

Wireshark Networking Lab

IP v8.0

Saiful Islam Tarek

Department of Computer Science and Engineering
University of Chittagong

December 20, 2022

Overview

1. Question 1
2. Question 2
3. Question 3
4. Question 4
5. Question 5
6. Question 6
7. Question 7
8. Question 8
9. Question 9
10. Question 10
11. Question 11
12. Question 12
13. Question 13
14. Question 14
15. Question 15

1. Select the first ICMP Echo Request message sent by your computer.....What is the IP address of your computer?

Answer

IP address of my computer is : 192.168.1.102

No.	Time	Source	Destination	Protocol	Length	Info
31	6.432918	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
32	6.439037	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23299/859, ttl=12 (n
→ 33	6.465882	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23555/860, ttl=13 (r
← 34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=23555/860, ttl=242 (
39	11.159759	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23811/861, ttl=1 (no

> Frame 33: 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:a
`- 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

0000	00	06	25	da	af	73	00	20	e0	8a
0010	00	54	32	dc	00	00	0d	01	21	20
0020	17	64	08	00	eb	ca	03	00	5c	03
0030	aa									
0040	aa									
0050	aa									
0060	aa	aa								

2. What is the value in the upper layer protocol field?

Answer

The value is : ICMP(1)

```
✓ Frame 0: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
  > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:a
    ▼ 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: 0x32dc (13020)
        ▼ 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: 13
        Protocol: ICMP (1) Protocol: ICMP (1)
        Header Checksum: 0x2120 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.1.102
        Destination Address: 128.59.23.100
    > Internet Control Message Protocol
```

3. How many bytes are in the IP header?

Answer

20 bytes

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
31	6.432918	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time
32	6.439037	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0
33	6.465882	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0
39	11.159759	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0

> Frame 33: 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: LinksysG_da:af:73 (00:06:25:da:a
▼ 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

0000 00
0010 00
0020 17
0030 aa
0040 aa
0050 aa
0060 aa

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

Answer

Total length - Header length = 64 bytes

icmp							
No.	Time	Source	Destination	Protocol	Length	Info	
31	6.432918	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time	
32	6.439037	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x03	
33	6.465882	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x03	
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time	
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x03	
39	11.159759	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x03	

> Frame 33: 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: LinksysG_da:af:73 (00:06:25:da:a
▼ 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: 0x32dc (13020)
 <--> 84 - 20 = 64 bytes
 <--> 000. = Flags: 0x0
 <--> 0000 00
 0010 00
 0020 17
 0030 aa
 0040 aa
 0050 aa
 0060 aa

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

Answer

This IP datagram is not fragmented.

If fragment flag is not set then datagram is not fragmented.

If fragment flag is set then datagram is fragmented.

Continue....

→	33	6.465882	192.168.1.102	[128.59.23.100]	ICMP	98	Echo (ping) request	i
	34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded	
←	35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply	i
	39	11.159759	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request	i

- Frame 33: 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: LinksysG_da:af:73 (00:06:25:da:a0:00)
- ▼ 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: 0x32dc (13020)

▼ 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: 13

000
001
002
003
004
005
006

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?

Answer

The Identification field.

TTL or Time to live field.

Header checksum field.

Continue....

```
> 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: LinksysG_da:af:73 (00:06:25:da:a
< 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)
    000. .... - Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

0000	00 06 25 da
0010	00 54 32 d0
0020	17 64 08 00
0030	aa aa aa aa
0040	aa aa aa aa
0050	aa aa aa aa
0060	aa aa

Continue....

```
> 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: LinksysG_da:af:73 (00:06:25:da:a
< 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)
    > 000. .... = Flags: 0x0
        ... 0 0000 0000 0000 = Fragment Offset: 0
    > Time to Live: 2
        Protocol: ICMP (1)
        Header Checksum: 0x2c2b [validation disabled]
            [Header checksum status: Unverified]
        Source Address: 192.168.1.102
        Destination Address: 128.59.23.100
    > Internet Control Message Protocol
```

000
001
002
003
004
005
006

6.Which fields stay constant? Which of the fields must stay constant?

Answer

Source address

Destination address

Header length

IP version

Continue...

```
1 12 6 224505 24 128 100 107 100 168 1 100 TCMP 70 Time to Live: 255
> 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: LinksysG_da:af:73 (00:06:25:da:a
< 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)
> 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 2
    Protocol: ICMP (1)
    Header Checksum: 0x2c2b [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

6.1 Which fields must change?

Answer

The Identification field.

