GAZİ ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ - BİLGİSAYAR MÜHENDİSLİĞİ

171180010 – Cansu AYTEN

BM402 BİLGİSAYAR AĞLARI

LAB ÖDEVİ

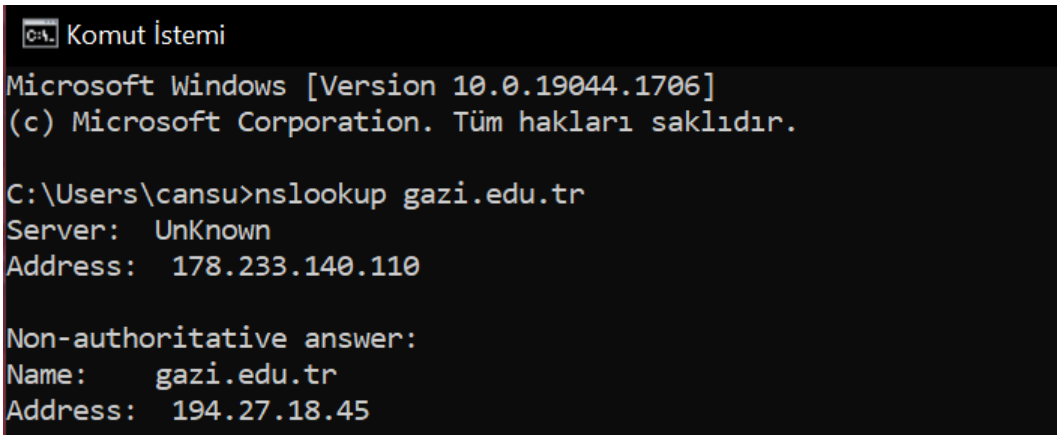
M. ALİ AKÇAYOL

DERS ASİSTANI: YASİN İNAĞ

İÇİNDEKİLER

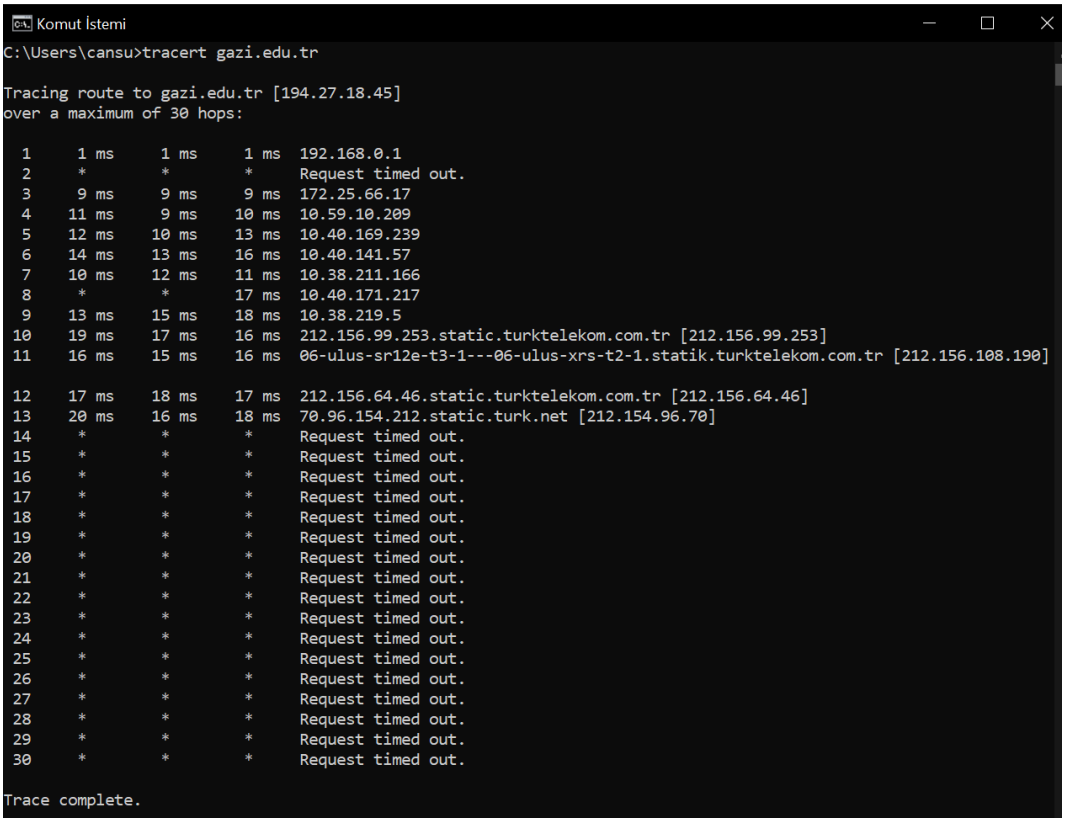
Sayfa

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



Şekil 1: nslookup komutu

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



