



Laboratuvar Raporu 5

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Özlem Kayıkcı

152120191043

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İindekiler

2	Giriş.....	3
3	Laboratuvar Uygulaması.....	3
3.1	1.soru	4
3.2	2.soru	4
3.3	3.soru	4
3.4	4.soru	5
3.5	5.soru	5
3.6	6.soru	6
3.7	7.soru	7
3.8	8.soru	7
3.9	9.soru	7
3.10	10.soru	8
3.11	11.soru	8
3.12	12.soru	9
3.13	13.soru	10
3.14	14.soru	11
3.15	15.soru	11
4	Kaynaka.....	14

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 sağlanmıştır. Bu sayede, IP protokolünün nasıl çalıştığı, paketlerin nasıl yönlendirildiği, IP adresleme, parçalama ve yeniden birleştirme gibi konuların anlaşılması hedeflenmiştir.

3 Laboratuvar Uygulaması

The screenshot shows a network analysis tool interface. The top menu bar includes: DOSYA, Düzenle, Görünüm, Git, Yakala, Analiz, İstatistikler, Telefon, Kablosuz, Araçlar, Yardım. Below the menu is a toolbar with various icons. The main window is titled 'icmp' and displays a list of captured packets. The columns are: No., Time, Source, Destination, Protocol, Length, and Info. The packets are ICMP Echo (ping) requests from 192.168.1.6 to 128.119.245.12.

No.	Time	Source	Destination	Protocol	Length	Info
293	15:05:20,108326	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
294	15:05:20,111379	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
295	15:05:20,112226	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
296	15:05:20,113016	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
297	15:05:20,114120	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
298	15:05:20,114959	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
299	15:05:20,115729	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
300	15:05:20,116477	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
301	15:05:20,117195	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
302	15:05:20,117919	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
303	15:05:20,118656	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
304	15:05:20,119391	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request
305	15:05:20,120200	192.168.1.6	128.119.245.12	ICMP	70	Echo (ping) request

Below the packet list, a detailed view of the selected packet (No. 293) is shown. The details are as follows:

- Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56
- Identification: 0xfdd6 (64982)
- > 000. = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 255
- Protocol: ICMP (1)
- Header Checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.6
- Destination Address: 128.119.245.12

The packet data is also shown in hexadecimal and ASCII format on the right side of the details pane.

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.

```
Total Length: 56
Identification: 0xfdd6 (64982)
▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
```

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?

```
Identification: 0xfdd7 (64983)
▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
```

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 bağlıdır.

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 değerın 1'er arttığını söyleyebiliriz.

3.8 8.soru

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

No.	Time	Source	Destination	Protocol	Length	Info
16643	15:15:11,621721	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
16543	15:15:10,621062	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
16443	15:15:09,620406	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
16343	15:15:08,620037	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
16243	15:15:07,619091	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
16143	15:15:06,619137	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
16039	15:15:05,618471	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
15938	15:15:04,618002	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
15837	15:15:03,632921	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
15736	15:15:02,615761	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
15635	15:15:01,614737	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
15532	15:15:00,612705	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
15431	15:14:59,610906	192.168.1.1	192.168.1.6	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)

Total Length: 576	
Identification: 0xf0a1 (61601)	0010 02 40 f0 a1 00 00
0... .. = Flags: 0x0	0020 01 06 0b 00 2e 39
0... .. = Reserved bit: Not set	0030 00 00 01 01 59 5c
..0... .. = Don't fragment: Not set	0040 c8 f3 00 01 55 31
..0... .. = More fragments: Not set	0050 20 20 20 20 20 20
0 0000 0000 0000 Fragment Offset: 0	0060 20 20 20 20 20 20
Time to Live: 64	0070 20 20 20 20 20 20
Protocol: ICMP (1)	0080 20 20 20 20 20 20
Header Checksum: 0x0404 [validation disabled]	0090 20 20 20 20 20 20
[Header checksum status: Unverified]	00a0 20 20 20 20 20 20
Source Address: 192.168.1.1	00b0 20 20 20 20 20 20
Destination Address: 192.168.1.6	00c0 20 20 20 20 20 20
Internet Control Message Protocol	00d0 20 20 20 20 20 20
	00e0 20 20 20 20 20 20
	00f0 20 20 20 20 20 20

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 ulaşmadan 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?

