



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),
```

```
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:

  0  1 ms    1 ms    <1 ms  192.168.1.1
  1  68 ms   87 ms   86 ms  212.156.201.20
  2  39 ms    9 ms    11 ms  81.212.77.33
  3  17 ms    45 ms   44 ms  81.212.218.102
  4  100 ms  117 ms  365 ms 81.212.210.104
  5  30 ms    36 ms    37 ms 212.156.108.190
  6  124 ms   18 ms    8 ms 212.156.64.46
  7  75 ms    87 ms   112 ms 212.154.96.70
  8  *        *        *      Request timed out.
  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:

  0  1 ms    2 ms    1 ms  192.168.1.1
  1  6 ms    6 ms    5 ms  212.156.201.20
  2  7 ms   15 ms    7 ms  81.212.77.33
  3  7 ms    6 ms    8 ms  81.212.218.102
  4  7 ms    7 ms    6 ms  81.212.210.104
  5  10 ms   7 ms    25 ms 81.212.217.5
  6  56 ms   56 ms   54 ms 212.156.101.126
  7  *        *        *      Request timed out.
  8  172 ms  181 ms  174 ms 4.69.208.229
  9  274 ms  318 ms  350 ms 4.59.34.66
 10  221 ms  260 ms  252 ms 128.107.2.5
 11  176 ms  185 ms  190 ms 72.163.0.102
 12  205 ms  172 ms  174 ms 72.163.0.190
 13  171 ms  175 ms  178 ms 72.163.3.2
 14 *        *        *      Request timed out.
 15 *        *        *      Request timed out.
 16  219 ms  235 ms  174 ms 72.163.4.129
 17  247 ms  225 ms  173 ms 72.163.4.185

