Laboratuvar Raporu 5

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Özlem Kayıkcı

152120191043

Dr. Öğr. Üyesi İlker Özçelik

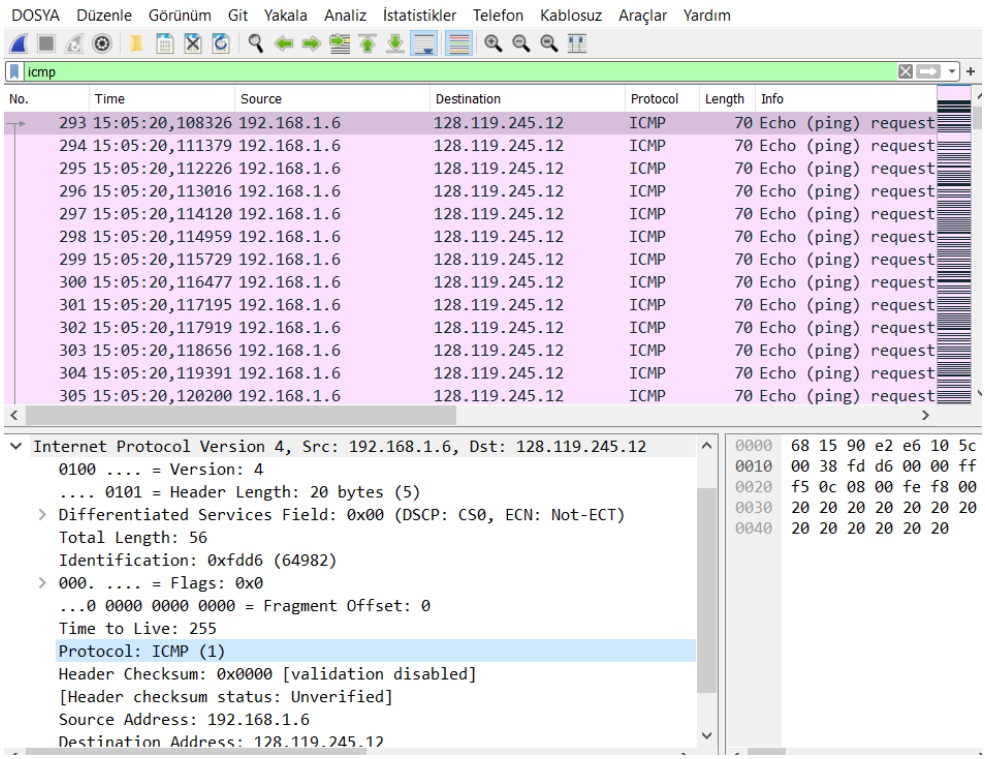
2022-2023

1 İçindekiler

2 Giriş

IP protokolü, paketlerin kaynak IP adresi, hedef IP adresi, protokol bilgisi ve diğer başlık bilgilerini içeren IP paketlerini kullanmaktadır ve bu başlık bilgileri, paketlerin doğru bir şekilde yönlendirilmesini sağlar.IP'nin en yaygın kullanılan sürümü, IPv4 (Internet Protocol version 4)'tür. IPv4 adresleri 32 bit uzunluğunda olup genellikle dört rakamdan oluşan noktalı ondalık formatta ifade edilmektedir ancak, IPv4 adres alanının tükenmesi nedeniyle yeni bir adresleme sistemi olan IPv6 (Internet Protocol version 6) geliştirilmiştir, IPv6 adresleri 128 bit uzunluğundadır. Bu laboratuvar uygulamasında IP protokolüne ait paketleri yakalayabilmesini, bu paketlerin içeriğini inceleyebilmesini ve IP protokolünün farklı özelliklerini anlama ve uygulaması sağlanılmıştır. Bu sayede, IP protokolünün nasıl çalıştığı, paketlerin nasıl yönlendirildiği, IP adresleme, parçalama ve yeniden birleştirme gibi konuların anlaşılması hedeflenmiştir.

3 Laboratuvar Uygulaması



Resim 1

3.1 1.soru

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

Bilgisayarımın IP adresi resim 1 de görülebileceği üzere wireshark ortamında ilk ICMP request segmenti üzerindeki Internet Protocol kısmında source olarak yer alan 192.168.1.6 adresidir.

