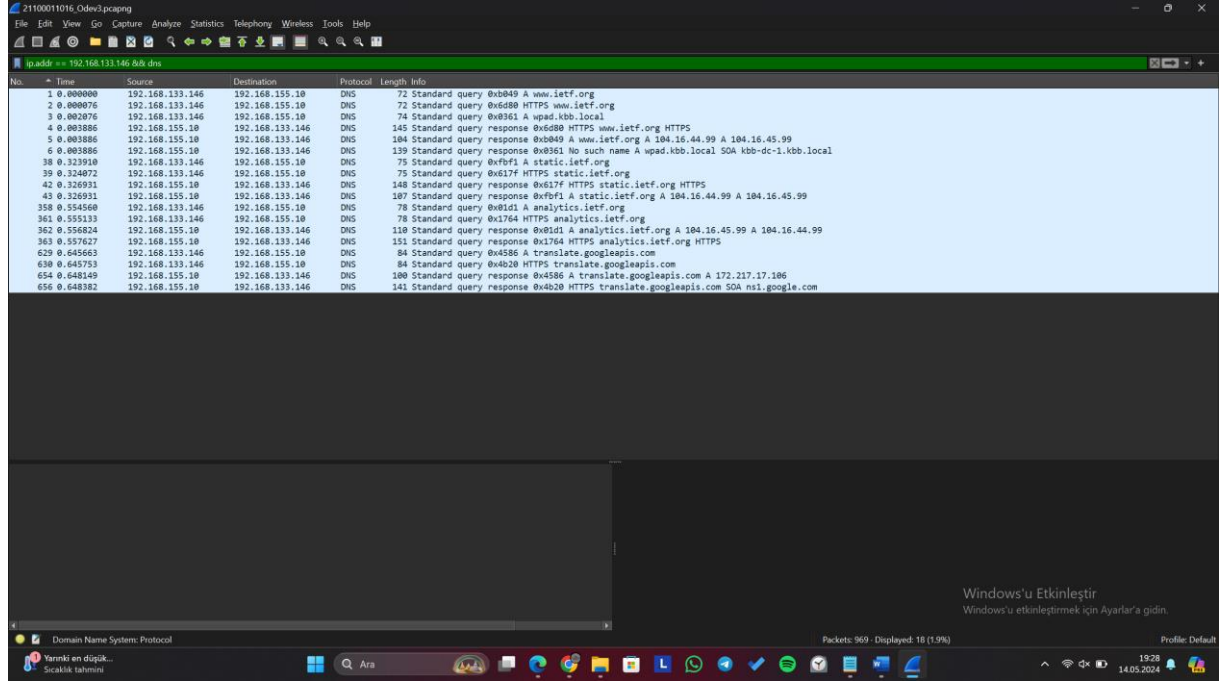
PS C:\Users\TRYun>
```

- 3 farklı güvenilir DNS sunucusundan bilgi aldım.
