

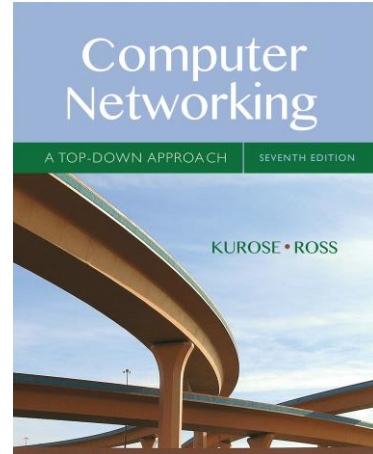
Name: Katie Schaumleffle

## Wireshark Lab: IP v7.0

Supplement to *Computer Networking: A Top-Down Approach*, 7<sup>th</sup> ed., J.F. Kurose and K.W. Ross

*“Tell me and I forget. Show me and I remember. Involve me and I understand.”* Chinese proverb

© 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved



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? **192.168.1.102**

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 (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)
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!)

> 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)
- > 0000. .... = Flags: 0x00
- ...0 0000 0000 0000 = Fragment Offset: 0
- > Time to Live: 1
- Protocol: ICMP (1)

Destination Hardware Address (eth.dst), 6 bytes

Packets: 380 · Displayed: 380 (100.0%)

Profile: Default

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”**

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 192.168.1.11? 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)
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!)

> 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)

> 000. .... = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

> Time to Live: 1

Protocol: ICMP (1)

Destination Hardware Address (eth.dst), 6 bytes

Packets: 380 · Displayed: 380 (100.0%)

Profile: Default

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: 20 bytes**

**Total bytes length: 84 bytes**

**Payload of the IP datagram = 84-20 = 64 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
1	0.000000	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.11? 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)
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!)

> 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)

> 000. .... = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

> Time to Live: 1

Protocol: ICMP (1)

Destination Hardware Address (eth.dst), 6 bytes

Packets: 380 · Displayed: 380 (100.0%)

Profile: Default

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

**This has not been fragmented. We can see that the “more fragments” flag is set to 0.**

The screenshot shows a Wireshark packet capture of network traffic. The packet list on the left shows several SSDP M-SEARCH messages and three ICMP Echo (ping) requests. The selected packet is an ICMP Echo (ping) request with ID 0x0300, sequence 20483/848, and TTL=1. The details pane on the right shows the IP header fields for this packet. The 'Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)' is expanded, showing the 'More fragments' flag is not set. The 'Time to Live: 1' is also visible.

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)
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!)

Details of selected packet (ICMP Echo request):