Şekil 2:tracert gazi.edu.tr

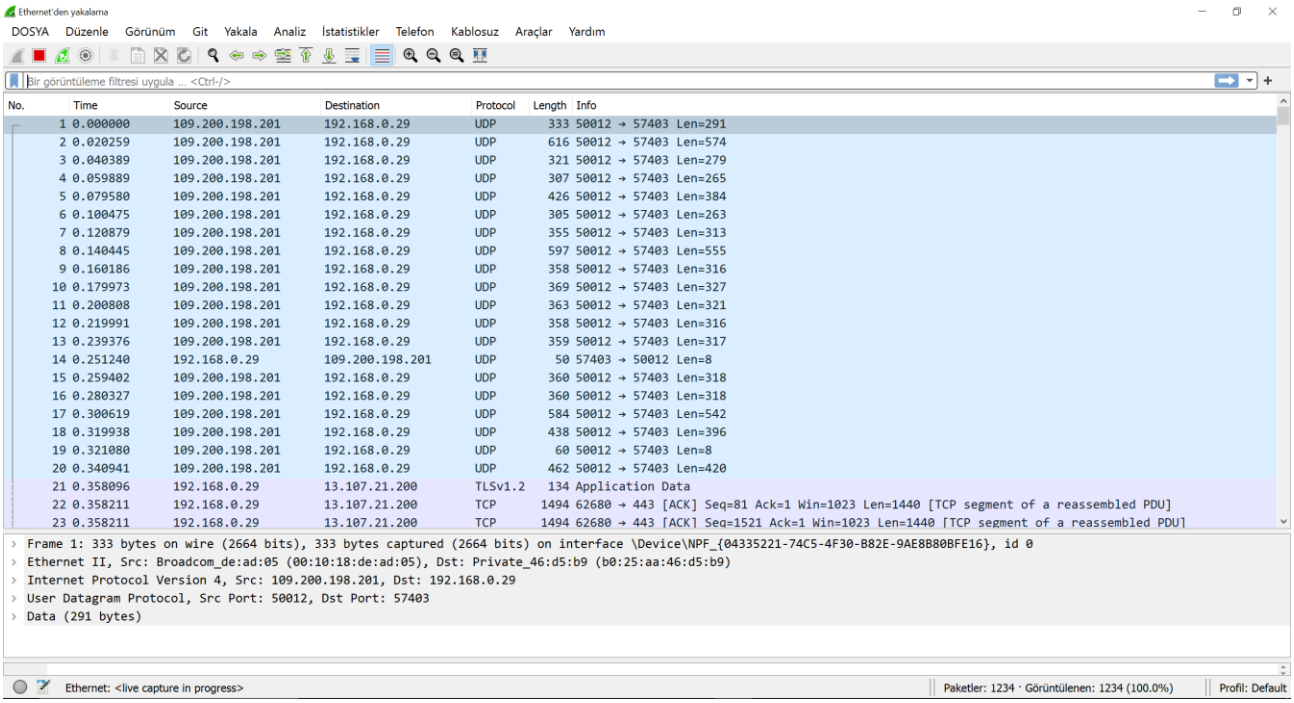
Kaynaktan hedefe giderken geçilen ara cihazların toplam sayısına atlama sayısı denir. tracert gazi.edu.tr komutu ile gazi.edu.tr adresine bağlanılmaya çalışılmıştır ama adrese ulaşılamamıştır. Bu nedenle başka bir adrese deneme yapılmıştır. tracert stackoverflow.com denendiğinde geçilen ara cihazlar 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