 - dns2.iitb.ac.in IP adresi → 103.21.126.129
 - dns1.iitb.ac.in IP adresi → 103.21.125.129
 - dns3.iitb.ac.in IP adresi → 103.21.127.129

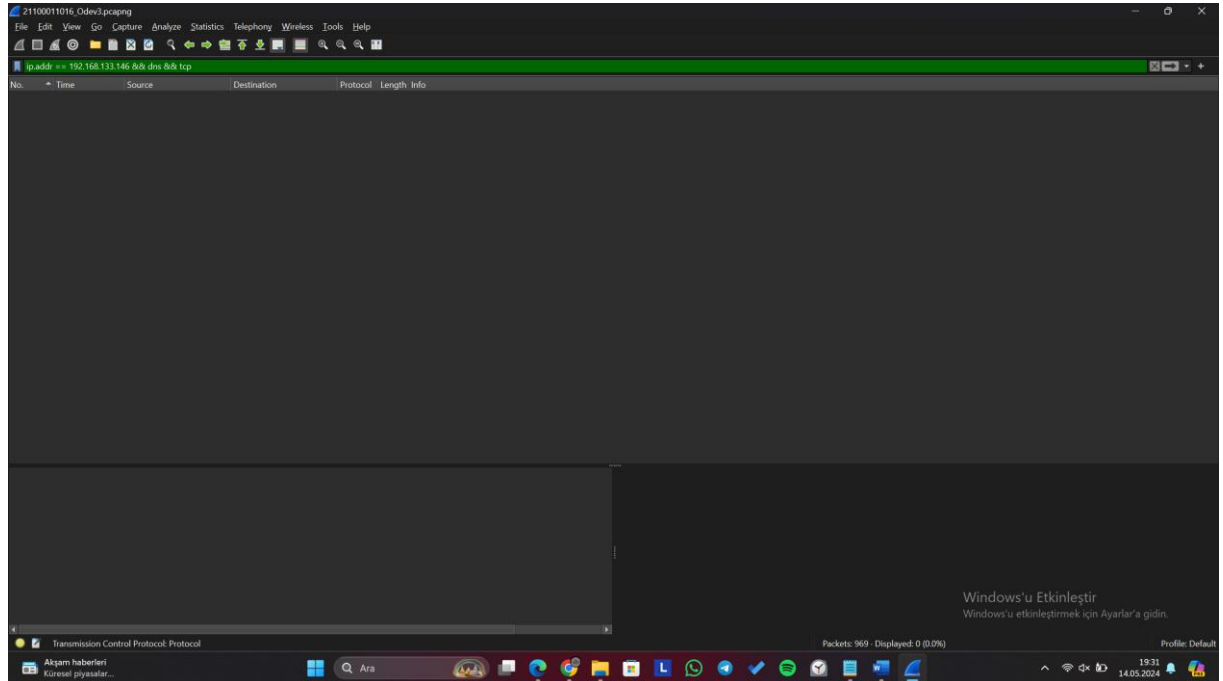
② Wireshark

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

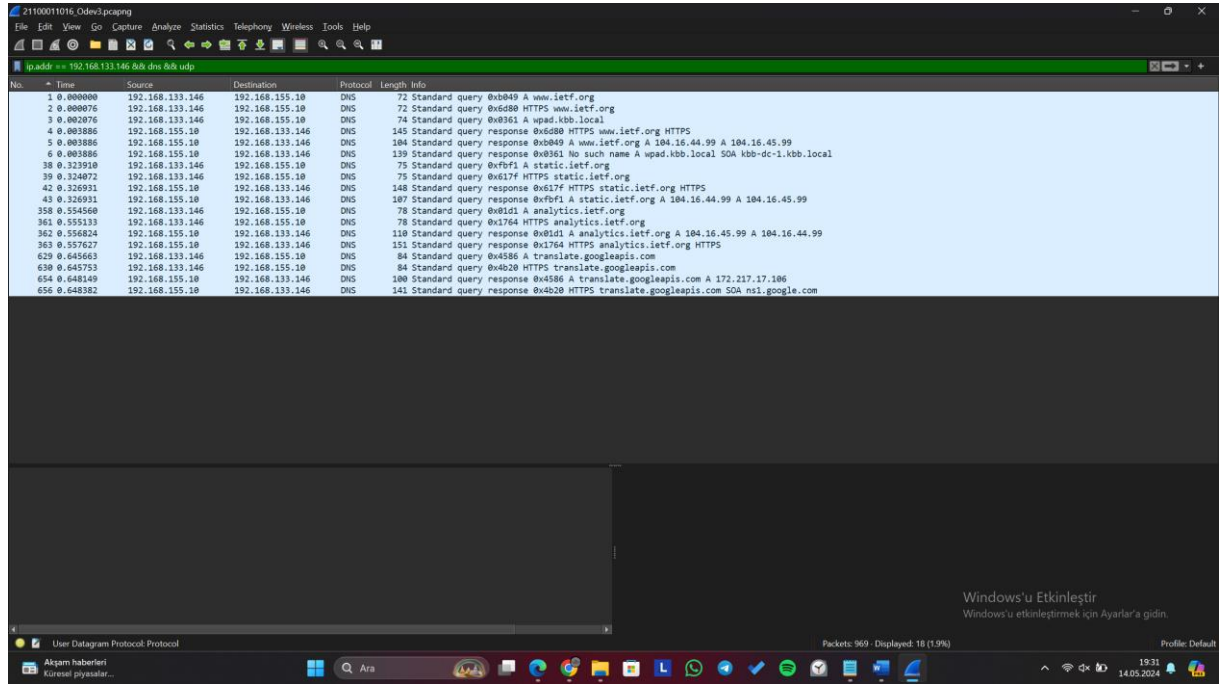
DNS sorgu (query) ve cevap (response) mesajları “**ip.addr == 192.168.133.146 && dns**” sorgusunu yapılarak bulunmaktadır.