3.2 2.soru

2. Within the IP packet header, what is the value in the upper layer protocol field?

Resim 1' de ilgili alanda Protocol: ICMP (1) değeri görülmüştür. ICMP, IP tabanlı iletişimin güvenliğini ve etkinliğini artıran bir protokoldü, ağ sorunlarının teşhisi ve hata bildirimleri gibi işlevleri sayesinde de ağ yöneticileri ağ trafiğini izleyebilir, hata durumlarını tespit edebilir ve ağ performansını optimize edebilmektedir.

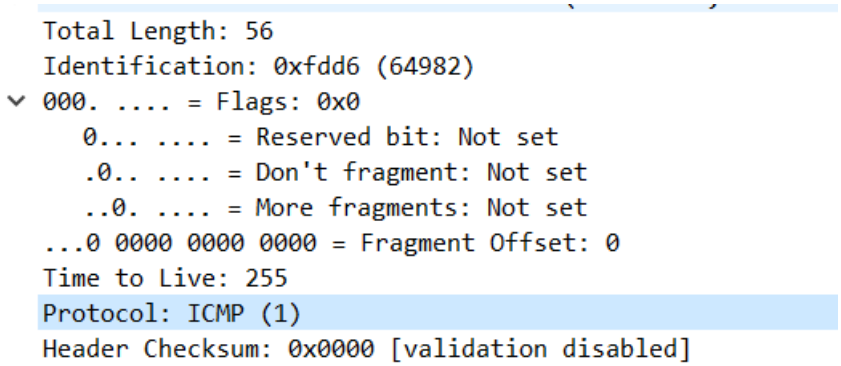
3.3 3.soru

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Resim 1' de ilgili alanda IP header'ının boyutu 20 byte olarak görülmekte iken, Total boyut (length) 56 byte olarak bulunmuştur, bu veriler üzerinde totalden header'ın boyutunu çıkarma işlemini yaparsak 56-20= 36 byte olarak payload bulunur.

3.4 4.soru

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

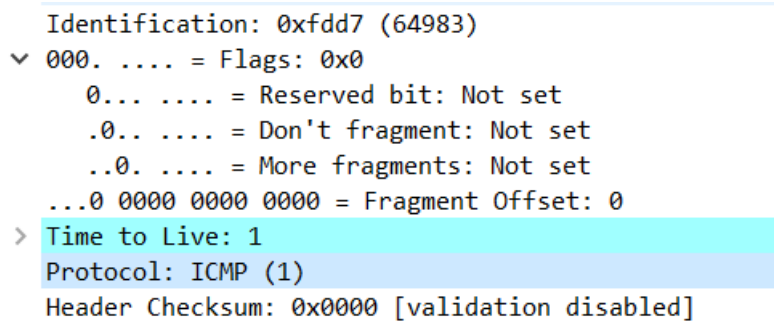


Resim 2

IP datagram'ın Fragment flag değerine bakarak çıkarımda bulunursak, 0 değerine set edilmiş olması olmadığı anlamını taşır, yine aynı şekilde 1 değerine set edilmiş olsaydı eğer , IP datagram için fragmented diyebilirdik .

3.5 5.soru

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?



Resim 3

Resim 2 'de ve Resim 3'de karşılaştırma yapıldığında görülen Time to Live, Header checksum ve Identification alanları daima değişmektedir.

3.6 6.soru

> 6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Resim 1'de görüleceği üzere source (kaynak) adresi ve Destination (alıcı) adreslerinin yanı sıra Header boyutu da sabit kalmıştır. Ayrıca IP versiyonu da hep aynı kalmış, hiç değişmemiştir. Time to Live, Header checksum ve Identification alanları ise diğer belirtilen alanların aksine daima değişmektedir ve değişmelidir. Time to Live (TTL), Header checksum ve Identification alanlarının değişebilmesinin sebebi ise IP protokolünün doğru ve güvenli bir şekilde veri iletimi sağlamak adına kullanılan bazı özelliklere sahip olmasına bağlanır.

