

1. The IP address is 192.168.1.102

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
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
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran

> 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)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d0 (13008)
> Flags: 0x0000
> Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]

Internet Protocol Version 4 (ip), 20 bytes

Packets: 380 · Displayed: 380 (100.0%)

Profile: Default

2. The value is ICMP (1)

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
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
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran

> 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)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d0 (13008)
> Flags: 0x0000
> Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]

Internet Protocol Version 4 (ip), 20 bytes

Packets: 380 · Displayed: 380 (100.0%)

Profile: Default

3. There are 20 bytes in the IP header and 84 bytes in the packet. Therefore, the payload is 64 bytes.

The screenshot shows a Wireshark capture of an ICMP Echo (ping) request. The packet list shows packet 8 at time 6.163045, source 192.168.1.102, destination 128.59.23.100, protocol ICMP, length 98. The packet details pane shows the Ethernet II header, followed by the Internet Protocol Version 4 header. The IP header fields are: Version: 4, Header Length: 20 bytes (5), Differentiated Services Field: 0x00, Total Length: 84, Identification: 0x32d0, Flags: 0x0000, Time to live: 1, Protocol: ICMP (1), Header checksum: 0x2d2c. The packet bytes pane shows the raw data of the packet.

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
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran

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]

Internet Protocol Version 4 (ip), 20 bytes

4. A Fragment offset of 0 indicates that the datagram has not been fragmented.

The screenshot shows the same Wireshark capture as above, but with the packet details pane expanded to show the fragmentation details. The IP header fields are: Version: 4, Header Length: 20 bytes (5), Differentiated Services Field: 0x00, Total Length: 84, Identification: 0x32d0, Flags: 0x0000, Time to live: 1, Protocol: ICMP (1), Header checksum: 0x2d2c. The packet bytes pane shows the raw data of the packet.

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
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tran

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
...0 0000 0000 0000 = Fragment offset: 0
> Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2d2c [validation disabled]

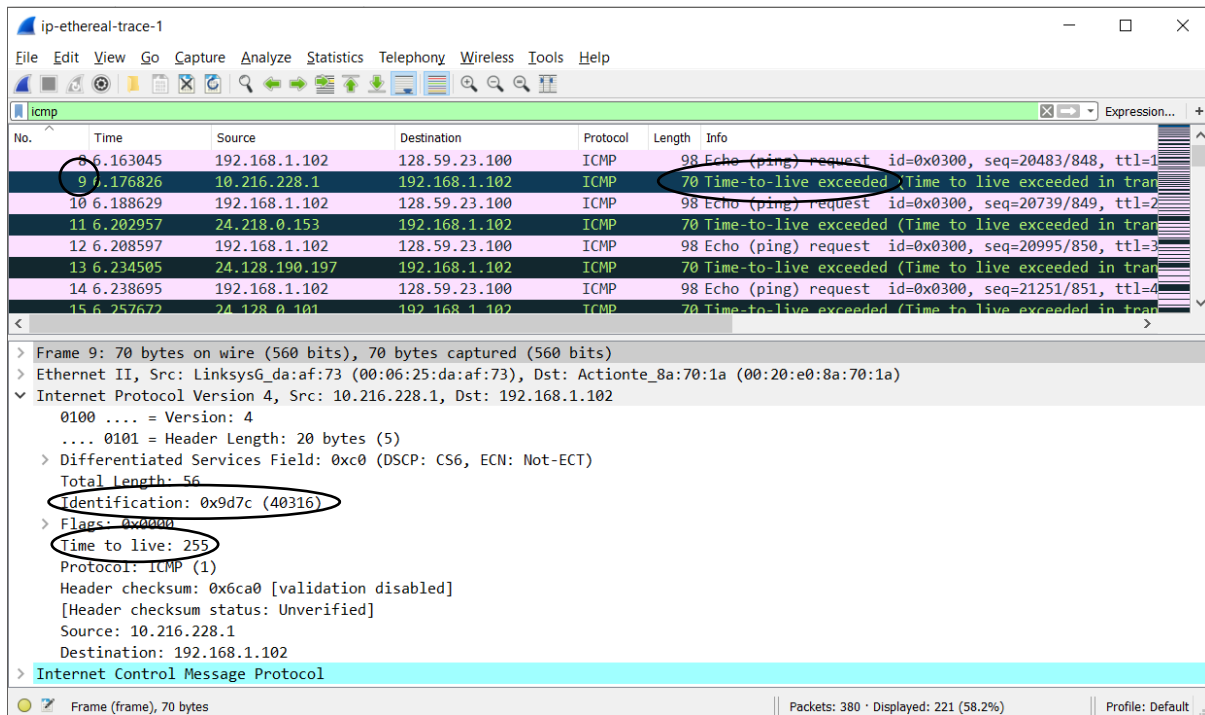
Fragment offset (13 bits) (ip.frag_offset), 2 bytes

- Header checksum, Time to Live and Identification change between datagrams.
- The fields that stay constant and must stay constant (indicated by red) are Version, Header Length, DSF, Protocol, and the Source and Destination IPs. The fields that must change (indicated by black) are the same as the fields from question 5.
- The patterns I noticed are that the TTL and the Identification increment by 1 each echo request.