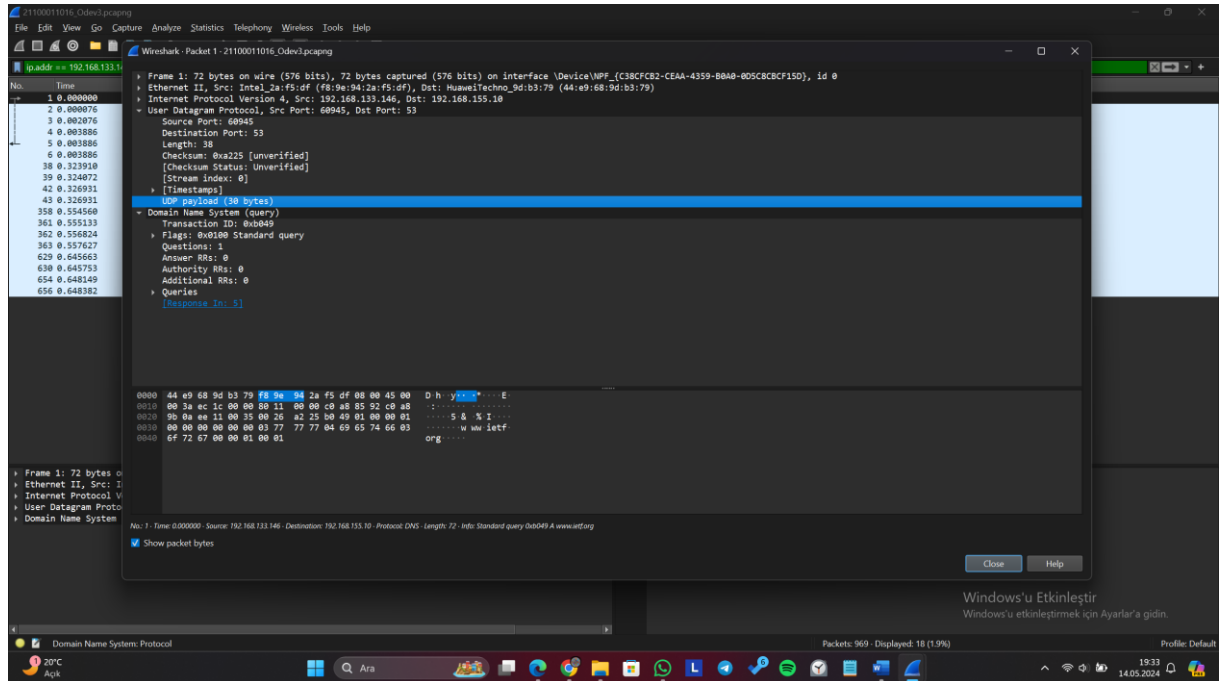
Bu mesajlardan TCP protokolü ile gönderilenler “**ip.addr == 192.168.133.146 && dns && tcp**” sorgusunu yapılarak bulunmaktadır.