TTL or Time to live field.

Header checksum field.

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

Answer

I see that the value of this field is increased by 1.

Continue....

```
> 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: LinksysG_da:af:73 (00:06:25:da:a
< 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)
    000. .... - Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

0000	00 06 25 da
0010	00 54 32 d0
0020	17 64 08 00
0030	aa aa aa aa
0040	aa aa aa aa
0050	aa aa aa aa
0060	aa aa

Continue....

```
> 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: LinksysG_da:af:73 (00:06:25:da:a
< 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)
> 000. .... = Flags: 0x0
    ... 0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 2
    Protocol: ICMP (1)
    Header Checksum: 0x2c2b [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

000
001
002
003
004
005
006

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

Answer

0xa60b and 244

No.	Time	Source	Destination	Protocol	Length	Info
376	54.659995	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
321	49.827260	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
265	44.655324	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
169	34.147910	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 376: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Linksys_G_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:01)
▼ Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 56
 Identification: 0xa60b (42507)
 000. = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 244
 Protocol: ICMP (1)
 Header Checksum: 0xdxfc5 [validation disabled]

0000 00 20 e0 8a 70 1a 00 06 25 da af
0010 00 38 a6 0b 00 00 f4 01 df c5 43
0020 01 66 0b 00 da 45 00 00 00 00 45
0030 20 00 01 01 d0 16 c0 a8 01 66 80
0040 84 cb 03 00 c2 03

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?

Answer

The Identification field value is changed but TTL remain unchanged

Continue....

No.	Time	Source	Destination	Protocol	Length	Info
376	54.659995	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
321	49.827260	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
265	44.655324	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
169	34.147910	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 376: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_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: 67.99.58.194, Dst: 192.168.1.102
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 56
 Identification: 0xa60b (42507)
 000. = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 244
 Protocol: ICMP (1)
 Header Checksum: 0xdxfc5 [validation disabled]

0000 00 20 e0 8a 70 1a 00 06 25 da af
0010 00 38 a6 0b 00 00 f4 01 df c5 43
0020 01 66 0b 00 da 45 00 00 00 00 45
0030 20 00 01 01 d0 16 c0 a8 01 66 80
0040 84 cb 03 00 c2 03

Continue....

No.	Time	Source	Destination	Protocol	Length	Info
376	54.659995	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
321	49.827260	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
265	44.655324	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
169	34.147910	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 321: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_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: 67.99.58.194, Dst: 192.168.1.102
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 56
 Identification: 0xa5e3 (42467)
 > 000. = Flags: 0x0
 ... 0 0000 0000 0000 - Fragment Offset: 0
 Time to Live: 244
 Protocol: ICMP (1)

0000 00 20 e0 8a 70 1a 00 06 25 da af
0010 00 38 a5 e3 00 00 f4 01 df ed 43
0020 01 66 0b 00 da 44 00 00 00 00 45
0030 20 00 01 01 d0 24 c0 a8 01 66 80
0040 91 cc 03 00 b5 03

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?

Answer

Yes , it has 2 fragment.

Continue....

Screenshot of NetworkMiner tool showing network traffic analysis.

The table lists captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
52	11.332109	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
75	16.312871	12.123.40.218	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
77	16.338078	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (request)
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (request)
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (request)
100	29.531202	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (request)

Selected packet details:

- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:d4)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - Version: 4
 - Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 548
 - Identification: 0x32f9 (13049)
 - Flags: 0x0
 - 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)]
- Internet Control Message Protocol
 - 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)

Hex dump of the selected ICMP request:

