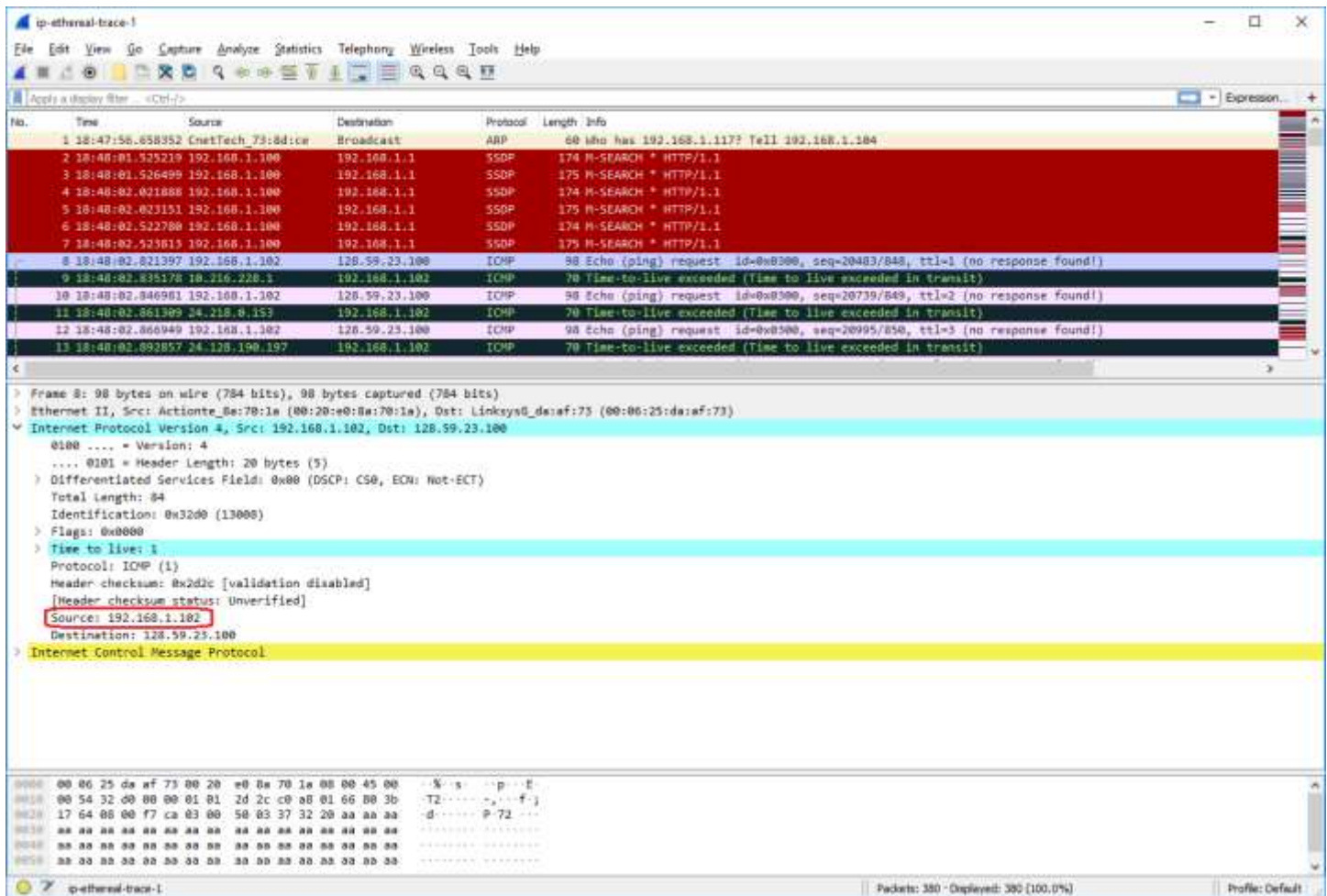


Lab 4: Wireshark

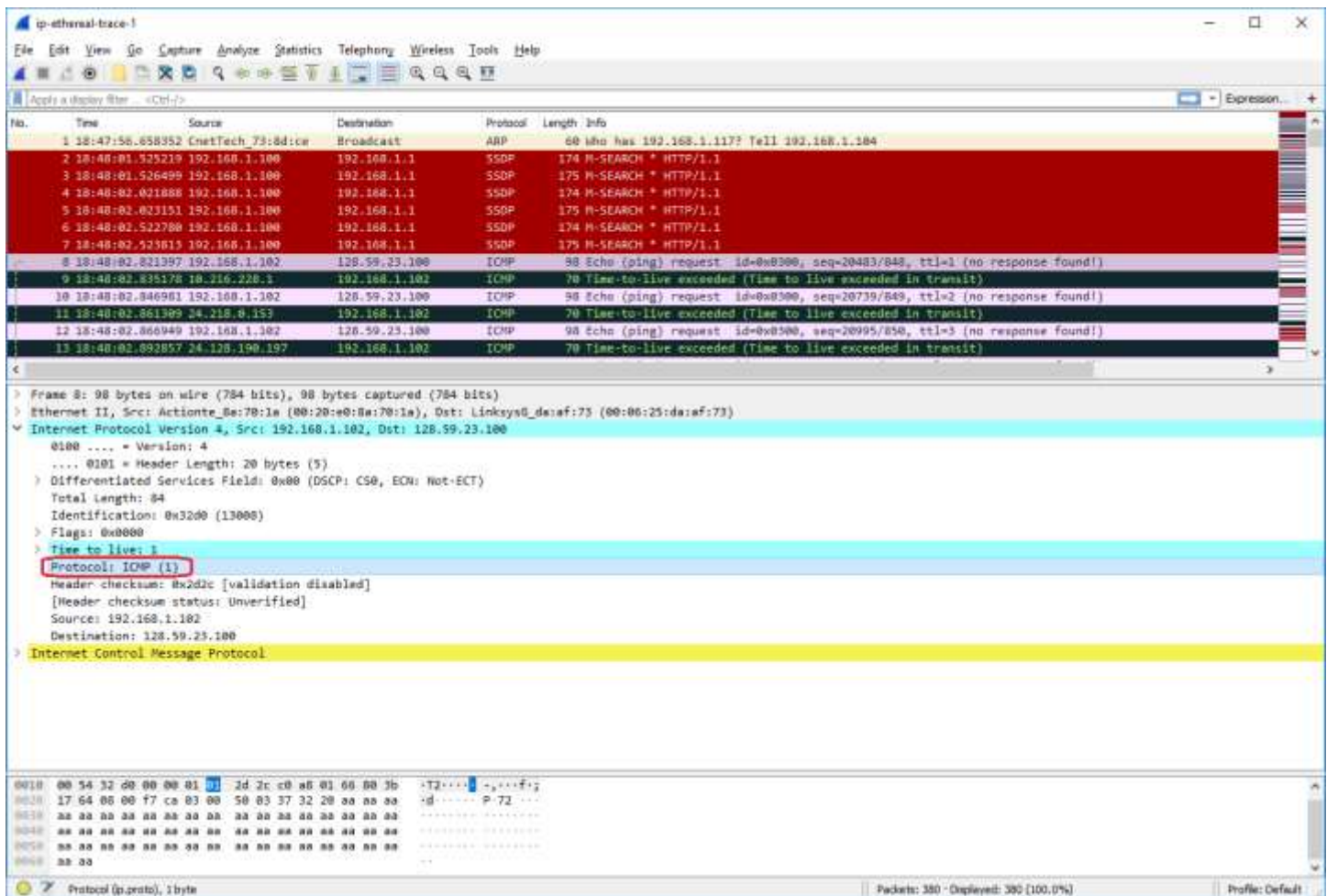
- 1) Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

