



**GAZİ ÜNİVERSİTESİ**  
**MÜHENDİSLİK FAKÜLTESİ - BİLGİSAYAR MÜHENDİSLİĞİ**

**171180010 – Cansu AYTEN**

**BM402 BİLGİSAYAR AĞLARI**

**LAB ÖDEVİ**

**M. ALİ AKÇAYOL**

**DERS ASİSTANI: YASİN İNAĞ**

## İÇİNDEKİLER

### Sayfa

|  |   |
|--|---|
| İÇİNDEKİLER.....   | i |
| 1. gazi.edu.tr Adresinin DNS Sunucusunun IP Adresi.....                              | 1 |
| 2. gazi.edu.tr Adresine Bağlanırken Kaç Atlama ile Ulaşıldığı .....                  | 1 |
| 3. Tarayıcıdan Bir Web Sitesine Erişim ve Wireshark ile Paketlerin Yakalanması ..... | 2 |
| 4. Yakalanan Paketlerin DNS Paketleri Olacak Şekilde Filtrelenmesi .....             | 3 |
| 5. Yakalan DNS Paketinde Tespit Edilen Veriler ve Açıklamaları .....                 | 3 |

## 1. gazi.edu.tr Adresinin DNS Sunucusunun IP Adresi

```
Komut İstemi
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\cansu>nslookup gazi.edu.tr
Server: UnKnown
Address: 178.233.140.110

Non-authoritative answer:
Name: gazi.edu.tr
Address: 194.27.18.45
```

Şekil 1: nslookup komutu

## 2. gazi.edu.tr Adresine Bağlanırken Kaç Atlama ile Ulaşıldığı

```
Komut İstemi
C:\Users\cansu>tracert gazi.edu.tr

Tracing route to gazi.edu.tr [194.27.18.45]
over a maximum of 30 hops:

 1  1 ms    1 ms    1 ms  192.168.0.1
 2  *        *        *      Request timed out.
 3  9 ms    9 ms    9 ms  172.25.66.17
 4  11 ms   9 ms   10 ms  10.59.10.209
 5  12 ms   10 ms  13 ms  10.40.169.239
 6  14 ms   13 ms  16 ms  10.40.141.57
 7  10 ms   12 ms  11 ms  10.38.211.166
 8  *        *        17 ms  10.40.171.217
 9  13 ms   15 ms  18 ms  10.38.219.5
10  19 ms   17 ms  16 ms  212.156.99.253.static.turktelekom.com.tr [212.156.99.253]
11  16 ms   15 ms  16 ms  06-ulus-sr12e-t3-1---06-ulus-xrs-t2-1.statik.turktelekom.com.tr [212.156.108.190]

12  17 ms   18 ms  17 ms  212.156.64.46.static.turktelekom.com.tr [212.156.64.46]
13  20 ms   16 ms  18 ms  70.96.154.212.static.turk.net [212.154.96.70]
14  *        *        *      Request timed out.
15  *        *        *      Request timed out.
16  *        *        *      Request timed out.
17  *        *        *      Request timed out.
18  *        *        *      Request timed out.
19  *        *        *      Request timed out.
20  *        *        *      Request timed out.
21  *        *        *      Request timed out.
22  *        *        *      Request timed out.
23  *        *        *      Request timed out.
24  *        *        *      Request timed out.
25  *        *        *      Request timed out.
26  *        *        *      Request timed out.
27  *        *        *      Request timed out.
28  *        *        *      Request timed out.
29  *        *        *      Request timed out.
30  *        *        *      Request timed out.

Trace complete.
```