TTL, bir IP paketinin ağ üzerindeki geçerlilik süresini belirler. Her bir yönlendirici (router) paketi ilettiğinde TTL değerini 1 azaltır. Böylece, eğer paket bir döngüye girerse veya yönlendirme hataları oluşursa, TTL değeri sıfıra ulaşacak ve paket ağda sonsuz bir döngüde kalmadan otomatik olarak atılacaktır bu da bizi istenilen performansa ulaştıracaktır. TTL değeri, her yönlendirici tarafından azaltıldığından dolayı, kaynak ve hedef adresler sabit kalmış olsa bile her yönlendirme aşamasında değişmektedir.

Header checksum için ise IP paketlerinin doğru bir şekilde iletilmesini sağlamak için kullanılan bir hata kontrol mekanizması olarak tanımlayabiliriz. Paketin başlık alanındaki verilerin tutarlılığını kontrol etmek adına kullanılmaktadır. Header alanındaki bilgiler değiştiğinde, örneğin TTL veya Identification alanları değiştiğinde, checksum değeri de değişmektedir. Böylece, paketin doğruluğu ve bütünlüğü de kontrol edilebilmektedir.

Identification alanı, IP paketlerinin parçalara bölünmesi ve yeniden birleştirilmesi gerektiğinde kullanılmaktadır.Kaynak tarafından gönderilen bir mesajı parçalamak zorunda kalan yönlendirici, her bir parçaya benzersiz bir Identification değeri atayacak ve bu sayede, parçalar hedefe ulaştığında doğru bir şekilde birleştirilebilir durumda olacaktır. Her parça ayrı bir IP paketi olduğundan, parça sayısı veya sırası değiştiğinde Identification değeri de değişmektedir.

Kısaca bu üç alan, IP protokolünün doğruluk, güvenlik ve doğru yönlendirme sağlaması için dinamik olarak değiştirilir. Her yönlendirme aşamasında TTL azalırken, Header checksum ve Identification alanları paketin içeriğine bağlı olarak güncellenecektir. Böylelikle, paketlerin doğru bir şekilde iletilmesi ve hataların tespit edilmesi sağlanmaktadır.