The image shows a Wireshark packet capture. The top pane displays a list of packets. Packet 93 is selected, showing an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. The details pane shows the Internet Control Message Protocol (ICMP) section with the following information:

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xd0c6 [correct]
- [Checksum Status: Good]
- Identifier (BE): 768 (0x0300)
- Identifier (LE): 3 (0x0003)
- Sequence Number (BE): 30467 (0x7703)
- Sequence Number (LE): 887 (0x0377)
- [No response seen]
- Data (2000 bytes)

The packet is fragmented into 2 IPv4 Fragments (2008 bytes): #92(1480), #93(528). The right pane shows the raw data of the selected packet, which is a 562-byte frame.

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.

```
[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: 0800d0c603007703373620aaaaaaaaaaaaaaaa]
```

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?

The image shows a Wireshark packet capture. The top pane displays a list of packets. Packet 92 is selected, showing an IPv4 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in]. The details pane shows the Internet Protocol (IP) section with the following information:

- Identification: 0x32f9 (13049)
- 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)

The right pane shows the raw data of the selected packet, which is a 1480-byte frame.

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: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
  [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 there 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)
  ▼ 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: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
  [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)
  ▼ 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
  ▼ [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: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...]
▼ 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?

The image shows a Wireshark packet capture of an ICMP Echo (ping) request. The packet list at the top shows three fragments of the request, each 582 bytes long, with IDs 0x0300 and sequence numbers 404, 407, and 407. The packet details pane shows the ICMP (1) protocol with a header checksum of 0x2983 (validation disabled) and a source address of 192.168.1.102. The destination address is 128.59.23.100. The packet is identified as an ICMP Echo (ping) request with a type of 8, code of 0, and a checksum of 0xa9c3 (correct). The identifier (BE) is 768 (0x0300) and the identifier (LE) is 3 (0x0003). The sequence number (BE) is 40451 (0x9e03) and the sequence number (LE) is 926 (0x039e). The packet is marked as '[No response seen]'. The data field shows a reassembled IPv4 data of 3500 bytes, with a length of 3500. The packet bytes pane shows the raw data of the packet, starting with 0000 and ending with 0180.

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 04:48:40,124488 192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in frame 218]
217 04:48:40,125160 192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in frame 218]
218 04:48:40,125981 192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found)
219 04:48:40,144138 10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

<ul style="list-style-type: none"> > Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73) ▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 <ul style="list-style-type: none"> 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1500 Identification: 0x3323 (13091) ▼ 001. = Flags: 0x1, More fragments <ul style="list-style-type: none"> 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: 0x0751 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 [Reassembled IPv4 in frame: 218] ▼ Data (1480 bytes) <ul style="list-style-type: none"> Data: 0800a9c303009e03373920aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa... [Length: 1480] 	<pre> 0000 00 06 25 da af 73 00 20 e0 8a 0010 05 dc 33 23 20 00 01 01 07 51 0020 17 64 08 00 a9 c3 03 00 9e 03 0030 aa aa aa aa aa aa aa aa aa aa 0040 aa aa aa aa aa aa aa aa aa aa 0050 aa aa aa aa aa aa aa aa aa aa 0060 aa aa aa aa aa aa aa aa aa aa 0070 aa aa aa aa aa aa aa aa aa aa 0080 aa aa aa aa aa aa aa aa aa aa 0090 aa aa aa aa aa aa aa aa aa aa 00a0 aa aa aa aa aa aa aa aa aa aa 00b0 aa aa aa aa aa aa aa aa aa aa 00c0 aa aa aa aa aa aa aa aa aa aa 00d0 aa aa aa aa aa aa aa aa aa aa 00e0 aa aa aa aa aa aa aa aa aa aa 00f0 aa aa aa aa aa aa aa aa aa aa 0100 aa aa aa aa aa aa aa aa aa aa 0110 aa aa aa aa aa aa aa aa aa aa 0120 aa aa aa aa aa aa aa aa aa aa 0130 aa aa aa aa aa aa aa aa aa aa 0140 aa aa aa aa aa aa aa aa aa aa 0150 aa aa aa aa aa aa aa aa aa aa 0160 aa aa aa aa aa aa aa aa aa aa 0170 aa aa aa aa aa aa aa aa aa aa 0180 aa aa aa aa aa aa aa aa aa aa 0190 aa aa aa aa aa aa aa aa aa aa </pre>
---	--

