Laboratuvar Raporu 5

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Şevval Ayça Çerence

152120211128

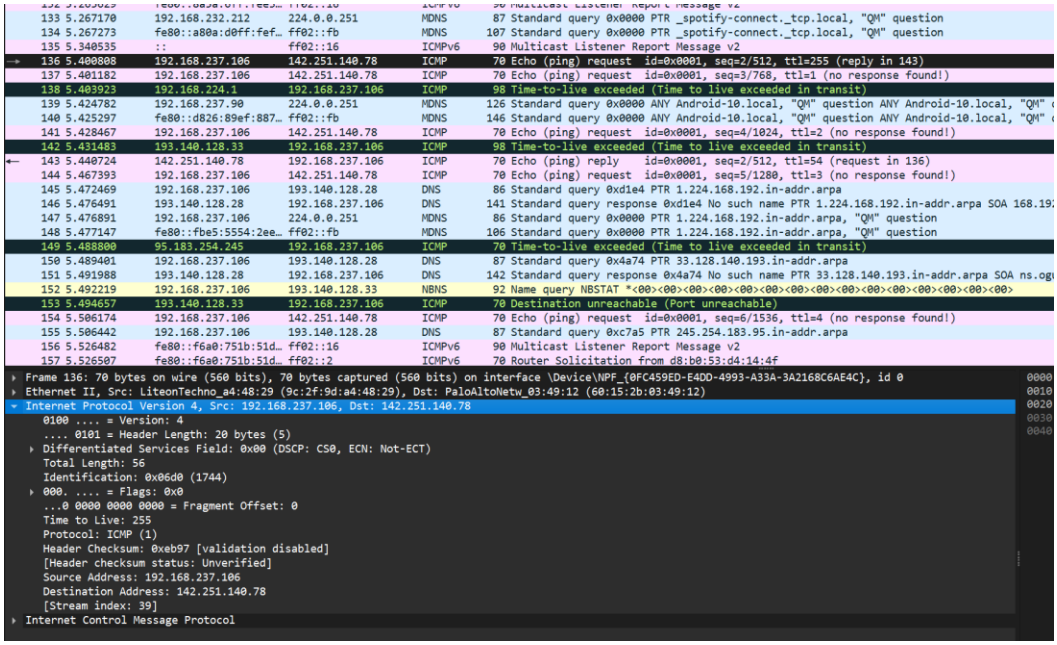
Dr. Öğr. Üyesi İlker Özçelik

2024-2025

2. Giriş

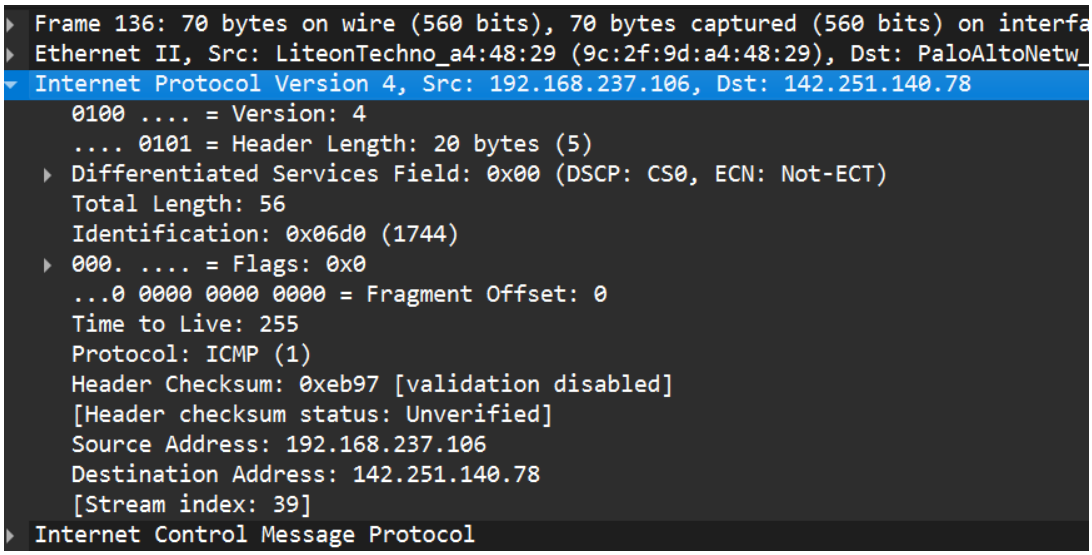
3.Sorular

3.1



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

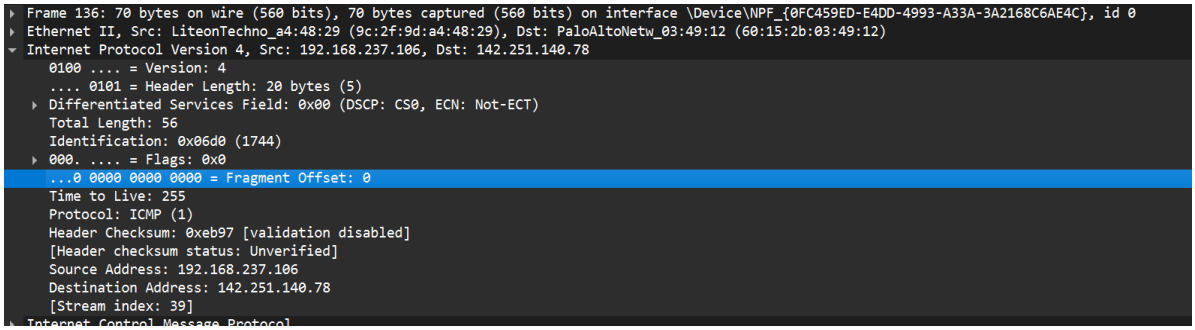


İncelenen paketin Internet Protocol başlığı altındaki Protocol alanında, protokol türü olarak ICMP (1) değeri yer almaktadır. ICMP (Internet Control Message Protocol), IP temelli ağlarda iletişimin