Wireshark Lab -- TCP

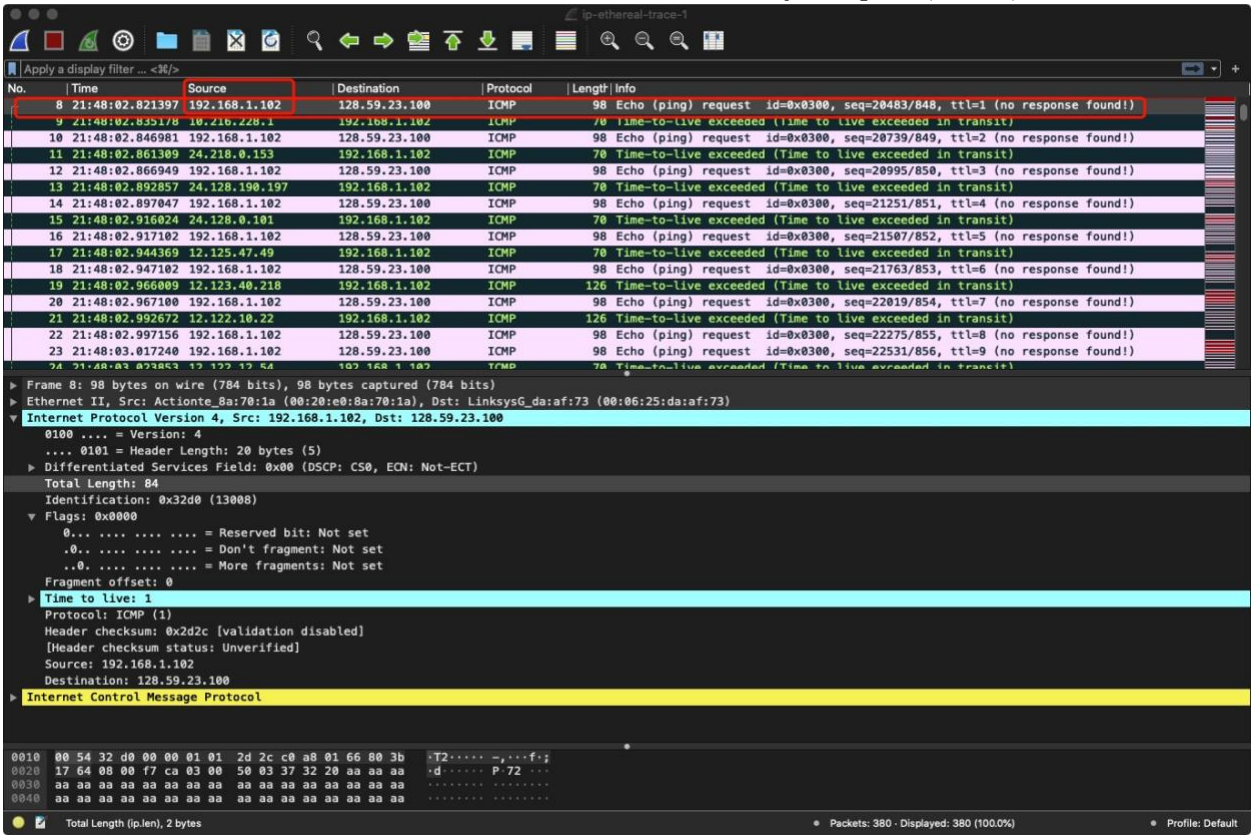
Jiaying Li
jl10919

Lab environment:

Answer: My PC uses macOS Catalina 10.15.6, shows the following setting with *ifconfig*:

Q1. 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?

Answer: As shown in the screenshot below, the IP address of my computer(source) is 192.168.1.102.