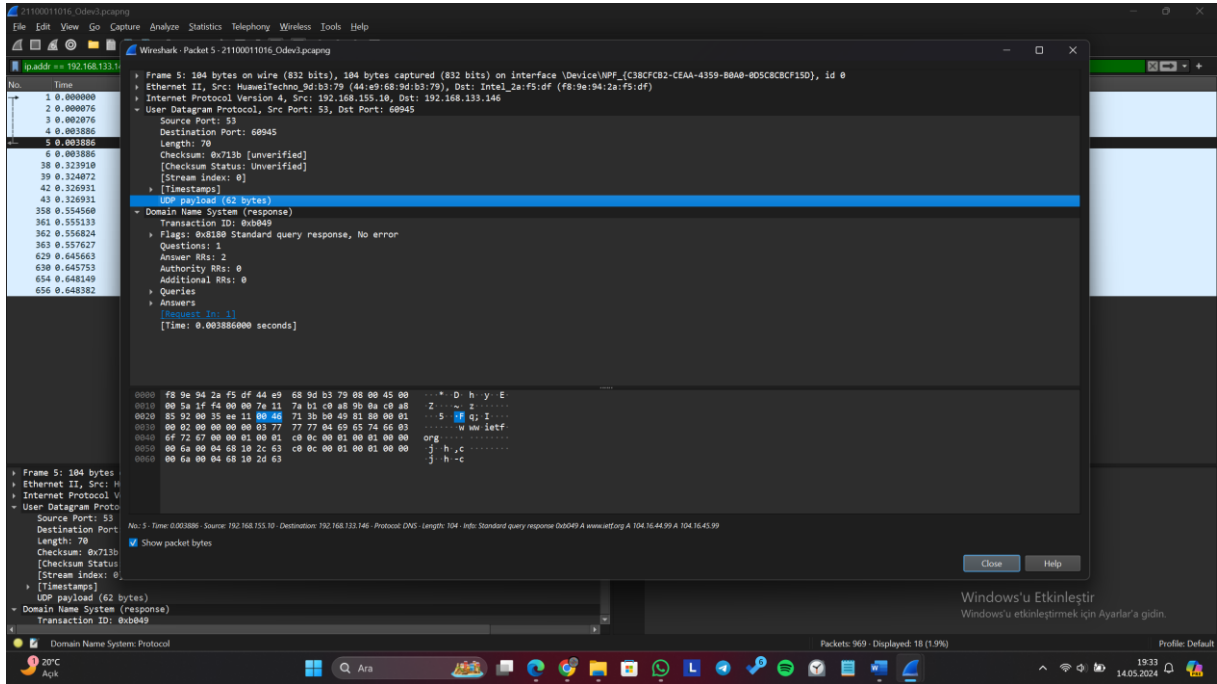
Bu mesajlardan UDP protokolü ile gönderilenler **“ip.addr == 192.168.133.146 && dns && udp”** sorgusunu yapılarak bulunmaktadır.



- Aşağıda (**Paket No: 1**) için DNS sorgu mesajında UDP protokolü kullanıldığı gösterilmektedir.

