

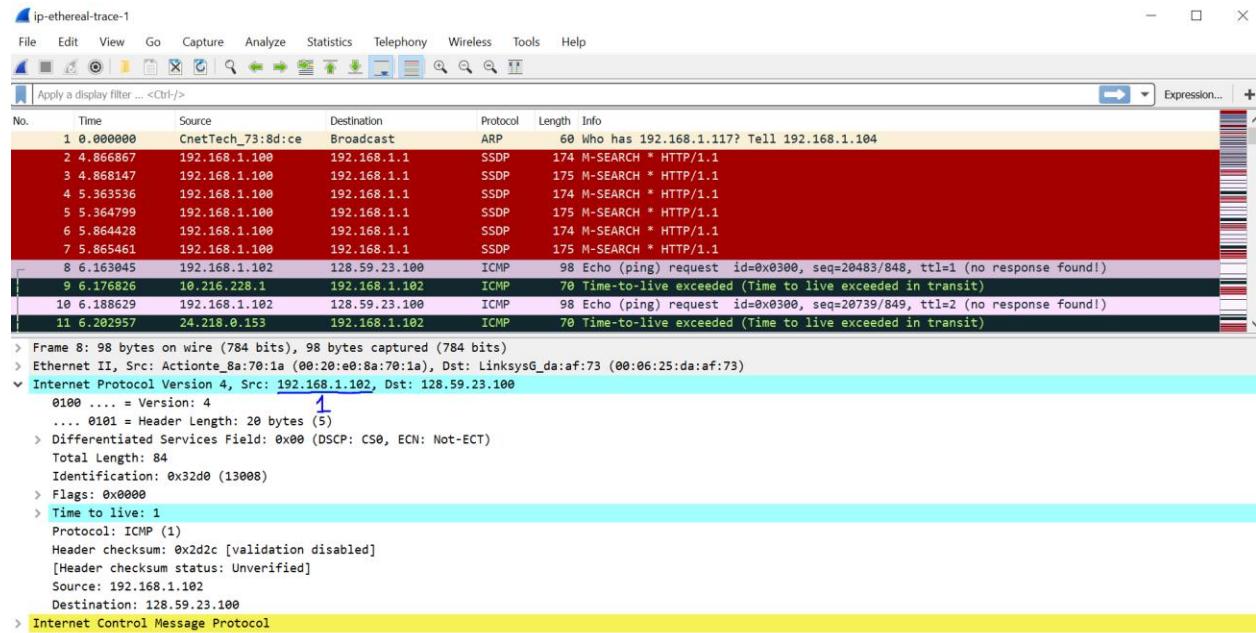
Lachlan Sinclair

11/20/19

Lab 4: CS\_372\_400

**Question 1: Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?**

IP address of my computer: 192.168.1.102



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

Value in the upper layer protocol field: ICMP(1)

ip-ethereal-trace-1

Apply a display filter ... <Ctrl/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
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!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
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!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```

> 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: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) 2
        Header checksum: 0xd2dc [validation disabled]
        [Header checksum status: Unverified]
        Source: 192.168.1.102
        Destination: 128.59.23.100
    > Internet Control Message Protocol

```

**Question 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.**

The header has a length of 20 bytes.

Total length - header size = payload size. The total length is 84 bytes, so  $84 - 20 = 64$  bytes of payload.

ip-ethereal-trace-1

Apply a display filter ... <Ctrl/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
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!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
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!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```

> 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: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) 3
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 84 3
        Identification: 0x32d0 (13008)
        Flags: 0x0000
        Time to live: 1
        Protocol: ICMP (1)
        Header checksum: 0xd2dc [validation disabled]
        [Header checksum status: Unverified]
        Source: 192.168.1.102
        Destination: 128.59.23.100
    > Internet Control Message Protocol

```

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

The IP datagram has not been fragmented, this is clear since the “more fragments” flag was not set.

ip-ethereal-trace-1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
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!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
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!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```

> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e8:8a: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
            0... .... .... = Reserved bit: Not set
            .0... .... .... = Don't fragment: Not set
            ..0.... .... .... = More fragments: Not set 4
            ...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

```

### Question 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?

The identification number always changes. Also, since it is a traceroute the time to live changes. The header checksum also always changes.

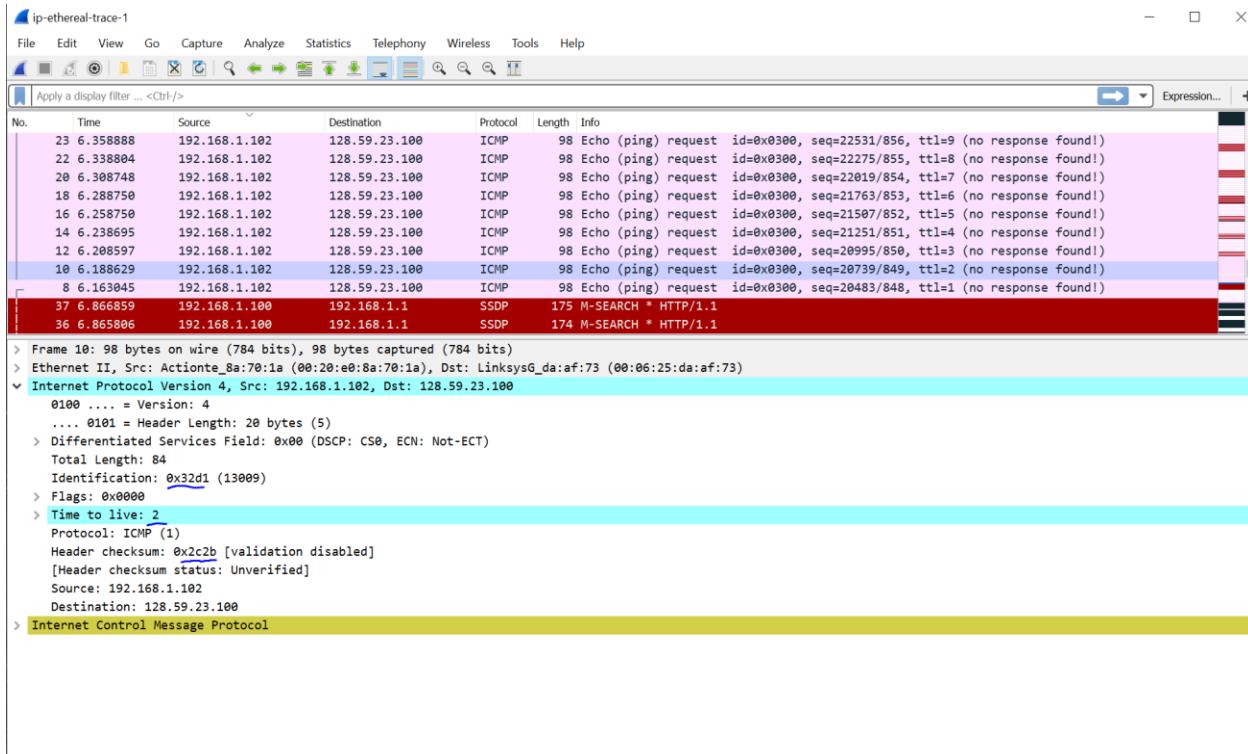
ip-ethereal-trace-1

No.	Time	Source	Destination	Protocol	Length	Info
23	6.358888	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22531/856, ttl=9 (no response found!)
22	6.338804	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)
20	6.308748	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
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!)
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!)
37	6.866859	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
36	6.865886	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1

```

> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e8:8a: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
            0... .... .... = Reserved bit: Not set
            .0... .... .... = Don't fragment: Not set
            ..0.... .... .... = More fragments: Not set 5
            ...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

```



**Question 6: Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?**

Constants:

The source and destination IP addresses need to stay the same otherwise the data would not follow the same path.

The IP version stays the same, it shouldn't be changed in order to maintain consistency for the traceroute.

Differentiated Services field stays the same, this should stay the same in order to insure the datagrams are treated in the same way at every router during the traceroute.

The upper layer protocol doesn't change since the traceroute always send ICMP packets.

The header length also stays the same, this maintains consistency during the traceroute, adding optional fields to the datagram header could affect the traceroute.

Changes: (note: by definition in the text book, these are the three values that should change)

The identification number needs to change for proper datagram tracking.

The header checksum changes since the contents of the header change with every packet.

Time to live changes with every packet since this is the fundamental way a traceroute works.

## Question 7: Describe the pattern you see in the values in the Identification field of the IP datagram

The value of the identification number increases by one with every ICMP message sent.