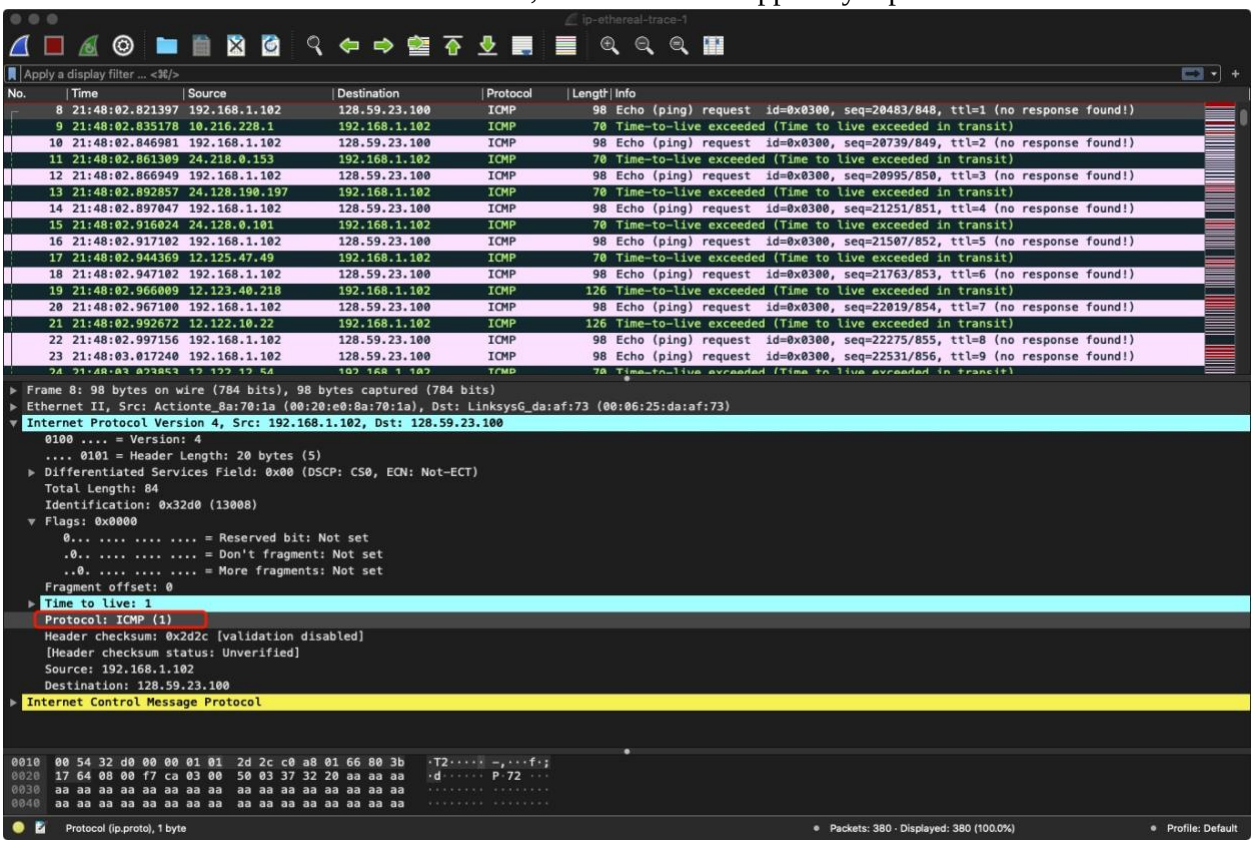


the first ICMP Echo Request message sent by your computer:

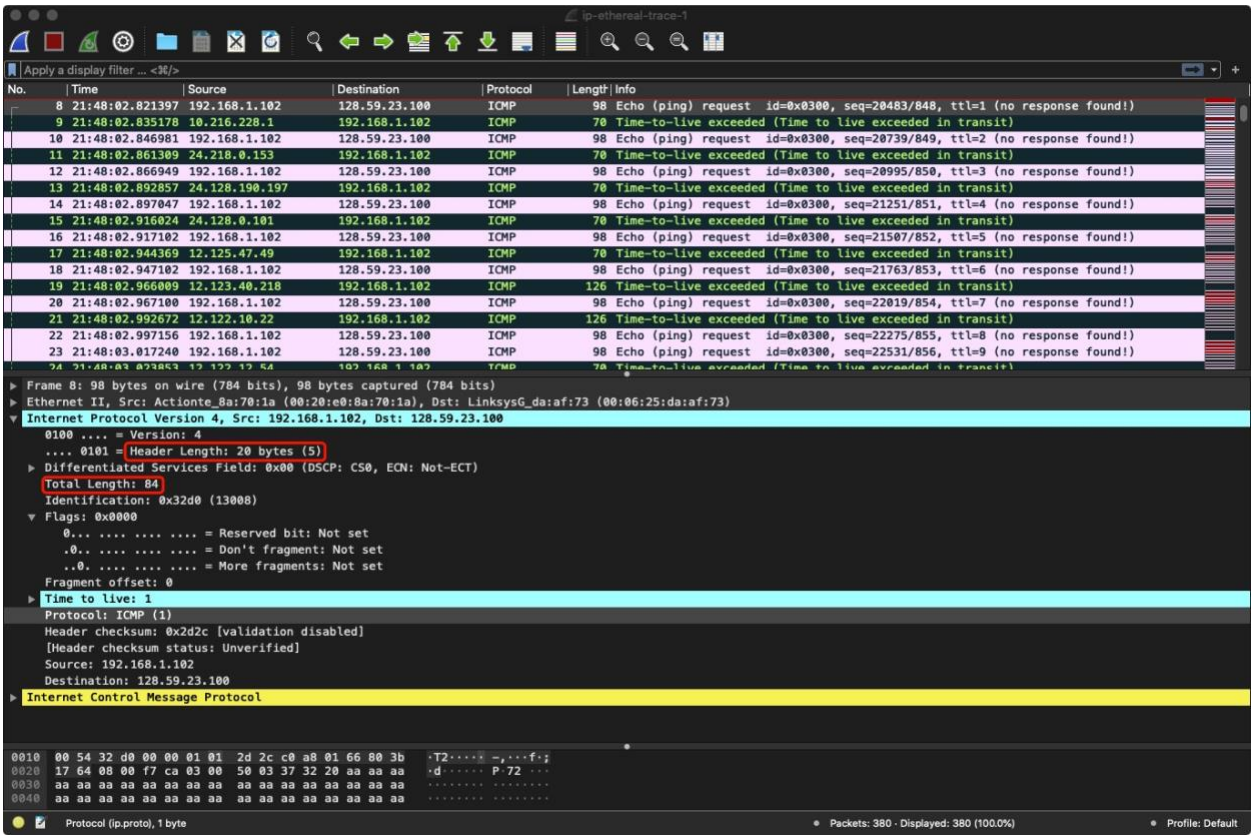
No. Time Source Destination Protocol Length Info
8 21:48:02.821397 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: 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
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)

Header checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
Internet Control Message Protocol

Q2. Within the IP packet header, what is the value in the upper layer protocol field?
Answer: As shown in the screenshot below, the value in the upper layer protocol field is ICMP.

