

Class: CS-372
Term: Fall 2017
Author: Jon-Eric Cook
Date: November 19, 2017
Lab: #4

1) What is the IP address of your computer?

Answer:

192.168.1.7

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
6	09:33:16.129076	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceeded
7	09:33:16.129751	192.168.1.7	192.168.1.1	DNS	84	Standard query 0xb
8	09:33:16.143367	192.168.1.1	192.168.1.7	DNS	84	Standard query res
9	09:33:16.144153	192.168.1.7	128.119.245.12	SKYPE	70	Unknown_0
10	09:33:16.145559	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceeded
11	09:33:16.145696	192.168.1.7	128.119.245.12	SKYPE	70	Unknown_0

► Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:
▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7

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

Answer:

ICMP (1)

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
6	09:33:16.129076	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceeded
7	09:33:16.129751	192.168.1.7	192.168.1.1	DNS	84	Standard query 0xb
8	09:33:16.143367	192.168.1.1	192.168.1.7	DNS	84	Standard query res
9	09:33:16.144153	192.168.1.7	128.119.245.12	SKYPE	70	Unknown_0
10	09:33:16.145559	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceeded
11	09:33:16.145696	192.168.1.7	128.119.245.12	SKYPE	70	Unknown_0

► Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:
▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x1583 (5507)
▼ Flags: 0x00
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 Fragment offset: 0
 Time to live: 64
 Protocol: ICMP (1)

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.

Answer:

Bytes in IP header: 20

Bytes in payload of IP datagram: 36

Explanation: total length of 56 bytes minus header of 20 bytes equals 36 bytes

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
1	09:33:09.985229	173.194.203.1...	192.168.1.7	TLSv1...	590	Application Data
2	09:33:09.985346	192.168.1.7	173.194.203.1...	TCP	66	57256 → 443 [ACK]
3	09:33:15.928877	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x0
4	09:33:16.126114	192.168.1.1	192.168.1.7	DNS	93	Standard query res
5	09:33:16.127309	192.168.1.7	128.119.245.12	SKYPE	70	Unknown_0
6	09:33:16.129076	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceed

► Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 ► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:
 ► Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7
 ▾ Internet Control Message Protocol
 Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0x2c69 [correct]
 [Checksum Status: Good]
 ▼ Internet Protocol Version 4, Src: 192.168.1.7, 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 ←

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

Answer:

No

The more fragments bit is not set.

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
1	09:33:09.985229	173.194.203.1...	192.168.1.7	TLSv1...	590	Application Data
2	09:33:09.985346	192.168.1.7	173.194.203.1...	TCP	66	57256 → 443 [ACK]
3	09:33:15.928877	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x0
4	09:33:16.126114	192.168.1.1	192.168.1.7	DNS	93	Standard query res
5	09:33:16.127309	192.168.1.7	128.119.245.12	SKYPE	70	Unknown_0
6	09:33:16.129076	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceed

► Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 ► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:
 ► Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ► Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x1583 (5507)
 ▼ Flags: 0x00
 0.... = Reserved bit: Not set
 .0.... = Don't fragment: Not set
 ..0.... = More fragments: Not set ←

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:

Identification and Header checksum

See screenshots below.

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

Answer:

Stays constant:

- Version (using IPv4 for all packets)
- Length of header (because of ICMP packets)
- Source IP (sending from the same source)
- Destination IP (sending to the same destination)
- Upper layer protocol (ICMP)
- Differentiated Services (all packets are ICMP, use same type of service)

Must stay constant:

- Version (IPv4) (use the same version for each datagram)
- Length of header (have the length of each datagram be the same)
- Source IP (send the datagram from the same location)
- Destination IP (send the datagram to the same destination)
- Upper layer protocol (ICMP) (use the same protocol)
- Differentiated Services (all packets are ICMP, use same type of service)

Must change:

- Header checksum (because the header being sent is different so there needs to be a different checksum to verify it)
- Identification (this needs to change as it identifies each packet being sent)

See screenshots below.