0000	08 00 d0 c6 03 00 77 03	37 3
0010	aa aa aa aa aa aa aa aa	aa a
0020	aa aa aa aa aa aa aa aa	aa a
0030	aa aa aa aa aa aa aa aa	aa a
0040	aa aa aa aa aa aa aa aa	aa a
0050	aa aa aa aa aa aa aa aa	aa a
0060	aa aa aa aa aa aa aa aa	aa a
0070	aa aa aa aa aa aa aa aa	aa a
0080	aa aa aa aa aa aa aa aa	aa a
0090	aa aa aa aa aa aa aa aa	aa a
00a0	aa aa aa aa aa aa aa aa	aa a
00b0	aa aa aa aa aa aa aa aa	aa a
00c0	aa aa aa aa aa aa aa aa	aa a
00d0	aa aa aa aa aa aa aa aa	aa a
00e0	aa aa aa aa aa aa aa aa	aa a
00f0	aa aa aa aa aa aa aa aa	aa a
0100	aa aa aa aa aa aa aa aa	aa a
0110	aa aa aa aa aa aa aa aa	aa a
0120	aa aa aa aa aa aa aa aa	aa a
0130	aa aa aa aa aa aa aa aa	aa a
0140	aa aa aa aa aa aa aa aa	aa a
0150	aa aa aa aa aa aa aa aa	aa a
0160	aa aa aa aa aa aa aa aa	aa a
0170	aa aa aa aa aa aa aa aa	aa a
0180	aa aa aa aa aa aa aa aa	aa a
0190	aa aa aa aa aa aa aa aa	aa a
01a0	aa aa aa aa aa aa aa aa	aa a
01b0	aa aa aa aa aa aa aa aa	aa a
01c0	aa aa aa aa aa aa aa aa	aa a
01d0	aa aa aa aa aa aa aa aa	aa a

Frame (562 bytes) Reassembled IPv4 (2008 bytes)

Bytes 8-2007: Data (data.data)

Continue....

52	11.332109	12.122.10.22	192.168.1.102	ICMP	126 Time-to-live exceeded (Time to live exceeded)
75	16.312871	12.123.40.218	192.168.1.102	ICMP	126 Time-to-live exceeded (Time to live exceeded)
77	16.338078	12.122.10.22	192.168.1.102	ICMP	126 Time-to-live exceeded (Time to live exceeded)
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=3046
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=3072
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=3097
100	28.531292	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=3122

```
Total Length: 548
Identification: 0x32f9 (13049)
000. .... = Flags: 0x0
...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)]
```

|      | 0000 | 08 | 00 | d0 | c6 | 03 |
|------|------|----|----|----|----|----|
| 0010 | aa   | aa | aa | aa | aa | aa |
| 0020 | aa   | aa | aa | aa | aa | aa |
| 0030 | aa   | aa | aa | aa | aa | aa |
| 0040 | aa   | aa | aa | aa | aa | aa |
| 0050 | aa   | aa | aa | aa | aa | aa |
| 0060 | aa   | aa | aa | aa | aa | aa |
| 0070 | aa   | aa | aa | aa | aa | aa |
| 0080 | aa   | aa | aa | aa | aa | aa |
| 0090 | aa   | aa | aa | aa | aa | aa |
| 00a0 | aa   | aa | aa | aa | aa | aa |
| 00b0 | aa   | aa | aa | aa | aa | aa |
| 00c0 | aa   | aa | aa | aa | aa | aa |
| 00d0 | aa   | aa | aa | aa | aa | aa |
| 00e0 | aa   | aa | aa | aa | aa | aa |
| 00f0 | aa   | aa | aa | aa | aa | aa |
| 0100 | aa   | aa | aa | aa | aa | aa |
| 0110 | aa   | aa | aa | aa | aa | aa |
| 0120 | aa   | aa | aa | aa | aa | aa |
| 0130 | aa   | aa | aa | aa | aa | aa |

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented?

### Answer

In the IP header of the first fragment the more fragment flag was set. It indicates that it has another fragment.

# Continue....

| No. | Time      | Source         | Destination    | Protocol | Length | Info                                          |
|-----|-----------|----------------|----------------|----------|--------|-----------------------------------------------|
| 90  | 22.928093 | 192.168.1.102  | 128.119.245.12 | SSH      | 74     | Client: Encrypted packet (len=20)             |
| 91  | 22.952738 | 128.119.245.12 | 192.168.1.102  | TCP      | 60     | 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0  |
| 92  | 28.441511 | 192.168.1.102  | 128.59.23.100  | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=0)  |
| 93  | 28.442185 | 192.168.1.102  | 128.59.23.100  | ICMP     | 562    | Echo (ping) request id=0x0300, seq=30467/88   |
| 94  | 28.462264 | 10.216.228.1   | 192.168.1.102  | ICMP     | 70     | Time-to-live exceeded (Time to live exceeded) |
| 95  | 28.470668 | 192.168.1.102  | 128.59.23.100  | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=55) |

> Frame 92: 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:aaf: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: 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