```

Frame 18: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actinote_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
    Identification: 0x32d0 (13008) 7
    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

```

```

Frame 19: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actinote_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
    Identification: 0x32d1 (13009) 7
    Flags: 0x0000
    Time to live: 2
    Protocol: ICMP (1)
    Header checksum: 0xc2cb [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Internet Control Message Protocol

```

## Question 8: What is the value in the Identification field and the TTL field?

The time to live value is 255, and the identification number is 40316 in the series of ICMP TTL-exceeded sent from the first router.

No.	Time	Source	Destination	Protocol	Length	Info
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
330	53.581082	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
274	48.493073	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
179	38.491817	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	16.179649	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	11.174495	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

**Question 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?**

The TTL values stay the same for all replies from the first router, however the identification number changes with every reply.

The identification number always needs to change, only datagrams that are fragmented can have the same identification number.

The TTL doesn't change since the replies are all originating from the same router, the router is assigning them the same TTL value and they all follow the same path to my computer.

No.	Time	Source	Destination	Protocol	Length	Info
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
330	53.501882	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
274	48.493073	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
179	38.491817	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	16.179649	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
48	11.174495	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

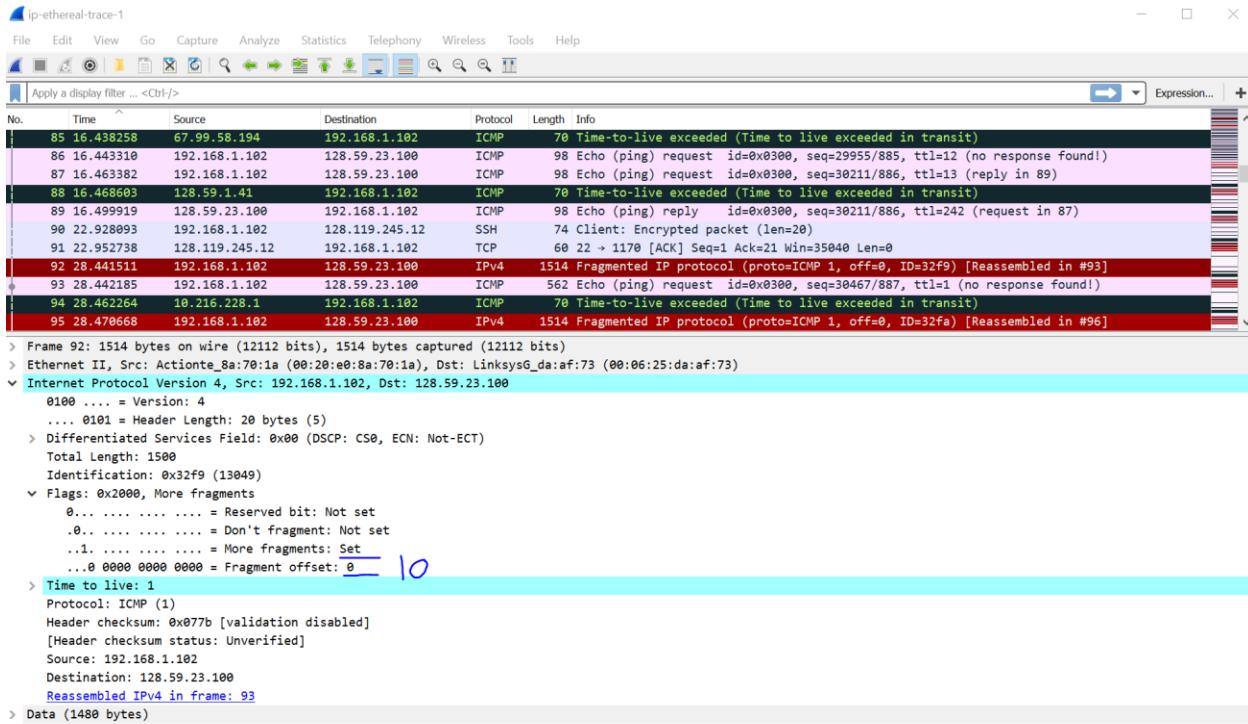
```
> Frame 40: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Linksys_G_da:a:f:73 (00:06:25:da:a:f:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
<-- Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x9d98 (40344)
    Flags: 0x0000
    Time to live: 255  9
    Protocol: ICMP (1)
    Header checksum: 0x6c84 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.216.228.1
    Destination: 192.168.1.102
    > Internet Control Message Protocol
```

No.	Time	Source	Destination	Protocol	Length	Info
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
330	53.501882	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
274	48.493073	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
179	38.491817	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	16.179649	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
48	11.174495	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```
> Frame 330: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Linksys_G_da:a:f:73 (00:06:25:da:a:f:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
<-- Internet Protocol Version 4, Src: 10.216.228.1, 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: 0x9ebb (40635)
    Flags: 0x0000
    Time to live: 255  9
    Protocol: ICMP (1)
    Header checksum: 0xb661 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.216.228.1
    Destination: 192.168.1.102
    > Internet Control Message Protocol
```