doğruluğunu ve verimliliğini artırmak amacıyla kullanılan yardımcı bir protokoldür. Temel işlevi, ağ üzerinde 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

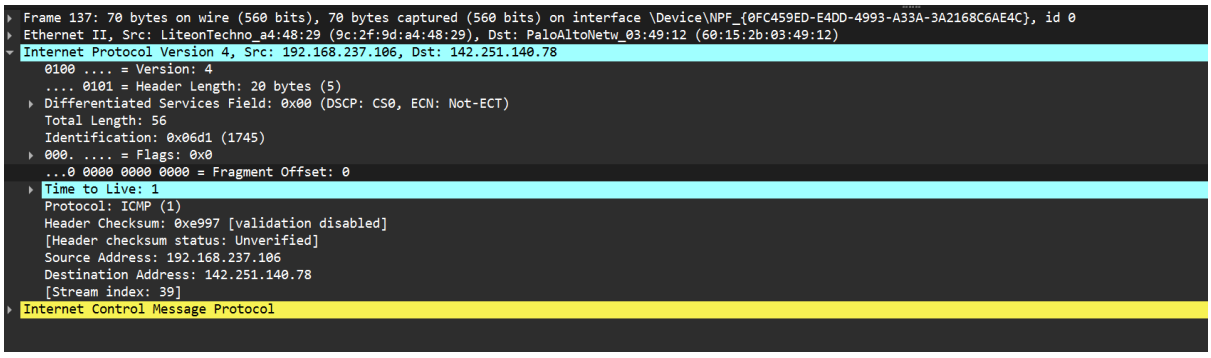
İlgili ekran görüntüsünde, IP başlığının (IP header) boyutu 20 bayt olarak belirtilmiş, Total Length alanı ise 56 bayt değerini göstermektedir. Bu bilgiler doğrultusunda, IP paketinin taşıdığı asıl veri kısmı olan payload (yük) miktarını hesaplamak mümkündür. Toplam uzunluktan başlık boyutu çıkarıldığında: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

