



Laboratuvar Raporu 5

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Ferdi İslam Yılmaz

152120191055

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İindekiler

2	Giriş.....	3
3	Laboratuvar Uygulaması.....	3
3.1.1	Bir traceroute uygulamasından paketleri yakalıyoruz.....	3
4	Kaynaka.....	10

2 Giriş

Internet protokolü, verilerin iletimini ve yönlendirmesini sağlayan bir dizi kurallar ve standartlardan oluşan bir iletişim protokolüdür. Bu protokol, verilerin bilgisayarlar, sunucular ve diğer ağ cihazları arasında güvenli ve etkili bir şekilde iletilmesini sağlar.

3 Laboratuvar Uygulaması

3.1.1 Bir traceroute uygulamasından paketleri yakalıyoruz.

1. Bilgisayarınızı IP adresi nedir?

192.168.0.108 benim IP adresimdir.

2. IP paket başlığı içerisindeki üst katman protokol alanındaki değer nedir?

The screenshot displays a network packet capture interface. The top section shows a list of captured packets. Packet 1492 is highlighted, showing it is an ICMP Echo request from 192.168.0.108 to 104.244.42.129. The bottom section shows the detailed header information for this packet, including the source and destination addresses, the ICMP type (Echo request), and the sequence number (8950). The 'Internet Control Message Protocol' section is expanded, showing the type, code, checksum, identifier, and sequence number. The 'Data' section is also visible, showing the payload of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1491	13.146354	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x0001, seq=8950/63010, ttl=13 (TTL=13)
1492	13.151748	195.2.14.82	192.168.0.108	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1493	13.168175	192.168.0.108	66.22.244.26	UDP	85	60621 → 50022 Len=43
1494	13.187369	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4868) [Reassembled]
1495	13.187369	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001, seq=8951/63266, ttl=255 (TTL=255)
1496	13.190118	192.168.0.108	66.22.244.26	UDP	85	60621 → 50022 Len=43
1497	13.207160	192.168.0.108	66.22.244.26	UDP	85	60621 → 50022 Len=43
1498	13.221257	66.22.244.26	192.168.0.108	RTCP	94	Receiver Report
1499	13.225067	192.168.0.108	66.22.244.26	UDP	85	60621 → 50022 Len=43

Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.108
Destination Address: 104.244.42.129
> [2 IPv4 Fragments (1980 bytes): #1490(1480), #1491(500)]
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x194d [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 8950 (0x22f6)
Sequence Number (LE): 63010 (0xf622)
> [No response seen]
> Data (1972 bytes)

Üst katman protokol alanındaki değer ICMP(0X01).

3. IP başlığında kaç byte vardır? IP datagramının yükü kaç byte'dır?

13	0.638325	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=48)
14	0.638325	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001, seq=8680/59425, ti
15	0.689382	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=48)
16	0.689382	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001, seq=8681/59681, ti
17	0.691044	192.168.0.1	192.168.0.108	ICMP	590	Time-to-live exceeded (Time to live exceeded in ti
18	0.740277	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=48)
19	0.740277	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001, seq=8682/59937, ti

> Frame 13: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interfa	0000	b0 95 75 59 20
> Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95	0010	05 dc 48 1d 20
> Internet Protocol Version 4, Src: 192.168.0.108, Dst: 172.217.20.68	0020	14 44 08 00 1a
0100 = Version: 4	0030	20 20 20 20 20
.... 0101 = Header Length: 20 bytes (5)	0040	20 20 20 20 20
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0050	20 20 20 20 20
Total Length: 1500	0060	20 20 20 20 20
Identification: 0x481d (18461)	0070	20 20 20 20 20
> 001. = Flags: 0x1, More fragments	0080	20 20 20 20 20
...0 0000 0000 0000 = Fragment Offset: 0	0090	20 20 20 20 20
Time to Live: 255	00a0	20 20 20 20 20
Protocol: ICMP (1)	00b0	20 20 20 20 20
Header Checksum: 0x0000 [validation disabled]	00c0	20 20 20 20 20
[Header checksum status: Unverified]	00d0	20 20 20 20 20
Source Address: 192.168.0.108	00e0	20 20 20 20 20
Destination Address: 172.217.20.68	00f0	20 20 20 20 20
[Reassembled IPv4 in frame: 14]	0100	20 20 20 20 20
	0110	20 20 20 20 20
	0120	20 20 20 20 20