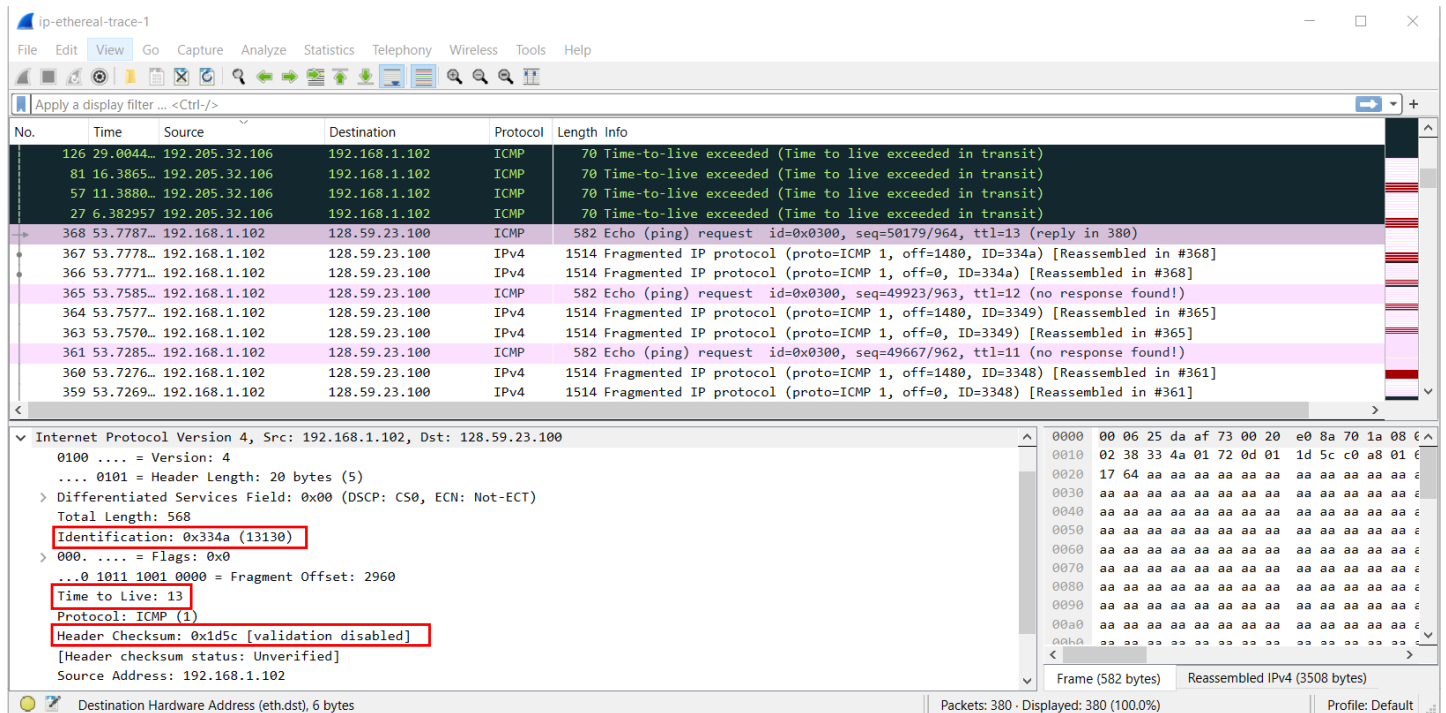
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x32d0 (13008)
- 000. .... = Flags: 0x0
  - 0... .. = Reserved bit: Not set
  - .0... .. = Don't fragment: Not set
  - ..0. .... = More fragments: Not set**
  - ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 1
- Protocol: ICMP (1)
- Header Checksum: 0x2d2c [validation disabled]
- [Header checksum status: Unverified]

Hex dump of packet data:

```
0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 00 00
0010 00 54 32 d0 00 00 01 01 2d 2c c0 a8 01 00 00 00
0020 17 64 08 00 f7 ca 03 00 50 03 37 32 20 00 00 00
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
```

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 fields in the IP datagram that always change from one datagram to the next within the ICMP messages sent by the computer are: Identification, Time to live, and Header checksum.**



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

The fields that must stay constant are:

Version- All packets use IPv4

**Header length-** The headers are the same length for ICMP packets

**Total length-** The total length stays the same for ICMP packets

Differentiated Service Fields- All packets are ICMP, therefore they use the same type of service class.

Source IP- All packets are sent from the same source.

Destination IP- All packets were sent to the same destination.

The fields that must change are:

**Identification-** Each packet has a unique ID

**Time to live-** The traceroute increments each subsequent packet

Header checksum- The header changes, therefore the checksum changes, too.

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
126	29.0044...	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	16.3865...	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	11.3880...	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	6.382957	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
368	53.7787...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (reply in 380)
367	53.7778...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
366	53.7771...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
365	53.7585...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
364	53.7577...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
363	53.7570...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
361	53.7285...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
360	53.7276...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]
359	53.7269...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3348) [Reassembled in #361]
358	53.7149...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49411/961, ttl=10 (no response found!)
357	53.7140...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3347) [Reassembled in #358]
356	53.7134...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3347) [Reassembled in #358]
355	53.6784...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49155/960, ttl=9 (no response found!)

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: 0x334a (13130)  
 000. .... = Flags: 0x0  
 ... 0 1011 1001 0000 = Fragment Offset: 2960  
 Time to Live: 13  
 Protocol: ICMP (1)  
 Header Checksum: 0x1d5c [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 192.168.1.102  
 Destination Address: 128.59.23.100  
 [3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]

Internet Control Message Protocol

Destination Hardware Address (eth.dst), 6 bytes

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

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

The pattern I see in the values in the ID field of the IP datagram, is that for each ICMP request, the identification increments.