216 numaralı ilk fragment

217 04:48:40,125160 192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in frame 218]
218 04:48:40,125981 192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found)
219 04:48:40,144138 10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

<ul style="list-style-type: none"> > Frame 217: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73) ▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 <ul style="list-style-type: none"> 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1500 Identification: 0x3323 (13091) ▼ 001. = Flags: 0x1, More fragments <ul style="list-style-type: none"> 0... = Reserved bit: Not set .0.. = Don't fragment: Not set ..1. = More fragments: Set ...0 0000 1011 1001 = Fragment Offset: 1480 > Time to Live: 1 Protocol: ICMP (1) Header Checksum: 0x0698 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 [Reassembled IPv4 in frame: 218] ▼ Data (1480 bytes) <ul style="list-style-type: none"> Data: aa... [Length: 1480] 	<pre> 0000 00 06 25 da af 73 00 20 e0 8a 0010 05 dc 33 23 20 b9 01 01 06 98 0020 17 64 aa aa aa aa aa aa aa aa aa 0030 aa aa aa aa aa aa aa aa aa aa 0040 aa aa aa aa aa aa aa aa aa aa 0050 aa aa aa aa aa aa aa aa aa aa 0060 aa aa aa aa aa aa aa aa aa aa 0070 aa aa aa aa aa aa aa aa aa aa 0080 aa aa aa aa aa aa aa aa aa aa 0090 aa aa aa aa aa aa aa aa aa aa 00a0 aa aa aa aa aa aa aa aa aa aa 00b0 aa aa aa aa aa aa aa aa aa aa 00c0 aa aa aa aa aa aa aa aa aa aa 00d0 aa aa aa aa aa aa aa aa aa aa 00e0 aa aa aa aa aa aa aa aa aa aa 00f0 aa aa aa aa aa aa aa aa aa aa 0100 aa aa aa aa aa aa aa aa aa aa 0110 aa aa aa aa aa aa aa aa aa aa 0120 aa aa aa aa aa aa aa aa aa aa 0130 aa aa aa aa aa aa aa aa aa aa 0140 aa aa aa aa aa aa aa aa aa aa 0150 aa aa aa aa aa aa aa aa aa aa 0160 aa aa aa aa aa aa aa aa aa aa 0170 aa aa aa aa aa aa aa aa aa aa 0180 aa aa aa aa aa aa aa aa aa aa 0190 aa aa aa aa aa aa aa aa aa aa </pre>
---	---

217 numaralı ikinci fragment

218	04:48:40,125981	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1
219	04:48:40,144138	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in tran
<					
✓ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 <div> 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 568 Identification: 0x3323 (13091) ✓ 000. = Flags: 0x0 0... = Reserved bit: Not set .0.. = Don't fragment: Not set ..0. = More fragments: Not set ...0 0001 0111 0010 = Fragment Offset: 2960 > Time to Live: 1 Protocol: ICMP (1) Header Checksum: 0x2983 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 ✓ [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)] [Frame: 216, payload: 0-1479 (1480 bytes)] [Frame: 217, payload: 1480-2959 (1480 bytes)] [Frame: 218, payload: 2960-3507 (548 bytes)] [Fragment count: 3] [Reassembled IPv4 length: 3508] [Reassembled IPv4 data: 0800a9c303009e03373920aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...] </div>					
✓ Internet Control Message Protocol <div> 0000 08 00 a9 c3 0010 aa aa aa aa 0020 aa aa aa aa 0030 aa aa aa aa 0040 aa aa aa aa 0050 aa aa aa aa 0060 aa aa aa aa 0070 aa aa aa aa 0080 aa aa aa aa 0090 aa aa aa aa 00a0 aa aa aa aa 00b0 aa aa aa aa 00c0 aa aa aa aa 00d0 aa aa aa aa 00e0 aa aa aa aa 00f0 aa aa aa aa 0100 aa aa aa aa 0110 aa aa aa aa 0120 aa aa aa aa 0130 aa aa aa aa 0140 aa aa aa aa 0150 aa aa aa aa 0160 aa aa aa aa 0170 aa aa aa aa 0180 aa aa aa aa </div>					
<					
✓ Frame (582 bytes) <div>Ref</div>					

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/sevir-defteri/blog/2013/09/06/icmp-\(internet-control-message-protocol-internet-kontrol-mesaj-protokol%C3%BC\)](https://bidb.itu.edu.tr/sevir-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