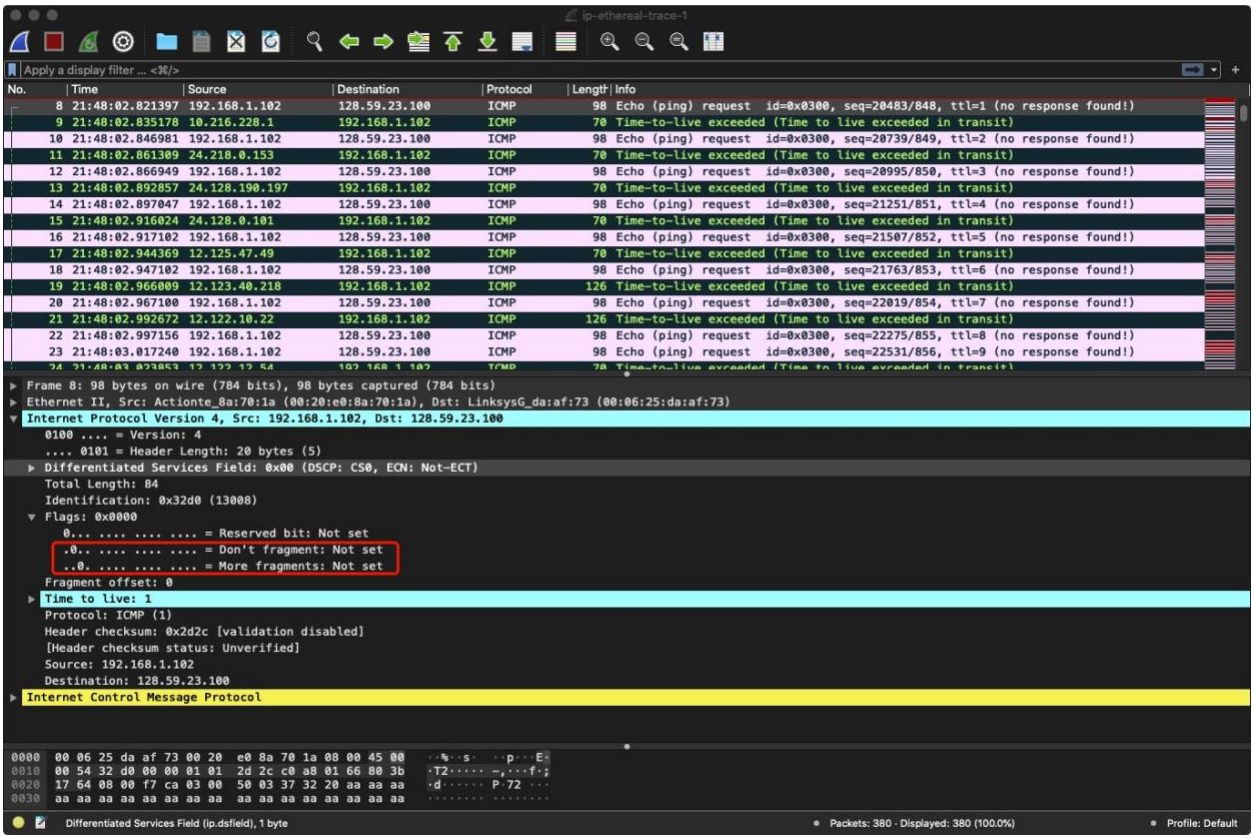


Q3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
Answer: As shown in the screenshot below, IP header is 20 bytes. Since the total length is 84 bytes, the payload of the IP datagram is 84-20=64 bytes. The length of payload of the IP datagram equals to the total length minus the header length.



Q4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Answer: As shown in the screenshot below, this IP datagram has not been fragmented, as the “more fragment” is not set.



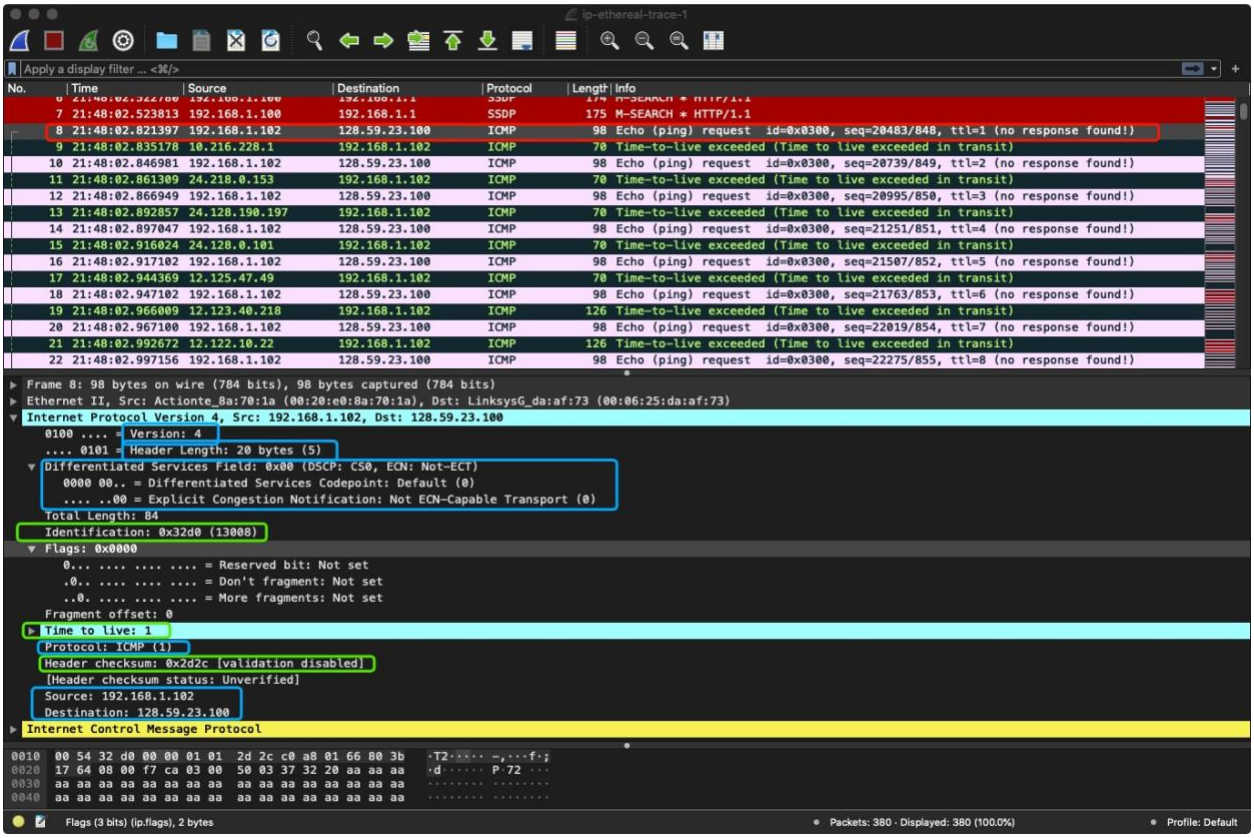
Q5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
Answer: "Identification", "header checksum", and "Time to live" always change. "Time to live" and "Identification" will increase by one, and checksum will be changed.