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
92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
83	16.4132...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29699/884, ttl=11 (no response found!)
82	16.3932...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29443/883, ttl=10 (no response found!)
79	16.3631...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29187/882, ttl=9 (no response found!)
78	16.3431...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=28931/881, ttl=8 (no response found!)
76	16.3130...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=28675/880, ttl=7 (no response found!)
74	16.2931...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=28419/879, ttl=6 (no response found!)
72	16.2785...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=28163/878, ttl=5 (no response found!)
70	16.2430...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=27907/877, ttl=4 (no response found!)
68	16.2129...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=27651/876, ttl=3 (no response found!)
66	16.1930...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=27395/875, ttl=2 (no response found!)
64	16.1668...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=27139/874, ttl=1 (no response found!)
61	11.4561...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=26883/873, ttl=13 (reply in 63)
60	11.4360...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=26627/872, ttl=12 (no response found!)

Destination: LinksysG\_da:af:73 (00:06:25:da:af:73)  
 Address: LinksysG\_da:af:73 (00:06:25:da:af:73)  
 .... 0. .... = LG bit: Globally unique address (factory default)  
 .... 0. .... = IG bit: Individual address (unicast)  
 Source: Actionte\_8a:70:1a (00:20:e0:8a:70:1a)  
 Address: Actionte\_8a:70:1a (00:20:e0:8a:70:1a)  
 .... 0. .... = LG bit: Globally unique address (factory default)  
 .... 0. .... = IG bit: Individual address (unicast)  
 Type: IPv4 (0x0800)

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: 0x32f2 (13042)  
 000. .... = Flags: 0x0  
 ... 0 0000 0000 0000 = Fragment Offset: 0

Destination Hardware Address (eth.dst), 6 bytes

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

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
92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74 Client: Encrypted packet (len=20)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
83	16.4132...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=29699/884, ttl=11 (no response found!)
82	16.3932...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=29443/883, ttl=10 (no response found!)
79	16.3631...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=29187/882, ttl=9 (no response found!)
78	16.3431...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=28931/881, ttl=8 (no response found!)
76	16.3130...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=28675/880, ttl=7 (no response found!)
74	16.2931...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=28419/879, ttl=6 (no response found!)
72	16.2705...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=28163/878, ttl=5 (no response found!)
70	16.2430...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=27907/877, ttl=4 (no response found!)
68	16.2129...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=27651/876, ttl=3 (no response found!)
66	16.1930...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=27395/875, ttl=2 (no response found!)
64	16.1668...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=27139/874, ttl=1 (no response found!)
61	11.4561...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=26883/873, ttl=13 (reply in 63)
60	11.4360...	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=26627/872, ttl=12 (no response found!)

Destination: LinksysG\_da:af:73 (00:06:25:da:af:73)  
 Address: LinksysG\_da:af:73 (00:06:25:da:af:73)  
 ...0... = LG bit: Globally unique address (factory default)  
 ...0... = IG bit: Individual address (unicast)  
 Source: Actionte\_8a:70:1a (00:20:e0:8a:70:1a)  
 Address: Actionte\_8a:70:1a (00:20:e0:8a:70:1a)  
 ...0... = LG bit: Globally unique address (factory default)  
 ...0... = IG bit: Individual address (unicast)  
 Type: IPv4 (0x0800)  
 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: 0x32f3 (13043)  
 > 000. .... = Flags: 0x0  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Destination Hardware Address (eth.dst), 6 bytes

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

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

**ID field: 20429**

**TTL field: 243**

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
131	29.2995...	128.59.23.100	192.168.1.102	ICMP	562 Echo (ping) reply id=0x0300, seq=33539/899, ttl=242 (request in 122)
130	29.2918...	128.59.23.100	192.168.1.102	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0954) [Reassembled in #131]
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98 Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
63	11.4800...	128.59.23.100	192.168.1.102	ICMP	98 Echo (ping) reply id=0x0300, seq=26883/873, ttl=242 (request in 61)
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98 Echo (ping) reply id=0x0300, seq=23555/860, ttl=242 (request in 33)
377	54.7748...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
320	49.7701...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
266	44.7639...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
212	39.2276...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
170	34.2121...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
129	29.2071...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
62	11.4670...	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
326	52.9921...	128.119.245.12	192.168.1.102	TCP	60 22 → 1170 [ACK] Seq=1 Ack=41 Win=35040 Len=0