Using the author's trace, the IP address of my computer is 192.168.1.102.



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

The value in the upper layer protocol field is 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.

There are 20 bytes in the IP header. This IP packet's total length is 84 bytes. Therefore, the payload of the IP datagram is 64 bytes (84 – 20 bytes = 64 bytes).

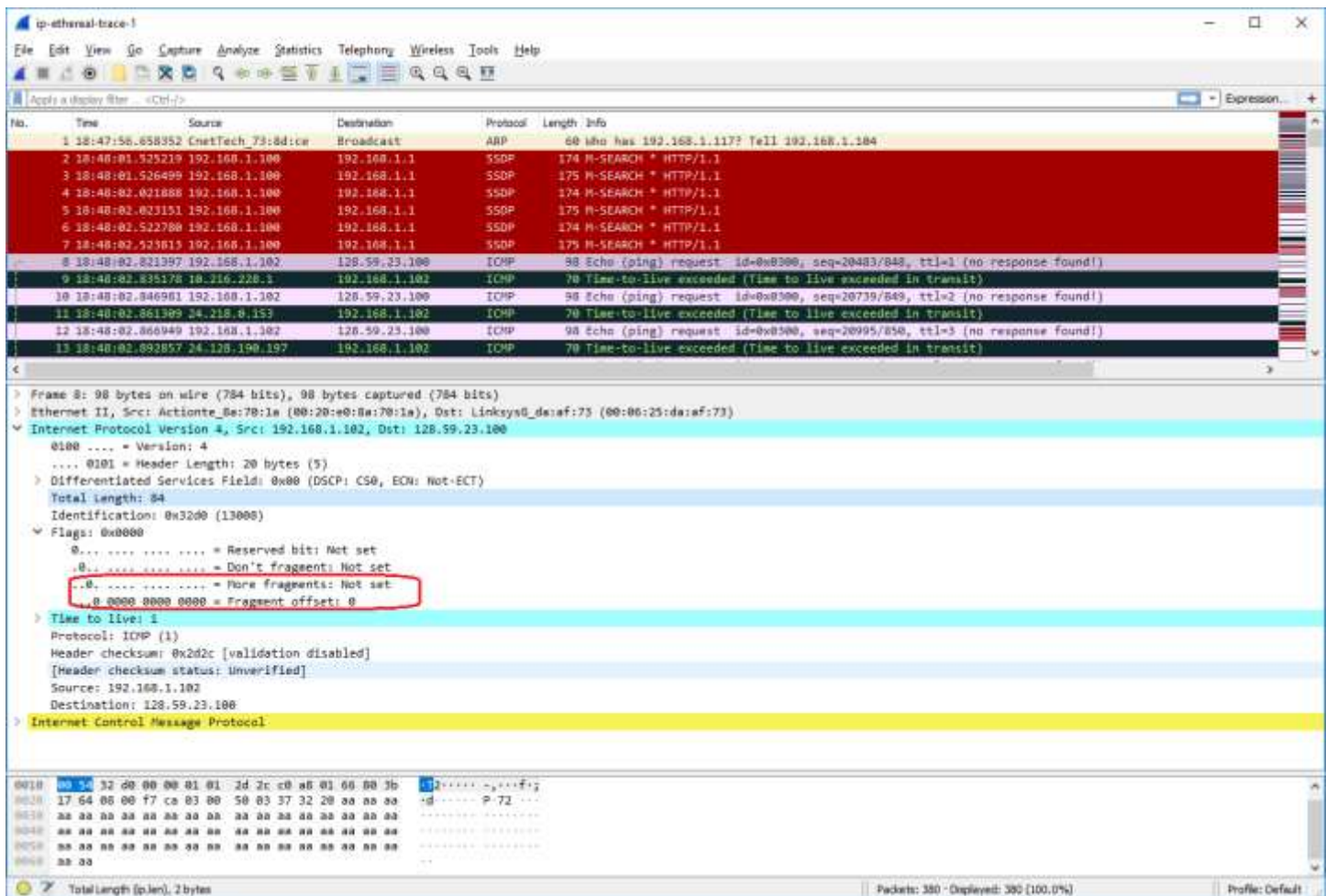
The image shows a Wireshark packet capture analysis. The packet list at the top shows a sequence of packets: ARP, SSDP, and ICMP. The packet details pane for the selected ICMP Echo (ping) request (packet 13) shows the following structure:

- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
- Total length: 84
- Identification: 0x3200 (13000)
- 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

The packet bytes pane at the bottom shows the raw hex and ASCII data of the packet, starting with 0010 00 54 32 00 00 00 01 01 2d 2c x0 a0 01 00 00 3b.

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

No, this IP datagram has not been fragmented. If it was fragmented, then this first IP datagram would either have the “More fragments” bit set or have a non-zero fragment offset, and the bottom of this IP datagram would have a list of IP fragments. Since this IP datagram does not have the More Fragments bit set and does not have a non-zero fragment offset and there is no list of fragments, it is not fragmented.



