

Notes: I've attached my screenshots and boxed in red where I annotated my output.
Using ip-ethereal-trace-1

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?

192.168.102

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

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.

Header is 20 bytes. Total Length is 56 bytes. See screenshot for boxed areas

The screenshot displays the Wireshark interface for a packet capture named 'ip-ethereal-trace-1'. The packet list pane shows several packets, with packet 8 selected. This packet is an ICMP Echo (ping) request from source IP 192.168.1.102 to destination IP 128.59.23.100. The packet details pane is expanded to show the 'Internet Protocol Version 4' header. Within this header, the 'Source' field is boxed in red and contains the value '192.168.1.102', and the 'Destination' field is also boxed in red and contains '128.59.23.100'. Below the IP header, the 'Internet Control Message Protocol' section is expanded, showing it is an 'Echo (ping) request' with a 'Total Length' of 56 bytes. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
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 (r)
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 (r)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (r)
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (r)

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)
Header checksum: 0x2d2c (validation disabled)
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ca [correct]
[Checksum Status: Good]
Identifier (BE): 768 (0x0300)
Identifier (LE): 3 (0x0003)
Sequence number (BE): 20483 (0x5003)
Sequence number (LE): 848 (0x0350)
[No response seen]
Data (56 bytes)

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. .p..E.
0010 00 54 32 d0 00 01 01 2d 2c c0 a8 01 66 80 3b .T2....-,...f;
0020 17 64 08 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 ..
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 ..
0060 aa aa ..

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

No, the fragments flag is 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?

ID, time to live, and header checksum

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

Constant: Version, header length, total length, flag, fragment offset, protocol, source, and destination.

Change: All else, header checksum, sequence number, frame #

The protocol, source, destination, and flag must stay constant since the same data is being transmitted from one device to another. The ID and time-to-live would change since they are attached to unique packets and not the data transmission. The header checksum changes since the header changes. Thus, the checksum would be different each time.

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

It will increment with each new call

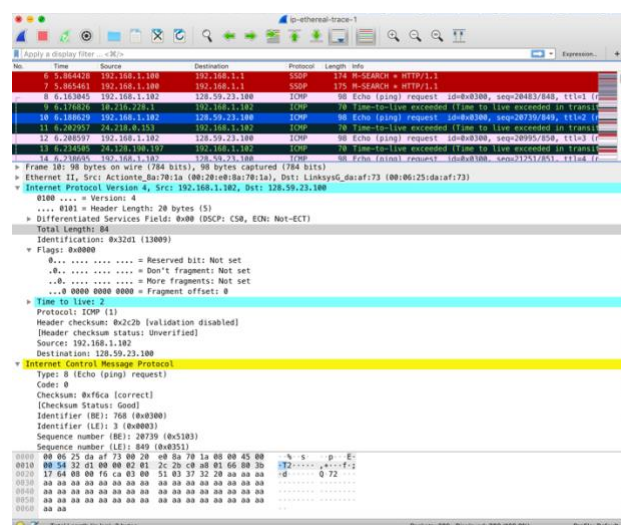
8. What is the value in the Identification field and the TTL field?

ID: 0x32d1 or 13009

TLL: 2

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?

No, the ID and TTL will change. The ID field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. The TTL field remains unchanged because the TTL for the first hop router is always the same.



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, the message was fragmented. We can see the “fragmented IP protocol”

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 Flags bit for more fragments is set “More fragments: Set”, indicating that the datagram has been fragmented. Since the fragment offset is 0, this is the first fragment. This first datagram has a total length of 1500.

The screenshot shows a Wireshark packet capture of an ICMP Echo request. The packet list pane displays a fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) with a total length of 1514 bytes. The packet details pane shows the Internet Protocol Version 4 header with flags set to 'More fragments: Set' and a total length of 1500 bytes. The packet bytes pane shows the raw data of the first fragment.

No.	Time	Source	Destination	Protocol	Length	Info
92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9)
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (r)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa)
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (r)
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb)
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (r)
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc)
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (r)

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
Identification: 0x32f9 (13049)
Flags: 0x2000, More fragments
0... .. = Reserved bit: Not set
.0.. .. = Don't fragment: Not set
..1. = More fragments: Set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x077b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Reassembled IPv4 in frame: 93
Data (1480 bytes)

0010 05 dc 32 f9 20 00 01 01 07 7b c0 a8 01 66 80 3b ..2. ... {...f;
0020 17 64 08 00 d0 c6 03 00 77 03 37 36 20 aa aa aa .d..... w 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
0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0070 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

Source (ip.src), 4 bytes

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default

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?

The fragment offset is not zero. No, more fragments flag is not set

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

Fields that changed are: total length, flags, fragment offset, and check sum.

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

From the given lab file (ip-ethereal-trace-1), I found 7 fragments. However, if we act in according to the Lab instructions, we'd have 3.

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

Fields changed: total length, flags, fragment offset, and checksum

The image shows a Wireshark packet capture analysis of a file named 'ip-ethereal-trace-1'. The packet list on the left shows several packets, with packets 133 and 134 highlighted in red, indicating they are fragments of a larger datagram. Packet 133 is an IPv4 packet with a length of 1514 bytes, and packet 134 is an ICMP packet with a length of 562 bytes. The packet details pane on the right shows the structure of the selected packet (packet 134). It is an Internet Control Message Protocol (ICMP) packet, specifically an Echo (ping) request. The details show the following fields: Type: 8 (Echo (ping) request), Code: 0, Checksum: 0xc3c5 [correct], Identifier (BE): 768 (0x0300), Identifier (LE): 3 (0x0003), and Sequence number (BE): 33795 (0x8403). The packet is fragmented, with a total length of 2008 bytes (1480 bytes for the first fragment and 528 bytes for the second fragment). The packet is captured on the Ethernet II interface, with source MAC address 00:20:e0:8a:70:1a and destination MAC address 00:06:25:da:af:73. The packet is sent from 192.168.1.102 to 128.59.23.100. The packet details pane also shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
130	29.291816	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0954)
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=242
132	32.067024	192.168.1.102	199.2.53.206	TCP	62	1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PE
133	33.451751	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3307)
134	33.452422	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=33795/900, ttl=1 (r
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
136	33.477857	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3308)
137	33.478525	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=34051/901, ttl=2 (r
138	33.497679	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3309)

Frame 134: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

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

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 548
- Identification: 0x3307 (13063)
- 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
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x2a6c [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [2 IPv4 Fragments (2008 bytes): #133(1480), #134(528)]

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xc3c5 [correct]
- [Checksum Status: Good]
- Identifier (BE): 768 (0x0300)
- Identifier (LE): 3 (0x0003)
- Sequence number (BE): 33795 (0x8403)

0010 02 24 33 07 00 b9 01 01 2a 6c c0 a8 01 66 80 3b .\$. *l . . . f . ;

0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa .d

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

0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

Frame (562 bytes) Reassembled IPv4 (2008 bytes)

Header checksum status (ip.checksum.status)

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