Barış Erkut 20401871

Bilgisayar Ağları LAB-3

1- İlk request'te source ip 192.168.1.9, benim ip adresim anlamına geliyor.

```
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 212.252.126.73
```

2- Protokol değeri 1'dir ICMP anlamına geliyor.

```
Protocol: ICMP (1)
```

3- IP başlığı 20 byte görünüyor

```
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 212.252.126.73
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

Toplam uzunluktan başlık değerini çıkararak payload'ı hesaplıyorum.

56-20= 36byte

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
```

4- Fragment Offset değeri 0'dan farklı olmadığı için paket parçalanmamış olarak yorumladım. Ayrıca parçalanmayı indike eden Flag bitleri de 0 değerine sahip.

```
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
```

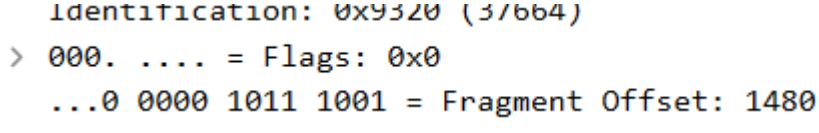
5- **Tüm traceroute aramalarında sabit kalan** alanlardan ikisi kaynak ve hedef IP adresleri , ayrıca protocol da her zaman sabit (ICMP)

Değişmek zorunda olan kısımlar ise en önemli olarak TTL değerleri, paketler sıra sıra gönderiliyor anlamına geliyor. Identification kısımları da her bir sorgu için değişiklik gösteriyor.

```
Identification: 0x92eb (37611)
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset
> Time to Live: 3
```

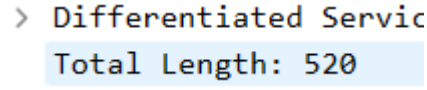
6- Önceki soruda cevapladığım gibi bu 2 kısım sürekli değişmek zorunda, identification her bir sorgunun özel olduğunu gösteriyor ve TTL kısmı ise her sorguda artarak ilerliyor sayı sayar gibi. Böylelikle her bir paketin bir sonraki ağa ulaşması sağlanıyor.

7- Evet 2000 değerine çevirdikten sonra çıkan ilk request sorgusundaki paket birden fazla parçaya ayrılmıştır. Değerleri değiştirdikten sonra ilk hangi isteği gönderdiğimi paket uzunluklarına bakarak anladım. 56 değerinden daha yüksek bir değere geçiş yapan sorguyu aldım. Datagramın parçalandığını ise



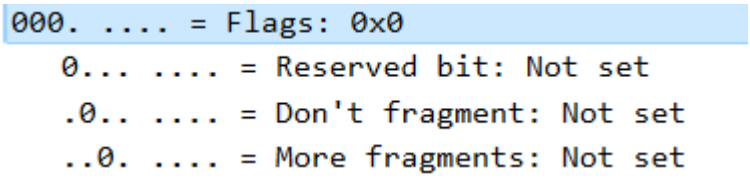
buradaki fragment offset değerinin 0'dan farklı olduğunu gördüğüm için anlıyorum. Eğer 0 olsaydı bu parçanın ilk parça olduğunu gösterirdi.

Datagramın toplam uzunluğunu ise IP kısmında görebiliyorum. 520 değeri



okunuyor.

8- Flags kısımlarında parçalanıp parçalanmadığını indike eden MF ve DF bitlerinde More fragments anlamına gelen bir göstergesi olan bir datagram bulamadım. Bunun sebebi trace dosyasını ilk oluştururken yapmış olabileceğim bir hata olabilir, eğer hatalı bir işlem yapmadıysam MF kısmının 0 olması bana son parça olduğunu bu datagramda daha fazla olan parça olmadığını gösteriyor.



9- 3500 e geçtikten sonra datagramlar 3 parçaya bölünmüş, bunu MF (more fragments biti) değeri 1 olan 2 adet paketi ve devamında MF değeri 0 olan paketten anlıyorum. İlk 2 si (mf değerinin 1 olması) daha devamı olduğunu gösteriyor ve 0'a gelince son parçaya geldiğimi anlıyorum. Üç parçanın toplam uzunluğu 3500 byte a ulaşıyor.

10- Önceki soruda belirttiğim gibi MF biti değişimi gerçekleşiyor.

Aynı zamanda Fragment Offset değeri de orijinal datagramın hangi kısımlarını taşıdığını gösterecek şekilde her bir sorguda farklı değer alabiliyor.
Identification kısmı ise her sorguda olduğu gibi bu sorgularda da farklı değerler gösteriyor.