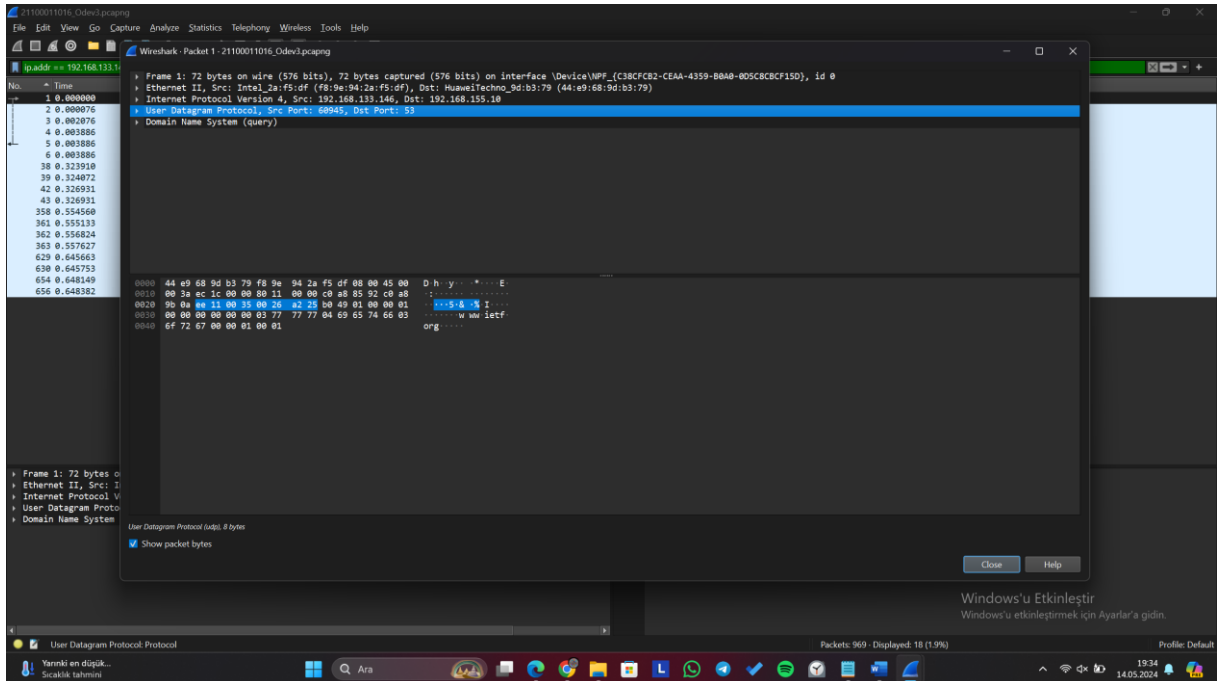


- Aşağıda (**Paket No: 5**) için DNS cevap mesajında UDP protokolü kullanıldığı gösterilmektedir.