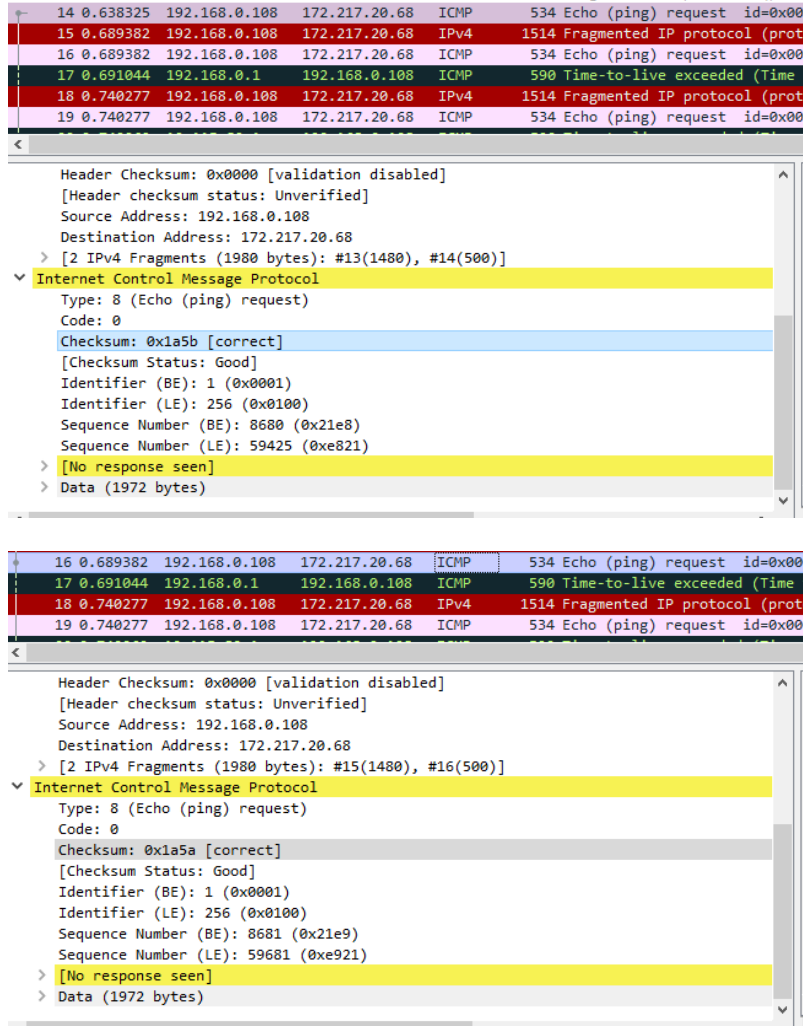
IP başlığında 20 byte vardır 36 byte ise IP datagram payload'ındadır çünkü gönderdiğimiz paketler 56 byte'dır.

4. Bu IP datagramı parçalara bölünmüş müdür?

> Frame 13: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interfa
> Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95
> Internet Protocol Version 4, Src: 192.168.0.108, Dst: 172.217.20.68
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x481d (18461)
> 001. = Flags: 0x1, More fragments
...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: 192.168.0.108
Destination Address: 172.217.20.68
[Reassembled IPv4 in frame: 14]

Fragment offset 0 olduğu için paket fragmente olmamış yani parçalara bölünmemiş.

5. IP datagramdaki hangi alanlar bir datagramdan sonraki datagrama geçildiğinde değişiyor?



The top screenshot shows a packet capture with several ICMP Echo (ping) requests and fragmented IP protocols. The bottom screenshot shows the details of an ICMP Echo (ping) request, highlighting the fields that change between packets: Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), and Sequence Number (LE).

Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.108
Destination Address: 172.217.20.68
> [2 IPv4 Fragments (1980 bytes): #13(1480), #14(500)]
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x1a5b [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 8680 (0x21e8)
Sequence Number (LE): 59425 (0xe821)
> [No response seen]
> Data (1972 bytes)

Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.108
Destination Address: 172.217.20.68
> [2 IPv4 Fragments (1980 bytes): #15(1480), #16(500)]
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x1a5a [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 8681 (0x21e9)
Sequence Number (LE): 59681 (0xe921)
> [No response seen]
> Data (1972 bytes)

Başlık checksum'ı ve kimlik değişiklikleri bir datagramdan sonrakine geçerken değişiyor.