**Question 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?**

Yes, it has been fragmented across multiple datagrams.

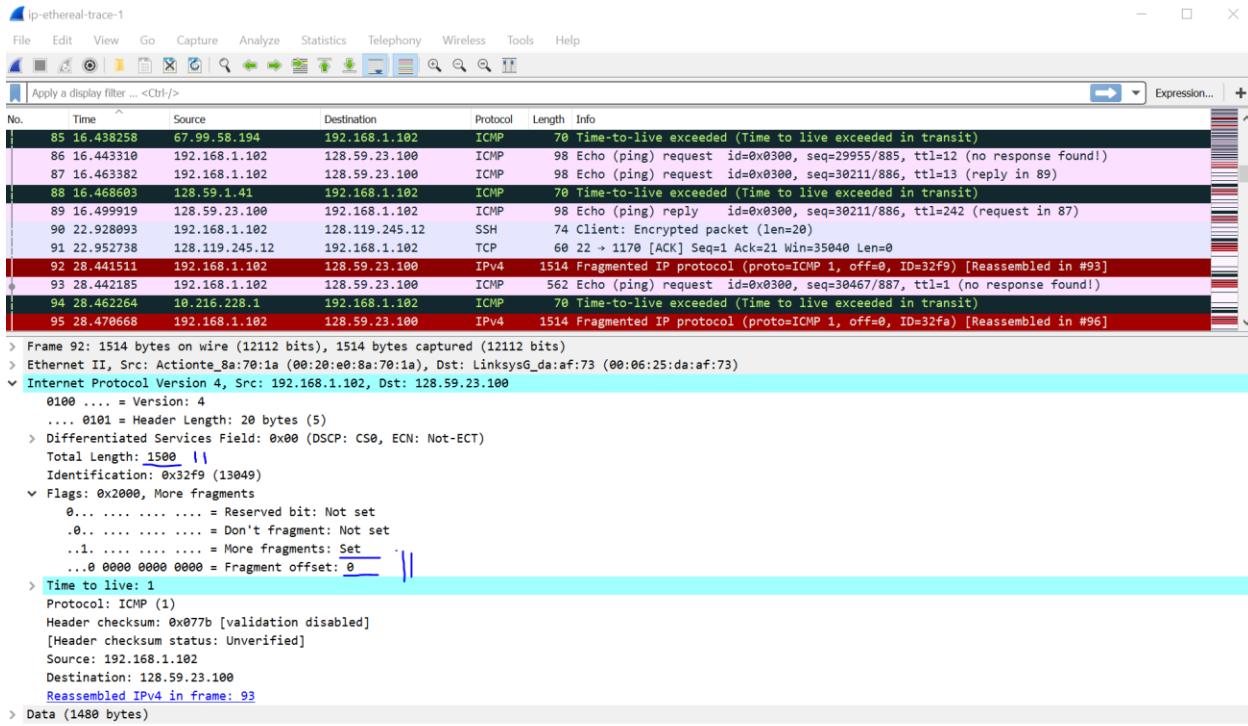


**Question 11:** Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter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

The more fragments flag has been set, this means that the datagram has been fragmented.

