

# Laboratuvar Raporu 5

# Eskişehir Osmangazi Üniversitesi Bilgisayar Ağları 152116028

Şevval Ayça Çerence 152120211128

Dr. Öğr. Üyesi İlker Özçelik 2024-2025

1. İçindekiler2
2. Giriş
3. Sorular
3.13
3.23
3.34
3.44
3.54
3.65
3.75
3.86
3.96
3.107
3.117
3.128
3.138
3.148
3.159
4.Kaynakça10

# 2. Giriş

#### 3.Sorular

#### 3.1

```
192.168.232.212 224.0.0.251
fe80::a80a:d0ff:fef... ff02::fb
ff02::16
                                                                                                                                                                                                                                                                                                                                        70 Echo (ping) request id=0x0001, seq=2/512, ttl=255 (reply in 143)
                                                                                           192.168.237.106 142.251.140.78
                                                                                                                                                                                                                                                                                                                             98 Time-to-live exceeded (Time to live exceeded intensit)
126 Standard query 0x0000 ANY Android-10.local, "QN" question ANY Android-10.local, "QN" (146 Standard query 0x0000 ANY Android-10.local, "QN" question ANY Android-10.local, "QN" (79 Etcho (ping) request id-0x0001, seq-4/1024, ttl=2 (no response found!)
78 Etcho (ping) reply id-0x0001, seq-2/512, ttl=54 (request in 136)
78 Etcho (ping) reply id-0x0001, seq-2/512, ttl=54 (request in 136)
78 Etcho (ping) reply id-0x0001, seq-2/512, ttl=54 (request in 136)
78 Etcho (ping) reply id-0x0001, seq-2/512, ttl=54 (request in 136)
78 Etcho (ping) reply id-0x0001, seq-2/512, ttl=54 (request in 136)
78 Etcho (ping) reply id-0x0001, seq-2/512, ttl=54 (request in 136)
78 Etcho (ping) reply id-0x0000 PTR 1.224.168.192.in-addr.arpa
143 Standard query 0x0000 PTR 1.224.168.192.in-addr.arpa, "QN" question
165 Standard query 0x0000 PTR 1.224.168.192.in-addr.arpa, "QN" question
78 Time-to-live exceeded (Time to live exceeded in transit)
87 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
142 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
143 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
144 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
157 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
168 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
169 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
170 Standard query 0x4a74 PTR 33.128.140.193.in-addr.arpa
                                                                                                                                                                                                                                                                                                                                       98 Time-to-live exceeded (Time to live exceeded in transit)
                                                                                             192.168.224.1
                                                                                                                                                                                       192.168.237.106
                 138 5.403923
                   139 5.424782
                                                                                                fe80::d826:89ef:887... ff02::fb
                140 5.425297
                                                                                               142.251.140.78
192.168.237.106
192.168.237.106
193.140.128.28
192.168.237.106
                143 5.440724
144 5.467393
145 5.472469
146 5.476491
147 5.476891
                                                                                                                                                                                           192.168.237.106
224.0.0.251
                   148 5.477147
                                                                                             fe80::fbe5:5554:2ee... ff02::fb
95.183.254.245 192.168.
                                                                                                                                                                                          192.168.237.106
                150 5.489401
151 5.491988
                                                                                           192.168.237.106
193.140.128.28
                                                                                                                                                                                       193.140.128.28
192.168.237.106
Frame 136: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_(dFC459ED-E400-4993-A33A-3A2168C6AE4C), id 0
Ethernet II, Src: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29), Dst: PaloAltoNetw_83:49:12 (68:15:2b:83:49:12)
               ternet Protocol Version 4, Src: 192.168.237.106, Dst: 142.251.0
8100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x06d0 (1744)
000. ... = Flags: 0x0
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0xeb97 [validation disabled]
[Header checksum status: Unverlided]
Source Address: 192.168.237.106
Destination Address: 142.251.140.78
[Stream index: 39]
     [Stream index: 39]
Internet Control Message Protocol
```

Wireshark ortamında incelenen ilk ICMP Echo Request segmenti temel alınarak, Internet Protocol başlığı altında yer alan Source (Kaynak) IP adresi bilgisayarımın ağ üzerindeki adresini göstermektedir. Bu alan incelendiğinde, bilgisayarıma ait IP adresinin 192.168.237.106 olduğu tespit edilmiştir. İlgili adres, ekran görüntüsünde açıkça görülebilmektedir.