    0010 05 dc 32 f9 20 00  
    0020 17 64 08 00 d0 c6  
    0030 aa aa aa aa aa aa  
    0040 aa aa aa aa aa aa  
    0050 aa aa aa aa aa aa  
    0060 aa aa aa aa aa aa  
    0070 aa aa aa aa aa aa  
    0080 aa aa aa aa aa aa  
    0090 aa aa aa aa aa aa  
    00a0 aa aa aa aa aa aa  
    00b0 aa aa aa aa aa aa  
    00c0 aa aa aa aa aa aa  
    00d0 aa aa aa aa aa aa  
    00e0 aa aa aa aa aa aa  
    00f0 aa aa aa aa aa aa  
    0100 aa aa aa aa aa aa

# 11.1 How long is this IP datagram?

## Answer

The IP datagram is 1480 bytes long.

| No. | Time      | Source         | Destination    | Protocol | Length | Info                                                            |
|-----|-----------|----------------|----------------|----------|--------|-----------------------------------------------------------------|
| 90  | 22.928093 | 192.168.1.102  | 128.119.245.12 | SSH      | 74     | Client: Encrypted packet (len=20)                               |
| 91  | 22.952738 | 128.119.245.12 | 192.168.1.102  | TCP      | 60     | 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0                    |
| 92  | 28.441511 | 192.168.1.102  | 128.59.23.100  | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Rea      |
| 93  | 28.442185 | 192.168.1.102  | 128.59.23.100  | ICMP     | 562    | Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no r       |
| 94  | 28.462264 | 10.216.228.1   | 192.168.1.102  | ICMP     | 70     | Time-to-live exceeded (Time to live exceeded in transit)        |
| 95  | 28.470669 | 192.168.1.102  | 128.59.23.100  | TCP      | 4      | 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Rea |

> Frame 92: 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:a  
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100  
▼ Data (1480 bytes)  
Data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaa...  
[Length: 1480]

0000 00 06 25 da af 73 00 20 e0 8a 70  
0010 05 dc 32 f9 20 00 01 01 07 7b c6  
0020 17 64 08 00 d0 c6 03 00 77 03 37  
0030 aa  
0040 aa  
0050 aa  
0060 aa  
0070 aa  
0080 aa  
0090 aa aa

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?

### Answer

The flag is 0x0. That means it has not any fragment. Therefore it is the last fragment but not first fragment.

# Continue....

|              |                |                |      |                                                       |
|--------------|----------------|----------------|------|-------------------------------------------------------|
| 90 22.928093 | 192.168.1.102  | 128.119.245.12 | SSH  | 74 Client: Encrypted packet (len=20)                  |
| 91 22.952738 | 128.119.245.12 | 192.168.1.102  | TCP  | 60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0       |
| 92 28.441511 | 192.168.1.102  | 128.59.23.100  | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID= |
| 93 28.442185 | 192.168.1.102  | 128.59.23.100  | ICMP | 562 Echo (ping) request id=0x0300, seq=30467/887, t   |
| 94 28.462264 | 10.216.228.1   | 192.168.1.102  | ICMP | 70 Time-to-live exceeded (Time to live exceeded in    |
| 95 28.470668 | 192.168.1.102  | 128.59.23.100  | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID= |

> 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:a  
▼ 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 0000 1011 1001 = Fragment Offset: 1480  
    > Time to Live: 1

0010 02 24 32 f9 00 b9 01 0:  
0020 17 64 aa aa aa aa aa aa  
0030 aa aa aa aa aa aa aa aa  
0040 aa aa aa aa aa aa aa aa  
0050 aa aa aa aa aa aa aa aa  
0060 aa aa aa aa aa aa aa aa  
0070 aa aa aa aa aa aa aa aa  
0080 aa aa aa aa aa aa aa aa  
0090 aa aa aa aa aa aa aa aa  
00a0 aa aa aa aa aa aa aa aa  
00b0 aa aa aa aa aa aa aa aa  
00c0 aa aa aa aa aa aa aa aa  
00d0 aa aa aa aa aa aa aa aa

# 12.1 Are the more fragments? How can you tell?

## Answer

If more fragment flag is set then it has more fragment. But if flag is not set, then this is the last fragment.

|              |                |                |      |                                                            |
|--------------|----------------|----------------|------|------------------------------------------------------------|
| 90 22.928093 | 192.168.1.102  | 128.119.245.12 | SSH  | 74 Client: Encrypted packet (len=20)                       |
| 91 22.952738 | 128.119.245.12 | 192.168.1.102  | TCP  | 60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0            |
| 92 28.441511 | 192.168.1.102  | 128.59.23.100  | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) |
| 93 28.442185 | 192.168.1.102  | 128.59.23.100  | ICMP | 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1    |
| 94 28.462264 | 10.216.228.1   | 192.168.1.102  | ICMP | 70 Time-to-live exceeded (Time to live exceeded in trans   |
| 95 28.470668 | 192.168.1.102  | 128.59.23.100  | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) |