Şekil 2:tracert gazi.edu.tr

Kaynaktan hedefe giderken geçilen ara cihazların toplam sayısına atlama sayısı denir. tracert gazi.edu.tr komutu ile gazi.edu.tr adresine bağlanılmaya çalışılmıştır ama adrese ulaşılamamıştır. Bu nedenle başka bir adrese deneme yapılmıştır. tracert stackoverflow.com denendiğinde geçilen ara cihazlar Şekil 3'tedir. Toplam 13 atlamada stackoverflow.com sunucusuna ulaşılmıştır.

```
C:\Users\cansu>tracert stackoverflow.com

Tracing route to stackoverflow.com [151.101.65.69]
over a maximum of 30 hops:

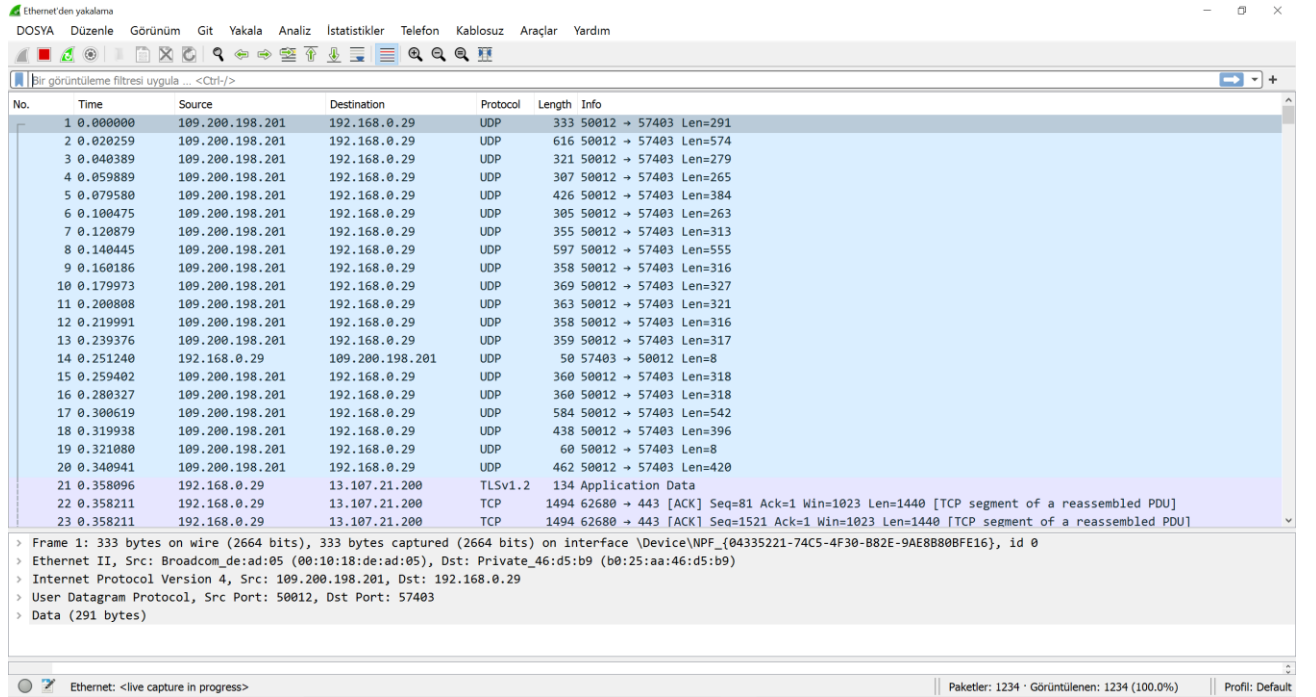
 1  <1 ms    <1 ms    <1 ms    192.168.0.1
 2  *         *         *         Request timed out.
 3  9 ms     9 ms     9 ms     172.25.66.17
 4  9 ms     13 ms    8 ms     10.59.10.209
 5  8 ms     9 ms    10 ms    10.40.169.239
 6  *         *         *         Request timed out.
 7  8 ms     9 ms     9 ms     10.38.211.166
 8  12 ms    14 ms    *         10.40.171.217
 9  7 ms     10 ms    8 ms     10.40.168.31
10  *         *         *         Request timed out.
11  58 ms    59 ms    58 ms    ae1.3111.edge7.Paris1.level3.net [4.69.133.234]
12  59 ms    58 ms    59 ms    213.242.127.138
13  54 ms    56 ms    55 ms    151.101.65.69

Trace complete.
```

Şekil 3: tracert stackoverflow.com

### 3. Tarayıcıdan Bir Web Sitesine Erişim ve Wireshark ile Paketlerin Yakalanması

Bir tarayıcı aracılığıyla <https://stackoverflow.com/> sitesine bağlanılmıştır. Bu sırada ise Wireshark kullanılarak paketler yakalanmaktadır.