Next, sort the traced packets according to IP source address by clicking on the *Source* column header; a small downward pointing arrow should appear next to the word *Source*. If the arrow points up, click on the *Source* column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

- 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, time to live, and header checksum fields always change from one datagram to the next in this series of ICMP messages, as shown below.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
22	18:48:02.997156	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22175/855, ttl=8 (no response found!)
20	18:48:02.967100	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
18	18:48:02.947102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
16	18:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	18:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	18:48:02.866940	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
10	18:48:02.846902	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
8	18:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
37	18:48:03.525211	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
36	18:48:03.524156	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
26	18:48:03.030435	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
25	18:48:03.029259	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	18:48:02.523013	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1

> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

> Ethernet II, Src: Actionte_0e:70:1a (08:20:e0:8a:70:1a), Dst: Linksys_0d: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: 0x3200 (13000)

Flags: 0x0000

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x242c (validation disabled)

[Header checksum status: Unverified]

Source: 192.168.1.102

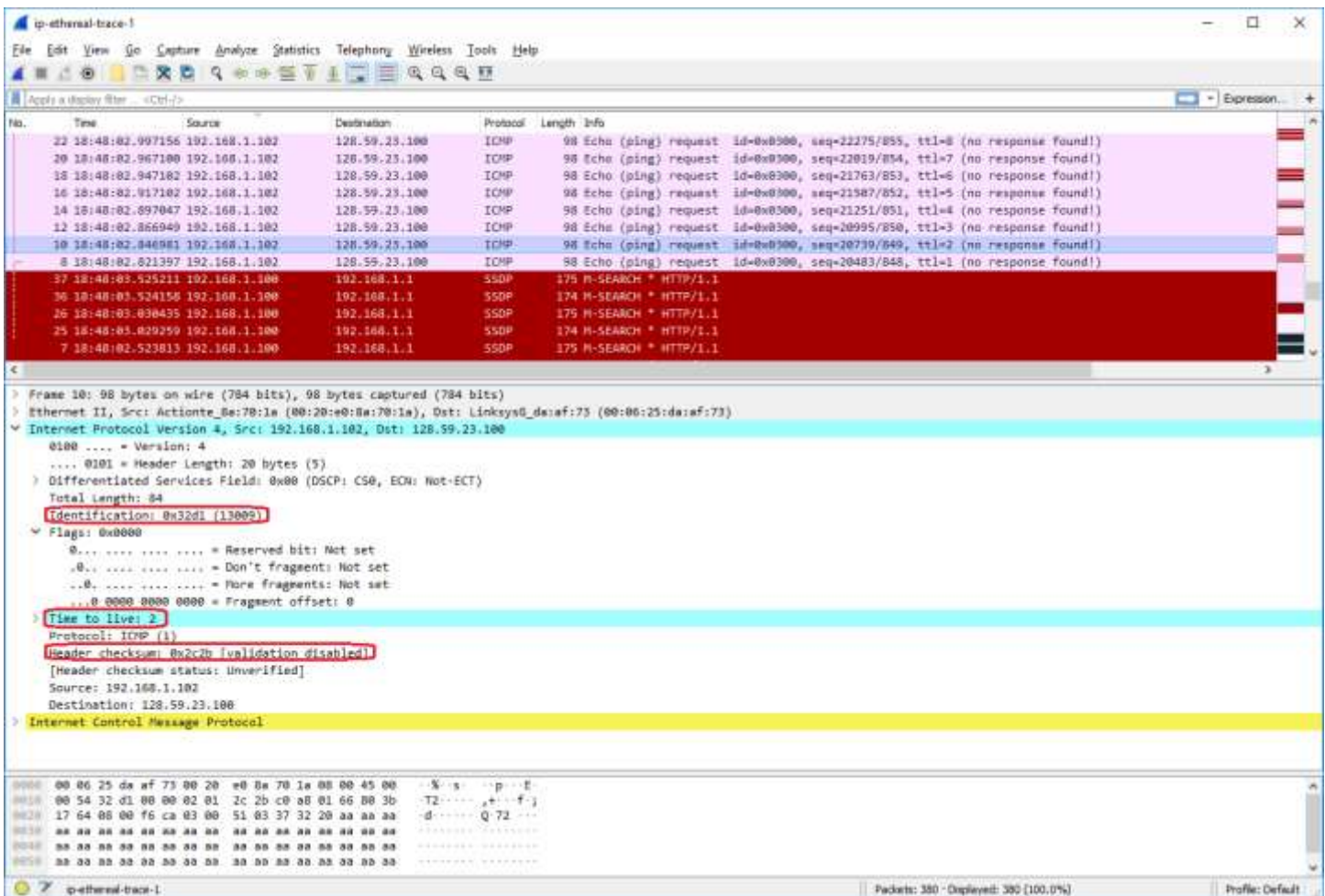
Destination: 128.59.23.100

> Internet Control Message Protocol

```

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 00 00 45 00  -X 3 -p -E-
0010 00 54 32 00 00 00 01 01 2d 2c c0 a0 01 66 00 3b  -T2 ---- -.-f-
0020 17 64 06 00 f7 ca 03 00 50 03 37 32 20 aa aa aa  -d-----P-72-
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
  
```

Packets: 380 - Displayed: 300 (100.0%) Profile: Default



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

The Version, Header Length, Differentiated Services Field, Protocol, Source, and Destination fields stay constant.

- Version does not change since all the ICMP echo packets are using the same IPv4 network protocol.
- Header Length does not change since these are all ICMP packets, which has a fixed size of 20 bytes.
- Differentiated Services does not change because all the ICMP packets don't use any service options, which is the default value 0x0 for Differentiated Services.
- Protocol does not change since all the packets are ICMP packets.
- Source address does not change since all of these ICMP packets are sent by the same source address.
- Destination address does not change since all of these ICMP packets are received by the same destination address.

The Version, Header Length, Differentiated Services, Protocol, Source, and Destination fields must stay constant.

- Version must stay constant since the IPv4 network protocol is used for all ICMP packets.
- Header Length must stay constant since we are referring to all ICMP packets and ICMP IP header packets have a fixed length of 20 bytes.
- Differentiated Services must stay constant because all the ICMP packets don't use any service options, which is the default value 0x0 for Differentiated Services.
- Protocol must stay constant since all the packets are ICMP packets.
- Source address must stay constant since all of these ICMP packets are sent by the same source address.
- Destination address must stay constant since all of these ICMP packets are received by the same destination address.

The screenshot displays a Wireshark interface with a packet capture of ICMP Echo requests. The packet list shows several requests from 192.168.1.102 to 128.59.23.100. The packet details pane for Frame 10 shows the IP header fields: Version: 4, Header Length: 20 bytes (5), Total Length: 84, Identification: 0x32d1 (13009), Time to live: 2, Protocol: ICMP (1), Header checksum: 0x2c2b [validation disabled], Source: 192.168.1.102, and Destination: 128.59.23.100. The packet bytes pane shows the raw hex and ASCII data.

The Identification, Time to Live, and Header Checksum fields must change.

- Identification must change because it uniquely identifies each IP packet that is transmitted.
- Time to Live must change because traceroute increments each IP datagram with each hop.
- Header Checksum must change because other fields within the header must change, such as Identification and Time to Live, which alter the checksum value of the header.