Trace complete.
```

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.

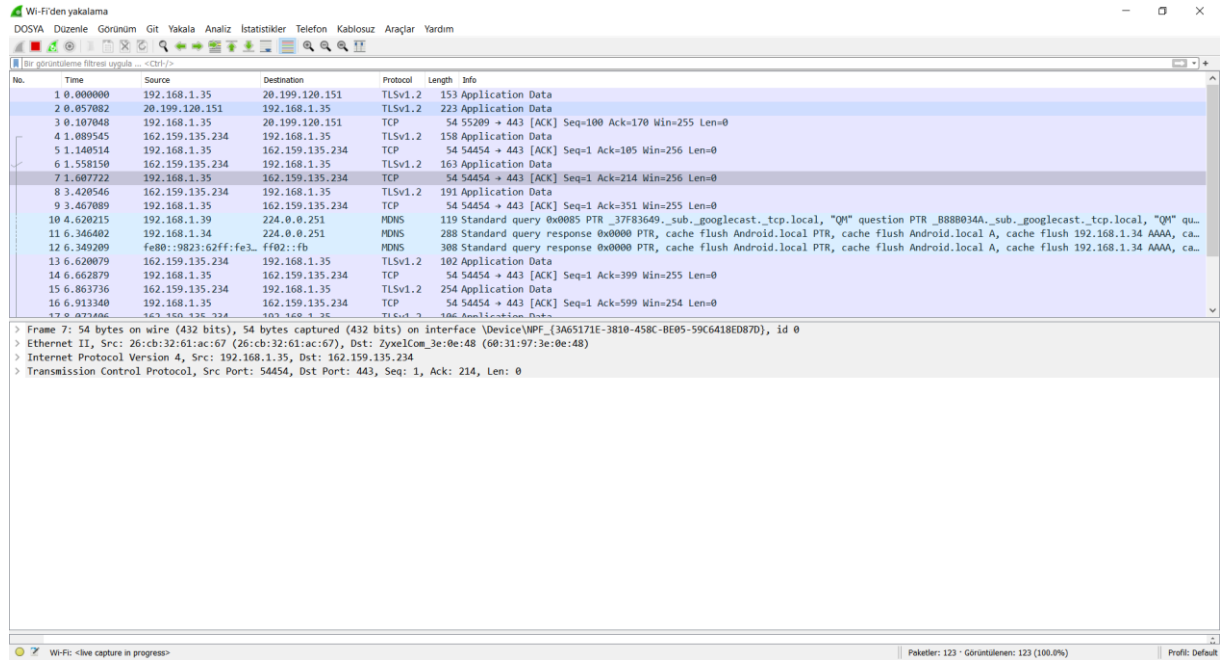
-d ile adres çözümlemesi kaldırılır.

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

18 atlama ile cisco.com sunucusuna ulaşılmıştır.

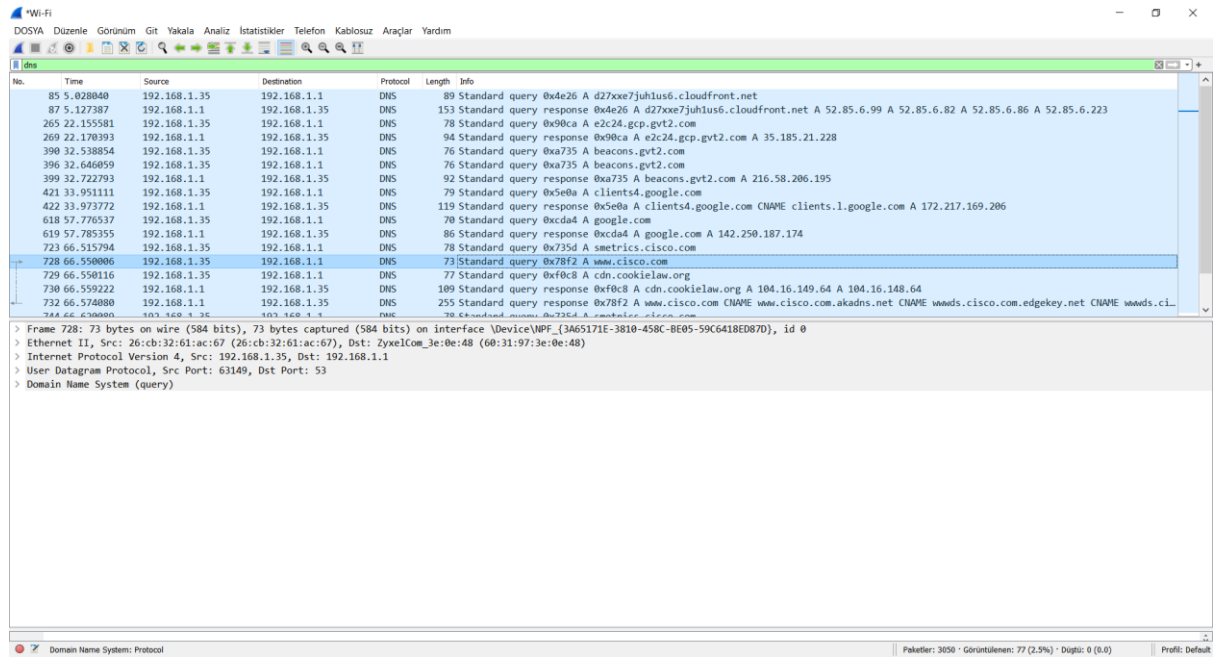
3. Wireshark

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



4. Filtreleme

Sadece DNS içeren paketleri filtreleme



Cisco içeren DNS paketlerini filtreleme

The screenshot displays two network analysis tools running on a Windows PC. The top window, titled 'lab_0dev pcapng', shows a list of network packets, primarily DNS queries and responses. The bottom window, titled 'lab_0dev pcapngs', provides a detailed view of a specific packet (No. 60), showing its hexadecimal and ASCII representations, and identifying it as a DNS query for 'www.cisco.com'.

Top Window: lab_0dev pcapng

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|--------------|--------------|----------|--------|---|
| 174 | 7.775252 | 192.168.1.35 | 192.168.1.1 | DNS | 80 | Standard query 0xa5f0 A cisco-tags.cisco.com |
| 177 | 7.813920 | 192.168.1.35 | 192.168.1.1 | DNS | 78 | Standard query 0xfce9 A smetrics.cisco.com |
| 180 | 7.853284 | 192.168.1.35 | 192.168.1.1 | DNS | 73 | Standard query 0xa546 A www.cisco.com |
| 187 | 7.883670 | 192.168.1.35 | 192.168.1.1 | DNS | 80 | Standard query 0xa5f0 A cisco-tags.cisco.com |
| 188 | 7.892991 | 192.168.1.1 | 192.168.1.35 | DNS | 96 | Standard query response 0xa5f0 A cisco-tags.cisco.com A 72.163.10.10 |
| 197 | 7.914216 | 192.168.1.35 | 192.168.1.1 | DNS | 78 | Standard query 0xfce9 A smetrics.cisco.com |
| 202 | 7.961268 | 192.168.1.35 | 192.168.1.1 | DNS | 73 | Standard query 0xa546 A www.cisco.com |
| 223 | 8.073196 | 192.168.1.1 | 192.168.1.35 | DNS | 167 | Standard query response 0xfce9 A smetrics.cisco.com CNAME cisco.com.ssl.sc.omtrdc.net A 15.188.95.229 A 13.36.218.177 A 15.236.1.1 |
| 229 | 8.130568 | 192.168.1.1 | 192.168.1.35 | DNS | 255 | Standard query response 0xa546 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.com |