Internet Protocol Version 4, Src: 128.59.1.41, Dst: 192.168.1.102  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total length: 56  
 Identification: 0x4fcd (20429)  
 > 000. .... = Flags: 0x0  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 243  
 Protocol: ICMP (1)  
 Header Checksum: 0x3485 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 128.59.1.41  
 Destination Address: 192.168.1.102  
 Internet Control Message Protocol  
 Destination Hardware Address (eth.dst), 6 bytes

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



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 Time to live remains unchanged for all the ICMP TTL-exceeded replies sent to the computer by the nearest router because the TTL for the first hop router is always going to be the same.**

**The ID changes for all of the ICMP TTL-exceeded replies because the ID field has a unique value.**

The screenshot shows a Wireshark packet capture of ICMP Echo (ping) replies. The packet list pane displays several ICMP Echo (ping) replies from 192.168.1.102 to 128.59.23.100. The packet details pane shows the structure of an ICMP Echo reply, with the Time to Live field highlighted at 243. The packet bytes pane shows the raw data of the packet, with the Time to Live field highlighted at 243.

No.	Time	Source	Destination	Protocol	Length	Info
131	29.2995	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=242 (request in 122)
130	29.2918	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0954) [Reassembled in #131]
89	16.4999	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
63	11.4808	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=26883/873, ttl=242 (request in 61)
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=23555/860, ttl=242 (request in 33)
377	54.7748	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
320	49.7701	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
266	44.7639	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	39.2276	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
170	34.2121	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
129	29.2071	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
88	16.4686	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
62	11.4670	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
326	52.9921	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=41 Win=35040 Len=0

Internet Protocol Version 4, Src: 128.59.1.41, Dst: 192.168.1.102

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56
- Identification: 0x4fcd (20429)
- > 0000 .... = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 243
- Protocol: ICMP (1)
- Header Checksum: 0x3485 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 128.59.1.41
- Destination Address: 192.168.1.102

Internet Control Message Protocol

Time to Live (ip.ttl), 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

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

No.	Time	Source	Destination	Protocol	Length	Info
131	29.2995...	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=242 (request in 122)
130	29.2918...	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0954) [Reassembled in #131]
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
63	11.4800...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=26883/873, ttl=242 (request in 61)
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=23555/860, ttl=242 (request in 33)
377	54.7748...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
320	49.7701...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
266	44.7639...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	39.2276...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
170	34.2121...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
129	29.2071...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
62	11.4670...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
326	52.9921...	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=41 Win=35040 Len=0

Internet Protocol Version 4, Src: 128.59.1.41, Dst: 192.168.1.102

- 0100 .... = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56
- Identification: 0x4ecd (20173)
- > 0000 .... = Flags: 0x00
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 243
- Protocol: ICMP (1)
- Header Checksum: 0x3585 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 128.59.1.41
- Destination Address: 192.168.1.102
- > Internet Control Message Protocol

