GAZİ ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

BM402 BİLGİSAYAR AĞLARI

Gamze AKSU

171180005

LAB ÖDEVİ

HAZİRAN 2022

İÇİNDEKİLER

Sayfa

İÇİNDEKİLER..... 1
1. nslookup Komutu 2
2. tracert Komutu..... 2
3. Wireshark 3
4. Filtreleme..... 3
5. DNS Paketindeki Veriler..... 4

1. nslookup Komutu

```
C:\WINDOWS\system32>nslookup gazi.edu.tr
Server:  UnKnown
Address:  192.168.1.1

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

2. tracert Komutu

```
C:\WINDOWS\system32>ping 194.27.18.45

Pinging 194.27.18.45 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 194.27.18.45:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ping komutu ile gazi.edu.tr adresine bağlanmaya çalışıldı ancak bağlanılamadı.

Bir adrese gidilirken geçilen router sayısına atlama (hop) denir.

tracert komutu ile gazi.edu.tr adresine bağlanmaya çalışıldığında geçilen routerların sayısı gösterilir.

-d ile adres çözümlemesi kaldırılır.

```
C:\WINDOWS\system32>tracert -d www.gazi.edu.tr

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

  1     1 ms     1 ms    <1 ms  192.168.1.1
  2    68 ms    87 ms    86 ms  212.156.201.20
  3    39 ms     9 ms    11 ms  81.212.77.33
  4    17 ms    45 ms    44 ms  81.212.218.102
  5   100 ms   117 ms   365 ms  81.212.210.104
  6    30 ms    36 ms    37 ms  212.156.108.190
  7   124 ms    18 ms     8 ms  212.156.64.46
  8    75 ms    87 ms   112 ms  212.154.96.70
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 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.
```

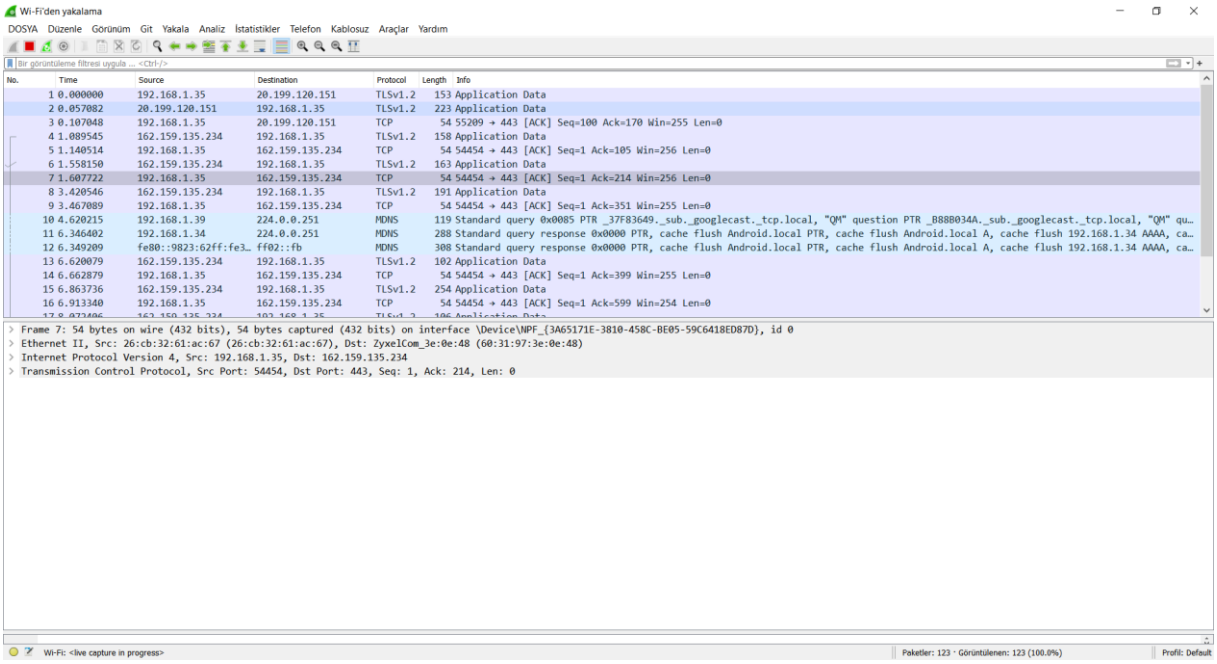
```
C:\WINDOWS\system32>tracert -d cisco.com

Tracing route to cisco.com [72.163.4.185]
over a maximum of 30 hops:

  1     1 ms     2 ms     1 ms  192.168.1.1
  2     6 ms     6 ms     5 ms  212.156.201.20
  3     7 ms    15 ms     7 ms  81.212.77.33
  4     7 ms     6 ms     8 ms  81.212.218.102
  5     7 ms     7 ms     6 ms  81.212.210.104
  6    10 ms     7 ms    25 ms  81.212.217.5
  7    56 ms    56 ms    54 ms  212.156.101.126
  8     *        *        *     Request timed out.
  9   172 ms   181 ms   174 ms  4.69.208.229
 10   274 ms   318 ms   350 ms  4.59.34.66
 11   221 ms   260 ms   252 ms  128.107.2.5
 12   176 ms   185 ms   190 ms  72.163.0.102
 13   205 ms   172 ms   174 ms  72.163.0.190
 14   171 ms   175 ms   178 ms  72.163.3.2
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17   219 ms   235 ms   174 ms  72.163.4.129
 18   247 ms   225 ms   173 ms  72.163.4.185

Trace complete.
```