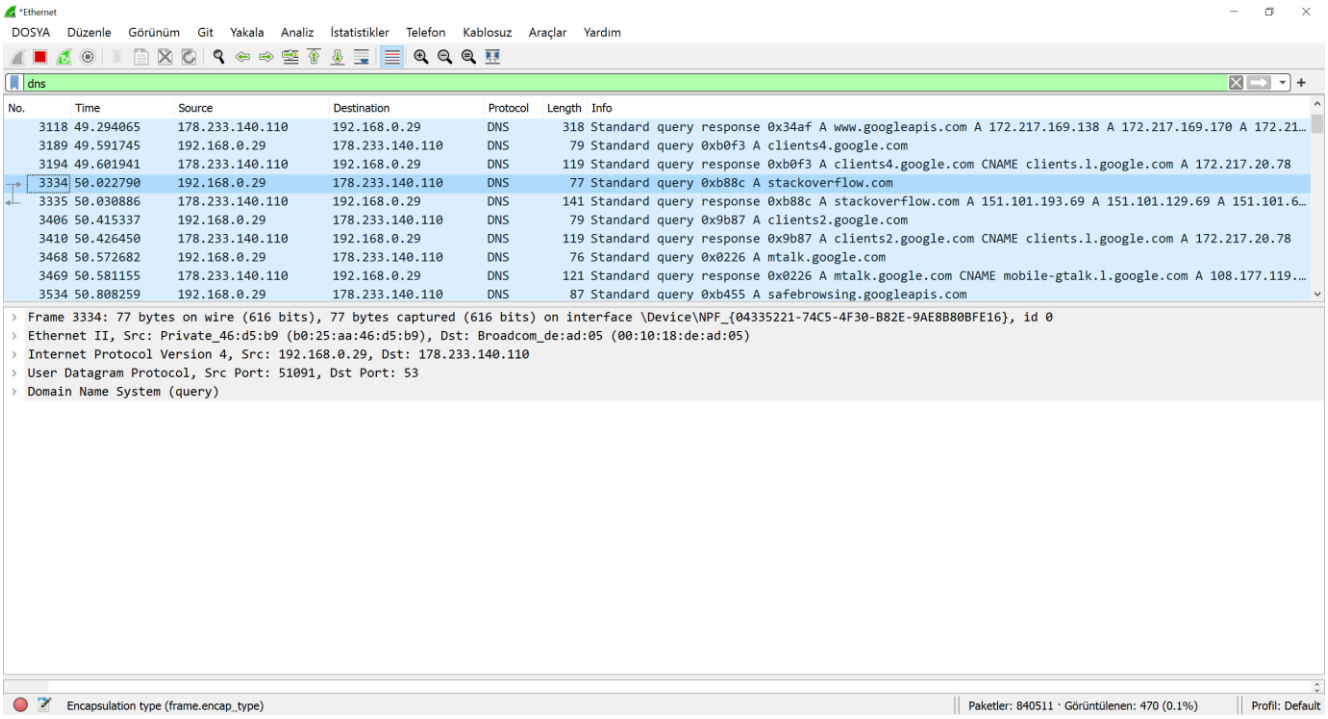
3. Tarayıcıdan Bir Web Sitesine Erişim ve Wireshark ile Paketlerin Yakalanması