Time to Live (ip.ttl), 1 byte

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

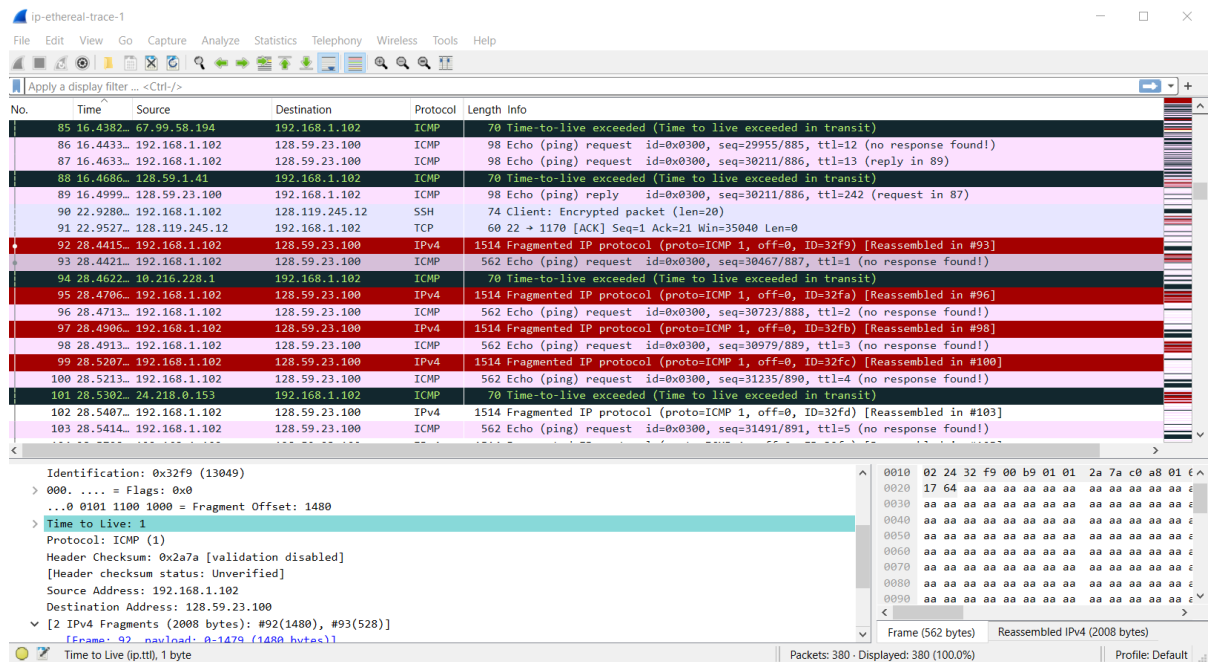
## Fragmentation

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

- 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 packet has been fragmented across more than one IP datagram.**





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 fragment's" is set to 1, which indicates that the datagram has been fragmented.**

**The fragment offset is set to 0, which indicates that this is the first fragment.**

**The IP datagram total length is 1500.**

Wireshark packet capture showing a fragmented IP datagram. The packet list shows a fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]. The packet details pane shows the IP header with the 'More fragments' flag set to 0 and the 'Fragment Offset' set to 1480. The packet bytes pane shows the raw data of the fragment.

No.	Time	Source	Destination	Protocol	Length	Info
83	16.4132...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29699/884, ttl=11 (no response found!)
84	16.4180...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.4382...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527...	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	28.4421...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	28.4622...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	28.4713...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	28.4906...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	28.4913...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	28.5207...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	28.5213...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!)
101	28.5302...	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Packet Details: IP Header (1)

- ... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 1500
- Identification: 0x32f9 (13049)
- 001. .... = Flags: 0x1, 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)

Time to Live (ip.ttl), 1 byte

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 set to 1480, which indicates that this is not the first fragment.**

**There are no more fragments, the “more fragments” flag is set to 0.**

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
83	16.4132..	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29699/884, ttl=11 (no response found!)
84	16.4180..	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.4382..	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.4433..	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	16.4633..	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	16.4686..	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999..	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	22.9280..	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527..	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.4415..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	28.4421..	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	28.4622..	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	28.4713..	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	28.4906..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	28.4913..	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	28.5207..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	28.5213..	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!)
101	28.5302..	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

.... 0101 = Header Length: 20 bytes (5)  
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 548  
 Identification: 0x32f9 (13049)  
 000. .... = Flags: 0x0  
 0... .... = Reserved bit: Not set  
 0... .... = Don't fragment: Not set  
 ..0... .... = More fragments: Not set  
 ...0 0101 1100 1000 = Fragment Offset: 1480  
 > Time to Live: 1  
 Protocol: ICMP (1)  
 Time to Live (ip.ttl), 1 byte

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

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

**The fields that change in the IP header between the fragments are: total length, flags, fragment offset, and checksum.**