Şekil 4: Wireshark paket yakalama

## 4. Yakalanan Paketlerin DNS Paketleri Olacak Şekilde Filtrelenmesi

The image shows a Wireshark capture of DNS traffic. The filter bar at the top is set to 'dns'. The packet list on the left shows several DNS packets. The packet details pane on the right shows the details of frame 3334, which is a DNS query for 'www.googleapis.com'. The packet bytes pane at the bottom shows the raw data of the packet.

| No.  | Time      | Source          | Destination     | Protocol | Length | Info  |
|------|-----------|-----------------|-----------------|----------|--------|---|
| 3118 | 49.294065 | 178.233.140.110 | 192.168.0.29    | DNS      | 318    | Standard query response 0x34af A www.googleapis.com A 172.217.169.138 A 172.217.169.170 A 172.21... |
| 3189 | 49.591745 | 192.168.0.29    | 178.233.140.110 | DNS      | 79     | Standard query 0xb0f3 A clients4.google.com   |
| 3194 | 49.601941 | 178.233.140.110 | 192.168.0.29    | DNS      | 119    | Standard query response 0xb0f3 A clients4.google.com CNAME clients.l.google.com A 172.217.20.78     |
| 3334 | 50.022790 | 192.168.0.29    | 178.233.140.110 | DNS      | 77     | Standard query 0xb88c A stackoverflow.com   |
| 3335 | 50.030886 | 178.233.140.110 | 192.168.0.29    | DNS      | 141    | Standard query response 0xb88c A stackoverflow.com A 151.101.193.69 A 151.101.129.69 A 151.101.6... |
| 3406 | 50.415337 | 192.168.0.29    | 178.233.140.110 | DNS      | 79     | Standard query 0x9b87 A clients2.google.com   |
| 3410 | 50.426450 | 178.233.140.110 | 192.168.0.29    | DNS      | 119    | Standard query response 0x9b87 A clients2.google.com CNAME clients.l.google.com A 172.217.20.78     |
| 3468 | 50.572682 | 192.168.0.29    | 178.233.140.110 | DNS      | 76     | Standard query 0x0226 A mtalk.google.com  |
| 3469 | 50.581155 | 178.233.140.110 | 192.168.0.29    | DNS      | 121    | Standard query response 0x0226 A mtalk.google.com CNAME mobile-gtalk.l.google.com A 108.177.119...  |
| 3534 | 50.808259 | 192.168.0.29    | 178.233.140.110 | DNS      | 87     | Standard query 0xb455 A safebrowsing.googleapis.com   |

Frame 3334: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF\_{04335221-74C5-4F30-B82E-9AE8B80BE16}, id 0

Ethernet II, Src: Private\_46:d5:b9 (b0:25:aa:46:d5:b9), Dst: Broadcom\_de:ad:05 (00:10:18:de:ad:05)

Internet Protocol Version 4, Src: 192.168.0.29, Dst: 178.233.140.110

User Datagram Protocol, Src Port: 51091, Dst Port: 53

Domain Name System (query)

Encapsulation type (frame.encap\_type) | Paketler: 840511 · Görüntülenen: 470 (0.1%) | Profil: Default

Şekil 5: DNS paketleri şeklinde filtreleme

## 5. Yakalan DNS Paketinde Tespit Edilen Veriler ve Açıklamaları

The image shows a Wireshark capture of a single DNS packet (frame 3334). The filter bar at the top is set to 'dns'. The packet details pane on the right shows the details of frame 3334, which is a DNS query for 'www.googleapis.com'. The packet bytes pane at the bottom shows the raw data of the packet.