The screenshots show a network capture of ICMP Echo (ping) requests. The first screenshot displays Frame 8, which is an Echo (ping) request with a TTL of 1 and an Identification of 13008. The second screenshot displays Frame 10, which is an Echo (ping) request with a TTL of 2 and an Identification of 13009. Red boxes highlight fields that remain constant across frames: Version (4), Header Length (20 bytes), DSF (0x00), Protocol (ICMP), Source IP (192.168.1.102), and Destination IP (128.59.23.100). Black boxes highlight fields that change: Identification (increases by 1) and Time to live (increases by 1).

No.	Time	Source	Destination	Protocol	Length	Info
20	6.308748	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1
380	54.973666	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=50179/964, ttl=7

8. The TTL is 255 and the Identification is 40316.



ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi

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

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

> Internet Protocol Version 4, Src: 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: 0x9d7c (40316)

> 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

Frame (frame), 70 bytes

Packets: 380 · Displayed: 221 (58.2%)

Profile: Default

9. The TTL value changes for some, not all, of the TTL-exceeded replies, while the Identification changes for each TTL-exceeded reply.

10. Yes, the message is fragmented.

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a packet list with several ICMP echo requests. Packet 92 is highlighted, and its details pane shows the 'Reassembled IPv4 in frame: 93' field. The bottom screenshot shows the same packet list, but packet 93 is highlighted, and its details pane shows the '2 IPv4 Fragments' section, indicating that the packet is fragmented.

Top Screenshot: Packet 92 Details

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
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
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
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
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc)

Packet 92 Details:

- 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
 - 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)

Bottom Screenshot: Packet 93 Details

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
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
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
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
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc)

Packet 93 Details:

- Total Length: 548
- Identification: 0x32f9 (13049)
- Flags: 0x00b9
- 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 (2008 bytes): #92(1480), #93(528)
 - [Frame: 92, payload: 0-1479 (1480 bytes)]
 - [Frame: 93, payload: 1480-2007 (528 bytes)]
 - [Fragment count: 2]
 - [Reassembled IPv4 length: 2008]
 - [Reassembled IPv4 data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaa...]
- Internet Control Message Protocol

11. The More fragments flag being set to 1 indicates a fragmented datagram. A Fragment offset of 0 indicates that this is the first fragment. The Total Length of the IP datagram is 1500.

The screenshot shows a Wireshark capture of an ICMP Echo request packet (Frame 92) from 192.168.1.102 to 128.59.23.100. The packet is fragmented, with a total length of 1514 bytes. The IP header shows a 'More fragments' flag set to 1 and a fragment offset of 0. The ICMP payload is an Echo request with ID 0x0300 and sequence 30467/887.

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
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9)
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9)
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9)

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

12. The Fragment offset is not 0 so this is not the first fragment. The More fragments flag being not set (0) indicates that there are no more fragments.

The screenshot shows a Wireshark capture of an ICMP Echo request packet (Frame 93) from 192.168.1.102 to 128.59.23.100. The packet is fragmented, with a total length of 562 bytes. The IP header shows a 'More fragments' flag set to 0 and a fragment offset of 185. The ICMP payload is an Echo request with ID 0x0300 and sequence 30467/887.

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

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

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 548
- Identification: 0x32f9 (13049)
- Flags: 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: 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)]
 - [Frame: 92, payload: 0-1479 (1480 bytes)]
 - [Frame: 93, payload: 1480-2007 (528 bytes)]
 - [Fragment count: 2]

13. The fields that change between the first and second fragments include Flags like Fragment offset and More fragments, the Header checksum, and the Total Length.

14. There are 3 fragments from the original datagram.

The screenshot shows a Wireshark packet capture of an ICMP Echo (ping) request. The packet list shows three fragments of the request, each 582 bytes long. The packet details pane shows the ICMP Echo (ping) request with a header checksum of 0x2983 and a destination of 128.59.23.100. The fragments are listed as follows:

- Fragment 1: [Frame: 216, payload: 0-1479 (1480 bytes)]
- Fragment 2: [Frame: 217, payload: 1480-2959 (1480 bytes)]
- Fragment 3: [Frame: 218, payload: 2960-3507 (548 bytes)]

The packet details pane also shows the reassembled IPv4 data: 0800a9c303009e03373920aaaaaaaaaaaaaaaaaaaaaaaaaa...

15. The fields that have changed are Fragment offset, Flags, Total Length and Header checksum.

The screenshot shows a Wireshark packet capture of an ICMP Echo (ping) request. The packet list shows three fragments of the request, each 582 bytes long. The packet details pane shows the ICMP Echo (ping) request with a header checksum of 0x2983 and a destination of 128.59.23.100. The fragments are listed as follows:

- Fragment 1: [Frame: 216, payload: 0-1479 (1480 bytes)]
- Fragment 2: [Frame: 217, payload: 1480-2959 (1480 bytes)]
- Fragment 3: [Frame: 218, payload: 2960-3507 (548 bytes)]

The packet details pane also shows the reassembled IPv4 data: 0800a9c303009e03373920aaaaaaaaaaaaaaaaaaaaaaaaaa...