6. Hangi alanlar sabit kalıyor? Hangi alanlar sabit kalmalı? Hangi alanlar değişmeli? Neden?

Sabit kalan ve sabit kalması gereken alanlar:

- Version(IPv4)
- Header boyutu
- Kaynak IP
- Hedef IP
- Üst katman protokolü

Değişmesi gereken alanlar:

- Başlık checksum
- Kimlikler

7. IP datagramının Kimlik(Identification) alanındaki gördüğünüz değerleri açıklayınız.

Kimlik alanında ki pattern her echo talebinde bir artmaktadır.

8. Kimlik alanının ve TTL(Time to Live) alanının değeri nedir?

11	0.108296	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x0001,
12	0.219301	66.22.244.26	192.168.0.108	RTCP	94	Receiver Report
13	0.638325	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=I
14	0.638325	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001,
15	0.689382	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=I
16	0.689382	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001,
17	0.691044	192.168.0.1	192.168.0.108	ICMP	590	Time-to-live exceeded (Time to
18	0.740277	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=I
19	0.740277	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001,
20	0.742269	10.115.80.1	192.168.0.108	ICMP	590	Time-to-live exceeded (Time to
21	0.790251	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=I

▼	Internet Protocol Version 4, Src: 192.168.0.108, Dst: 104.244.42.129
	0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
	Total Length: 520
	Identification: 0xbfe3 (49123)
>	000. = Flags: 0x0
	...0 0000 1011 1001 = Fragment Offset: 1480
	Time to Live: 13
	Protocol: ICMP (1)
	Header Checksum: 0x0000 [validation disabled]
	[Header checksum status: Unverified]
	Source Address: 192.168.0.108
	Destination Address: 104.244.42.129
>	[2 IPv4 Fragments (1980 bytes): #10(1480), #11(500)]
▼	Internet Control Message Protocol

TTL değeri 13. Kimlik alanının değeri ise 49123(0xbfe3)'tür.

9. Bu değerler neden en yakın router tarafından bilgisayarınıza gönderilen tüm ICMP TTL-exceeded yanıtları değişmeden kalıyor?

Kimlik alanı tüm yanıtlarda değişir çünkü bu değer benzersiz olması gerekir. Eğer yanıtlar aynı değere sahipse daha büyük bir paketin parçaları olmalıdır. TTL alanı da değişmez çünkü ilk atlama router'ına kadar geçen süre her zaman aynıdır.

10. Pingplotter'daki paket boyutunu 2000 yaptıktan sonra bilgisayarınız tarafından gönderilen ilk ICMP echo istek mesajını bulun. Bu mesaj birden fazla IP datagramına bölünmüş müdür?

The screenshot shows a Wireshark packet capture of an ICMP echo request (ping) from 192.168.0.108 to 104.244.42.129. The packet is fragmented into two parts. The first part is highlighted in blue and shows the following details:

- Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95:4d:59:20:3e)
- Internet Protocol Version 4, Src: 192.168.0.108, Dst: 104.244.42.129
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 520
 - Identification: 0xbfe1 (49121)
 - 000. = Flags: 0x0
 - ...0 0000 1011 1001 = Fragment Offset: 1480
 - Time to Live: 11
 - Protocol: ICMP (1)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.0.108
 - Destination Address: 104.244.42.129
 - [2 IPv4 Fragments (1980 bytes): #4(1480), #5(500)]
- Internet Control Message Protocol

The second part of the packet is highlighted in yellow and shows the following details:

- Internet Control Message Protocol

The packet list on the left shows the following details for the selected packet (packet 19):

No.	Time	Source	Destination	Protocol	Length	Info
19	0.740277	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x0001, ...

Bu mesaj bir IP datagramından fazla parçaya bölünmüştür.

11. IP başlığındaki hangi bilgiler datagramın parçalandığını gösterir? IP başlığındaki hangi bilgi bunun ilk parça mı yoksa ikinci parça mı olduğunu gösterir? IP datagramının boyutu nedir?