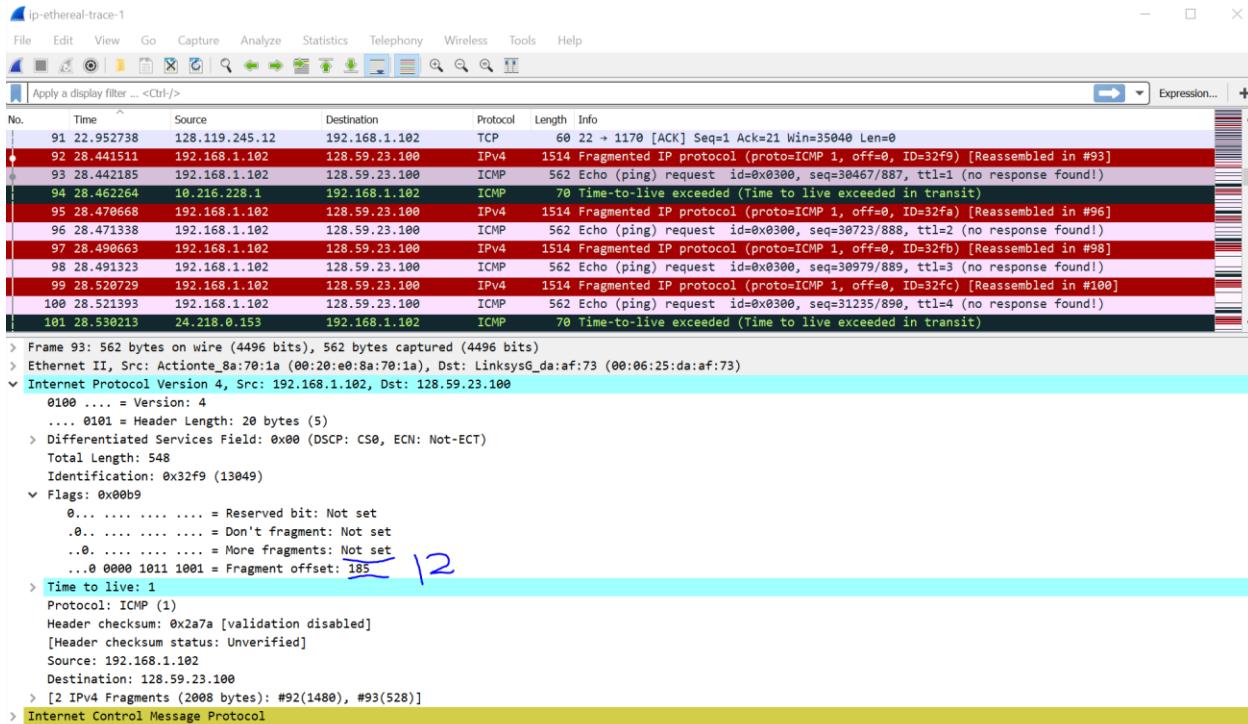
The fragment offset is 0 which means it is the first fragment of the datagram.

The length of this datagram is 1500 bytes including the 20 byte header. The length of all of the datagrams fragments combined including the second fragments 20 byte header is 1948 bytes.



**Question 12:** Screenshot the second fragment of the 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 the more fragments? How can you tell?

The fragments offset is set to 185 which means it is not the data fragment. The more fragments flag is not set which means there is not more fragments.



### Question 13: What fields change in the IP header between the first and second fragment?

The header check sum, fragments offset, more fragments flag, and the total length fields change between the two fragments IP headers.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
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) [Reassembled in #93]
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=30467/887, ttl=1 (no response found!)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, 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]
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, 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 #100]
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=31235/890, ttl=4 (no response found!)
101	28.530213	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```

> 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: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 13
        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 13
    > Time to live: 1
    Protocol: ICMP (1) 13
    Header checksum: 0x077a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 93
> Data (1480 bytes)

```

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
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) [Reassembled in #93]
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=30467/887, ttl=1 (no response found!)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, 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]
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, 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 #100]
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=31235/890, ttl=4 (no response found!)
101	28.530213	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```

> 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 13
        Identification: 0x32f9 (13049)
    > Flags: 0x00b9
        0... .... .... .... = Reserved bit: Not set
        .0... .... .... .... = Don't fragment: Not set
        ..0.... .... .... = More fragments: Not set
        ...0 0000 1011 1001 = Fragment offset: 185 13
    > Time to live: 1
    Protocol: ICMP (1) 13
    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