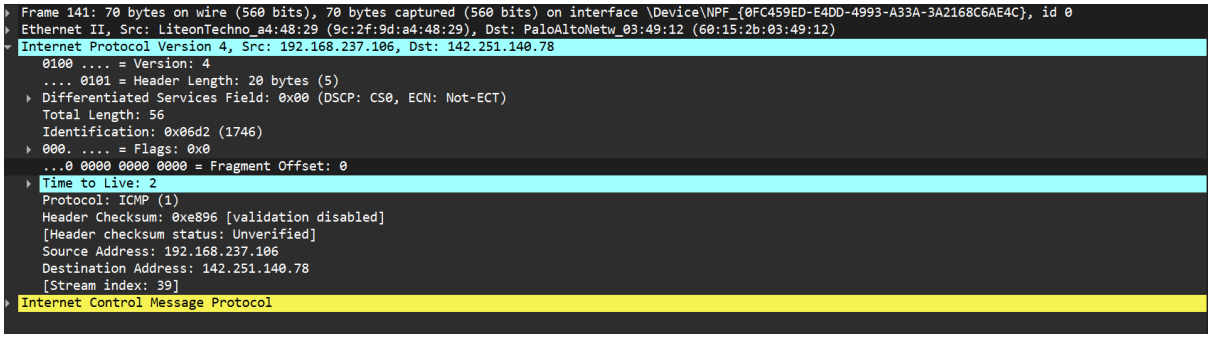
3.4



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





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.

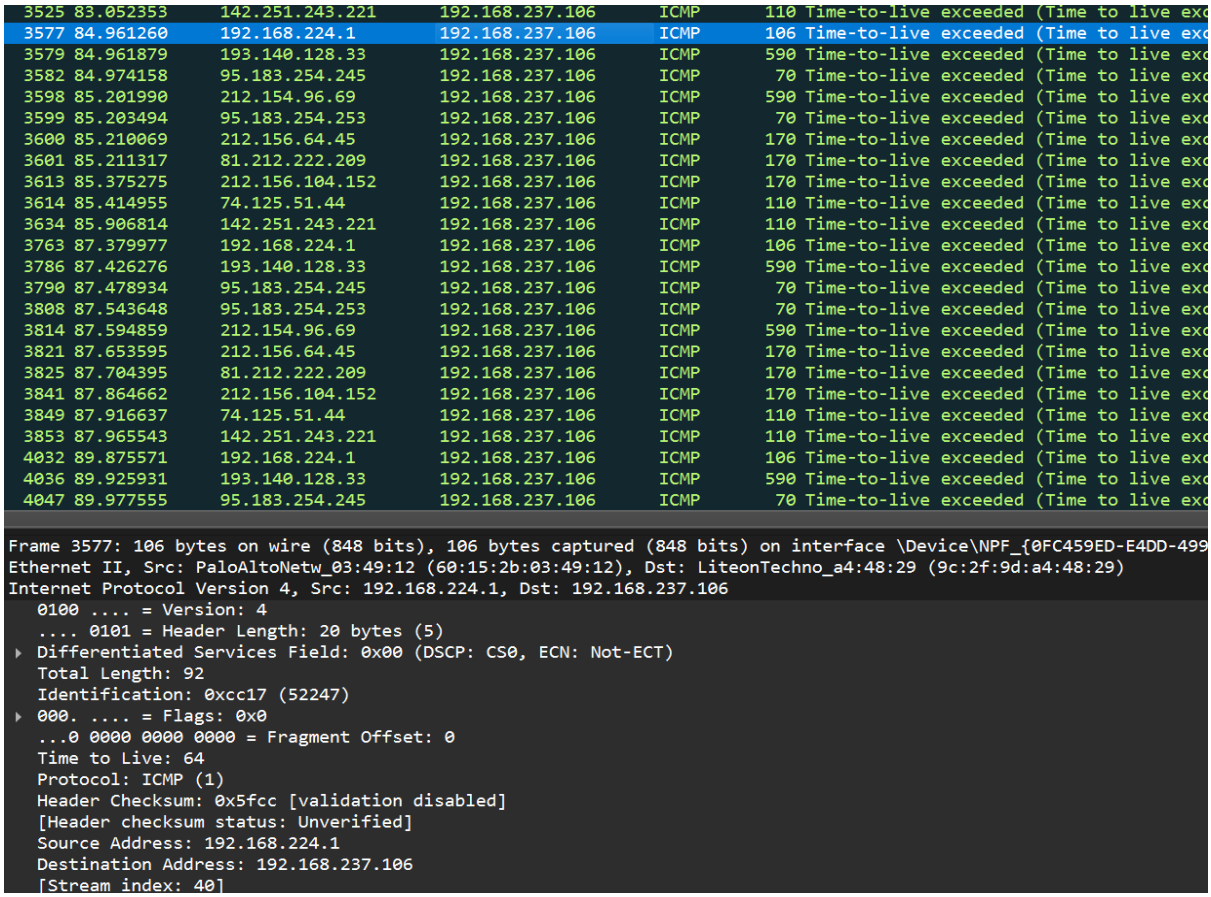
TTL, bir IP paketinin ağdaki ömrünü tanımlar; her yönlendiriciden geçişte bu değer bir azaltılır ve sıfıra ulaştığında paket düşürülür. Bu mekanizma, ağda sonsuz döngülerin oluşmasını engeller. Header Checksum ise, IP başlığındaki bilgilerin bütünlüğünü doğrulamak amacıyla kullanılır. TTL veya Identification 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.