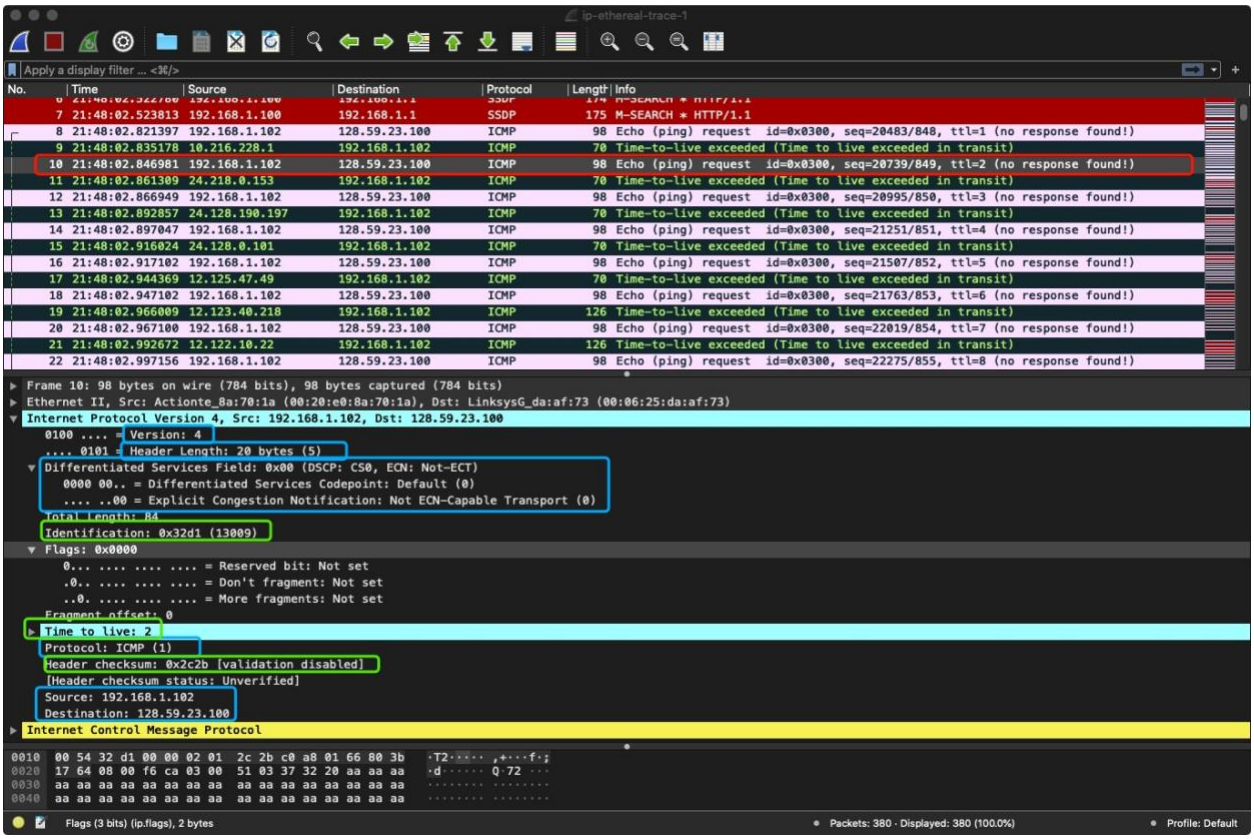
Q6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
Answer: As we can see below, the first screen shot is the first packet sent to destination and the second screenshot is the second packet sent.

These fields stay constant and must stay constant:
"Version" stays "4", as we use IPv4 for all packets.
"Header length" stays 20 bytes, as the header length of ICMP packets should be the same.
"Differentiated Services" stays the same, as ICMP packets use the same type of service.
"Upper Layer Protocl" stays "ICMP", as all of them are ICMP packets.
"Source" stays "192.168.1.102", as all of the them are sent from our PC and the IP of our PC should be the same.
"Destination" stays "128.59.23.100", as all of the them are sent to "gaia.cs.umass.edu" and the IP of it should be the same.

These fields must change:
"Identification" must change, as different packets must have different Identification ids.

“Time to live” must change, as in the traceroute rules, TTL would increase by one for each subsequent packet.
“Header checksum” must change, as the header of the packet changes thus checksum should also change