> 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:a  
v 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)

|                                 |
|---------------------------------|
| 0010 02 24 32 f9 00 b9 01 01 2a |
| 0020 17 64 aa aa aa aa aa aa aa |
| 0030 aa aa aa aa aa aa aa aa aa |
| 0040 aa aa aa aa aa aa aa aa aa |
| 0050 aa aa aa aa aa aa aa aa aa |
| 0060 aa aa aa aa aa aa aa aa aa |
| 0070 aa aa aa aa aa aa aa aa aa |
| 0080 aa aa aa aa aa aa aa aa aa |
| 0090 aa aa aa aa aa aa aa aa aa |
| 00a0 aa aa aa aa aa aa aa aa aa |
| 00b0 aa aa aa aa aa aa aa aa aa |
| 00c0 aa aa aa aa aa aa aa aa aa |
| 00d0 aa aa aa aa aa aa aa aa aa |
| 00e0 aa aa aa aa aa aa aa aa aa |
| 00f0 aa aa aa aa aa aa aa aa aa |
| 0100 aa aa aa aa aa aa aa aa aa |
| 0110 aa aa aa aa aa aa aa aa aa |

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

Answer

Total Length

Flags

More Fragments

Fragment Offset

# First Fragment

| No. | Time      | Source         | Destination    | Protocol | Length | Info                                     |
|-----|-----------|----------------|----------------|----------|--------|------------------------------------------|
| 90  | 22.928093 | 192.168.1.102  | 128.119.245.12 | SSH      | 74     | Client: Encrypted packet (len=20)        |
| 91  | 22.952738 | 128.119.245.12 | 192.168.1.102  | TCP      | 60     | 22 → 1170 [ACK] Seq=1 Ack=21 Win=350     |
| 92  | 28.441511 | 192.168.1.102  | 128.59.23.100  | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1)    |
| 93  | 28.442185 | 192.168.1.102  | 128.59.23.100  | ICMP     | 562    | Echo (ping) request id=0x0300, seq=1     |
| 94  | 28.462264 | 10.216.228.1   | 192.168.1.102  | ICMP     | 70     | Time-to-live exceeded (Time to live)     |
| 95  | 28.470668 | 192.168.1.102  | 128.59.23.100  | TCP      | 1514   | Fragmented TCP segment 1 / proto: ICMP 1 |

> Frame 92: 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:aaf: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: 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

0010 05 dc 32 f9  
0020 17 64 08 00  
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

# Second Fragment

| Frame | Time      | Source IP      | Destination IP | Protocol | Description                                                 |
|-------|-----------|----------------|----------------|----------|-------------------------------------------------------------|
| 90    | 22.928093 | 192.168.1.102  | 128.119.245.12 | SSH      | 74 Client: Encrypted packet (len=20)                        |
| 91    | 22.952738 | 128.119.245.12 | 192.168.1.102  | TCP      | 60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0             |
| 92    | 28.441511 | 192.168.1.102  | 128.59.23.100  | IPv4     | 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=1514)  |
| 93    | 28.442185 | 192.168.1.102  | 128.59.23.100  | ICMP     | 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=64    |
| 94    | 28.462264 | 10.216.228.1   | 192.168.1.102  | ICMP     | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| 95    | 29.478658 | 192.168.1.102  | 128.59.23.100  | IPv4     | 1514 Fragmented IP protocol (proto=TCP 1, off=0, ID=1514)   |

> 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:a  
▼ 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: TCPMP (1)

0010 02 24 32 f9 00 b9 01 01  
0020 17 64 aa aa aa aa aa aa  
0030 aa aa aa aa aa aa aa aa  
0040 aa aa aa aa aa aa aa aa  
0050 aa aa aa aa aa aa aa aa  
0060 aa aa aa aa aa aa aa aa  
0070 aa aa aa aa aa aa aa aa  
0080 aa aa aa aa aa aa aa aa  
0090 aa aa aa aa aa aa aa aa  
00a0 aa aa aa aa aa aa aa aa  
00b0 aa aa aa aa aa aa aa aa  
00c0 aa aa aa aa aa aa aa aa  
00d0 aa aa aa aa aa aa aa aa  
00e0 aa aa aa aa aa aa aa aa  
00f0 aa aa aa aa aa aa aa aa  
0100 aa aa aa aa aa aa aa aa  
0110 aa aa aa aa aa aa aa aa