3.8



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.

3.10

```
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 10
    Protocol: ICMP (1)
    Header Checksum: 0xdcd8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.237.106
    Destination Address: 142.251.140.78
  ▾ [2 IPv4 Fragments (1980 bytes): #3606(1480), #3607(500)]
       [Frame: 3606, payload: 0-1479 (1480 bytes)]
       [Frame: 3607, payload: 1480-1979 (500 bytes)]
       [Fragment count: 2]
       [Reassembled IPv4 length: 1980]
       [Reassembled IPv4 data […]: 08003b0a000101392020202020202020202020202020202020202020202020202020202020202020202020202
    [Stream index: 39]
 Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x3b0a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 313 (0x0139)
    Sequence Number (LE): 14593 (0x3901)
  ▸ [No response seen]
  ▾ Data (1972 bytes)
```

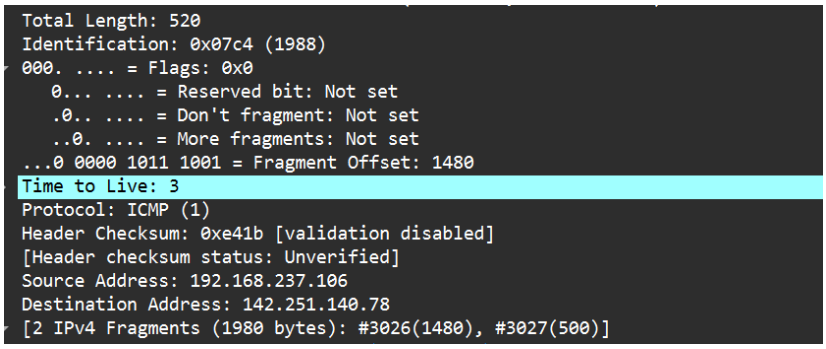
Bu bölümde, zip dosyasında yer alan ilgili izleme (trace) dosyası kullanılarak analiz gerçekleştirilmiştir. Yapılan incelemede, ilk 2000 bayt veriyi içeren bir ICMP Echo (Ping) Request paketi tespit edilmiştir. Bu paketin boyutu, tek bir IP paketine sığamayacak kadar büyük olduğundan dolayı, IP protokolü 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.

```
ternet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x3b85 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 190 (0x00be)
 Sequence Number (LE): 48640 (0xbe00)
 [No response seen]
 Data (1972 bytes)
    Data […]: 202020202020202020202020202020202020202020202020202020202020202020202020202020202020202020202020202020202020202020
    [Length: 1972]
```

3.12



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.