ip-ethereal-trace-1

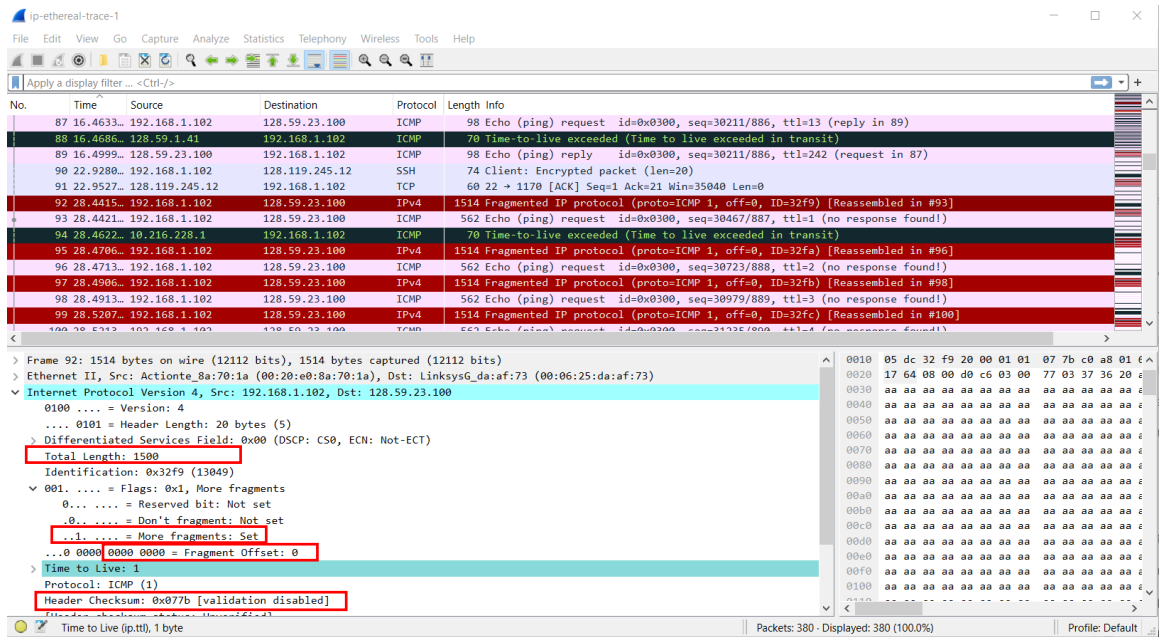
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
87	16.4633..	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	16.4686..	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999..	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	22.9280..	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527..	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.4415..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	28.4421..	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	28.4622..	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	28.4713..	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	28.4906..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	28.4913..	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	28.5207..	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 548  
 Identification: 0x32f9 (13049)  
 000. .... = Flags: 0x0  
 0... .... = Reserved bit: Not set  
 0... .... = Don't fragment: Not set  
 ..0... .... = More fragments: Not set  
 ...0 0101 1100 1000 = Fragment Offset: 1480  
 > Time to Live: 1  
 Protocol: ICMP (1)  
 Header Checksum: 0x2a7a [validation disabled]  
 (Header checksum status: Unverified)  
 Source Address: 192.168.1.102  
 Destination Address: 128.59.23.100  
 [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]  
 [Frame: 92, payload: 0-1479 (1480 bytes)]  
 Time to Live (ip.ttl), 1 byte

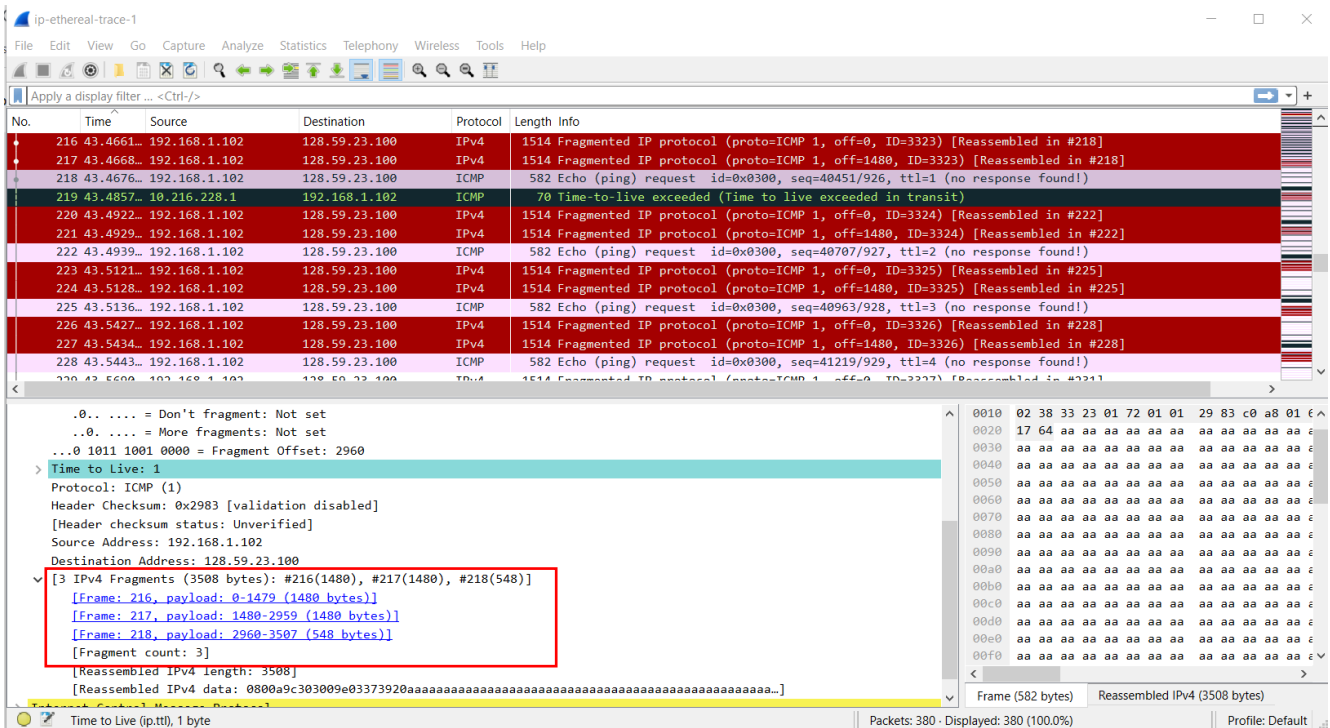
Packets: 380 - Displayed: 380 (100.0%) Profile: Default