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

## Answer

### 3 Fragment

| No. | Time      | Source        | Destination   | Protocol | Length | Info                                |
|-----|-----------|---------------|---------------|----------|--------|-------------------------------------|
| 205 | 38.756348 | 192.168.1.102 | 128.59.23.100 | ICMP     | 562    | Echo (ping) request id=0x0300, seq= |
| 214 | 39.322566 | 128.59.23.100 | 192.168.1.102 | TCP      | 562    | Echo (ping) reply id=0x0300, seq=   |
| 218 | 43.467629 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0x0300, seq= |
| 222 | 43.493901 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0x0300, seq= |
| 225 | 43.513660 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0x0300, seq= |
| 228 | 43.544327 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0x0300, seq= |
| 231 | 43.570577 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0x0300, seq= |

> 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]

0010 02 38 33 2  
0020 17 64 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

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

Answer

Total Length

Flags

More Fragments

Fragment Offset

# First Fragment

| No. | Time      | Source        | Destination   | Protocol | Length | Info                                     |
|-----|-----------|---------------|---------------|----------|--------|------------------------------------------|
| 216 | 43.466136 | 192.168.1.102 | 128.59.23.100 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP)      |
| 217 | 43.466808 | 192.168.1.102 | 128.59.23.100 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP)      |
| 218 | 43.467629 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0x0300, seq=1     |
| 219 | 43.485786 | 10.216.228.1  | 192.168.1.102 | ICMP     | 70     | Time-to-live exceeded (Time to live = 1) |

> 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:aaf: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: 1500  
        Identification: 0x3323 (13091)  
    ▼ 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)

0010 05 dc 33  
0020 17 64 08  
0030 aa aa aa  
0040 aa aa aa  
0050 aa aa aa  
0060 aa aa aa  
0070 aa aa aa  
0080 aa aa aa  
0090 aa aa aa  
00a0 aa aa aa  
00b0 aa aa aa  
00c0 aa aa aa  
00d0 aa aa aa  
00e0 aa aa aa  
00f0 aa aa aa  
0100 aa aa aa  
0110 aa aa aa

# Second Fragment

| No. | Time      | Source        | Destination   | Protocol | Length | Info                                                        |
|-----|-----------|---------------|---------------|----------|--------|-------------------------------------------------------------|
| 216 | 43.466136 | 192.168.1.102 | 128.59.23.100 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reas |
| 217 | 43.466808 | 192.168.1.102 | 128.59.23.100 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [R |
| 218 | 43.467629 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no re  |
| 219 | 43.485786 | 10.216.228.1  | 192.168.1.102 | ICMP     | 70     | Time-to-live exceeded (Time to live exceeded in transit)    |

> 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: Linksys6\_da:af:73 (00:06:25:da:a  
v 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: 0x3323 (13091)  
v 001. .... = Flags: 0x1, More fragments  
    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

0010 05 dc 33 23 20 b9 01 01 06 98 c0  
0020 17 64 aa aa aa aa aa aa aa aa aa  
0030 aa  
0040 aa  
0050 aa  
0060 aa  
0070 aa  
0080 aa  
0090 aa  
00a0 aa  
00b0 aa  
00c0 aa  
00d0 aa  
00e0 aa  
00f0 aa  
0100 aa  
-----

# Third Fragment

| No. | Time      | Source        | Destination   | Protocol | Length | Info                      |
|-----|-----------|---------------|---------------|----------|--------|---------------------------|
| 216 | 43.466136 | 192.168.1.102 | 128.59.23.100 | IPv4     | 1514   | Fragmented IP protocol (p |
| 217 | 43.466808 | 192.168.1.102 | 128.59.23.100 | IPv4     | 1514   | Fragmented IP protocol (p |
| 218 | 43.467629 | 192.168.1.102 | 128.59.23.100 | ICMP     | 582    | Echo (ping) request id=0  |
| 219 | 43.485786 | 10.216.228.1  | 192.168.1.102 | ICMP     | 70     | Time-to-live exceeded (Ti |

> Frame 218: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)

> Ethernet II, Src: Actionte\_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG\_da:af:73 (00:06:25:d)

▼ 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)

▼ 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

0010  
0020  
0030  
0040  
0050  
0060  
0070  
0080  
0090  
00a0  
00b0  
00c0  
00d0  
00e0  
00f0  
0100

# The End