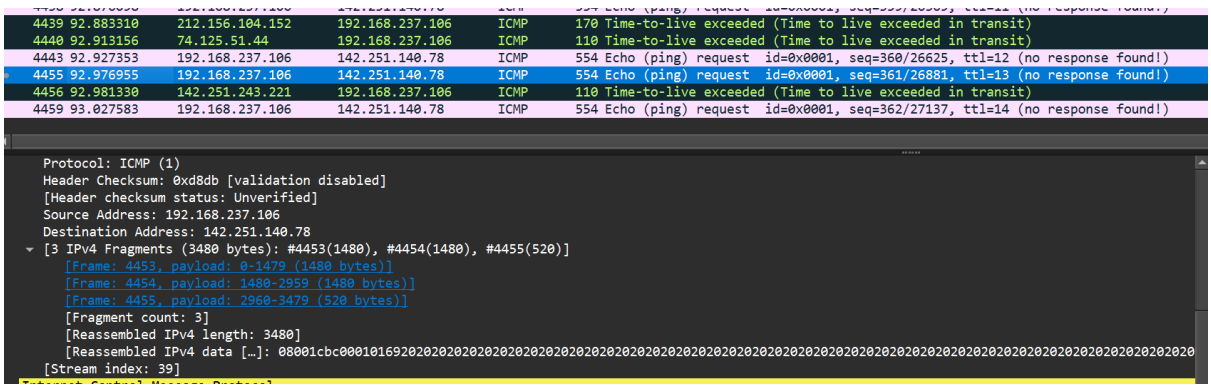
3.13

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 fragmentın 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

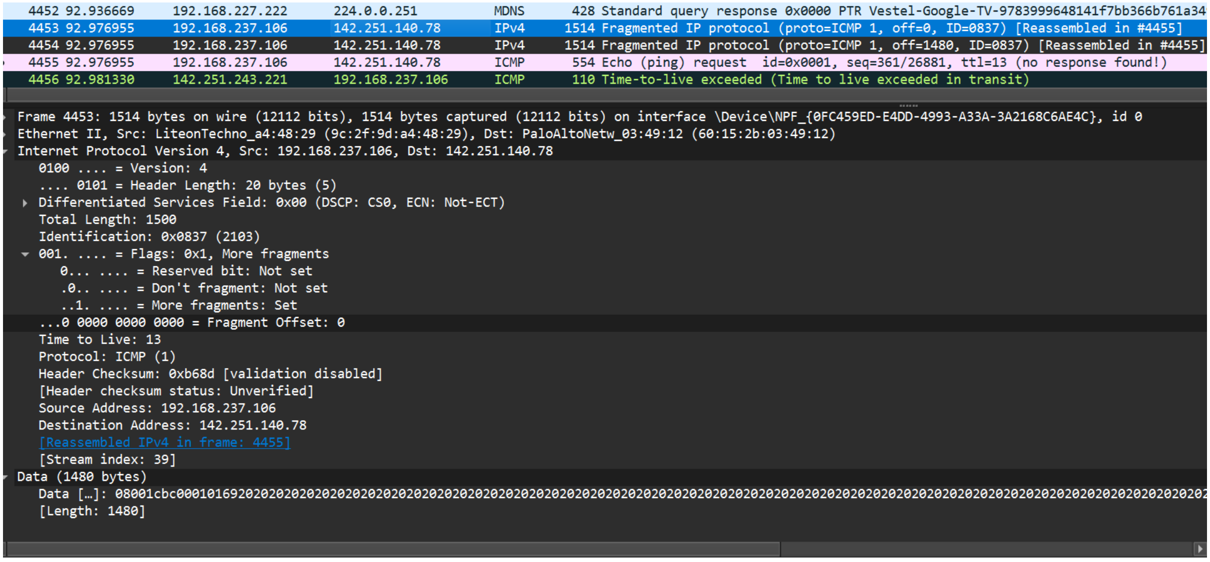


Ekran görüntüsünde ilgili alana bakıldığında, paketin üç ayrı fragmente bölündüğü açıkça görülmektedir. Bu durum, IP parçalama (fragmentation) sürecinin bir sonucudur ve her bir fragment, orijinal verinin farklı bir kısmını taşımaktadır. Fragment sayısı, başlıktaki More Fragments bayrağı ve Fragment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