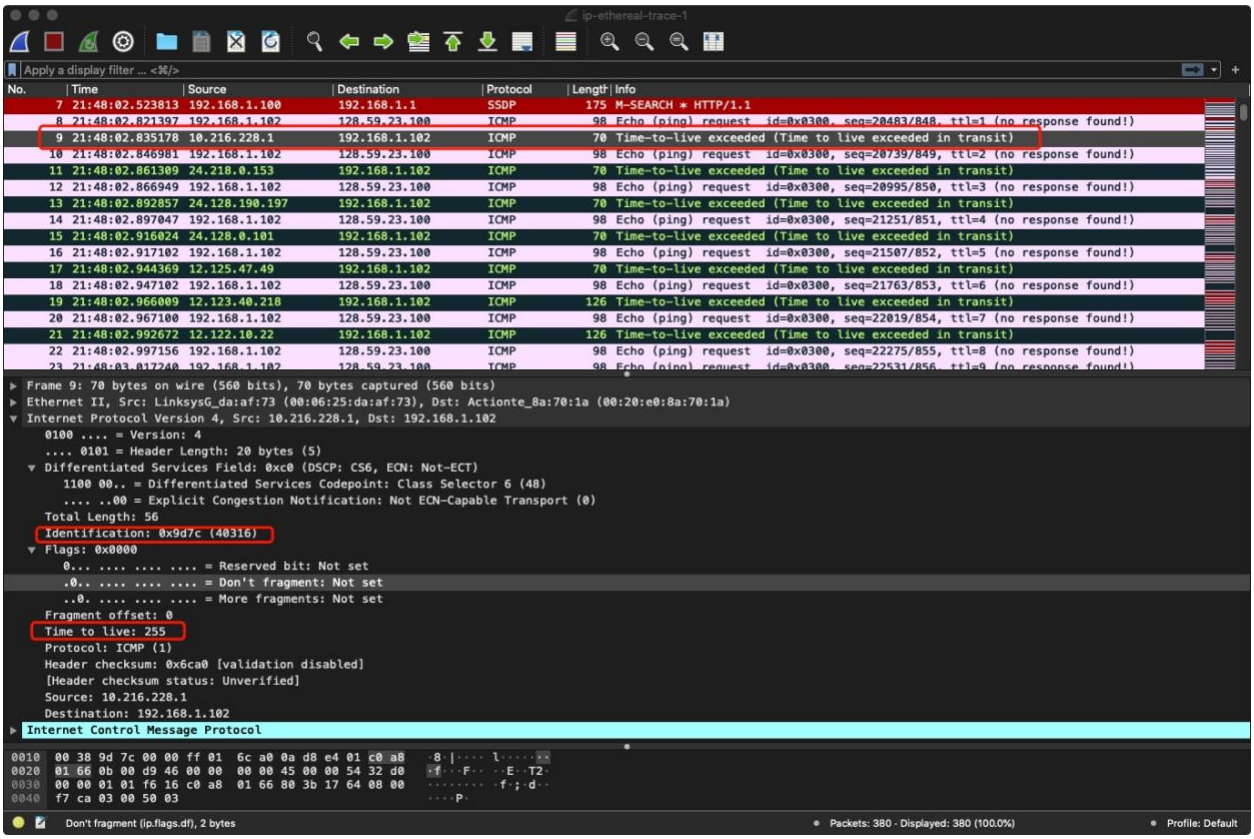


Q7. Describe the pattern you see in the values in the Identification field of the IP Datagram

Answer: "Identification" of each packet increases by one.

Q8. Next (with the packets still sorted by source address) find the series of ICMP TTLexceeded replies sent to your computer by the nearest (first hop) router. What is the value in the Identification field and the TTL field?

Answer: As shown in the screenshot below, the value of Identification is 40316, and the TTL is 255



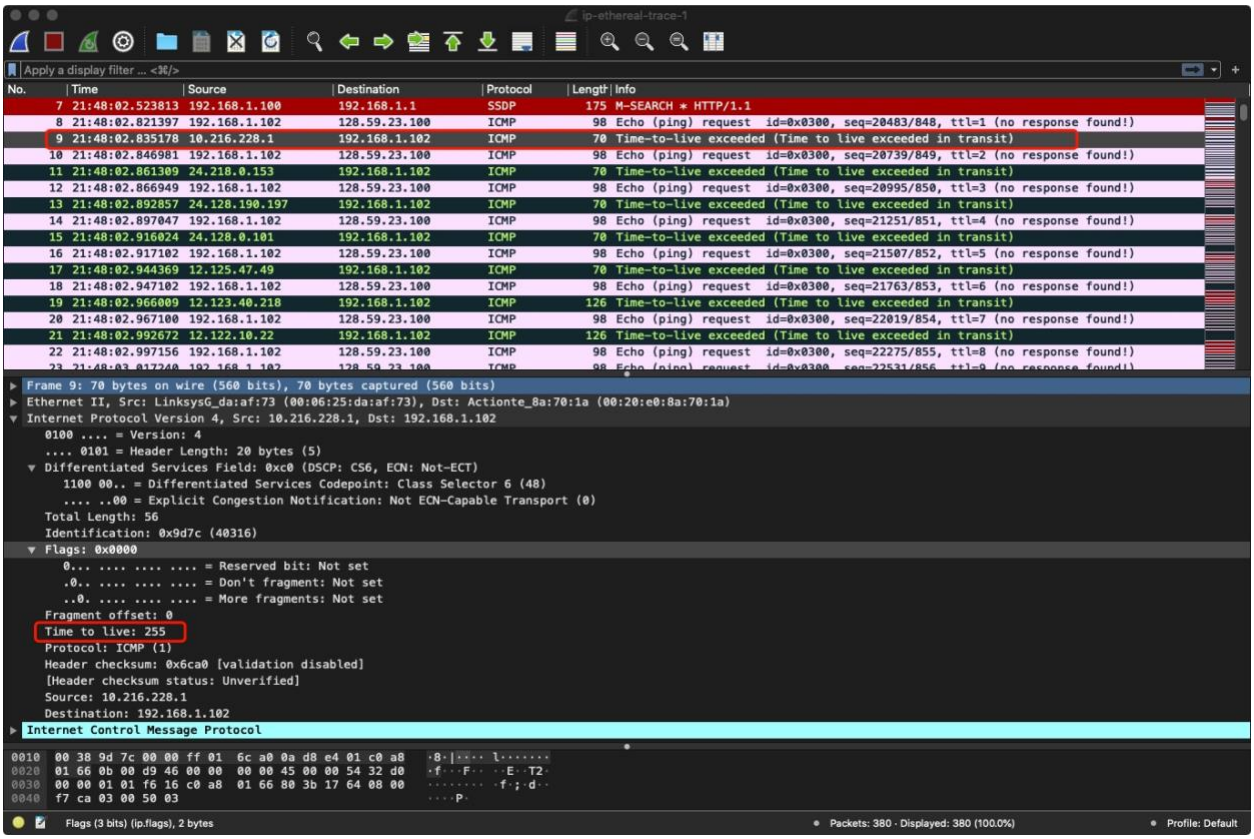
Q9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