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.**



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

**The IP header fields that change between all of the packets are: fragment offset and checksum.**

**The fields that change from 216 & 217 to 218: The first two packets differ from the last packet in total length, and flags. 216 & 217 have a total length of 1500, and the last packet has a length of 540. The first two packets have the “more fragments” flag set to 1, whereas 217 has that flag set to 0.**

**216:**

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
216	43.4661	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.4668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	43.4676	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	43.4857	192.168.1.102	128.59.23.100	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	43.4922	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.4929	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	43.4939	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223	43.5121	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224	43.5128	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225	43.5136	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)
226	43.5427	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled in #228]
227	43.5434	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3326) [Reassembled in #228]
228	43.5443	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
229	43.5500	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3327) [Reassembled in #231]

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

Total Length: 1500

Identification: 0x3323 (13091)

001. .... = Flags: 0x1, 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 Address: 192.168.1.102

Destination Address: 128.59.23.100

[Reassembled IPv4 in frame: 218]

> Data (1480 bytes)

Time to Live (p.ttl), 1 byte

Packets: 380 · Displayed: 380 (100.0%)

Profile: Default

**217:**

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
216	43.4661	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.4668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	43.4676	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	43.4857	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	43.4922	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.4929	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	43.4939	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223	43.5121	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224	43.5128	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225	43.5136	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)
226	43.5427	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled in #228]
227	43.5434	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3326) [Reassembled in #228]
228	43.5443	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
229	43.5600	102.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3327) [Reassembled in #231]

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

Total Length: 1500

Identification: 0x3323 (13091)

001. .... = Flags: 0x1, More fragments

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

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

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

...0 0101 1100 1000 = Fragment Offset: 1480

Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x0698 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

[Reassembled IPv4 in frame: 218]

Data (1480 bytes)

Time to Live (ip.ttl), 1 byte

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default

218:

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
216	43.4661	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.4668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	43.4676	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	43.4857	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	43.4922	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.4929	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	43.4939	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223	43.5121	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224	43.5128	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225	43.5136	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)
226	43.5427	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled in #228]
227	43.5434	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3326) [Reassembled in #228]
228	43.5443	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
229	43.5600	102.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3327) [Reassembled in #231]

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

Total Length: 568

Identification: 0x3323 (13091)

000. .... = Flags: 0x0

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

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

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

...0 1011 1001 0000 = Fragment Offset: 2960

Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x2983 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 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: 1480-3059 (1480 bytes)]

[Frame: 218, payload: 3060-3507 (448 bytes)]

Time to Live (ip.ttl), 1 byte

Frame (582 bytes) Reassembled IPv4 (3508 bytes)

Packets: 380 - Displayed: 380 (100.0%)

Profile: Default