#### 3.2

```
Frame 136: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interfa
Ethernet II, Src: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29), Dst: PaloAltoNetw_
Internet Protocol Version 4, Src: 192.168.237.106, Dst: 142.251.140.78
  0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x06d0 (1744)
▶ 000. .... = Flags: 0x0
   ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0xeb97 [validation disabled]
   [Header checksum status: Unverified]
  Source Address: 192.168.237.106
  Destination Address: 142.251.140.78
   [Stream index: 39]
Internet Control Message Protocol
```

İncelenen paketin Internet Protocol başlığı altındaki Protocol alanında, protokol türü olarak ICMP (1) değeri yer almaktadır. ICMP (Internet Control Message Protocol), IP temelli ağlarda iletişimin doğruluğunu ve verimliliğini artırmak amacıyla kullanılan yardımcı bir protokoldür. Temel işlevi, ağ üzerinde meydana gelen bağlantı sorunlarını bildirmek, hataları tanımlamak ve bu sayede iletişimdeki olası aksaklıkların önüne geçmektir. Bu protokol sayesinde ağ yöneticileri, ağ trafiğini daha etkin biçimde izleyebilir, arıza veya performans sorunlarını teşhis edebilir ve ağ altyapısını daha sağlıklı bir şekilde yönetebilir.

#### 3.3

İlgili ekran görüntüsünde, IP başlığının (IP header) boyutu 20 bayt olarak belirtilmiş, Total Length alanı ise 56 bayt değerini göstermektedir. Bu bilgiler doğrultusunda, IP paketinin taşıdığı asıl veri kısmı olan payload (yük) miktarını hesaplamak mümkündür. Toplam uzunluktan başlık boyutu çıkarıldığında: 56 - 20 = 36 bayt sonucuna ulaşılır. Dolayısıyla, bu paketin taşıdığı veri yükü 36 bayt olarak belirlenmiştir.

#### 3.4

İncelenen IP datagramının Fragmentation Flags alanı değerlendirildiğinde, ilgili flag'in 0 değerine ayarlanmış olduğu görülmektedir. Bu durum, söz konusu datagramın parçalanmadan (fragmentation olmaksızın) iletildiğini göstermektedir. Eğer bu alan 1 değerini almış olsaydı, bu durumda paketin birden fazla parçaya bölündüğü, yani fragmented bir iletim gerçekleştiği yorumu yapılabilirdi.

#### 3.5

```
Frame 141: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C}, id 0

Ethernet II, Src: LiteonTechno_a4:48:29 (9c:2f:3d:a4:48:29), Dst: PaloAltoNetw_03:49:12 (60:15:2b:03:49:12)

Internet Protocol Version 4, Src: 192.168.237.106, Dst: 142.251.140.78

0100 ... = Version: 4

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

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

Total Length: 56

Identification: 0x086d2 (1746)

000. ... = Flags: 0x0

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

Time to live: 2

Protocol: ICMP (1)

Header Checksum: 0xe896 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.237.106

Destination Address: 142.251.140.78

[Stream index: 39]

Internet Control Message Protocol
```

Time to Live, Header checksum ve Identification alanları daima değişmektedir.

#### 3.6

5.soruya ait ekran görüntüleri incelendiğinde, Source (kaynak) ve Destination (hedef) IP adreslerinin, IP versiyonu ile birlikte header (başlık) boyutunun sabit kaldığı görülmektedir. Buna karşılık, Time to Live (TTL), Header Checksum ve Identification alanlarının her pakette değişkenlik gösterdiği tespit edilmiştir.

TTL, bir IP paketinin ağdaki ömrünü tanımlar; her yönlendiriciden geçişte bu değer bir azaltılır ve sıfıra ulaştığında paket düşürülür. Bu mekanizma, ağda sonsuz döngülerin oluşmasını engeller. Header Checksum ise, IP başlığındaki bilgilerin bütünlüğünü doğrulamak amacıyla kullanılır. TTL veya Identification gibi başlıktaki herhangi bir değişiklik, checksum değerinin de yeniden hesaplanmasına neden olur. Identification alanı ise, paketlerin parçalanması durumunda, her bir parçaya aynı kimlik numarasını vererek bunların hedefte doğru şekilde yeniden birleştirilmesini sağlar.

Sonuç olarak, bu üç alanın dinamik yapısı, IP protokolünün hem güvenli hem de hatasız bir veri iletimini sürdürebilmesi açısından kritik bir rol oynamaktadır.