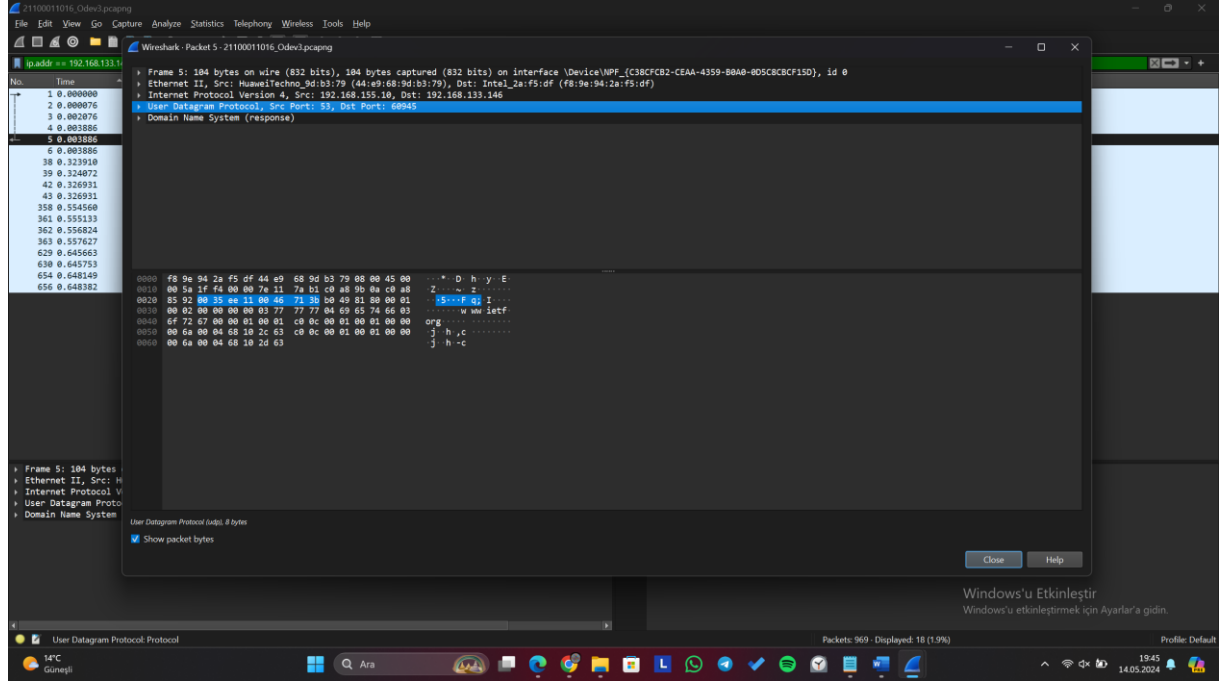
2. DNS sorgu mesajının port numarası nedir?

Her bir DNS sorgu mesajının port numarasını belirlemek için ilgili paketin içeriği görüntülenir. DNS sorgu mesajlarında port numarası genellikle rasgele seçilmiş büyük bir sayı olmaktadır. Aşağıda (**Paket No: 1**) için port numarası gösterilmektedir. DNS sorgu mesajı port numarası “60945” tir.



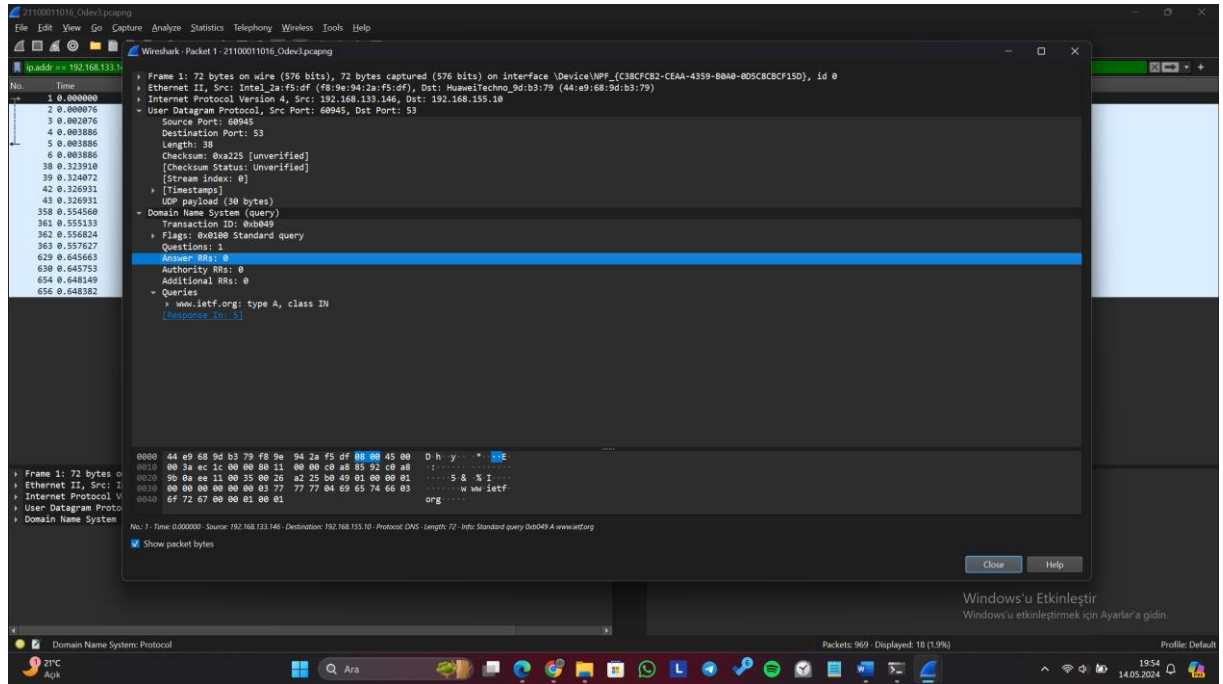
3. DNS cevap mesajının port numarası nedir?

Her bir DNS cevap mesajının port numarasını belirlemek için ilgili paketin içeriği görüntülenir. DNS cevap mesajlarında port numarası genellikle “53” olmaktadır. Aşağıda (**Paket No: 5**) için port numarası gösterilmektedir. DNS cevap mesajı port numarası “53” tür.