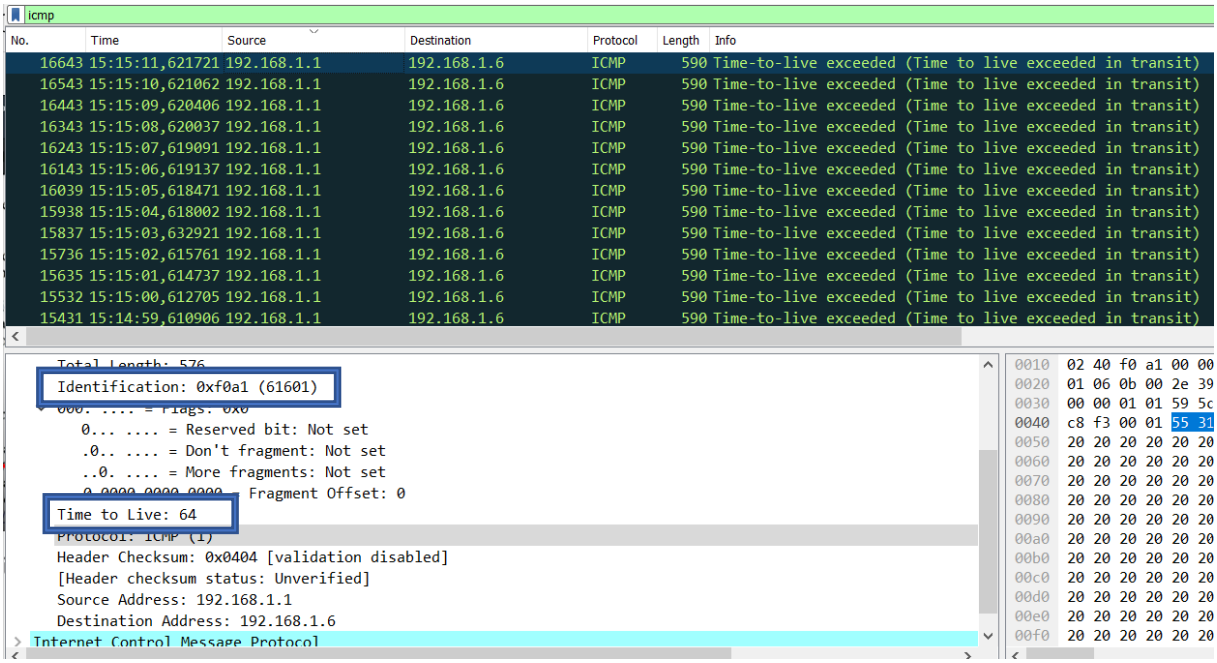
3.7 7.soru

7. Describe the pattern you see in the values in the Identification field of the IP datagram

Resim 2 ve Resim 3 ‘de Identification değerlerine bakıldığında aralarındaki farkın 1 olduğunu, sırayı gözeterek diğer paketlere de ilgili alana bakıldığında bu değerin 1’er arttığını söyleyebiliriz.

3.8 8.soru

8. What is the value in the Identification field and the TTL field?



Identification değeri 0xf0a1 (61601) , TTL değeri ise 64 olarak görülmüştür.

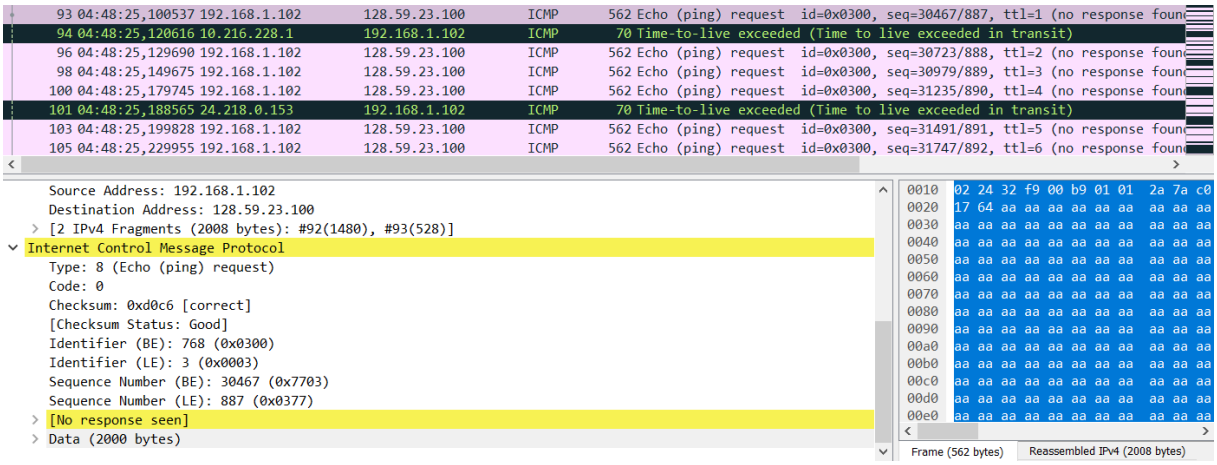
3.9 9.soru

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

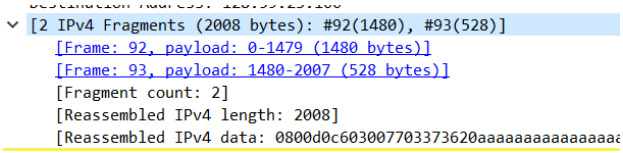
Identification alanı değişmiştir ancak Time to Live(TTL) alanı için değişim olmamıştır. ICMP TTL-exceeded yanıt mesajları, bir IP paketinin TTL değeri sıfıra ulaştığında oluşturulan mesajlardır dolayısıyla bu mesajlar, IP paketinin hedefe ulaşamadan atıldığını ve TTL değerinin tükendiğini bildirmektedir. ICMP TTL-exceeded mesajlarında TTL değerinin değişmemesi, ICMP mesajlarının kaynak paketin özelliklerini koruyarak IP protokolüne yönelik yanıt vermesinden kaynaklanmakta iken Identification alanı ise parçalama veya yeniden birleştirme gerektirmeyen ICMP mesajlarında genellikle değişmemektedir.