```

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

3 fragments were created from the original datagram.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
213	39.314263	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
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=1468 SACK_PERM=1
216	43.466136	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.466808	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
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!)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	43.492284	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.492953	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
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 found!)
223	43.512145	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]

```
> Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    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: 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: 0x0751 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 218
> Data (1480 bytes)
```

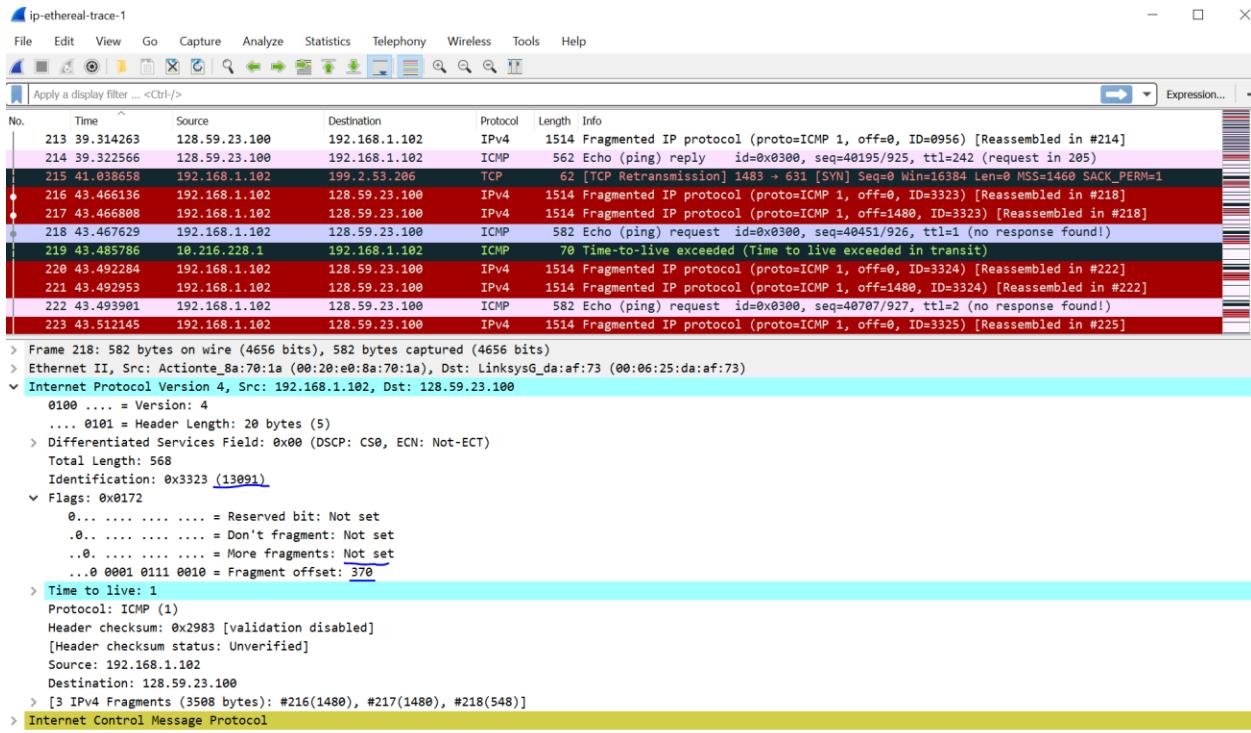
ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
213	39.314263	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
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=1468 SACK_PERM=1
216	43.466136	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.466808	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
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!)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	43.492284	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.492953	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
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 found!)
223	43.512145	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]

```
> Frame 217: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    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: 0x20b9, More fragments
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..1. .... .... .... = More fragments: Set
        ...0 0000 1011 1001 = Fragment offset: 185
    > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x0698 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 218
> Data (1480 bytes)
```



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

The fragments offset and checksum change for all three as expected. The first two both have the “more fragments” flag set, whereas the third fragment’s “more fragments flag” is not set. The first two also have the same total length at 1500 bytes, and the third only has a total length of 568 bytes. See the screen shots above for reference.