gazi.edu.tr adresine ulaşılamadı. Bu yüzden tracert komutu ile cisco.com adresine gitmek için geçilen routerların sayısı gösterilecektir.

18 atlama ile cisco.com sunucusuna ulaşılmıştır.

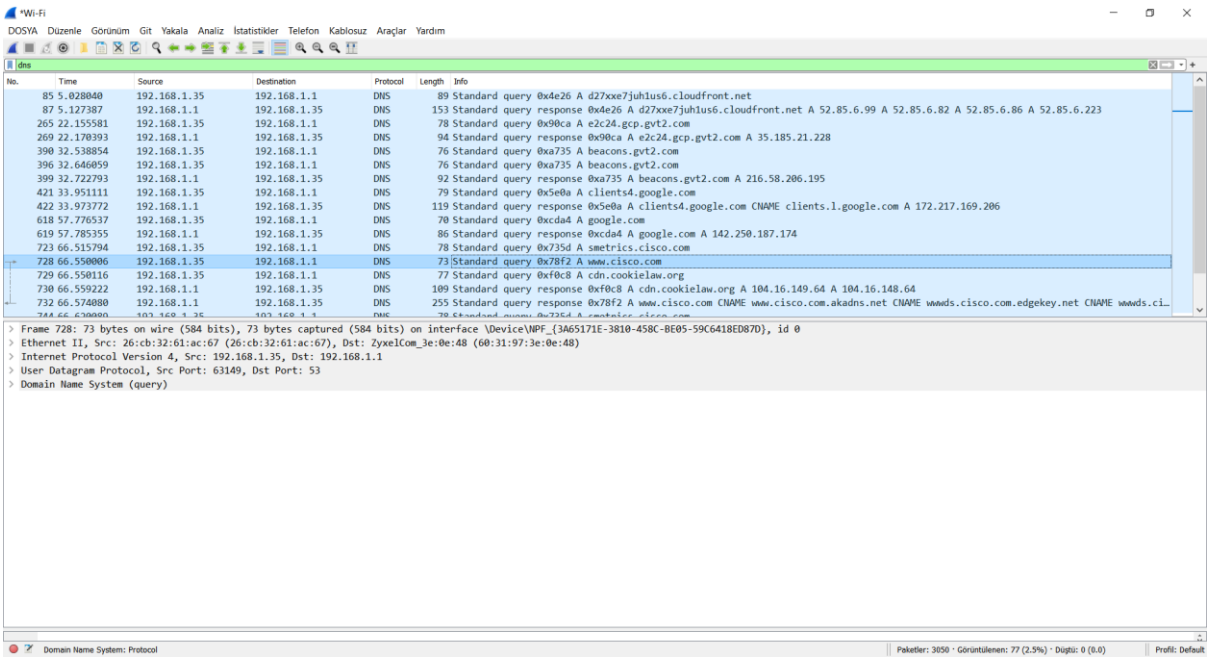
3. Wireshark

www.cisco.com web sitesine bağlanırken wireshark ile paketler yakalanmaya başlanır.