Frame 3334: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF\_{04335221-74C5-4F30-B82E-9AE8B80BE16}, id 0

Interface id: 0 (\Device\NPF\_{04335221-74C5-4F30-B82E-9AE8B80BE16})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 3, 2022 23:00:34.558085000 Türkiye Standart Saati

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1654286434.558085000 seconds

[Time delta from previous captured frame: 0.000707000 seconds]

[Time delta from previous displayed frame: 0.420849000 seconds]

[Time since reference or first frame: 50.022790000 seconds]

Frame Number: 3334

Frame Length: 77 bytes (616 bits)

Capture Length: 77 bytes (616 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: Private\_46:d5:b9 (b0:25:aa:46:d5:b9), Dst: Broadcom\_de:ad:05 (00:10:18:de:ad:05)

Destination: Broadcom\_de:ad:05 (00:10:18:de:ad:05)

Source: Private\_46:d5:b9 (b0:25:aa:46:d5:b9)

Type: IPv4 (0x0000)

Internet Protocol Version 4, Src: 192.168.0.29, Dst: 178.233.140.110

0100 .... = Version: 4

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

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

Total Length: 63

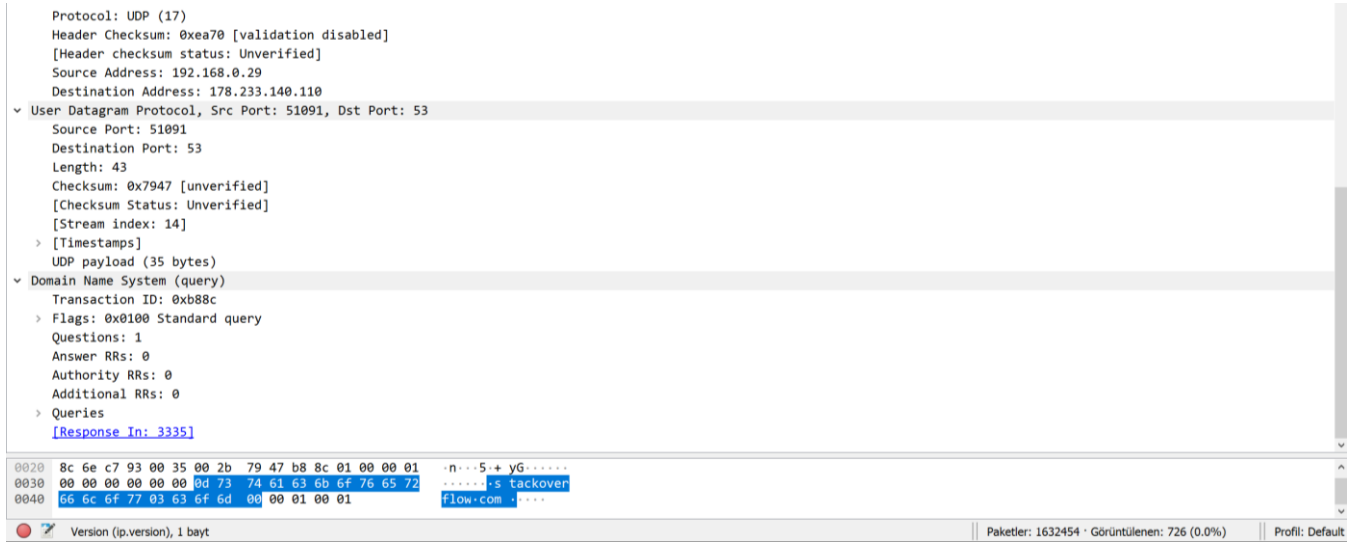
Identification: 0x5020 (20512)

Flags: 0x00

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

Time to Live: 128

Version (p.version), 1 bayt | Paketler: 1612662 · Görüntülenen: 696 (0.0%) | Profil: Default



Şekil 6: DNS Paketinde Tespit Edilen Veriler

**Interface id:** 0 ile başlayan arayüzlerin bir numaralandırmasıdır. Paket Ethernet arayüzünden yakalanmıştır.

- ▼ Interface id: 0 (\Device\NPF\_{04335221-74C5-4F30-B82E-9AE8B80BFE16})
  - Interface name: \Device\NPF\_{04335221-74C5-4F30-B82E-9AE8B80BFE16}
  - Interface description: Ethernet

**Encapsulation type:** Yakalanmış olan paketin enkapsülasyon tipi Ethernet'tir.

Enkapsülasyon tipine göre zayıflıklardan faydalanılarak farklı saldırılar yapılabilir.