4	0.007288	192.168.0.108	104.244.42.129	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off
5	0.007288	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x0001, seq=8677/
6	0.051790	195.2.31.42	192.168.0.108	ICMP	70	Time-to-live exceeded (Time to live excee
7	0.058187	192.168.0.108	104.244.42.129	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off
8	0.058187	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x0001, seq=8678/
9	0.103931	195.2.14.82	192.168.0.108	ICMP	70	Time-to-live exceeded (Time to live excee
10	0.108296	192.168.0.108	104.244.42.129	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off
11	0.108296	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x0001, seq=8679/
12	0.219301	66.22.244.26	192.168.0.108	RTCP	94	Receiver Report
13	0.638325	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off
14	0.638325	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001, seq=8680/
15	0.689382	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off
16	0.689382	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001, seq=8681/
17	0.691044	192.168.0.1	192.168.0.108	ICMP	590	Time-to-live exceeded (Time to live excee
18	0.740277	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off
19	0.740277	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x0001, seq=8682/

> Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95: ^	0000	b0 95
✓ Internet Protocol Version 4, Src: 192.168.0.108, Dst: 104.244.42.129	0010	05 dc
0100 = Version: 4	0020	2a 81
.... 0101 = Header Length: 20 bytes (5)	0030	20 20
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0040	20 20
Total Length: 1500	0050	20 20
Identification: 0xbfe1 (49121)	0060	20 20
> 001. = Flags: 0x1, More fragments	0070	20 20
...0 0000 0000 0000 = Fragment Offset: 0	0080	20 20
Time to Live: 11	0090	20 20
Protocol: ICMP (1)	00a0	20 20
Header Checksum: 0x0000 [validation disabled]	00b0	20 20
[Header checksum status: Unverified]	00c0	20 20
Source Address: 192.168.0.108	00d0	20 20
Destination Address: 104.244.42.129	00e0	20 20
[Reassembled IPv4 in frame: 5]	00f0	20 20
> Data (1480 bytes)	0100	20 20
	0110	20 20
	0120	20 20

Flag alanı datagramın birden fazla alana ayrıldığını göstermektedir. Fragment(bölünme) offset'i 0 olduğu için bu ilk paket olduğunu görüyoruz sonraki paketin fragment offset'i 1480'dir. Datagramı total boyutu 1500'dür.

12. İkinci paketi incelediğimizde hangi bilgi bunun ilk datagram paketi olmadığını gösterir? Daha fazla bölünme var mıdır?

5	0.007288	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x000
6	0.051790	195.2.31.42	192.168.0.108	ICMP	70	Time-to-live exceeded (Time
7	0.058187	192.168.0.108	104.244.42.129	IPv4	1514	Fragmented IP protocol (prot
8	0.058187	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x000
9	0.103931	195.2.14.82	192.168.0.108	ICMP	70	Time-to-live exceeded (Time
10	0.108296	192.168.0.108	104.244.42.129	IPv4	1514	Fragmented IP protocol (prot
11	0.108296	192.168.0.108	104.244.42.129	ICMP	534	Echo (ping) request id=0x000
12	0.219301	66.22.244.26	192.168.0.108	RTCP	94	Receiver Report
13	0.638325	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (prot
14	0.638325	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x000
15	0.689382	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (prot
16	0.689382	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x000
17	0.691044	192.168.0.1	192.168.0.108	ICMP	590	Time-to-live exceeded (Time
18	0.740277	192.168.0.108	172.217.20.68	IPv4	1514	Fragmented IP protocol (prot
19	0.740277	192.168.0.108	172.217.20.68	ICMP	534	Echo (ping) request id=0x000

>	Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95 ^
▼	Internet Protocol Version 4, Src: 192.168.0.108, Dst: 104.244.42.129
	0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
	Total Length: 520
	Identification: 0xbfe1 (49121)
>	000. = Flags: 0x0
	...0 0000 1011 1001 = Fragment Offset: 1480
	Time to Live: 11
	Protocol: ICMP (1)
	Header Checksum: 0x0000 [validation disabled]
	[Header checksum status: Unverified]
	Source Address: 192.168.0.108
	Destination Address: 104.244.42.129
>	[2 IPv4 Fragments (1980 bytes): #4(1480), #5(500)]
▼	Internet Control Message Protocol

Bunun ikinci fragment olduğu belli çünkü önceki soruda bahsettiğim gibi ikinci fragmentin offset'i 1480 olacaktır demişim ve bunun fragment offset'i 1480. Artık daha fazla bölünme yoktur çünkü Flag alanında daha fazla bölünme var yazmıyor.

13. Birinci ve ikinci fragment'in IP başlığında hangi alanlar değişiyor?

Yukarıdaki resimlere bakıldığında değişen alanlar şunlardır:

- Length
- Flag Set
- Fragment offset
- Başlık checksum

14. Orijinal datagramdan kaç tane fragment oluşturulmuştur?

3500 byte'a yükselttikten sonra 3 fragment oluşmuş.

15. Fragmentler değiştikçe IP başlığındaki hangi alanlar değişir?

Fragment offset ve checksum değişir.

4 Kaynakça