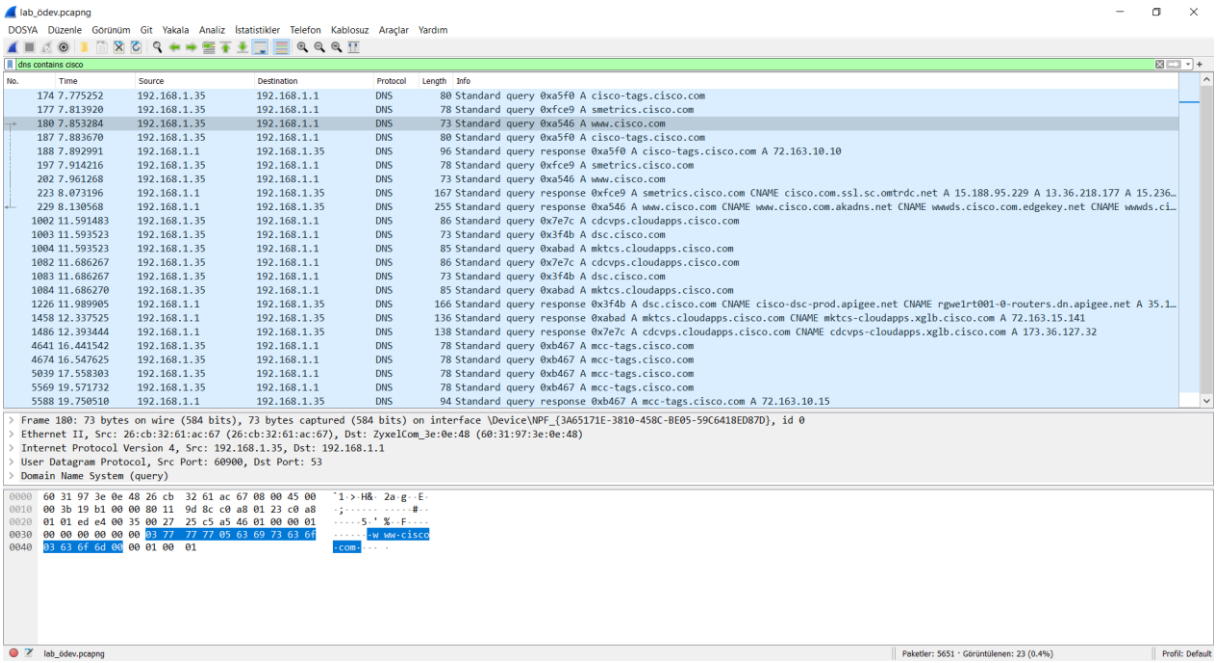


4. Filtreleme

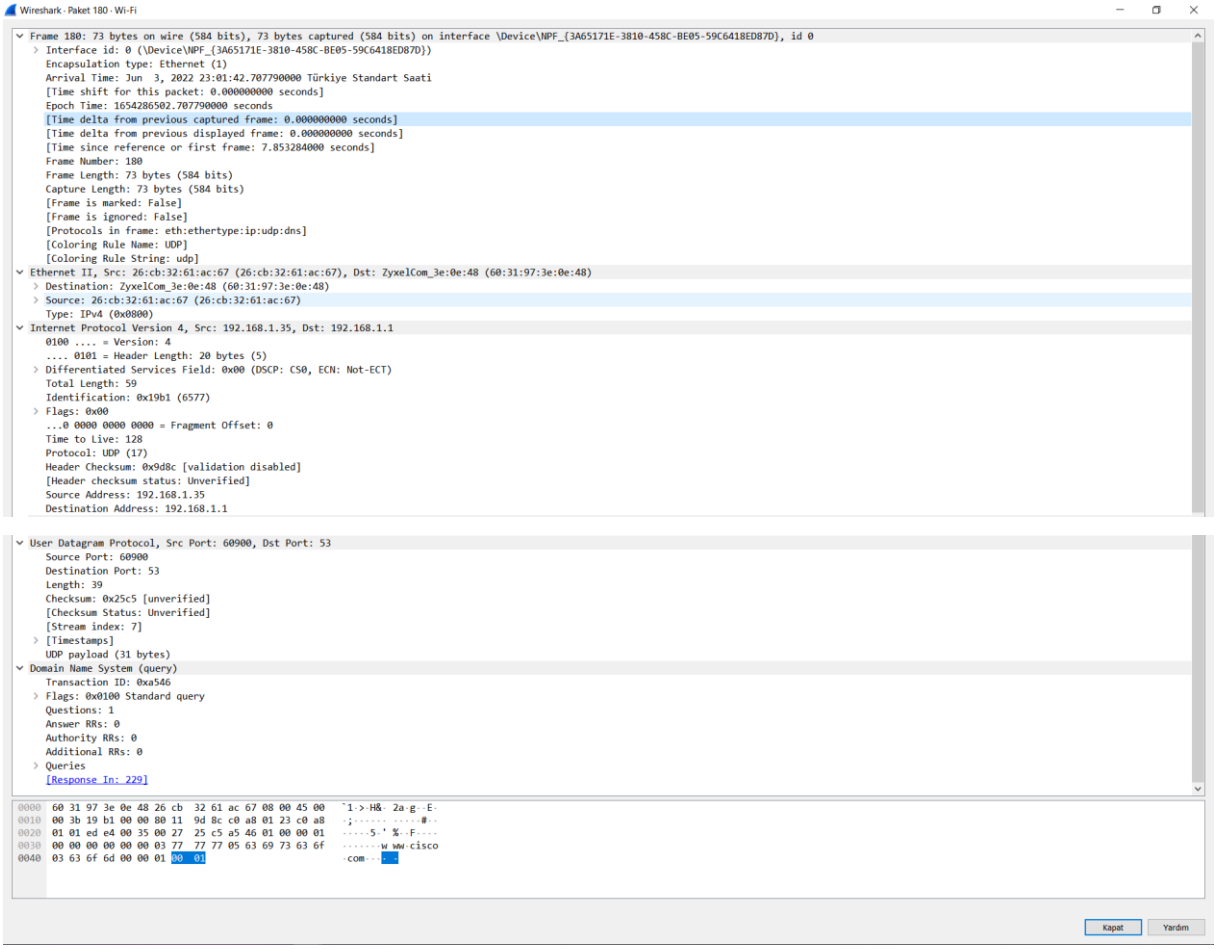
Sadece DNS içeren paketleri filtreleme



Cisco içeren DNS paketlerini filtreleme



5. DNS Paketindeki Veriler



Interface id: Yakalanan paketin hangi arayüzden geldiğini gösterir. Paket wi-fi arayüzünden yakalanmıştır.

```
Interface id: 0 (\Device\NPF_{3A65171E-3810-458C-BE05-59C6418ED87D})
    Interface name: \Device\NPF_{3A65171E-3810-458C-BE05-59C6418ED87D}
    Interface description: Wi-Fi
```

Encapsulation type: Yakalanan paketin enkapsülasyon tipi Ethernet'tir. Bu bilgi ile enkapsülasyon tipine yönelik saldırılar düzenlenebilir.

Arrival time: Yakalanan paketinin varış zamanını gösterir. Zamanı ay/ gün/ yıl/ saat/ dakika/ saniye/ salise olarak kaydeder. Doğru olması için sistem saati UTC'ye çevirmelidir.

Epoch time: Ocak 1 1970 tarihinden şu ana kadar geçen saniyelerin sayısını gösterir. Bu şekilde saatin yanlış olma ihtimali ortadan kalkar.

Frame Number: Yakalan paketin frame numarasını gösterir. Yakalanan paketin frame numarası 180'dir.

Frame Length: Yakalanan paketin toplam frame uzunluğunu gösterir. Frame uzunluğu 73 bayttır.

Capture Length: Yakalanan Frame uzunluğunu gösterir. 73 bayttır.

Ethernet II Destination: Paketin hedef MAC adresini gösterir.

Ethernet II Source: Paketin kaynak MAC adresini gösterir.