**Arrival Time:** Yakalanmış olan paketin varış zamanını ay/ gün/ yıl/ saat/ dakika/ saniye/ salise şeklinde gösterir.

**Epoch time:** 1 Ocak 1970'den bu yana geçen saniye sayısını gösterir. Zamanın hatalı olması epoch time ile engellenmiş olur.

**Frame Number:** Yakalanmış olan paketin frame numarasını gösterir ve 3334 bulunmuştur.

**Frame Length:** Yakalanmış olan paketin toplam frame bayt uzunluğunu gösterir ve 77 bayt bulunmuştur.

**Capture Length:** Yakalanan frame uzunluğudur ve 77 bayt bulunmuştur.

**Ethernet II Destination:** Pakete ait hedef MAC adresini gösterir.

- ▼ Destination: Broadcom\_de:ad:05 (00:10:18:de:ad:05)
  - Address: Broadcom\_de:ad:05 (00:10:18:de:ad:05)
  - .... ..0. .... = LG bit: Globally unique address (factory default)
  - .... ...0 .... = IG bit: Individual address (unicast)

**Ethernet II Source:** Pakete ait kaynak MAC adresini gösterir.

```
▼ Source: Private_46:d5:b9 (b0:25:aa:46:d5:b9)
  Address: Private_46:d5:b9 (b0:25:aa:46:d5:b9)
  .... ..0. .... = LG bit: Globally unique address (factory default)
  .... ..0. .... = IG bit: Individual address (unicast)
```

Bir saldırgan MAC adreslerini kolaylıkla dinleyip tespit edebilir (Sniff). Kendi MAC adresini bulduğu yeni bir MAC adresiyle değiştirebilir. Ekipmanı ve kablosuz bir ağı varsa Spoofing saldırısı yapabilir.

**Version:** Hangi ip sürümünün kullanıldığını gösterir. IPv4 için 4, IPv6 için 6 bilgisine ulaşılır. Yakalanan paketin IP sürümü 4 yani IPv4'tür.

**Header Length:** IP başlığının uzunluğunu gösterir ve 20 bayttır.

**Differentiated Services Field:** Hizmet kalitesi (QoS) için kullanılır ve pakete belirli bir işlem atanırken kullanılacak paketi işaretlemek için 8 bit bulunur.

```
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```

**Differentiated Services Code Point (DSCP):** QoS için kullanılır, VoIP paketlerinin önemine göre işaretlenmesini sağlar ve paket sınıflandırması amacıyla 6 bit bulunur.

DDOS paketleri en yüksek önceliğe sahip olacak şekilde işaretlenirse ses trafiği etkilenir.

**Explicit Congestion Notification:** İki nokta arası tıkanıklık bildirimini etkinleştirir ve 2 bitten oluşur.

**Total Length:** IP paketinin toplam boyutunu bayt cinsinden gösterir ve 63 bayttır.

**Identification:** IP paketinin parçalanması halinde parçalanmış paketler için hangi IP paketine ait olduğunu belirtmek amacıyla kullanılır. 0x5020'dir.

**Flags:** Üç bitten oluşur -ilki 0, ikincisi DF (Don't Fragment), üçüncüsü MF (More Fragments)-, parçalanma ve parçaları kontrol etme için kullanılır.