3.10 10.soru

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

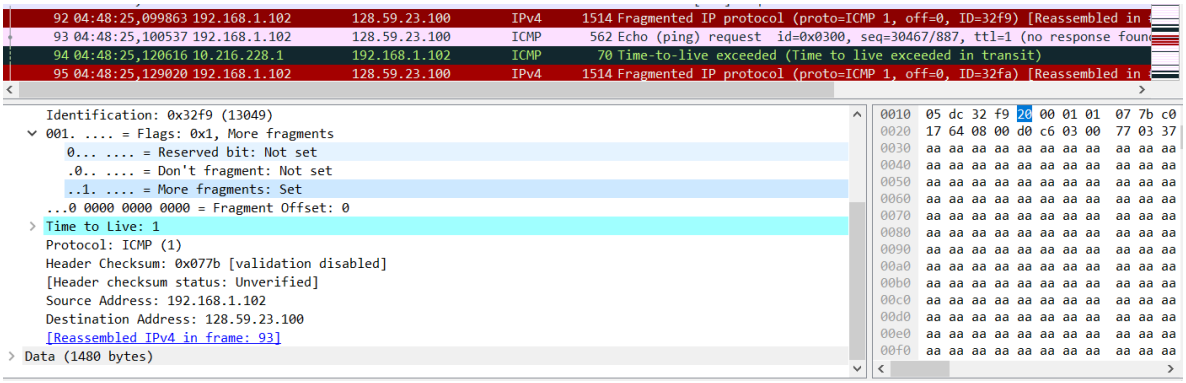


Bu bölümde zip dosyasından ilgili trace kullanılmış olup ilk 2000 byte içeren Echo (ping) Request bulunup incelenmiş, sonuç olarak 2 IPv4 Fragments alanında 2 fragment bulunmuştur.



3.11 11.soru

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?



İlgili alana gidilip incelendiğinde more fragments kısmının set edildiği görülmektedir, bu başka bir fragmentinin olduğunun göstergesidir.

```
[Reassembled IPv4 in frame: 93]
Data (1480 bytes)
    Data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa…
    [Length: 1480]
```

Datagramın boyutu ilgili alanda 1480 byte olarak bulunmuş olup ekran görüntüsünde gösterilmiştir. Ayrıca ,total uzunluktan headerin boyutu çıkarıldığında 1500-20=1480 byte olarak IP datagram boyutu bulunur.

3.12 12.soru

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

İlk ve ikinci datagram’lar incelendiğinde ilkin için flag 0x1 iken ikinci için 0x0 olduğu görülür, dolayısıyla ilk değil son fragmenttir.More fragment kısmı set edilmediğinden daha fazla fragment yok demektir ki bu da son olduğuna işaret eder.

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  v 001. .... = Flags: 0x1, More fragments
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 93]
Data (1480 bytes)
    Data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa…
    [Length: 1480]
```

→ilk fragmented IP datagram

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x32f9 (13049)
  v 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: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  v [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
        [Frame: 92, payload: 0-1479 (1480 bytes)]
        [Frame: 93, payload: 1480-2007 (528 bytes)]
        [Fragment count: 2]
        [Reassembled IPv4 length: 2008]
        [Reassembled IPv4 data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa…]
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd0c6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
```

→ikinci fragmented IP datagram

3.13 13.soru

13. What fields change in the IP header between the first and second fragment?

İlk ve ikinci fragmentler incelendiğinde IP başlığı altında değişen alanlar Flags, more fragments, fragment offset ve total length olarak saptanmıştır.

1. Flags (Bayraklar): Flags alanı, parçalama işlemiyle ilgili bilgileri içerir. Bu alanın içindeki bayraklar, parçalama sürecini kontrol etmektedir. İlk fragmentta Flags alanında "1" olarak ayarlanan "More Fragments" bayrağı, daha fazla fragment olduğunu belirtmektedir. İkinci fragmentta ise bu bayrak "0" olarak ayarlanır, çünkü daha fazla fragment kalmadığı anlamına gelmektedir.