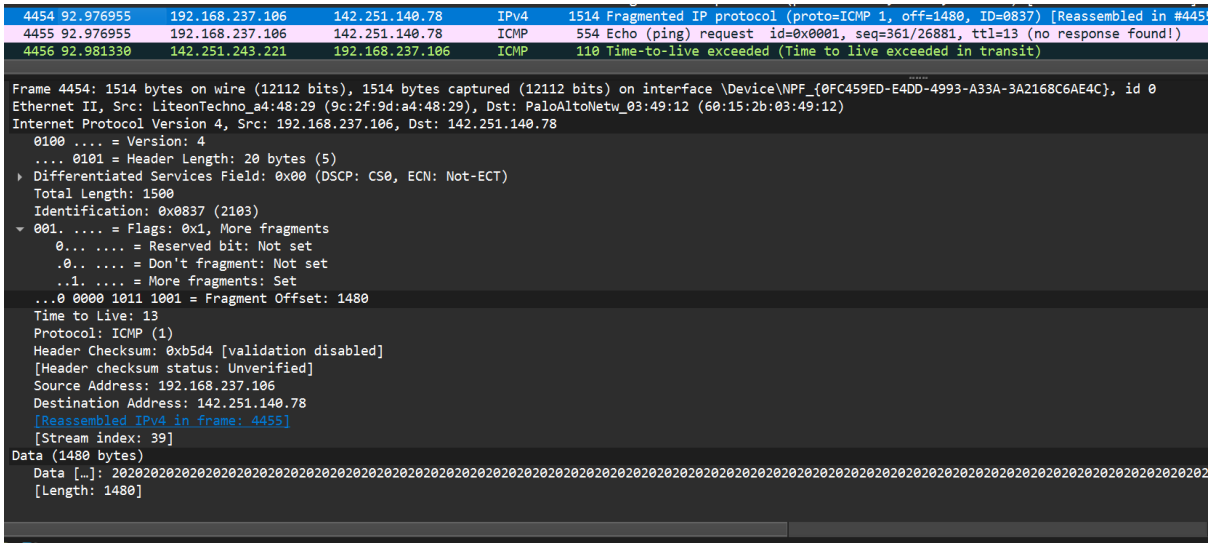
3.15

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.

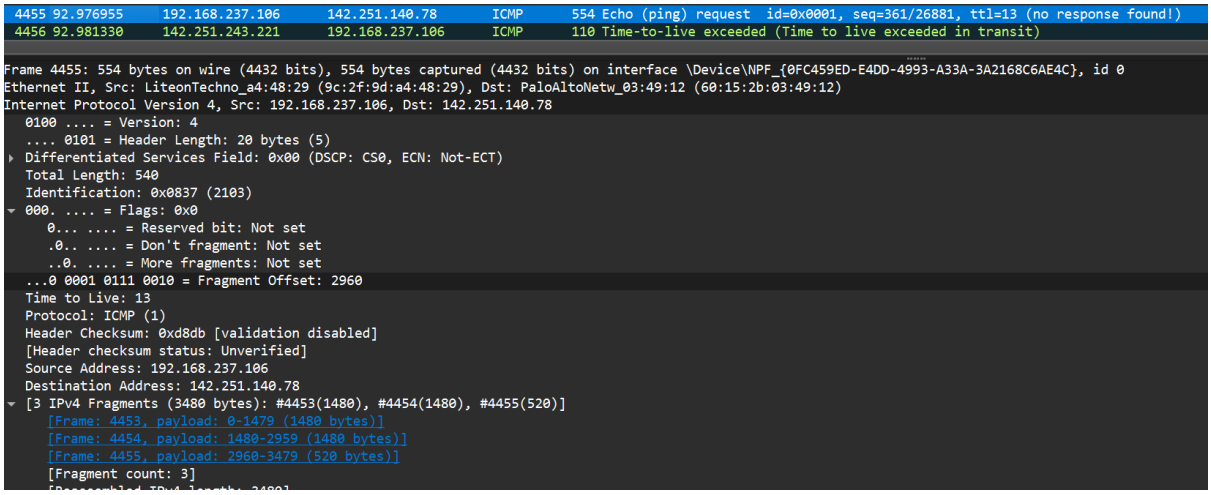
- Flags ve More Fragments alanları, paketlerin parçalanma durumunu ve devam eden fragmentlerin olup olmadığını belirtmektedir.
- Fragment Offset, her fragmentın orijinal veri içindeki konumunu göstermektedir.
- Total Length ise her bir fragmentın boyutunu ifade etmektedir.



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