```
Flags: 0x00
  0... .... = Reserved bit: Not set
  .0... .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
```

Veri iletimi için yapılan parçalanmadan bazı saldırılarda yararlanılabilir. Parçaları yeniden birleştirme mekanizmaları hedef alınabilir. Örneğin Teardrop saldırısında saldırgan büyük verileri çok fazla parçaya bölüp yeniden birleştirme mekanizmasını değiştirir ve böylelikle

demonte işlemi önlenmiş olur. Ya da başka bir saldırı olarak bu paketler değiştirilip yeniden birleştirilemeyecek hale getirilir.

**Fragment Offset:** Orijinal parçalanmış IP paketindeki parça konumunu gösterir. 0'dır.

**Time to Live (TTL):** Paketin sistemde kalmasına izin verilen maksimum süreyi belirtir. Paketlerin sonsuza kadar dolaşmasını önlemek için kullanılır. Gönderen tarafından doldurulur her noktada datagram işlenirken harcanan zaman nedeniyle azalır. Bu süre 0 olduğunda datagram atılır.

Bir saldırgan TTL değeri düşük olan yani neredeyse süresi dolmakta olan büyük bir paket göndermek isterse cihazın CPU'sunu doldurur. Bunun dışında TTL değerleri ile işletim sistemleri arasında ilgi bulunmaktadır. Örneğin TTL değeri Windows'ta 128'den başlamaktadır. Bu bilgi ile işletim sistemlerinin zayıflıkları kullanılarak saldırılar da gerçekleştirilebilir.

**Protocol:** IP paketinde kapsüllenen protokolü gösterir. UDP'dir.

**Header Checksum:** Başlık verilerinin hata denetimi için kullanılır ve başlığın checksum'ını (sağlaması) tutar. 0xea70'dir. Temel olarak güvenilirlik için vardır.

**Source Address:** Kaynak IP adresini gösterir. 192.168.0.29'dur.

**Destination Address:** Hedef IP adresini gösterir. 178.233.140.110'dur.

**Source Port:** Paketin kaynak port numarasını gösterir. 51091'dir

**Destination Port:** Paketin hedef port numarasını gösterir. 53'tür

Land saldırısında hedef sistemin IP adresi ve portu ile kaynak IP adresi ve portu aynı yapılır. Bu durumda sistem kendi kendine paket gönderiyormuş gibi gözükür ve sistemin kaynakları (CPU, RAM vs.) tüketilmiş olur.

**Length:** Toplam UDP verisi ve UDP başlık uzunluğunu gösterir. 43'tür.

**Checksum:** Hata tespitinde kullanılan sağlama toplamını bulundurur fakat UDP'de checksum zorunlu değildir. Temel olarak güvenilirlik için vardır.

**DNS Transaction ID:** İşlem kimliği sorguyu başlatan nameserver tarafından oluşturulan rastgele bir sayıdır ve yanıtlayan nameserver'ın cevabından sonra ona da aynı işlem kimliği ayarlanır. 00xb88c'dir.



Saldırgan bir DNS sunucusunun yanıtlarını taklit edip bir yanıt paketi gönderebilir. Bunu yaparken doğru transaction ID kullanılmalıdır. Transaction ID ise rastgele bir sayı olduğundan tahmin edilebilirliği yüksektir.

**Flags:** Mesajın bir query (sorgu) olup olmadığını belirten (0-1) response alanı, opcode (geçerli değerler 0,1,2) alanı, mesajın iletim kanalında izin verilen daha uzun olması durumunda kesilmesi ya da uzun değilse kesilmemesi gibi bilgileri içeren truncated alanı, recursion desired alanı gibi toplamda altı alan barındırır.

▼ **Flags: 0x0100 Standard query**

```
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
.... ...1 .... = Recursion desired: Do query recursively
.... .... .0.. .... = Z: reserved (0)
.... .... ...0 .... = Non-authenticated data: Unacceptable
```

**Questions:** Sorgu bölümündeki giriş sayısını gösterir.

**Answer RRs:** (RR: resource record) Cevap bölümündeki giriş sayısını gösterir. Paket bir sorgu paketidir bu nedenle 0 değerine sahiptir.

**Authority RRs:** Yetki bölümündeki giriş sayısını gösterir. Paket bir sorgu paketidir bu nedenle 0 değerine sahiptir.

**Additional RRs:** Ek bölümdeki giriş sayısını gösterir. Ek bilgiler veya önyükleme sağlar. Paket bir sorgu paketidir bu nedenle 0 değerine sahiptir.

**Queries:** Sorgu verilerini bulundurur.