#### 3.7

5.soruya ait ekran görüntüleri incelendiğinde, Identification alanındaki değerlerin her pakette bir önceki değerden tam olarak 1 fazla olduğu dikkat çekmektedir. Bu durum, her IP paketine artan sıra numarasıyla benzersiz bir kimlik atandığını ve paketlerin sıralı olarak oluşturulduğunu göstermektedir. Bu sistem, özellikle parçalanma durumunda paketlerin doğru şekilde birleştirilmesine yardımcı olurken, aynı zamanda paket takibini ve analizini de kolaylaştırmaktadır.

```
3525 83.052353
                         142.251.243.221
                                                    192.168.237.106
                                                                                             110 Time-to-live exceeded (Time to live exc
                                                                                                   Time-to-live exceeded
  3579 84.961879
                          193.140.128.33
                                                      192.168.237.106
                                                                                              590 Time-to-live exceeded (Time to live
                                                                                             70 Time-to-live exceeded (Time to live ex 590 Time-to-live exceeded (Time to live ex 70 Time-to-live exceeded (Time to live ex
  3582 84.974158
                          95.183.254.245
                                                     192.168.237.106
                                                                                ICMP
  3598 85.201990
                          212.154.96.69
                                                     192.168.237.106
                                                                                ICMP
  3599 85.203494
                          95.183.254.253
                                                     192.168.237.106
                                                                                ICMP
                                                                                             170 Time-to-live exceeded (Time to live 170 Time-to-live exceeded (Time to live
                          212.156.64.45
                                                     192.168.237.106
  3600 85.210069
                                                                                ICMP
                                                                                                                                                ex
                          81.212.222.209
                                                                                ICMP
  3601 85.211317
                                                     192.168.237.106
                                                                                                                               (Time to live
  3613 85.375275
                          212.156.104.152
                                                     192.168.237.106
                                                                                ICMP
                                                                                             170 Time-to-live exceeded
                                                                                                                               (Time to live
(Time to live
                                                     192.168.237.106
  3614 85.414955
                          74.125.51.44
                                                                                ICMP
                                                                                             110 Time-to-live exceeded
  3634 85.906814
                          142.251.243.221
                                                     192.168.237.106
                                                                                ICMP
                                                                                             110 Time-to-live exceeded
                          192.168.224.1
193.140.128.33
                                                                                             106 Time-to-live exceeded (Time to live ex
  3763 87.379977
                                                     192.168.237.106
                                                                                TCMP
  3786 87,426276
                                                                                ICMP
                                                                                             590 Time-to-live exceeded (Time to live ex
                                                     192.168.237.106
                                                                                              70 Time-to-live exceeded (Time to live ex
70 Time-to-live exceeded (Time to live ex
  3790 87.478934
                          95.183.254.245
                                                     192.168.237.106
                                                                                ICMP
  3808 87.543648
                          95.183.254.253
                                                                                ICMP
                                                     192.168.237.106
                                                                                             590 Time-to-live exceeded (Time to live ex. 170 Time-to-live exceeded (Time to live ex. 170 Time-to-live exceeded (Time to live ex.
                                                     192.168.237.106
  3814 87.594859
                          212.154.96.69
                                                                                ICMP
  3821 87.653595
                          212.156.64.45
                                                     192.168.237.106
                                                                                ICMP
  3825 87.704395
                          81.212.222.209
                                                     192.168.237.106
                                                                                ICMP
  3841 87.864662
                          212.156.104.152
                                                                                ICMP
                                                                                             170 Time-to-live exceeded (Time to live ex 110 Time-to-live exceeded (Time to live ex
                                                     192.168.237.106
  3849 87.916637
                          74.125.51.44
                                                     192.168.237.106
                                                                                ICMP
  3853 87.965543
                          142.251.243.221
                                                     192.168.237.106
                                                                                ICMP
                                                                                             110 Time-to-live exceeded
                                                                                                                               (Time to live ex
  4032 89.875571
                          192.168.224.1
                                                     192.168.237.106
                                                                                             106 Time-to-live exceeded
                                                                                                                               (Time to live ex
                                                                                ICMP
  4036 89.925931
                          193.140.128.33
                                                     192.168.237.106
                                                                                ICMP
                                                                                             590 Time-to-live exceeded
                                                                                ICMP
  4047 89.977555
                         95.183.254.245
                                                     192,168,237,106
                                                                                              70 Time-to-live exceeded (Time to live ex
Frame 3577: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{0FC459ED-E4DD-499
Ethernet II, Src: PaloAltoNetw_03:49:12 (60:15:2b:03:49:12), Dst: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29)
Internet Protocol Version 4, Src: 192.168.224.1, Dst: 192.168.237.106
   0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
   Identification: 0xcc17 (52247)
   000. .... = Flags: 0x0 ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x5fcc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.224.1
    Destination Address: 192.168.237.106
```

Identification değeri 0xcc17 (52247), TTL değeri ise 64 olarak görülmüştür.