2. More Fragments: More Fragments bayrağı, parçalanmış IP paketinin diğer fragmentlarının olup olmadığını belirtmektedir. İlk fragmentta bu bayrak "1" olarak ayarlanır, çünkü daha fazla fragment vardır ve ikinci fragmentta ise "0" olarak ayarlanır, çünkü bu son fragmenttır yani daha fazla fragment kalmamıştır ,bu şekilde son olduğu ayırt edilebilmektedir.

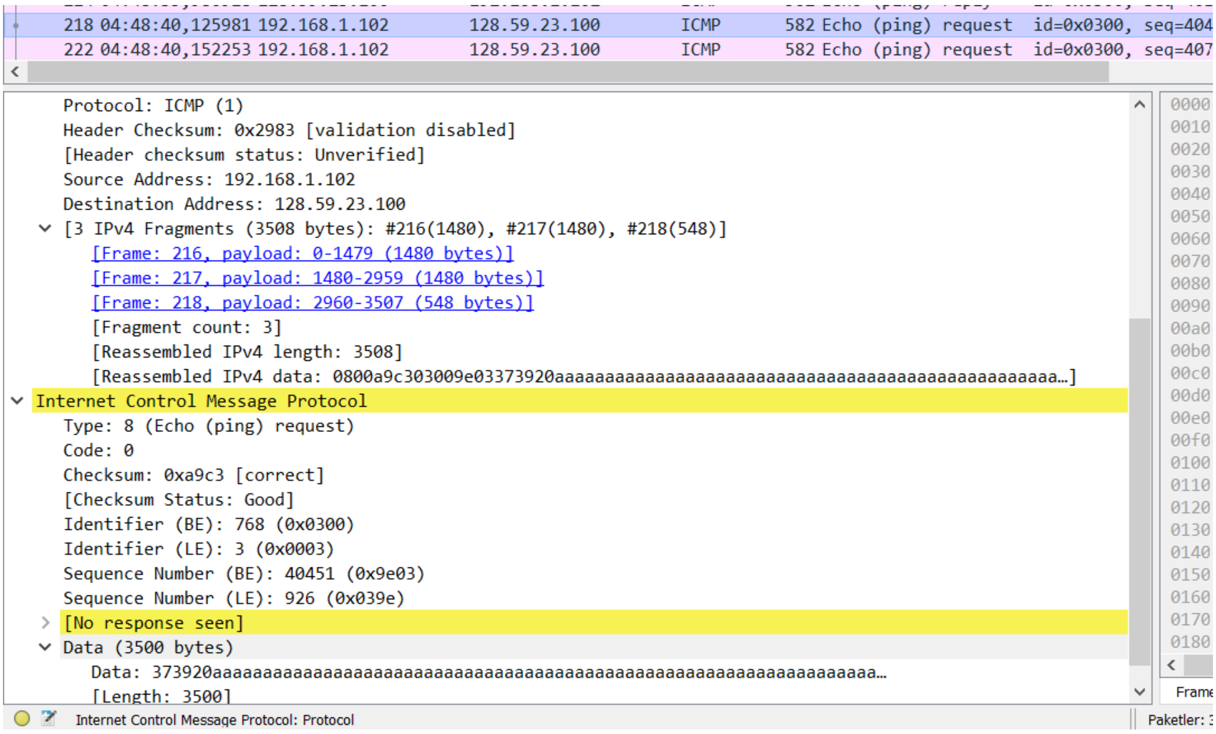
3. Fragment Offset: Fragment Offset, fragmentın tam IP paketi içindeki konumunu belirtmektedir. İlk fragmentta Fragment Offset değeri genellikle "0" olarak ayarlanır çünkü ilk fragmentın başlangıç noktasındadır. İkinci ve sonraki fragmentlarda ise Fragment Offset değeri, önceki fragmentların boyutuna göre ayarlanmaktadır.

4. Total Length: Total Length alanı, parçalanmış IP paketinin toplam boyutunu belirtmektedir. İlk fragmentta bu alan, orijinal IP paketinin boyutunu yansıtırken, ikinci ve sonraki fragmentlarda bu alan, parçalara bölünmüş fragmentın boyutunu yansıtmaktadır.