| 1002 | 11.591483 | 192.168.1.35 | 192.168.1.1 | DNS | 86 | Standard query 0x7e7c A cdvps.cloudapps.cisco.com |
| 1003 | 11.593523 | 192.168.1.35 | 192.168.1.1 | DNS | 73 | Standard query 0x3fab A dsc.cisco.com |
| 1004 | 11.593523 | 192.168.1.35 | 192.168.1.1 | DNS | 85 | Standard query 0xabad A mktcs.cloudapps.cisco.com |
| 1002 | 11.596267 | 192.168.1.35 | 192.168.1.1 | DNS | 86 | Standard query 0x7e7c A cdvps.cloudapps.cisco.com |
| 1003 | 11.686267 | 192.168.1.35 | 192.168.1.1 | DNS | 73 | Standard query 0x3fab A dsc.cisco.com |
| 1004 | 11.686270 | 192.168.1.35 | 192.168.1.1 | DNS | 85 | Standard query 0xabad A mktcs.cloudapps.cisco.com |
| 1226 | 11.989905 | 192.168.1.1 | 192.168.1.35 | DNS | 166 | Standard query response 0x3fab A dsc.cisco.com CNAME cisco-dsc-prod.apigee.net CNAME rgwlr001-0-routers.dn.apigee.net A 35.1.1.1 |
| 1458 | 12.337525 | 192.168.1.1 | 192.168.1.35 | DNS | 136 | Standard query response 0xabad A mktcs.cloudapps.cisco.com CNAME mktcs-cloudapps.xgbl.cisco.com A 72.163.15.141 |
| 1486 | 12.393444 | 192.168.1.1 | 192.168.1.35 | DNS | 138 | Standard query response 0x7e7c A cdvps.cloudapps.cisco.com CNAME cdvps-cloudapps.xgbl.cisco.com A 173.36.127.32 |
| 4641 | 16.441542 | 192.168.1.35 | 192.168.1.1 | DNS | 78 | Standard query 0xb467 A mcc-tags.cisco.com |
| 4674 | 16.547625 | 192.168.1.35 | 192.168.1.1 | DNS | 78 | Standard query 0xb467 A mcc-tags.cisco.com |
| 5039 | 17.558303 | 192.168.1.35 | 192.168.1.1 | DNS | 78 | Standard query 0xb467 A mcc-tags.cisco.com |
| 5569 | 19.571732 | 192.168.1.35 | 192.168.1.1 | DNS | 78 | Standard query 0xb467 A mcc-tags.cisco.com |
| 5588 | 19.750510 | 192.168.1.1 | 192.168.1.35 | DNS | 94 | Standard query response 0xb467 A mcc-tags.cisco.com A 72.163.10.15 |

Bottom Window: lab_0dev pcapngs

> Frame 180: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF{3A65171E-3810-458C-8E05-59C6418ED07D}, id 0
 > Ethernet II, Src: 26:cb:32:61:ac:67 (26:cb:32:61:ac:67), Dst: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48)
 > Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1
 > User Datagram Protocol, Src Port: 60900, Dst Port: 53
 > Domain Name System (query)