#### 3.9

İlgili ekran görüntüleri değerlendirildiğinde, Identification alanının her pakette değiştiği gözlemlenirken, Time to Live (TTL) alanında herhangi bir değişiklik olmadığı görülmektedir. Bu durumu, ICMP protokolünün doğası açıklamaktadır. ICMP TTL-exceeded mesajları, bir IP paketinin TTL değeri sıfıra ulaştığında oluşturulan ve paketin hedefe ulaşamadan ağda "tükendiğini" bildiren yanıt mesajlarıdır. Bu tür ICMP yanıtlarında, gönderilen mesajın TTL değeri sabit kalmakta, çünkü bu mesajlar IP protokolüne özgü bir bildirim niteliğindedir ve genellikle kaynak paketin özelliklerini yansıtacak şekilde yapılandırılır.

Buna karşın, Identification alanı parçalanma ya da yeniden birleştirme işlemi gerektirmeyen ICMP mesajlarında çoğu zaman sabit kalır veya değişkenlik göstermeyebilir. Ancak bazı durumlarda sistem, her paket için yine de farklı Identification değerleri atayabilir. Bu nedenle, TTL sabitken Identification alanında değişim gözlemlenmesi olağandır ve paket işleme sürecinin bir parçası olarak değerlendirilmelidir.

Bu bölümde, zip dosyasında yer alan ilgili izleme (trace) dosyası kullanılarak analiz gerçekleştirilmiştir. Yapılan incelemede, ilk 2000 bayt veriyi içeren bir ICMP Echo (Ping) Request paketi tespit edilmiştir. Bu paketin boyutu, tek bir IP paketine sığamayacak kadar büyük olduğundan dolayı, IP protokolü tarafından parçalara (fragments) ayrılmış şekilde iletilmiştir. Analiz sonucunda, IPv4 Fragments altında bu pakete ait 2 ayrı fragment bulunduğu görülmüştür. Bu durum, IP protokolünün büyük veri paketlerini daha küçük parçalara bölerek iletim sırasında ağ uyumluluğunu sağlamaya yönelik işleyişini açıkça göstermektedir.

#### 3.11

İncelenen fragment'lardan birinde, "More Fragments" (MF) bayrağının 1 değerine ayarlandığı görülmektedir. Bu durum, söz konusu paketin ardından başka bir fragmentin daha geleceğini ifade eder; yani paket henüz tamamlanmamıştır. Ayrıca, datagramın toplam boyutu ilgili alanda 1972 bayt olarak belirtilmiştir ve bu değer ekran görüntüsünde de açıkça gösterilmektedir. Bu boyut, IP protokolü çerçevesinde tanımlanan Total Length alanından IP header uzunluğunun çıkarılmasıyla da doğrulanabilir. Yani, toplam uzunluktan başlık (örneğin 20 bayt) çıkarıldığında, kalan 1972 baytlık veri, paketin asıl yükü (payload) olarak tanımlanır.

```
Total Length: 520
Identification: 0x07c4 (1988)

000. ... = Flags: 0x0

0... = Reserved bit: Not set

.0. ... = Don't fragment: Not set

.0. ... = More fragments: Not set

.0. 0000 1011 1001 = Fragment Offset: 1480

Time to Live: 3

Protocol: ICMP (1)

Header Checksum: 0xe41b [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.237.106

Destination Address: 142.251.140.78

[2 IPv4 Fragments (1980 bytes): #3026(1480), #3027(500)]
```

İlk ve ikinci datagramlar incelendiğinde, ilkinde bayrak (flag) değeri 0x1 iken, ikincisinde bu değerin 0x0 olduğu görülmektedir. Bu durum, ilk datagramın son parça olmadığını, ancak ikinci datagramın son parça olduğunu göstermektedir. Çünkü "More Fragments" (MF) bayrağı ayarlı değilse, bu parçadan sonra başka bir fragment yoktur, bu da o parçanın son fragment olduğunu ifade eder.

#### 3.13

İlk ve ikinci fragmentler karşılaştırıldığında, IP başlığında değişen alanlar Flags, More Fragments, Fragment Offset ve Total Length olarak öne çıkar.