4. DNS sorgu mesajını inceleyiniz. Bu sorgu mesajı herhangi bir cevap (answer) içermekte midir? İçeriyorsa bu cevabın içeriği nedir?

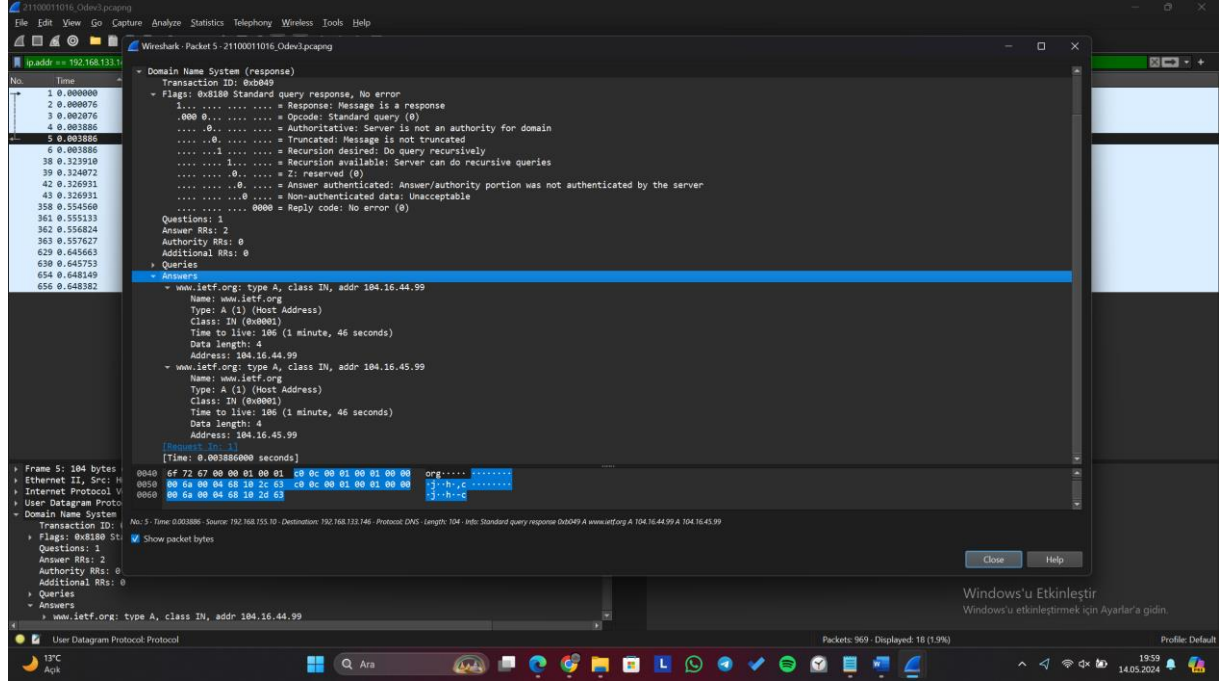
Aşağıda (**Paket No: 1**) için sorgu mesajının içeriği incelendiğinde bir cevap (answer) içermediği görülmektedir.



5. DNS cevap mesajını inceleyiniz. Kaç tane cevap (answer) içermektedir? Bu cevapların her birinin içeriği nedir?

Aşağıda (**Paket No: 5**) için cevap mesajı gösterilmektedir. **2 adet** cevap (answer) içermektedir.

Cevapların içeriği aşağıdaki şekilde gösterilmektedir.



- Cevaplarda ilgili hostun adı, tipi, sınıfı, TTL bilgisi, veri uzunluğu, IP adres bilgileri bulunmaktadır.