No.	Time	Source	Destination	Protocol	Length	Info
449	09:34:45.937604	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
445	09:34:45.926939	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
441	09:34:45.916060	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
190	09:33:55.170664	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
187	09:33:55.160556	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
184	09:33:55.140568	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded

► Frame 445: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:
▼ Internet Protocol Version 4, Src: 96.120.86.129, Dst: 192.168.1.7

 0100 = Version: 4 ←
 0101 = Header Length: 20 bytes (5) ←
 0000 = Total Length: 56 ←
 Identification: 0x6312 (25362) ←
 Flags: 0x00
 0.... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 Fragment offset: 0
 Time to live: 63
 Protocol: ICMP (1) ←
 Header checksum: 0xa00a [validation disabled] ←
 [Header checksum status: Unverified]
 Source: 96.120.86.129
 Destination: 192.168.1.7
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

► Internet Control Message Protocol

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

Answer:

It appears that the Identification field follows a pattern where the value is increased by one for each ICMP Echo request.

See the screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
449	09:34:45.937604	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
445	09:34:45.926939	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
441	09:34:45.916060	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
190	09:33:55.170664	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
187	09:33:55.160556	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
184	09:33:55.140568	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded

► Frame 441: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 ► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:
 ▼ Internet Protocol Version 4, Src: 96.120.86.129, Dst: 192.168.1.7
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 56
 Identification: 0x630f (25359)

No.	Time	Source	Destination	Protocol	Length	Info
449	09:34:45.937604	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
445	09:34:45.926939	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
441	09:34:45.916060	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
190	09:33:55.170664	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
187	09:33:55.160556	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded
184	09:33:55.140568	96.120.86.129	192.168.1.7	ICMP	70	Time-to-live exceeded

► Frame 445: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 ► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:
 ▼ Internet Protocol Version 4, Src: 96.120.86.129, Dst: 192.168.1.7
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 56
 Identification: 0x6312 (25362)

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

Answer:

Identification: 5507

Time to live: 64

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
12	09:33:16.146825	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceeded
10	09:33:16.145559	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceeded
8	09:33:16.143367	192.168.1.1	192.168.1.7	DNS	84	Standard query response
6	09:33:16.129076	192.168.1.1	192.168.1.7	ICMP	98	Time-to-live exceeded
4	09:33:16.126114	192.168.1.1	192.168.1.7	DNS	93	Standard query response
684	09:35:32.299514	173.194.203.1...	192.168.1.7	TLSv1...	125	Application Data

► Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

► Ethernet II, Src: Netgear_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple_38:94:d0 (f4:0f:24:38:94:d0)

▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7

 0100 = Version: 4

 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

 Total Length: 84

 Identification: 0x1583 (5507) →

▼ Flags: 0x00

 0... = Reserved bit: Not set

 .0. = Don't fragment: Not set

 ..0. = More fragments: Not set

 Fragment offset: 0

 Time to live: 64 →

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:

No, the Identification field does change for all the ICMP TTL-exceeded replies. This is so because the Identification field is unique. If there were in fact two or more IP datagrams that had the same Identification value, this would mean that they are fragments of a single large IP datagram.

The TTL field remains unchanged because the TTL for the first hop router is always the same.

NOTE: For questions 10-15, I will be using the ip-ethereal-trace-1 packet from <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

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, the message has been fragmented across more than one IP datagram.
See screenshots below.

No.	Time	Source	Destination	Protocol	Length	Info
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
93	18:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
94	18:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceed
95	18:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
96	18:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
97	18:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
98	18:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
99	18:48:25.179081	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
100	18:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
101	18:48:25.188565	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceed
102	18:48:25.199110	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
103	18:48:25.199828	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
104	18:48:25.229200	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
105	18:48:25.229955	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
106	18:48:25.249153	192.168.1.102	128.59.23.100	TPv4	1514	Fragmented IP prot

► Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
► Ethernet II, Src: PremaxPe_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: 1500
 Identification: 0x32f9 (13049)
 ▼ Flags: 0x01 (More Fragments) ←
 0... = Reserved bit: Not set
 ..0... = Don't fragment: Not set
 ..1.... = More fragments: Set

11) Screenshot the first fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram has been fragmented? What information in the IP header indicates whether this is the first fragment of the fragment versus a later fragment? How long is this IP datagram?