- 1. Flags & More Fragments: İlk fragmentta "More Fragments" bayrağı 1'dir, yani devam eden fragmentlar vardır. İkinci fragmentta ise bu bayrak 0'dır; bu da onun son fragment olduğunu gösterir.
- 2. Fragment Offset: İlk fragmentin offset değeri genellikle 0'dır. İkinci fragmentta bu değer artar ve verinin IP paketi içindeki yerini belirtir.
- 3. Total Length: İlk fragment, genellikle orijinal paketin başlangıcını taşıdığı için daha büyüktür. İkinci fragment, kalan veriyi içerdiğinden daha kısa olabilir.

Bu alanlar, parçaların sırasını ve tamamlanma durumunu anlamamızı sağlar.

## 3.14

```
4439 92.883310 212.156.104.152 192.168.237.106 ICMP 170 Time-to-live exceeded (Time to live exceeded in transit)
4440 92.913156 74.125.51.44 192.168.237.106 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4443 92.927553 192.168.237.106 142.251.140.78 ICMP 554 Echo (ping) request id-0x0001, seq=360/26625, ttl=12 (no response found!)
4455 92.976955 192.168.237.106 142.251.140.78 ICMP 554 Echo (ping) request id-0x0001, seq=361/26881, ttl=13 (no response found!)
4456 92.981330 142.251.243.221 192.168.237.106 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4459 93.027583 192.168.237.106 142.251.140.78 ICMP 554 Echo (ping) request id-0x0001, seq=361/26881, ttl=13 (no response found!)

Protocol: ICMP (1)
Header Checksum: 0xd8db [validation disabled]
[Header Checksum: 0xd8db [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.237.106

Destination Address: 142.251.140.78

[3 IPV4 Fragments (3480 bytes): #4453(1480), #4454(1480), #4455(520)]
[Frame: 4453, payload: 0-1479 (1480 bytes)]
[Frame: 4454, payload: 0-1479 (1480 bytes)]
[Frame: 4454, payload: 1480-2959 (1480 bytes)]
[Fragme: 4455, payload: 1480-2959 (1480 bytes)]
[Fragme: 4457, payload: 1480-2959 (1480 bytes)]
[Fragme: 4458, payload: 1480-2959 (1480 bytes)]
[Fragme: 4459, payload: 1480-2959 (1480 bytes)]
[Fragme: 4459, payload: 1480-2959 (1480 bytes)]
[Fragme: 4459, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
[Fragme: 4450, payload: 1480-2959 (1480 bytes)]
```

Ekran görüntüsünde ilgili alana bakıldığında, paketin üç ayrı fragmente bölündüğü açıkça görülmektedir. Bu durum, IP parçalama (fragmentation) sürecinin bir sonucudur ve her bir fragment, orijinal verinin farklı bir kısmını taşımaktadır. Fragment sayısı, başlıktaki More Fragments bayrağı ve Fragment Offset değerleri yardımıyla belirlenebilmektedir.

### 3.15

Aşağıda, ilgili fragmentlerin Wireshark ortamında incelenmiş ekran görüntüsü yer almaktadır. Bu görüntüde her bir fragmentin IP başlığı dikkatle incelendiğinde Flags, More Fragments, Fragment Offset ve Total Length alanlarının fragmentler arasında değiştiği görülmektedir.

- Flags ve More Fragments alanları, paketlerin parçalanma durumunu ve devam eden fragmentlerin olup olmadığını belirtmektedir.
- Fragment Offset, her fragmentın orijinal veri içindeki konumunu göstermektedir.
- Total Length ise her bir fragmentin boyutunu ifade etmektedir.

```
4455 92.936659 102.168.237.106 142.251.140.78 IPV4 1514 Fragmented IP protocol (proto=ICMP 1, off=69, ID=0837) [Reassembled in #4455] 4454 92.976955 192.168.237.106 142.251.140.78 IPV4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0837) [Reassembled in #4455] 4454 92.976955 192.168.237.106 142.251.140.78 IPV4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0837) [Reassembled in #4455] 4454 92.976955 192.168.237.106 142.251.140.78 IPV4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0837) [Reassembled in #4455] 4455 92.976955 192.168.237.106 142.251.140.78 ICMP 554 Etcho (pring) request id=0x0001, seq=351/26881, ttl=13 (no response found!) 4455 92.976955 192.168.237.106 142.251.140.78 ICMP 554 Etcho (pring) request id=0x0001, seq=351/26881, ttl=13 (no response found!) 4455 92.981330 142.251.243.221 192.168.237.106 ICMP 110 Time-to-live exceeded (Time to live exceeded in #4455] ICMP 100 Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invertor Invert
```

4453 nolu 1.Fragment

4454 nolu 2.Fragment

4455 nolu 3.Fragment

# 4. Kaynakça

Wireshark Lab: IP v8.0 Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross