

Computer Networks Lab 6

Shane Cincotta

May 11, 2020

```
/home/cincottash/Documents/School-Classes/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-trace-1 380 total packets, 380 shown

No.      Time      Source      Destination      Protocol Length Info
 8 6.163045 192.168.1.102 128.59.23.100    ICMP      98      Echo (ping) request id=0x0300,
seq=20483/848, ttl=1 (no response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)
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: 84
Identification: 0x32d0 (13008)
Flags: 0x0000
 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: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ca [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 20483 (0x5003)
Sequence number (LE): 848 (0x0350)
[No response seen]
Data (56 bytes)
0000 37 32 20 aa aa aa aa aa aa aa aa aa aa aa aa 72 .....
0010 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0020 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0030 aa aa aa aa aa aa aa .....
Data: 373220aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
[Length: 56]
```

Figure 1:

What is the IP address of your computer?

According to figure 1, the IP address of my computer is 192.168.1.102.

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

According to figure 1, the value in the upper layer protocol field is ICMP (1).

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.

According to figure 1, there are 20 bytes in the IP header. There are 36 bytes in the payload. This can be calculated by subtracting the IP header size (20) from the total data size (56).

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

According to figure 1, the data has not been fragmented. This can be determined by the value of the more fragments bit, which is set to 0.

```

No.      Time      Source      Destination      Protocol Length Info
 0 6.163045      192.168.1.102      128.59.23.100      ICMP      96      Echo (ping) request id=0x0300,
seq=20483/848, ttl=1 (no response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)
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: 84
Identification: 0x32d0 (13008)
Flags: 0x0000
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ca [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 20483 (0x5003)
Sequence number (LE): 848 (0x0350)
[No response seen]
Data (56 bytes)
0000 37 32 20 aa aa aa aa aa aa aa aa aa aa aa aa aa aa 72 .....
0010 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0020 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....

No.      Time      Source      Destination      Protocol Length Info
10 6.180629      192.168.1.102      128.59.23.100      ICMP      96      Echo (ping) request id=0x0300,
seq=20739/849, ttl=2 (no response found!)
Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)
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: 84
Identification: 0x32d1 (13009)
Flags: 0x0000
Time to live: 2
Protocol: ICMP (1)
Header checksum: 0x2c2b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf6ca [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 20739 (0x5103)
Sequence number (LE): 849 (0x0351)
[No response seen]
Data (56 bytes)
0000 37 32 20 aa aa aa aa aa aa aa aa aa aa aa aa aa aa 72 .....
0010 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0020 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....

```

Figure 2:

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

According to figure 2, the Identification, Time to live, Header checksum and sequence number never change.

```

No.    Time    Source                Destination            Protocol Length Info
 8 6.163045  192.168.1.102        128.59.23.100         ICMP      98      Echo (ping) request id=0x0300,
seq=20483/849, ttl=1 (no response found)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_Ba: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
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d0 (13008)
Flags: 0x0000
Time to Live: 1
Protocol: ICMP (1)
Header checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ca [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 20483 (0x5003)
Sequence number (LE): 849 (0x0350)
[No response seen]
Data (56 bytes)
0000 37 32 20 aa aa aa aa aa aa aa aa aa aa aa aa aa aa 72 .....
0010 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0020 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
No.    Time    Source                Destination            Protocol Length Info
10 6.188629  192.168.1.102        128.59.23.100         ICMP      98      Echo (ping) request id=0x0300,
seq=20739/849, ttl=2 (no response found)
Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_Ba: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
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d1 (13009)
Flags: 0x0000
Time to Live: 2
Protocol: ICMP (1)
Header checksum: 0x2c2b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf6ca [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 20739 (0x5103)
Sequence number (LE): 849 (0x0351)
[No response seen]
Data (56 bytes)
0000 37 32 20 aa aa aa aa aa aa aa aa aa aa aa aa aa aa 72 .....
0010 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0020 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....

```

Figure 3:

Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

According to figure 3: version, header length, source IP, destination IP differentiated services and upper layer protocol all remain constant.

The fields that must stay constant are: version (because we are using IPv4), header length (because each packet is ICMP), source IP (because we are sending from the same source PC), destination IP (because we are sending to the same source PC), differentiated services (because each packet is ICMP thus they use the same type of service) and upper layer protocol (because each packet is ICMP).

The fields that must change are: identification (because each packet has a different ID), time to live (because each TTL is incremented after each packet) and header checksum (because the checksum changes along with the header).

0000	00 06 25	da af 73 00 20	e0 8a 70 1a 08 00 45 00	..%..s. .p...E.
0010	00 54 32	d1 00 00 02 01	2c 2b c0 a8 01 66 80 3b	..T2.....,+.f.;
0020	17 64 08 00	f6 ca 03 00	51 03 37 32 20 aa aa aa	..d.....Q.72...
0030	aa aa aa aa	aa aa aa aa	aa aa aa aa aa aa aa aa
0040	aa aa aa aa	aa aa aa aa	aa aa aa aa aa aa aa aa
0050	aa aa aa aa	aa aa aa aa	aa aa aa aa aa aa aa aa
0060	aa aa			..

Figure 4:

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

According to figure 4, the pattern I observe is that the IP header Identification fields increment after each ICMP Echo.

```
/home/cincotach/Documents/School-Courses/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-trace-1.380 total packets, 380 shown

No.      Time            Source            Destination      Protocol Length Info
27 6.382957      192.205.32.106    192.168.1.102    ICMP             70      Time-to-live exceeded (Time to live
exceeded in transit)
Frame 27: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: Linksys6_da:af:73 (00:06:25:da:af:73), Dst: Actionte_Ba:70:1a (00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 192.205.32.106, Dst: 192.168.1.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x0000 (0)
Flags: 0x0000
Time to live: 240
Protocol: ICMP (1)
Header checksum: 0x217f [validation disabled]
[Header checksum status: Unverified]
Source: 192.205.32.106
Destination: 192.168.1.102
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xd946 [correct]
[Checksum Status: Good]
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: 84
Identification: 0x32d8 (13016)
Flags: 0x0000
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0xf60e [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xefca [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 22531 (0x5603)
Sequence number (LE): 856 (0x0358)
```

Figure 5:

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

According to figure 5, the value of the identification field is 0 and the value of the TTL field is 240.

```

/home/cincostash/Documents/School-Courses/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-tace-1.380 total packets, 380 shown

No.      Time      Source      Destination  Protocol Length Info
 27 6.382957 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live
exceeded in transit)
Frame 27: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: Linksys6_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 192.205.32.106, Dst: 192.168.1.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x0000 (0)
Flags: 0x0000
Time to live: 246
Protocol: ICMP (1)
Header checksum: 0x217f [validation disabled]
[Header checksum status: Unverified]
Source: 192.205.32.106
Destination: 192.168.1.102
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xd946 [correct]
[Checksum Status: Good]
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: 84
Identification: 0x32d8 (13016)
Flags: 0x0000
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0xf60e [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xefca [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 22531 (0x5803)
Sequence number (LE): 856 (0x0358)

No.      Time      Source      Destination  Protocol Length Info
 57 11.388011 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live
exceeded in transit)
Frame 57: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: Linksys6_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 192.205.32.106, Dst: 192.168.1.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x0000 (0)
Flags: 0x0000
Time to live: 246
Protocol: ICMP (1)
Header checksum: 0x217f [validation disabled]
[Header checksum status: Unverified]
Source: 192.205.32.106
Destination: 192.168.1.102
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xd947 [correct]
[Checksum Status: Good]
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: 84
Identification: 0x32e6 (13030)
Flags: 0x0000
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0xf600 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0

```

Figure 6:

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

According to figure 6, the identification field does not change. The reason for this is when two or more IP datagrams have the same ID value, they are fragments of a larger IP datagram.

According to figure 6, the TTL fields remains unchanged because the TTL for the first hop router is always the same.

92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found)
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found)
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found)
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #

Figure 7:

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?