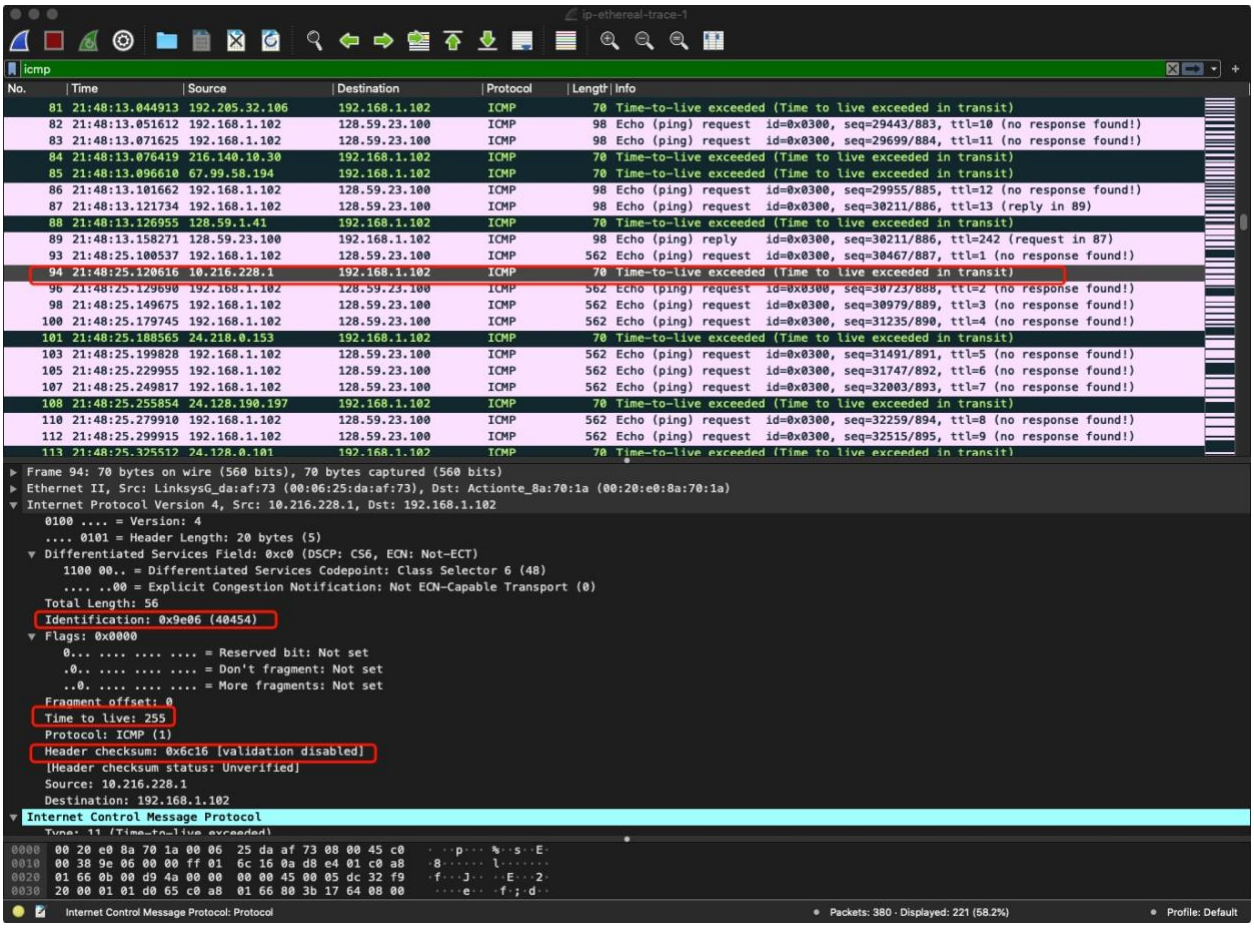
Answer: As shown in the screenshot below, the first screenshot is the first ICMP TTL-exceeded replies when sent datagrams of 56 bytes and the second screenshot is the first ICMP TTL-exceeded replies when sent datagrams of 2000 bytes.

Other values would be the same except “Identification” and “Header checksum”, as Identification should be unique for each datagram, and since the header of the packet changes, checksum would also change.

“Time to live” remains the same (255), since the TTL for the first hop router should be the same.

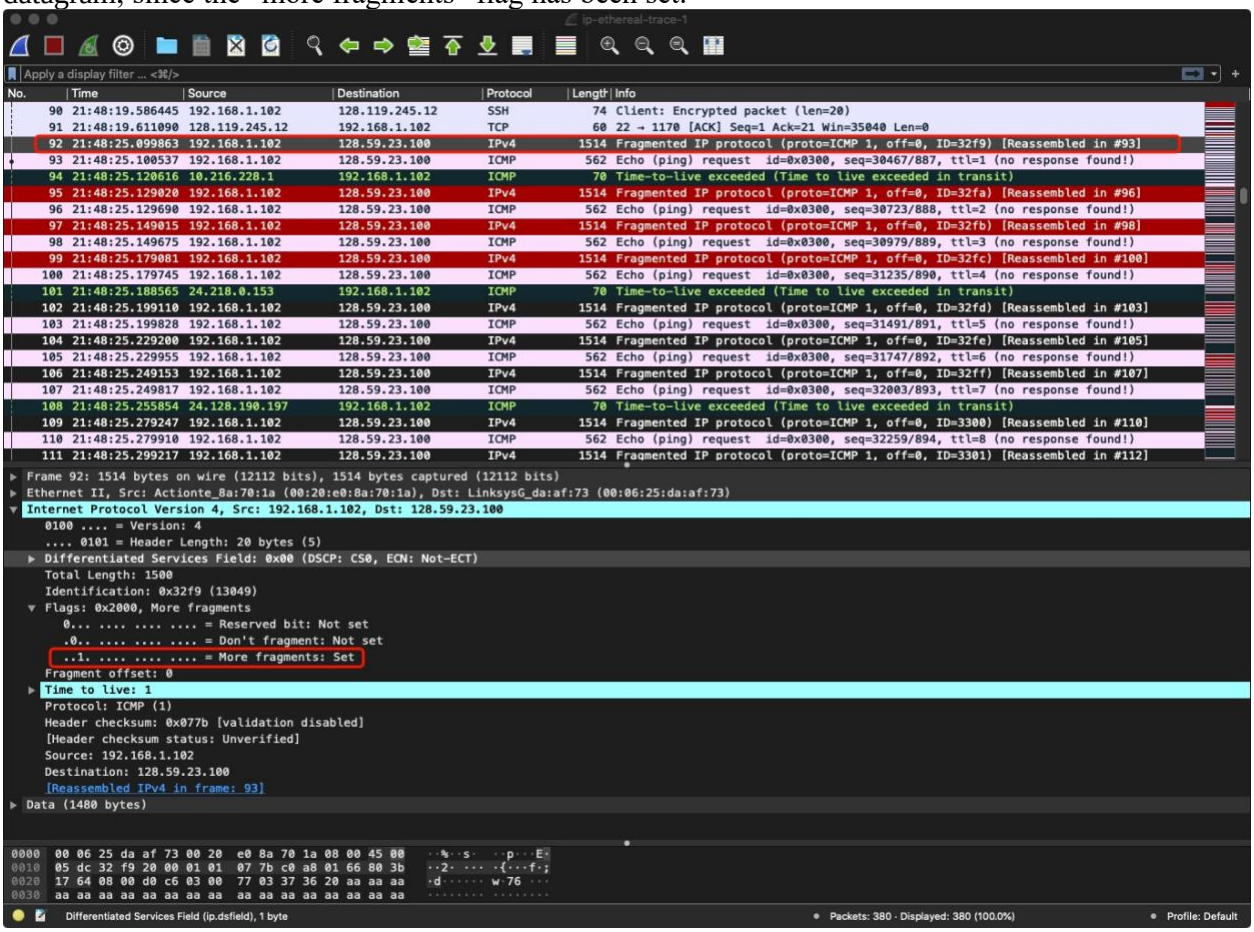
Other values remains the same because we didn’t change these values. They are still ICMP packets, using IPv4, using the same type of service and sent from/to the same IP address.