Bayraklar ve Fragment Offset, parçalama sürecini kontrol etmek ve fragmentları düzgün bir şekilde sıralamak için kullanılırken, Total Length ise her bir fragmentın boyutunu belirlemek için kullanılmaktadır.

3.14 14.soru

14. How many fragments were created from the original datagram?

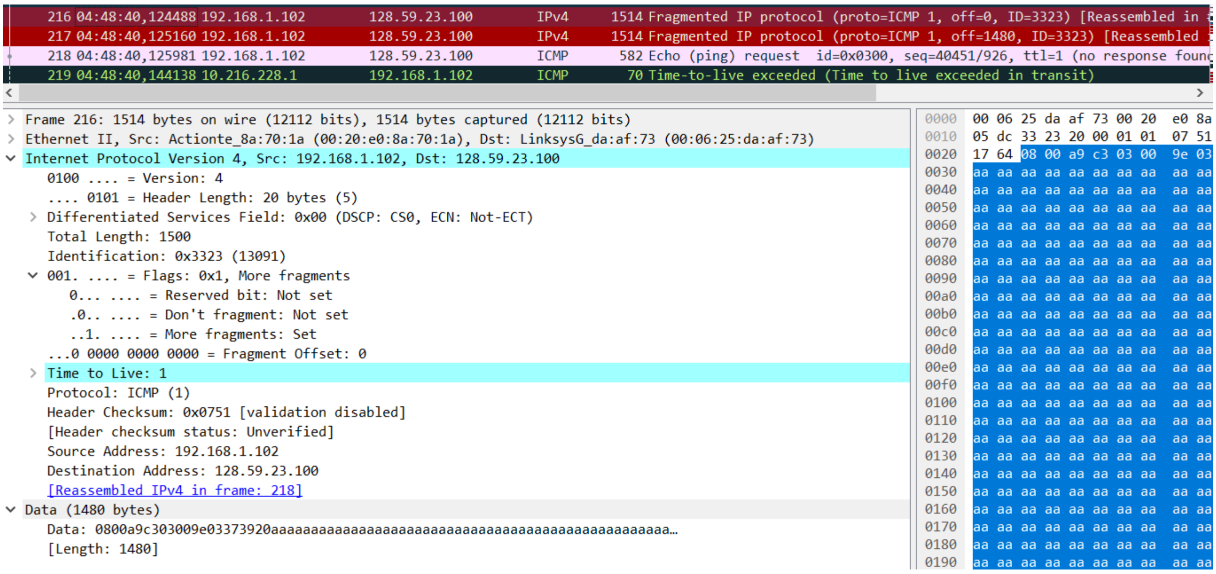


Ekran görüntüsünde ilgili alanda gözüktüğü üzere 3 Fragment bulunmuştur.