The image shows a Wireshark packet capture with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
22	18:48:02.997156	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22175/855, ttl=8 (no response found!)
20	18:48:02.967100	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
18	18:48:02.947102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
16	18:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	18:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	18:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
10	18:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
8	18:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
37	18:48:03.525211	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
36	18:48:03.524156	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
26	18:48:03.030435	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
25	18:48:03.029259	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	18:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1

Packet 10 details:

- Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
- Ethernet II, Src: Actionte_0e:70:1a (08:20:e0:8a:70:1a), Dst: Linksys_0d:af:73 (08:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total length: 84
 - Identification: 0x32d1 (13009)
 - Flags: 0x0000
 - 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: 2
 - Protocol: ICMP (1)
 - Header checksum: 0x2c2b [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.102
 - Destination: 128.59.23.100
- Internet Control Message Protocol

Packet 10 hex dump:

```

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 06 25 00  --% 3 --p--E-
0010 00 54 32 d1 00 00 02 01 2c 2b c0 a0 01 66 00 3b  -T2-----,+--f-
0020 17 64 06 00 f6 ca 03 00 51 03 37 32 20 aa aa aa  -d-----Q 72---
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa  -----
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa  -----
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa  -----

```

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

Each subsequent ICMP Echo request has an Identification value that is incremented by 1.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http get

No.	Time	Source	Destination	Protocol	Length	Info
20	18:48:03.047273	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22787/857, ttl=10 (no response found!)
23	18:48:03.017240	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22531/856, ttl=9 (no response found!)
22	18:48:02.997156	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)
20	18:48:02.967100	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
18	18:48:02.947102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
16	18:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	18:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	18:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
10	18:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
8	18:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
37	18:48:03.525211	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
36	18:48:03.524158	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
26	18:48:03.038435	192.168.1.100	192.168.1.1	SSDP	175	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 (08:20:e0:8a:70:1a), Dst: LinksysG_daraf:73 (08:06:25:da:af:73)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

..... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 84

Identification: 0x52d0 (13008)

> Flags: 0x0000

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x2d2c [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.102

Destination: 128.59.23.100

> Internet Control Message Protocol

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 --X--s--p--E--

0010 00 54 32 00 00 00 01 01 2d 2c e0 a8 01 66 00 3b --T2-----P--F--

0020 17 64 00 00 f7 c8 03 00 50 03 37 32 20 00 00 00 ..d-----P-72---

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Header Length (p.hdr.len), 1 byte

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.get

No.	Time	Source	Destination	Protocol	Length	Info
28	18:48:03.047273	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22787/857, ttl=10 (no response found!)
29	18:48:03.017240	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22531/856, ttl=9 (no response found!)
22	18:48:02.997156	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)
20	18:48:02.967100	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
18	18:48:02.947102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
16	18:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	18:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	18:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
10	18:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
8	18:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
37	18:48:03.525211	192.168.1.100	192.168.1.1	SSDP	179	M-SEARCH * HTTP/1.1
36	18:48:03.524158	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
26	18:48:03.038435	192.168.1.100	192.168.1.1	SSDP	179	M-SEARCH * HTTP/1.1

> Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

> Ethernet II, Src: Actionte_8e:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_08:af:73 (00:06:25:da:af:73)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 84

Identification: 0x32d1 (13009)

> Flags: 0x0000

> Time to live: 2

Protocol: ICMP (1)

Header checksum: 8x2c2b [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.102

Destination: 128.59.23.100

> Internet Control Message Protocol

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 00 00 00 00 ..% .s. .p. .

0010 00 54 32 d1 00 00 02 01 2c 2b c0 a0 01 66 00 3b ..T2.....,e...f..j

0020 17 64 06 00 f6 ca 03 00 51 03 37 32 20 aa aa aa ..d.....Q 72...

0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

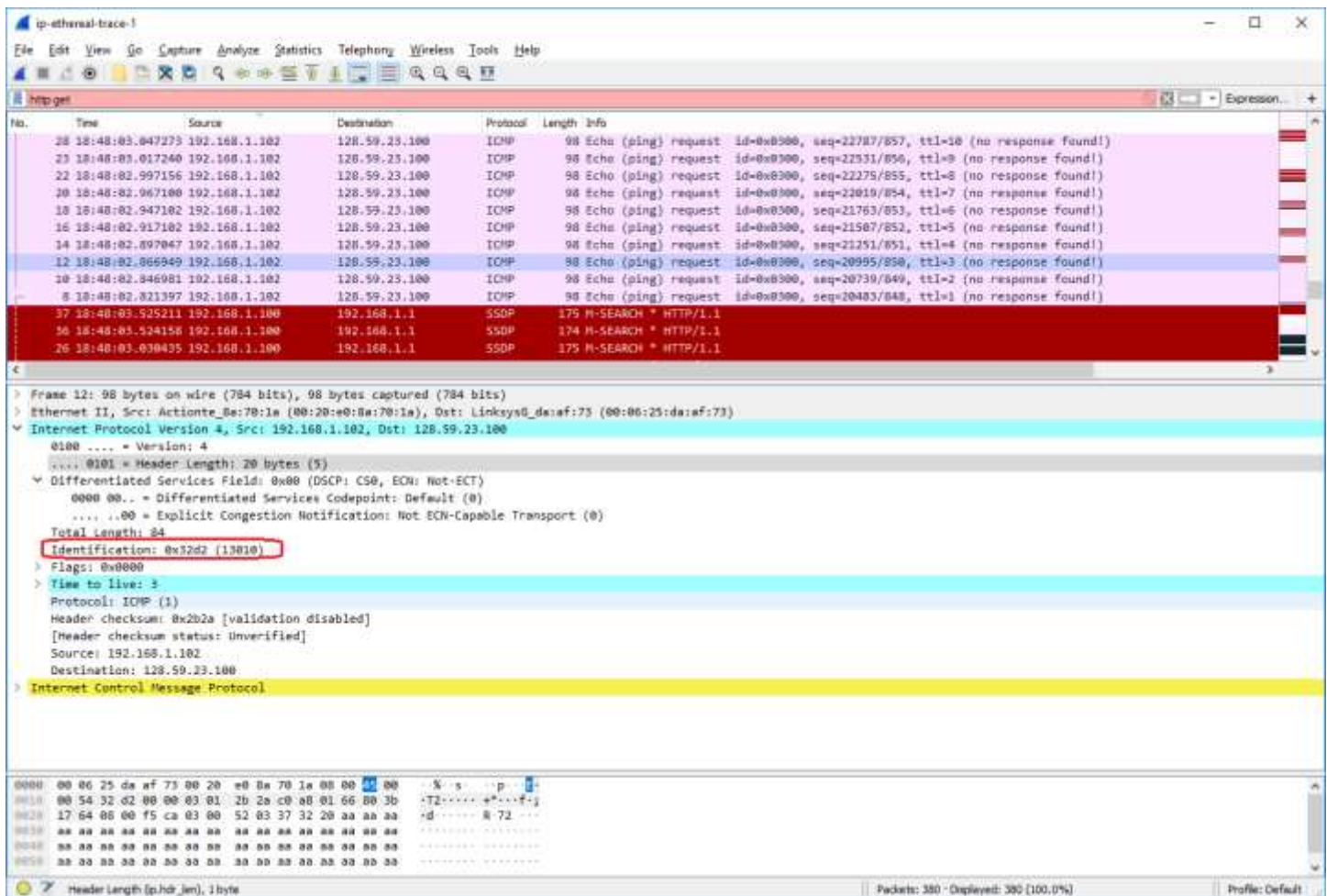
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