```

0000  60 31 97 3e 0e 48 26 cb 32 61 ac 67 08 00 45 00  "1->Hb. 2a g.-E-
0010  00 3b 19 b1 00 00 80 11 9d 8c a0 c8 01 23 c0 a8  :.....:##-
0020  01 01 ed e4 00 35 20 27 25 c5 a5 46 01 00 00 01  :....S.%-F....
0030  .....w.w.cisco
0040  35 53 6f 0d 00 00 01 00 01                      .com.
  
```

Paketler: 5651 - Gösterilenler: 23 (0.4%)

5. DNS Paketindeki Veriler

Wireshark - Paket 180 - Wi-Fi

- > Frame 180: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{3A65171E-3B10-45BC-BE05-59C6418ED87D}, id 0
 - > Interface id: 0 (\Device\NPF_{3A65171E-3B10-45BC-BE05-59C6418ED87D})
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Jun 3, 2022 23:01:42.707790000 Türkiye Standart Saati
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1654286502.707790000 seconds
 - [Time delta from previous captured frame: 0.000000000 seconds]
 - [Time delta from previous displayed frame: 0.000000000 seconds]
 - [Time since reference or first frame: 7.853284000 seconds]
 - Frame Number: 180
 - Frame Length: 73 bytes (584 bits)
 - Capture Length: 73 bytes (584 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: 26:cb:32:61:ac:67 (26:cb:32:61:ac:67), Dst: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48)
 - > Destination: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48)
 - > Source: 26:cb:32:61:ac:67 (26:cb:32:61:ac:67)
 - Type: IPv4 (0x0800)
 - > Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 59
 - Identification: 0xi9b1 (6577)
 - > Flags: 0x00
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 128
 - Protocol: UDP (17)
 - Header Checksum: 0x9d8c [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.35
 - Destination Address: 192.168.1.1
- > User Datagram Protocol, Src Port: 60900, Dst Port: 53
 - Source Port: 60900
 - Destination Port: 53
 - Length: 39
 - Checksum: 0x25c5 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 7]
 - > [Timestamps]
 - UDP payload (31 bytes)
- > Domain Name System (query)
 - Transaction ID: 0xa546
 - > Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - > Queries
 - [Response In: 229]

| No. | Time | Source | Destination | Ethernet II | Internet Protocol Version 4 | User Datagram Protocol | Domain Name System |
|------|---|--------------|-------------|--|---|------------------------------------|---|
| 0000 | 60.31.97.3e.0e.48.26.cb.32.61.ac.67.08.00.45.00 | 192.168.1.35 | 192.168.1.1 | Ethernet II, Src: Realtek USB-WiFi (26:cb:32:61:ac:67), Dst: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48) | IPv4, Src: 192.168.1.35, Dst: 192.168.1.1 | UDP, Src Port: 60900, Dst Port: 53 | DNS Query Standard query transaction 0xa546 |
| 0010 | 00.3b.19.b1.00.00.80.11.9d.8c.c0.a8.01.23.c0.a8 | 192.168.1.35 | 192.168.1.1 | Ethernet II, Src: Realtek USB-WiFi (26:cb:32:61:ac:67), Dst: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48) | IPv4, Src: 192.168.1.35, Dst: 192.168.1.1 | UDP, Src Port: 60900, Dst Port: 53 | DNS Query Standard query transaction 0xa546 |
| 0020 | 01.01.ed.e4.00.35.00.27.25.c5.a5.46.01.00.00.01 | 192.168.1.35 | 192.168.1.1 | Ethernet II, Src: Realtek USB-WiFi (26:cb:32:61:ac:67), Dst: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48) | IPv4, Src: 192.168.1.35, Dst: 192.168.1.1 | UDP, Src Port: 60900, Dst Port: 53 | DNS Query Standard query transaction 0xa546 |
| 0030 | 00.00.00.00.00.00.03.77.77.05.63.69.73.63.6f | 192.168.1.35 | 192.168.1.1 | Ethernet II, Src: Realtek USB-WiFi (26:cb:32:61:ac:67), Dst: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48) | IPv4, Src: 192.168.1.35, Dst: 192.168.1.1 | UDP, Src Port: 60900, Dst Port: 53 | DNS Query Standard query transaction 0xa546 |
| 0040 | 03.63.6f.6d.00.00.01.20.01 | 192.168.1.35 | 192.168.1.1 | Ethernet II, Src: Realtek USB-WiFi (26:cb:32:61:ac:67), Dst: ZyxelCom_3e:0e:48 (60:31:97:3e:0e:48) | IPv4, Src: 192.168.1.35, Dst: 192.168.1.1 | UDP, Src Port: 60900, Dst Port: 53 | DNS Query Standard query transaction 0xa546 |

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: Yakalanan 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 headeri için hata kontrolü için kullanılır.

Checksum değeri değiştirilerek saldırılar gerçekleştirilebilir. İçeriği 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 kontrol 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.