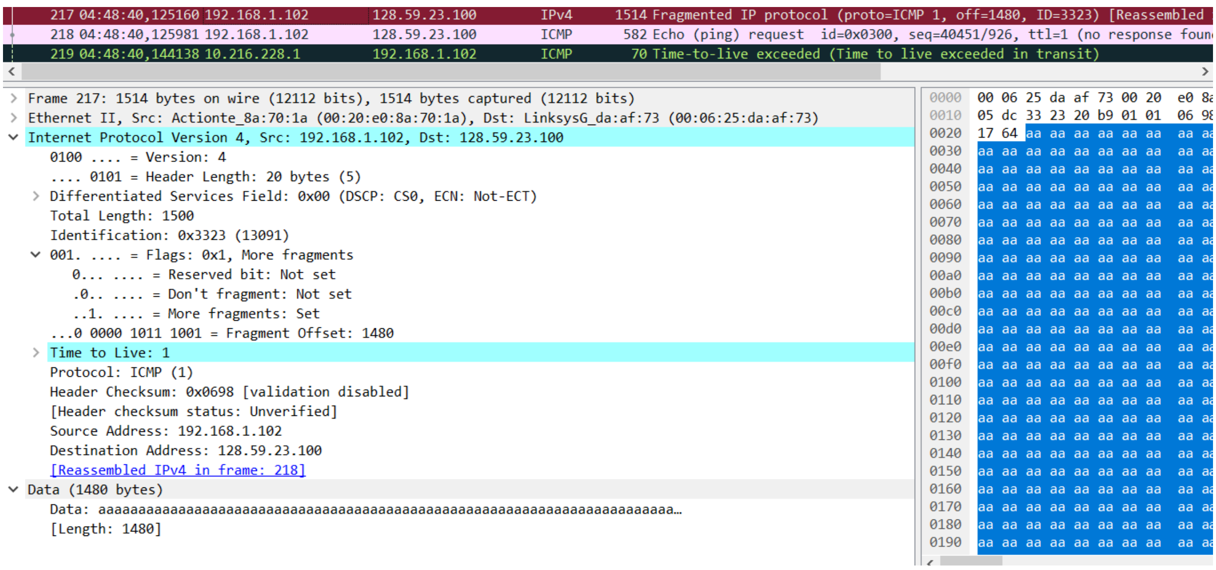
3.15 15.soru

15. What fields change in the IP header among the fragments?

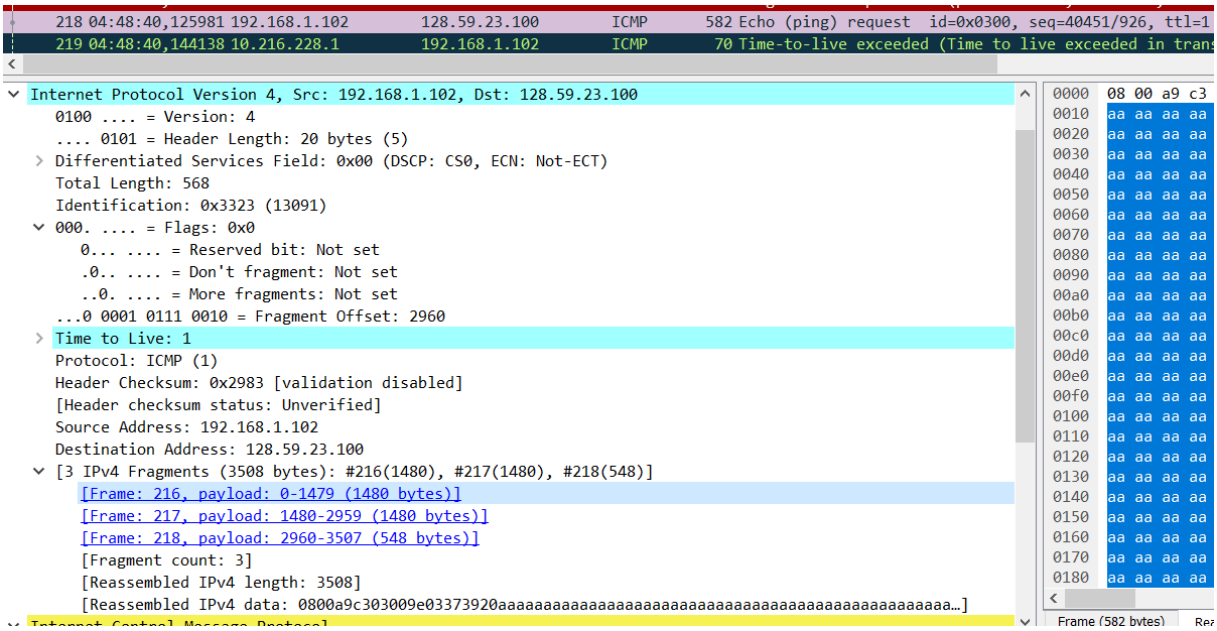
Aşağıda ilgili fragmentlerin wireshark ortamında incelenmiş ekran görüntüsü bulunmaktadır ve fragmentler arasında Flags, More fragments, fragment offset ve total length alanları değişmektedir.



216 numaralı ilk fragment



217 numaralı ikinci fragment



218 numaralı üçüncü 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
- https://www.kaspersky.com.tr/resource-center/definitions/what-is-an-ip-address
- https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/icmp-(internet-control-message-protocol-internet-kontrol-mesaj-protokol%C3%BC)
- https://tr.wikipedia.org/wiki/IP_par%C3%A7alama