Header Length (p.hdr.len), 1 byte

Packets: 380 - Displayed: 300 (100.0%)

Profile: Default



Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

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

The value in the Identification field is 0x9d7c (40316). The value in the TTL field is 255.

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of captured packets, including several ICMP messages. The middle pane shows the detailed structure of a selected packet, highlighting fields such as Identification, Time to live, and Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
124	18:48:25.538386	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
77	18:48:12.996430	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
52	18:48:07.998461	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
21	18:48:02.992672	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
330	18:48:50.159434	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
274	18:48:45.151425	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
219	18:48:40.144150	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
179	18:48:35.150169	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	18:48:30.128980	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	18:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	18:48:12.838801	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	18:48:07.832647	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	18:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface II, Src: Linksys0_da:af:73 (08:00:27:da:af:73), Dst: Actionte_8a:70:1a (08:20: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)

0100 00.. = Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

1100 00.. = Differentiated Services Codepoint: Class Selector 0 (48)

.... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total length: 56

Identification: 0x9d7c (40516)

Flags: 0x0000

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x5ca0 [validation disabled]

[Header checksum status: Unverified]

Source: 10.216.228.1

Destination: 192.168.1.102

Internet Control Message Protocol

- 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 Identification field changes for each ICMP IP datagram sent to my computer because each packet needs a unique value that identifies it. The Time to Live field stays at 255 for each ICMP TTL-exceeded packet and does not change because traceroute only increments the TTL with each hop. Since all of these ICMP TTL-exceeded packets are replies from the nearest (first hop) router, they all have the same TTL value.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http get

No.	Time	Source	Destination	Protocol	Length	Info
124	18:48:25.538306	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
77	18:48:12.996438	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
52	18:48:07.990461	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
21	18:48:02.992672	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
530	18:48:50.159454	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
274	18:48:45.151425	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
219	18:48:40.144138	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
179	18:48:35.150169	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	18:48:30.128908	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	18:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	18:48:12.838001	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	18:48:07.832847	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	18:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Ethernet II, Src: LinksysG_d8:af:73 (08:06:25:d8:af:73), Dst: Actionte_8a:70:1a (08:20: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)

1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total length: 55

Identification: 0x9d7c (40516)

Flags: 0x0000

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x6ca0 [validation disabled]

[Header checksum status: Unverified]

Source: 10.216.228.1

Destination: 192.168.1.102

Internet Control Message Protocol

```

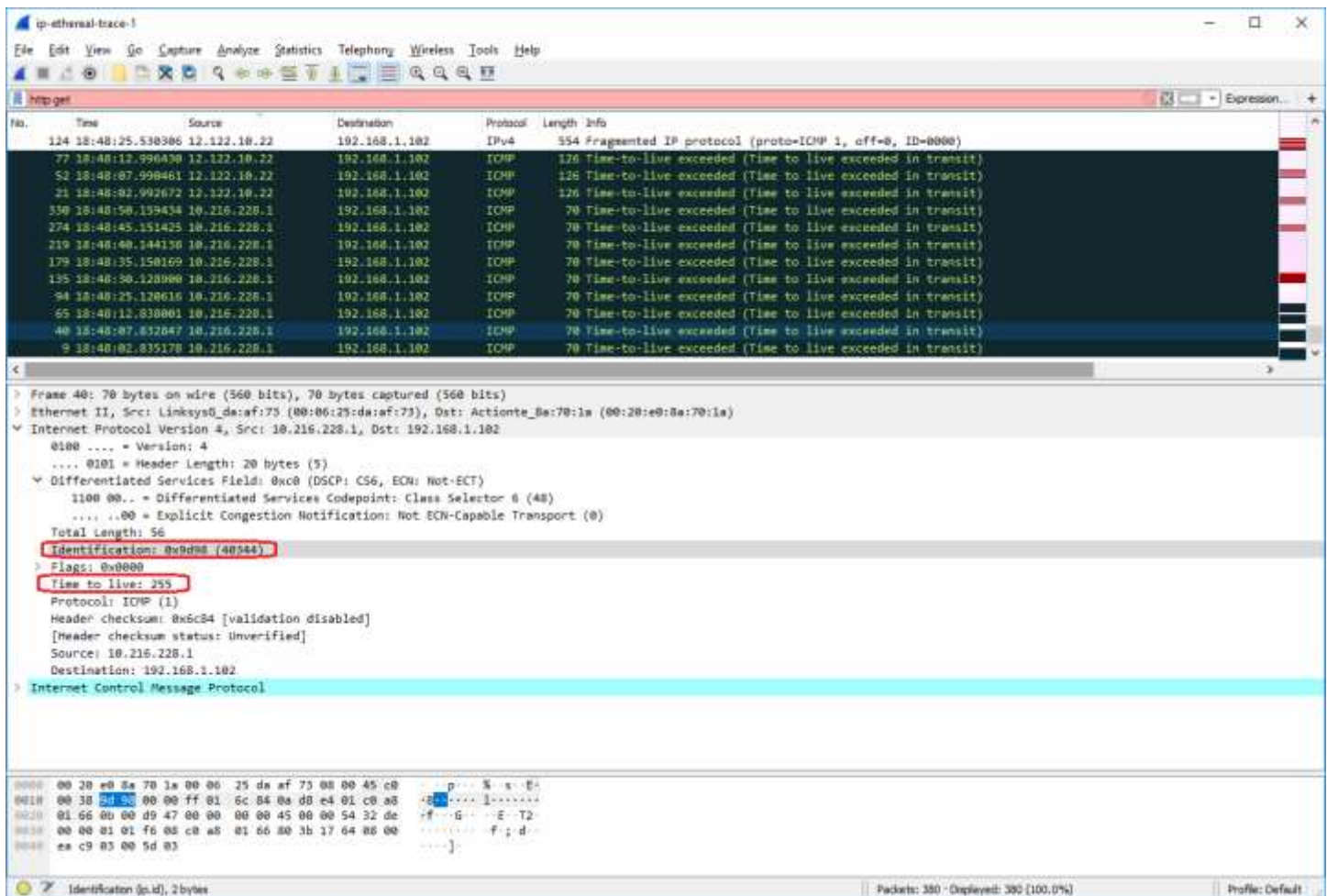
0000  00 20 e0 8a 70 1a 00 06 25 d8 af 73 08 00 45 c0  -...P...%..s..E-
0010  00 38 9d 7c 00 00 ff 01 6c a0 0a d8 e4 01 c0 a0  -H.....I.....
0020  01 66 0b 00 d9 46 00 00 00 00 45 00 00 54 32 00  -f...F...-E..T2-
0030  00 00 01 01 f6 16 c0 a8 01 66 80 3b 17 64 00 00  -.....f..d...P-
0040  f7 ca 05 00 50 03