ip-ethereal-trace-1
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
7 21:48:02.523813 192.168.1.100 192.168.1.1 SSDP 175 M-SEARCH * HTTP/1.1
8 21:48:02.821397 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9 21:48:02.835178 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
10 21:48:02.846981 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11 21:48:02.861309 24.218.0.153 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
12 21:48:02.866949 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13 21:48:02.892857 24.128.190.197 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
14 21:48:02.897047 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15 21:48:02.916024 24.128.0.101 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
16 21:48:02.917102 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17 21:48:02.944369 12.125.47.49 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
18 21:48:02.947102 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19 21:48:02.966009 12.123.40.218 192.168.1.102 ICMP 126 Time-to-live exceeded (Time to live exceeded in transit)
20 21:48:02.967100 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
21 21:48:02.992672 12.122.10.22 192.168.1.102 ICMP 126 Time-to-live exceeded (Time to live exceeded in transit)
22 21:48:02.997156 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)
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)
1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 56
Identification: 0x9d7c (40316)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 0
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
0010 00 38 9d 7c 00 00 ff 01 6c a0 0a d8 e4 01 c0 a8
0020 01 66 0b 00 d9 46 00 00 00 00 45 00 00 54 32 d0
0030 00 00 01 01 f6 16 c0 a8 01 66 80 3b 17 64 08 00
0040 f7 ca 03 00 50 03
Flags (3 bits) (ip.flags), 2 bytes
Packets: 380 · Displayed: 380 (100.0%)
Profile: Default



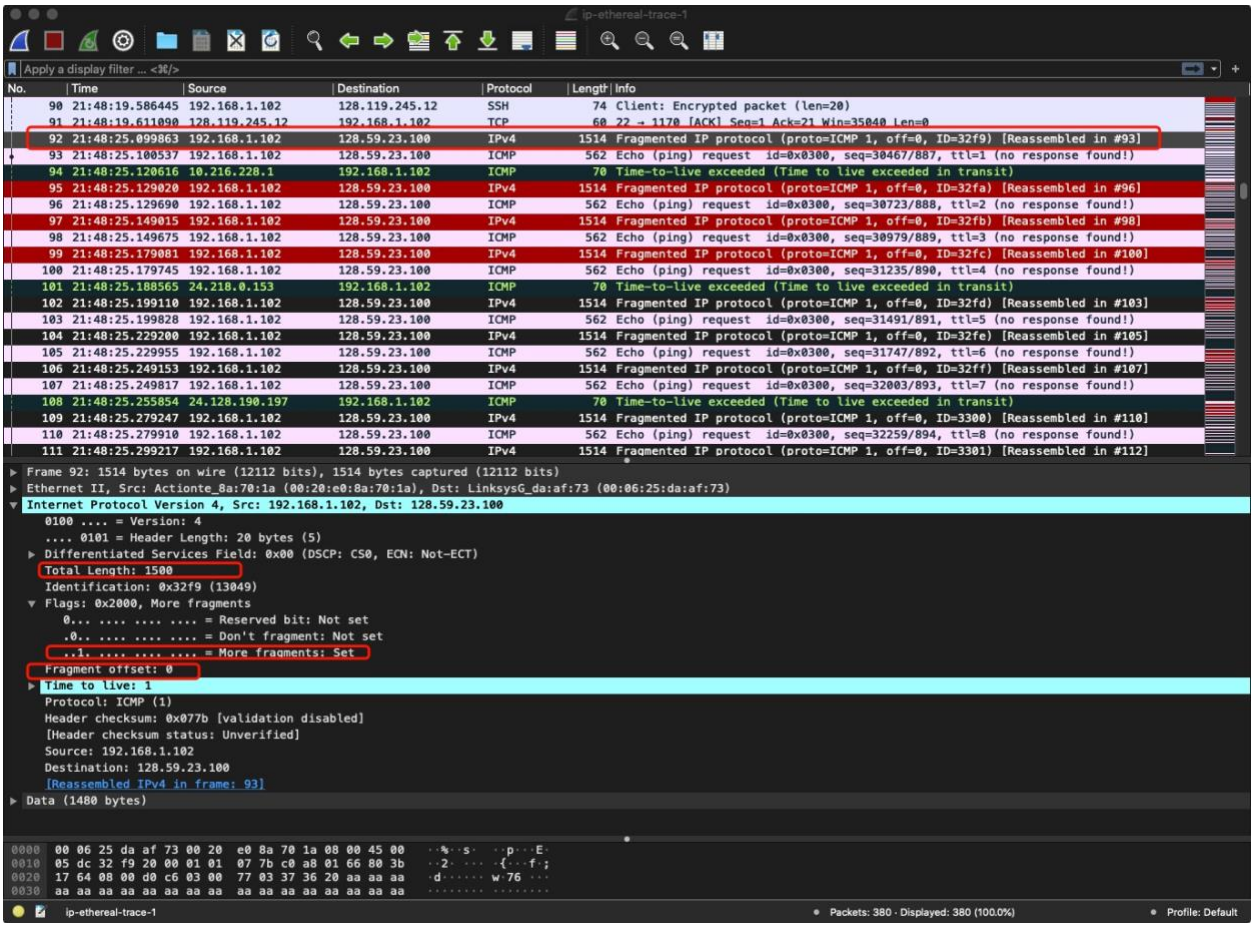
Q10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]