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



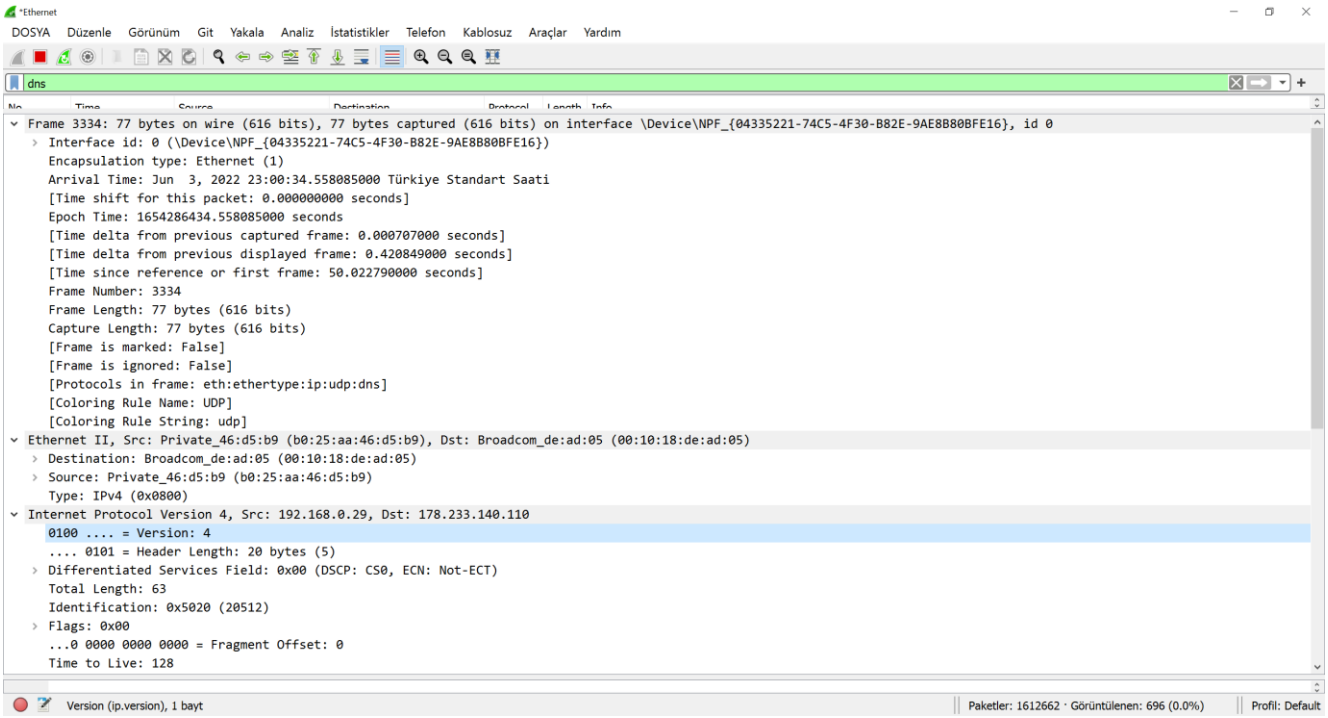
Şekil 4: Wireshark paket yakalama

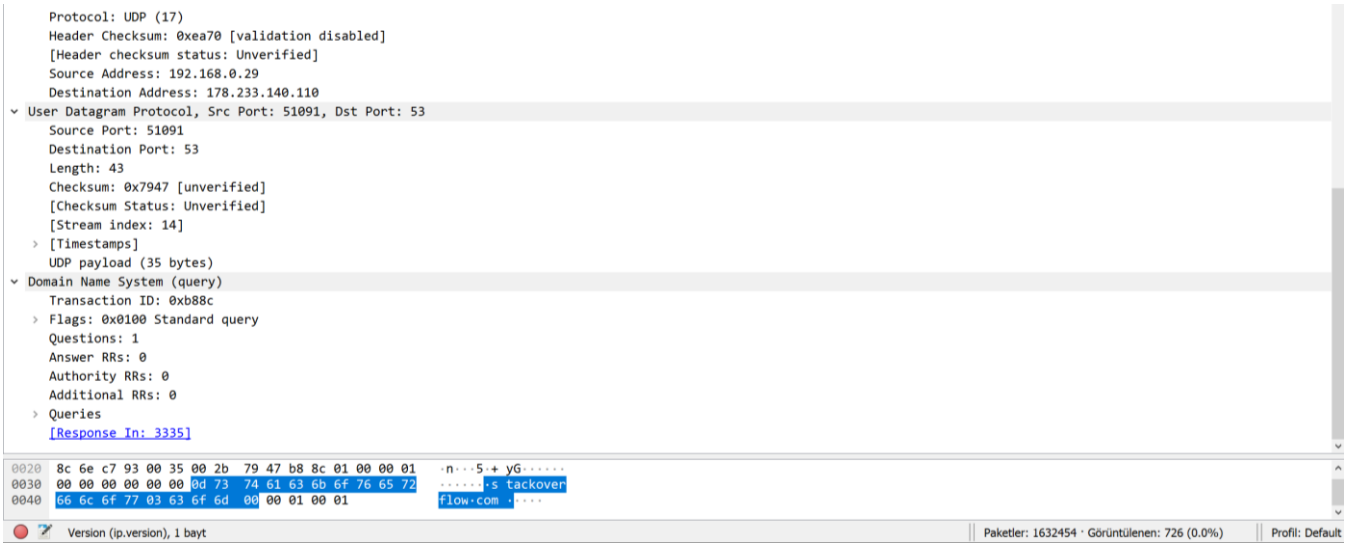
4. Yakalanan Paketlerin DNS Paketleri Olacak Şekilde Filtrelenmesi



Şekil 5: DNS paketleri şeklinde filtreleme

5. Yakalan DNS Paketinde Tespit Edilen Veriler ve Açıklamaları





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 parçalanan 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 kullanmalıdır. 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.