```

Identification (p.id), 2 bytes

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default



Sort the packet listing according to time again by clicking on the *Time* column.

- 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? [Note: if you find your packet has not been fragmented, you should download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the *ip-ethereal-trace-1* packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.¹]

Yes, this message was fragmented into 2 IP datagrams in frames 92 and 93. Frame 92 stored 1480 bytes of data and Frame 93 stored 528 bytes of data.

¹ The packets in the *ip-ethereal-trace-1* trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> are all less than 1500 bytes. This is because the computer on which the trace was gathered has an Ethernet card that limits the length of the maximum IP packet to 1500 bytes (40 bytes of TCP/IP header data and 1460 bytes of upper-layer protocol payload). This 1500 byte value is the standard maximum length allowed by Ethernet. If your trace indicates a datagram longer than 1500 bytes, and your computer is using an Ethernet connection, then Wireshark is reporting the wrong IP datagram length; it will likely also show only one large IP datagram rather than multiple smaller datagrams. This inconsistency in reported lengths is due to the interaction between the Ethernet driver and the Wireshark software. We recommend that if you have this inconsistency, that you perform this lab using the *ip-ethereal-trace-1* trace file.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.get

No.	Time	Source	Destination	Protocol	Length	Info
85	18:48:13.006610	192.168.1.102	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	18:48:13.101662	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	18:48:13.121734	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	18:48:13.126955	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	18:48:13.158271	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	18:48:19.586445	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	18:48:19.611000	128.119.245.12	192.168.1.102	TCP	60	72 → 1170 [ACK] Seq=71 Win=35040 len=0
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	18:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	18:48:25.120616	10.716.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	18:48:25.129820	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	18:48:25.129698	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	18:48:25.149815	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]

> Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: Actionte_8e:70:1a (08:20:e0:8a:70:1a), Dst: Linksys_0a:af:73 (00:06:25:da:af:73)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total length: 1500

Identification: 0x32f9 (13049)

> Flags: 0x2000, More fragments

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x077b [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.102

Destination: 128.59.23.100

Reassembled IPv4 in frame: 93

> Data (1488 bytes)

Data: 0000d8c603007703373620aaaaaaaaaaaaaaaaaaaaaaaa.....

[Length: 1488]

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 00 00 45 00 -X- -s- -p- -E-

0010 05 dc 32 f9 20 00 01 01 07 7b c0 a0 01 66 00 3b -Z- -f- -f- -f-

0020 17 64 00 00 d0 c0 03 00 77 03 37 36 20 aa aa aa -d- -m- 76 -

0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

Invalid filter: "get" was unexpected in this context.

Packets: 380 - Displayed: 300 (100.0%)

Profile: Default

The screenshot shows a Wireshark packet capture of a fragmented IP datagram. The packet list at the top shows a fragmented IP protocol (proto=ICMP, off=0, ID=32f9) reassembled in #93. The packet details pane shows the reassembled IPv4 data with a length of 2000 bytes. The packet bytes pane shows the raw data with a length of 2000 bytes.

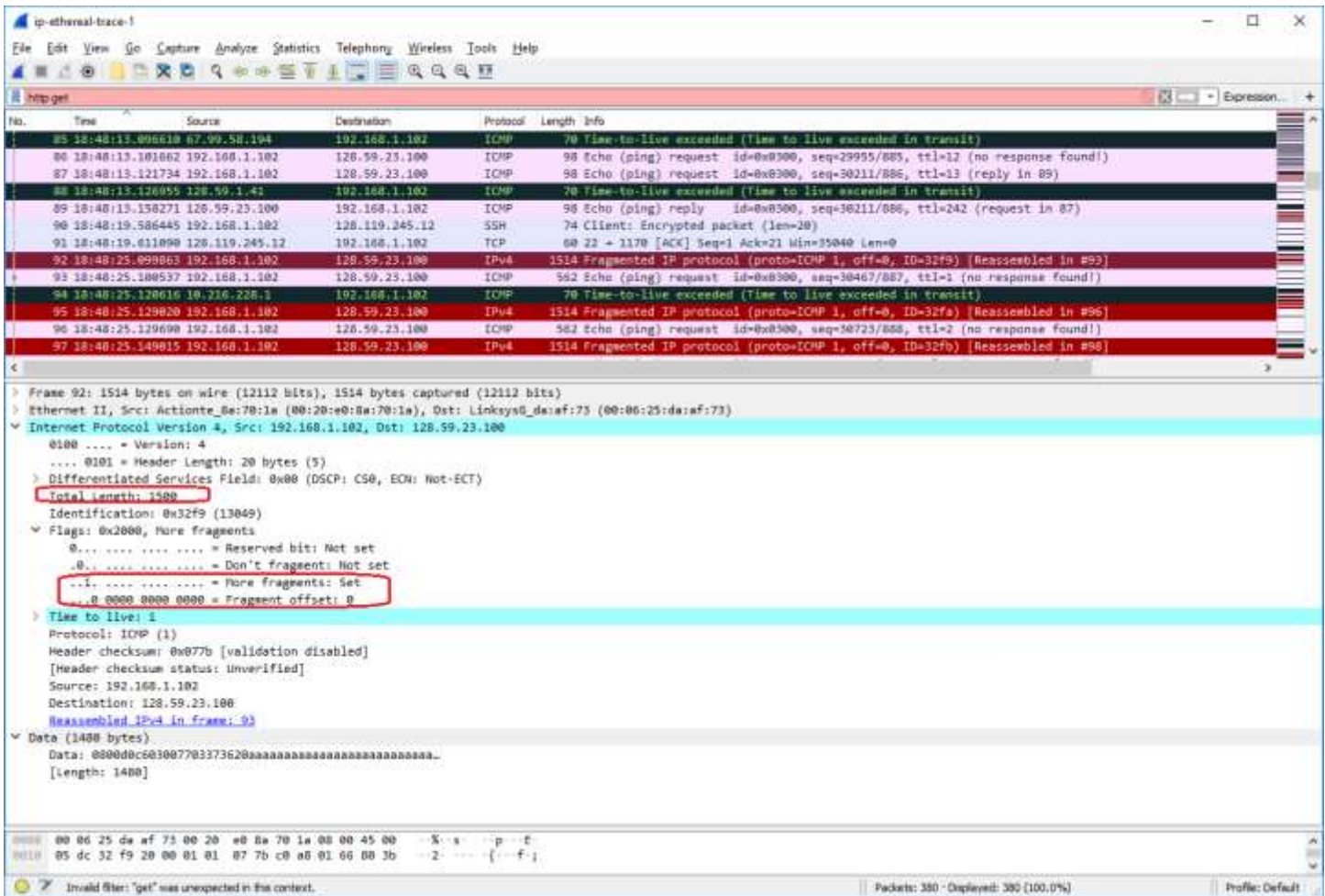
No.	Time	Source	Destination	Protocol	Length	Info
85	18:48:13.006610	192.168.1.102	128.59.23.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	18:48:13.101662	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	18:48:13.121734	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	18:48:13.126955	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	18:48:13.158271	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	18:48:19.586445	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	18:48:19.631898	128.119.245.12	192.168.1.102	TCP	68	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	18:48:25.109537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	18:48:25.120616	128.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	18:48:25.129820	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #96]
96	18:48:25.129698	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	18:48:25.149815	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #98]

Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x2a7a [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.102
 Destination: 128.59.23.100
 [2 IPv4 Fragments (2000 bytes): #92(1488), #93(520)]
 [Frame 92, payload: 0-1479 (1488 bytes)]
 [Frame 93, payload: 1488-2007 (520 bytes)]
 [Fragment count: 2]
 [Reassembled IPv4 length: 2000]
 [Reassembled IPv4 data: 080808c683007763375620aaaaaaaaaaaaaaaaaaaaaa...]
 Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x08c6 [correct]
 [Checksum Status: Good]
 Identifier (BE): 766 (0x0300)
 Identifier (LE): 3 (0x0003)
 Sequence number (BE): 30467 (0x7763)
 Sequence number (LE): 887 (0x0377)
 [No response seen]
 Data (2000 bytes)
 Data: 373620aa...
 [Length: 2000]

0000 08 00 d8 c6 03 00 77 63 17 56 20 aa aa aa aaw 76
 Frame (562 bytes) Reassembled IPv4 (2000 bytes)
 Sequence number (big endian representation) (icmp.seq), 2 bytes

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?

In the first fragment of the fragmented IP datagram, the Flags field is set to 0x2000 and bit 13 is set. Since bit 13 controls the More Fragments bit field and this bit is set, then this indicates that the datagram has been fragmented. Since the Fragment Offset is set to 0, then this indicates that this IP datagram is the first fragment. This IP datagram has Total Length = 1500 bytes.



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 there more fragments? How can you tell?

Firstly, the More Fragments field = 0 and the Fragment Count = 2, which means that there are no more fragments after this IP datagram and there are 2 total fragments, so this IP datagram cannot be the first fragment. Secondly, Fragment Offset = 185 bytes, which is a non-zero value, so this IP datagram cannot be the first datagram fragment. There are no more fragments because the IP header indicates that the Fragment Count = 2, which means that Frame 92 and 93 are the only packets associated with this 2000-byte IP packet.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.get

No.	Time	Source	Destination	Protocol	Length	Info
85	18:48:13.006610	192.168.1.102	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	18:48:13.101662	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	18:48:13.121734	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	18:48:13.126955	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	18:48:13.158271	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	18:48:19.586445	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	18:48:19.611898	128.119.245.12	192.168.1.102	TCP	68	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	18:48:25.180537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	18:48:25.120616	10.716.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	18:48:25.129820	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	18:48:25.129698	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	18:48:25.149815	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]

> Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: Actionte_0e:70:1a (00:20:e0:8a:70:1a), Dst: Linksys_0a: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: 0x08 (DSCP: CS0, ECN: Not-ECT)

Total length: 1500

Identification: 0x32f9 (13049)

Flags: 0x2000, More fragments

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

.1... .. = More fragments: Set

...0 0000 0000 0000 = Fragment offset: 0

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x077b [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.102

Destination: 128.59.23.100

Reassembled IPv4 in frame: 93

> Data (1400 bytes)

Data: 000000c003007703373620aaaaaaaaaaaaaaaaaaaaaaaa...

[length: 1400]

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 00 00 45 00 --[s]--p--t--

0010 05 dc 32 f9 20 00 01 01 07 7b c0 a0 01 66 00 3b --2--{--f--}

Invalid filter: "get" was unexpected in this context.

Packets: 380 - Displayed: 300 (100.0%)

Profile: Default

The image shows a Wireshark packet capture window titled "ip-ethereal-trace-1". The packet list pane displays several ICMP Echo (ping) requests and responses. The packet details pane for packet 93 shows the IP header and ICMP Echo (ping) request details. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
85	18:48:13.006610	67.99.58.104	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	18:48:13.101662	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	18:48:13.121734	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	18:48:13.126955	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	18:48:13.158271	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	18:48:19.586445	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	18:48:19.611898	128.119.245.12	192.168.1.102	TCP	68	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	18:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	18:48:25.104537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=38467/887, ttl=1 (no response found!)
94	18:48:25.120616	10.716.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	18:48:25.129820	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	18:48:25.129698	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=38723/888, ttl=2 (no response found!)
97	18:48:25.149815	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]

Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface II, Src: Actionte_8e:70:1a (08:20:e0:8a:70:1a), Dst: Linksys_0a:af:73 (08:06:25: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: 0x08 (DSCP: CS0, ECN: Not-ECT)
- Total length: 548
- 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: 105
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x2a7a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [2 IPv4 Fragments (2088 bytes): #92(1480), #93(528)]

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xd0c6 [correct]
- [Checksum Status: Good]
- Identifier (RFC1191): 768 (0x0300)

0000 08 00 d0 c6 03 00 72 01 37 56 20 aa aa aa aa 76

Frame (562 bytes) Reassembled IPv4 (2088 bytes)

Sequence number (big endian representation) (icmp.seq), 2 bytes

Packets: 380 - Displayed: 380 (100.0%) Profile: Default

Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500.