According to figure 7, this packet has been fragmented across more than one IP diagram.

```

/home/cincomash/Documents/School-Courses/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-tace-1 380 total packets, 380 shown

No.      Time            Source            Destination        Protocol Length Info
 92 28.441511      192.168.1.102      128.59.23.100      IPv4      1514    Fragmented IP protocol (proto=ICMP 1,
off=0, ID=32f9) [Reassembled in #93]
Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Actionte_Ba: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
 0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
  .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0x32f9 (13049)
Flags: 0x2000, 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: 192.168.1.102
Destination: 128.59.23.100
Reassembled IPv4 in frame: 93
Data (1480 bytes)

```

Figure 8:

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?

According to figure 8, the flags bit for more fragments is set, this tells us that the datagram is fragmented. Also, since the fragment offset is 0, we know that this is the first fragment. This datagram has a total length of 1500 (1480 + header size).

```

/home/cincomash/Documents/School-Courses/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-tace-1 380 total packets, 380 shown

No.      Time            Source            Destination        Protocol Length Info
 96 28.471338      192.168.1.102      128.59.23.100      ICMP      562     Echo (ping) request id=0x0300,
seq=30723/888, ttl=2 (no response found)
Frame 96: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: Actionte_Ba: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
 0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 548
Identification: 0x32fa (13050)
Flags: 0x0009
 0... .. = Reserved bit: Not set
 .0... .. = Don't fragment: Not set
 ..0... .. = More fragments: Not set
 ...0 0000 1011 1001 = Fragment offset: 105
Time to live: 2
Protocol: ICMP (1)
Header checksum: 0x2079 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[2 IPv4 Fragments (2098 bytes): #95(1480), #96(520)]
Internet Control Message Protocol

```

Figure 9:

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?

According to figure 9, we can tell that this is not the first fragment because the fragment offset is 185, also we know it is the last fragment because the more fragments flag is not set.

```

/home/cincomash/Documents/School-Classes/CISC 450 (Computer Networks 1)/Labs/Lab6/ip-ethereal-trace-1 380 total packets, 380 shown

No.      Time            Source            Destination      Protocol Length Info
 93 28.442185      192.168.1.102     128.59.23.100    ICMP             562    Echo (ping) request id=0x0300,
seq=30467/887, ttl=1 (no response found!)
Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 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
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 548
Identification: 0x32f9 (13049)
Flags: 0x0009
 0... .. = Reserved bit: Not set
.0... .. = Don't fragment: Not set
..0... .. = More fragments: Not set
...0 0000 1011 1001 = Fragment offset: 185
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xd8c6 [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 (2008 bytes)

```

Figure 10:

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

According to figure 10, we can see that the total length, checksum, flags and fragment offset are changed.

215	41.038658	192.168.1.102	199.2.53.206	TCP	62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
216	43.466136	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled]
217	43.466808	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled]
218	43.467629	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response)
220	43.492284	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled]
221	43.492953	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled]
222	43.493901	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response)
223	43.512145	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled]
224	43.512818	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled]
225	43.513660	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response)
226	43.542792	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled]
227	43.543462	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3326) [Reassembled]

Figure 11:

How many fragments were created from the original datagram?

According to figure 11, after switching to 3500, there are 3 packets created.

```

No.      Time            Source            Destination      Protocol Length Info
 218 43.467629      192.168.1.102      128.59.23.100    ICMP      582    Echo (ping) request id=0x0300,
seq=40451/926, ttl=1 (no response found!)
Frame 218: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
Ethernet II, Src: Actionte_Ba: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
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 568
Identification: 0x3323 (13091)
Flags: 0x0172
 0... .... = Reserved bit: Not set
.0... .... = Don't fragment: Not set
..0... .... = More fragments: Not set
...0 0001 0111 0010 = Fragment offset: 370
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2983 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xa9c3 [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 40451 (0x9e03)
Sequence number (LE): 926 (0x039e)
[No response seen]
Data (3500 bytes)

```

Figure 12:

What fields change in the IP header among the fragments?

According to figure 12, the fragment offset and checksum change among the fragments.