MAC adresi bilgileri ile MAC adresine özel ARP poisoning gibi saldırılar gerçekleştirilebilir.

```
Destination: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48)
    Address: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 26:cb:32:61:ac:67 (26:cb:32:61:ac:67)
    Address: 26:cb:32:61:ac:67 (26:cb:32:61:ac:67)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Type: Bir üst katmanda kullanılacak olan adresleme tipini gösterir.

Version: Yakalanan paketin kullandığı IP versiyonunu gösterir. IPv4 için 4, IPv6 için 6 olarak sabittir. Yakalanan paketin IPv4 kullanmaktadır.

Header Length: IPv4 başlığının boyutunu gösterir.

Differentiated Services Code Point: VoIP gibi farklılaştırılmış hizmetlerin kullanıldığına dair bilgiyi gösterir.

Explicit Congestion Notification: Ağ tıkanıklığının bildirilmesi için kullanılan bir alandır.

```
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)
```

Total Length: header ve data dahil toplam paket boyutunu gösterir.

```
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
```

Flags: IPv4 paketlerin fragment olarak gönderilmesini desteklemektedir. Bu yüzden Flags kısmında paketlerin fragment edilmesi ile ilgili bilgiler bulunmaktadır. IPS yazılımlarını çok yorup çökertmek için normalde 10 frame bölünmesi gereken bir paketin 1000 frame bölünmesi gibi saldırılar gerçekleşebilir. Bu duruma dikkat edilmesi gerekir. Bunun için IPv6 fragmantasyonu desteklememektedir.

Time to live (TTL): Gönderilen paketin yaşama süresidir. Pratikte atlama (hop) sayısını gösterir. TTL bilgisi her işletim sistemine göre değişir. Kullanılan cihazın işletim sisteminin Windows olduğu 128 TTL bilgisine bakılarak öğrenilebilir ve işletim sistemine özgü saldırılar gerçekleştirilebilir. Ek olarak TTL değeri değiştirilerek de saldırılar gerçekleştirilebilir.

Protokol: Verinin iletilmesinde kullanılan protokolü gösterir. DNS sorgularında kayıp paketler çok önemli olmadığı için UDP kullanılır.

Header checksum: IPv4 headerı için hata kontrolu için kullanılır.

Checksum değeri değiştirilerek saldırılar gerçekleştirilebilir. İçerigi normal olan bir paket bozuk checksum ile gönderilebilir. Bozuk checksum sonucu paket atılır ve sonra zararlı içerik ile doğru checksum paketi gönderilir. IPS cihazı double check yapmamak için içeriği control etmeden paketi geçirebilir.

Source Address: Kaynak IP adresidir.

Destination Address Hedef IP adresidir.IP adresine özgü bir çok saldırı mevcuttur. En basit örnek IP Spoofing saldırılarıdır.

Source Port: Kaynak port numarasıdır.

Destination Port: Hedef port numarasıdır. DNS port numarası 53'tür. DNS trafiği genelde izlenmediğinden 53. port içeriye saldırı gerçekleştirdikten sonra çıkmak için kullanılan kapı görevi görür.

Length: UDP datagram header ve verisinin uzunluğunu gösterir.

Checksum: Datagram header ve verilerin hata denetimi için kullanılır.

DNS Transaction ID: DNS sunucusuna bir sorguda bulunurken rastgele bir işlem ID gönderilir. Bu ID sayesinde istemci, aldığı yanıtı gönderdiği sorguyla eşleştirebilir.

Flags: 16 bitlik bir alandır ve bir çok parçaya ayrılmıştır her bir parça DNS sorgusuna dair farklı bir bilgi göstermektedir.

Question: Mesajın Question bölümündeki soru sayısını belirtir.

Answer RRs: Cevap kayıtlarının sayısını belirtir. sorgu mesajlarında 0 değerini alır. Bu incelenen pakette bir sorgu paketi olduğundan 0 değerindedir.

Authority RRs: Mesajın Authority bölümündeki kaynak kayıtlarının sayısını gösterir. Sorgu mesajlarında 0 değerine sahiptir.

Additional RRs: Çözümleyiciye yardımcı olmak amacıyla tutulan ek kayıtlar gösterir. Sorgu mesajlarında 0 değerine sahiptir.