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

http get

No.	Time	Source	Destination	Protocol	Length	Info
206	18:48:35.482361	12.123.48.218	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
207	18:48:35.551866	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
208	18:48:35.614678	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
209	18:48:35.694731	192.205.32.100	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
210	18:48:35.757288	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	18:48:35.822521	67.99.56.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	18:48:35.886001	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
213	18:48:35.972615	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	18:48:35.988918	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215	18:48:37.637010	192.168.1.102	192.2.53.206	TCP	62	TCP Retransmission! 1483 -> 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
216	18:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	18:48:40.125168	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found)
219	18:48:40.144138	10.210.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	18:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	18:48:40.151395	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 568
 Identification: 0x3323 (13091)
 > Flags: 0x0172
 0... .. = Reserved bit: Not set
 .0... .. = Don't fragment: Not set
 ..0... .. = More fragments: Not set
 ...0 0001 0111 0010 = Fragment offset: 370
 > Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x2983 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.102
 Destination: 128.59.23.100
 > [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
 [Frame: 216, payload: 0-1479 (1480 bytes)]
 [Frame: 217, payload: 1488-2959 (1480 bytes)]
 [Frame: 218, payload: 2968-3507 (548 bytes)]
 [Fragment count: 3]
 [Reassembled IPv4 length: 3508]
 [Reassembled IPv4 data: 080000c303000e03375920aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...]
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xa0c3 [correct]
 [Checksum Status: Good]
 Identifier (BE): 768 (0x0300)
 Identifier (LE): 3 (0x0003)
 Sequence number (BE): 40451 (0x9e05)

0000 00 00 a9 c1 05 00 0a 01 37 30 20 aa aa aa aa 79
 0010 aa 00 aa 00 aa 00 aa 00 aa 00 aa 00 aa 00 aa 00
 Frame (562 bytes) Reassembled IPv4 (3508 bytes)

Sequence number (big endian representation) (icmp.seq), 2 bytes

Packets: 380 - Displayed: 380 (100.0%) Profile: Default

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

Total Length, Flags (More Fragments and Fragment Offset bit fields), and Header Checksum fields change in the IP header among the fragments.

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http get

No.	Time	Source	Destination	Protocol	Length	Info
206	18:48:35.482361	12.123.48.218	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8000)
207	18:48:35.551866	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8000)
208	18:48:35.614678	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
209	18:48:35.694731	192.205.32.100	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
210	18:48:35.757288	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	18:48:35.822521	67.99.56.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	18:48:35.886001	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
213	18:48:35.972615	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8056) [Reassembled in #214]
214	18:48:35.988918	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/926, ttl=242 (request in 205)
215	18:48:37.697010	192.168.1.102	192.168.1.102	TCP	62	[TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
216	18:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	18:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	18:48:40.144138	10.216.226.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	18:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	18:48:40.151395	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	18:48:40.157763	10.216.226.1	192.168.1.102	TCP	62	[TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: Actionte_8a:70:1a (08:120e:08a:70:1a), Dst: Linksys6_daa:f73 (00:06:25:da:a:f73)

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 (13085)
 > 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 (1400 bytes)
 Data: 0000a9c303009e03373928aaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
 [Length: 1400]

0000 00 06 25 da af 73 00 20 e8 8a 70 1a 00 00 45 00 --s-a--p--E-
 0010 05 dc 33 23 20 00 01 01 07 51 c0 a8 01 66 00 3b --34---Q---f;
 0020 17 64 08 00 a9 c3 03 00 9e 03 37 39 20 aa aa aa d-----79---

Invalid filter: "get" was unexpected in this context.

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http get

No.	Time	Source	Destination	Protocol	Length	Info
206	18:48:35.482361	12.123.48.218	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8888)
207	18:48:35.551866	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8888)
208	18:48:35.614678	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
209	18:48:35.694731	192.205.32.100	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
210	18:48:35.757288	216.148.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	18:48:35.822521	67.99.56.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	18:48:35.886001	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
213	18:48:35.972615	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8956) [Reassembled in #214]
214	18:48:35.988918	128.59.23.100	192.168.1.102	ICMP	502	Echo (ping) reply id=80300, seq=40195/925, ttl=242 (request in 205)
215	18:48:37.697010	192.168.1.102	199.2.53.206	TCP	62	[TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
216	18:48:40.124468	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	18:48:40.125168	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=80300, seq=40451/926, ttl=1 (no response found)
219	18:48:40.144138	10.216.226.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	18:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	18:48:40.151395	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	18:48:40.157763	10.216.226.1	192.168.1.102	TCP	62	[TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Frame 217: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: Actionte_8a:70:1a (08:120e:08a:70:1a), Dst: Linksys6_daa:f73 (00:06:25:da:a:f73)

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: 1508
 Identification: 0x3323 (13303)
 > 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: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.102
 Destination: 128.59.23.100
 Reassembled IPv4 in frame: 218

Data (1480 bytes)
 Data: aa...
 [Length: 1480]

0000 00 06 25 da af 73 00 20 e8 8a 70 1a 00 00 45 00 --S-a--p--E-
 0010 05 dc 33 23 20 b9 01 01 06 9b c0 a8 01 66 00 3b --3B-----f;
 0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa d-----

Invalid filter: "get" was unexpected in this context.

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http get

No.	Time	Source	Destination	Protocol	Length	Info
206	18:48:35.482361	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8000)
207	18:48:35.551866	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8000)
208	18:48:35.614678	12.122.10.22	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
209	18:48:35.694731	192.168.1.102	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
210	18:48:35.757288	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
211	18:48:35.822521	67.99.56.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	18:48:35.886001	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
213	18:48:35.972615	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8956) [Reassembled in #214]
214	18:48:35.988918	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=80000, seq=40195/925, ttl=242 (request in 205)
215	18:48:37.697010	192.168.1.102	199.2.53.206	TCP	62	[TCP Retransmission] 1483 -> 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
216	18:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #218]
217	18:48:40.125168	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	18:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=80000, seq=40451/926, ttl=1 (no response found)
219	18:48:40.144138	10.210.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	18:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	18:48:40.151305	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	18:48:40.157551	10.210.228.1	192.168.1.102	TCP	62	[TCP Retransmission] 1483 -> 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

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

Ethernet II, Src: Actionte_8a:70:1a (80:120:e0:8a:70:1a), Dst: Linksys6_daa:f:73 (00:06:25:da:a:f:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 568

Identification: 0x3323 (13001)

Flags: 0x0172

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0... .. = More fragments: Not set

...0 0001 0111 0010 = Fragment offset: 370

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x2983 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.102

Destination: 128.59.23.100

[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]

> Internet Control Message Protocol

0000 00 00 00 c1 81 00 0a 05 17 30 20 00 00 00 00 70

0018 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Frame (582 bytes) Reassembled IPv4 (3508 bytes)

IPv4Fragments [p.Fragments], 3508 bytes

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default