Answer:

The Flags bit for more fragments is set. This indicates that the datagram has been fragmented. Also, because the fragment offset is set to 0, this tells us that this is the first fragment. The length of the first fragmented datagram is 1500, including the header.

See screenshot below.

12) Screenshot the second fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

Answer:

Seeing that the fragment offset is 1480, this indicates that this is not the first fragmented datagram. Also, it is the last fragment because the more fragments flag is not set.

See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
• 92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
• 93	18:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
94	18:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded
95	18:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
96	18:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
97	18:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
98	18:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
99	18:48:25.179081	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
100	18:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
101	18:48:25.188565	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded
102	18:48:25.199110	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
103	18:48:25.199828	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
104	18:48:25.229200	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
105	18:48:25.229955	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request
106	18:48:25.249153	192.168.1.102	128.59.23.100	TPv4	1514	Fragmented TP prot

► Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
► Ethernet II, Src: PremaxPe_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: 0x00
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0.... = More fragments: Not set ←
 Fragment offset: 1480 ←

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

Answer:

Total length, Flags, Fragment offset, Checksum

See screenshots below.

No.	Time	Source	Destination	Protocol	Length	Info
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
93	18:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
94	18:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceed
95	18:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
96	18:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
97	18:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
98	18:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
99	18:48:25.179081	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
100	18:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
101	18:48:25.188565	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceed
102	18:48:25.199110	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
103	18:48:25.199828	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
104	18:48:25.229200	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
105	18:48:25.229955	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
106	18:48:25.240153	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot

- ▶ Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
- ▶ Ethernet II, Src: PremaxPe_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: 1500 ←
 - Identification: 0x32f9 (13049)
 - ▼ Flags: 0x01 (More Fragments)
 - 0.... = Reserved bit: Not set
 - .0... = Don't fragment: Not set
 - ..1.... = More fragments: Set ←
 - Fragment offset: 0 ←
 - Time to live: 1
 - Protocol: ICMP (1)
 - Header checksum: 0x077b [validation disabled] ←

No.	Time	Source	Destination	Protocol	Length	Info
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
93	18:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
94	18:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceed
95	18:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
96	18:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
97	18:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
98	18:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
99	18:48:25.179081	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
100	18:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
101	18:48:25.188565	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceed
102	18:48:25.199110	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
103	18:48:25.199828	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
104	18:48:25.229200	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
105	18:48:25.229955	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) reques
106	18:48:25.240153	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot

- ▶ Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
- ▶ Ethernet II, Src: PremaxPe_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: 0x00
 - 0.... = Reserved bit: Not set
 - .0... = Don't fragment: Not set
 - ..0.... = More fragments: Not set ←
 - Fragment offset: 1480 ←
 - Time to live: 1
 - Protocol: ICMP (1)
 - Header checksum: 0x2a7a [validation disabled] ←

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

Answer:

3 fragments were created after changing to 3500 bytes
See screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
216	18:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
217	18:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
• 218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request

15) What fields changes in the IP header among the fragments?

Answer:

Fragment offset (0, 1480, 2960), Checksum
See screenshots below.

No.	Time	Source	Destination	Protocol	Length	Info
216	18:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
217	18:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
• 218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request
219	18:48:40.144138	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded
220	18:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
221	18:48:40.151305	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
222	18:48:40.152253	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request
223	18:48:40.170497	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
224	18:48:40.171170	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
225	18:48:40.172012	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request
226	18:48:40.201144	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
227	18:48:40.201814	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
228	18:48:40.202679	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request
229	18:48:40.227363	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot
230	18:48:40.228032	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP prot

► Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
► Ethernet II, Src: PremaxPe_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: 1500
 Identification: 0x3323 (13091)
 ▼ Flags: 0x01 (More Fragments)
 0.... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..1. = More fragments: Set
 Fragment offset: 0 ←
 ► Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x0751 [validation disabled] ←