Answer: As shown in the screenshot below, the message been fragmented across more than one IP datagram, since the "more fragments" flag has been set.



Q11. Print out the first fragment of the fragmented IP datagram. 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?

Answer: As shown in the screenshot below, the "more fragments" flag has been set, thus the datagram has been fragmented. And as we can see, the offset of this fragment is 0, which means that this fragment is the first fragment. And the total length is 1500.

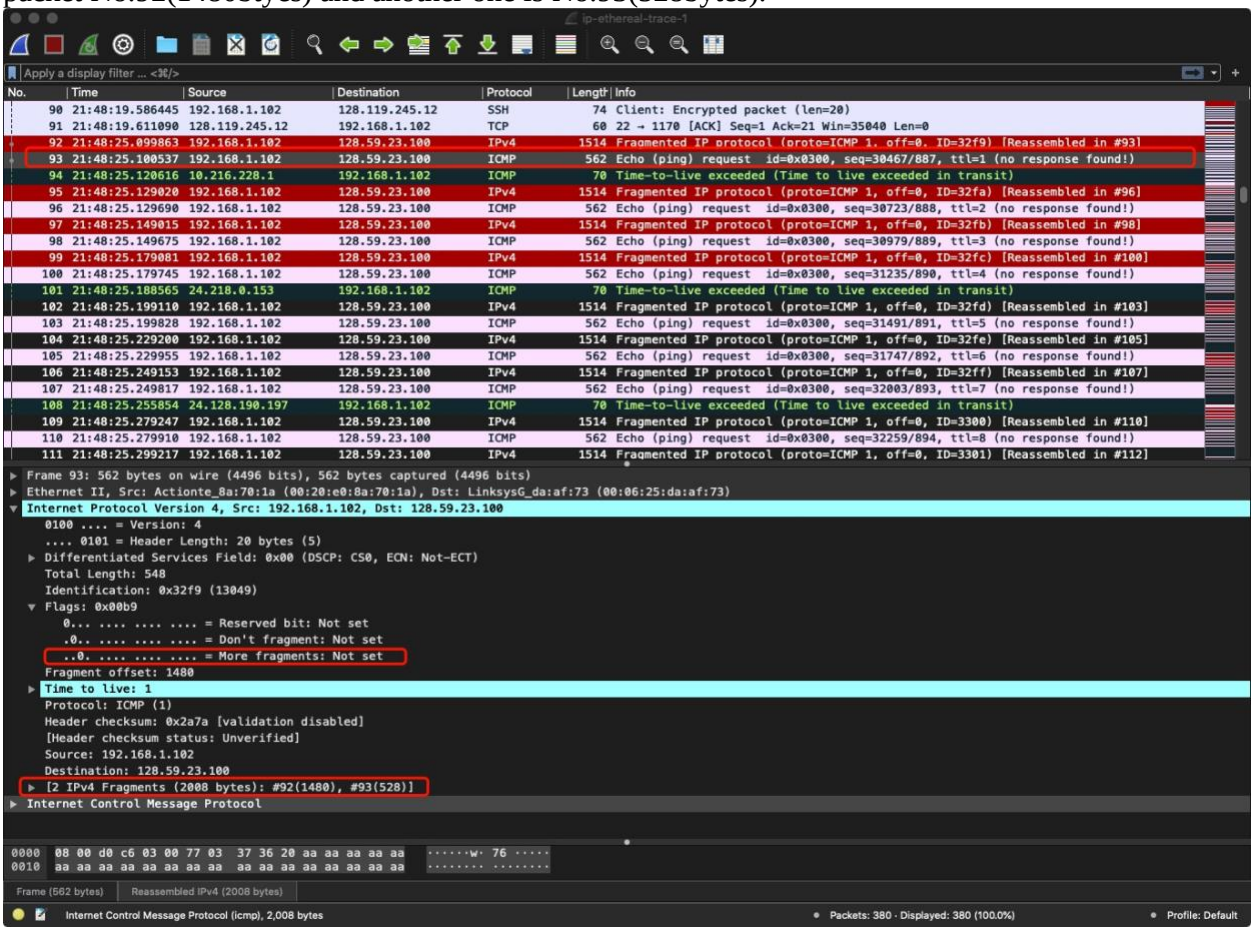


First fragment of 2000 datagram:
No. Time Source Destination Protocol Length Info
92 21:48:25.099863 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented
IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, 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
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)

Q12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

Answer: As shown in the screenshot below, the “Fragment offset” is 1480, which means that this fragment is not the first one. And the “More fragments” flag is not set, which means that there is no more fragments after it. Also, we can know that there is two fragments of this datagram, one is packet No.92(1480btyes) and another one is No.93(528bytes).



Second Fragment of 2000 datagram:

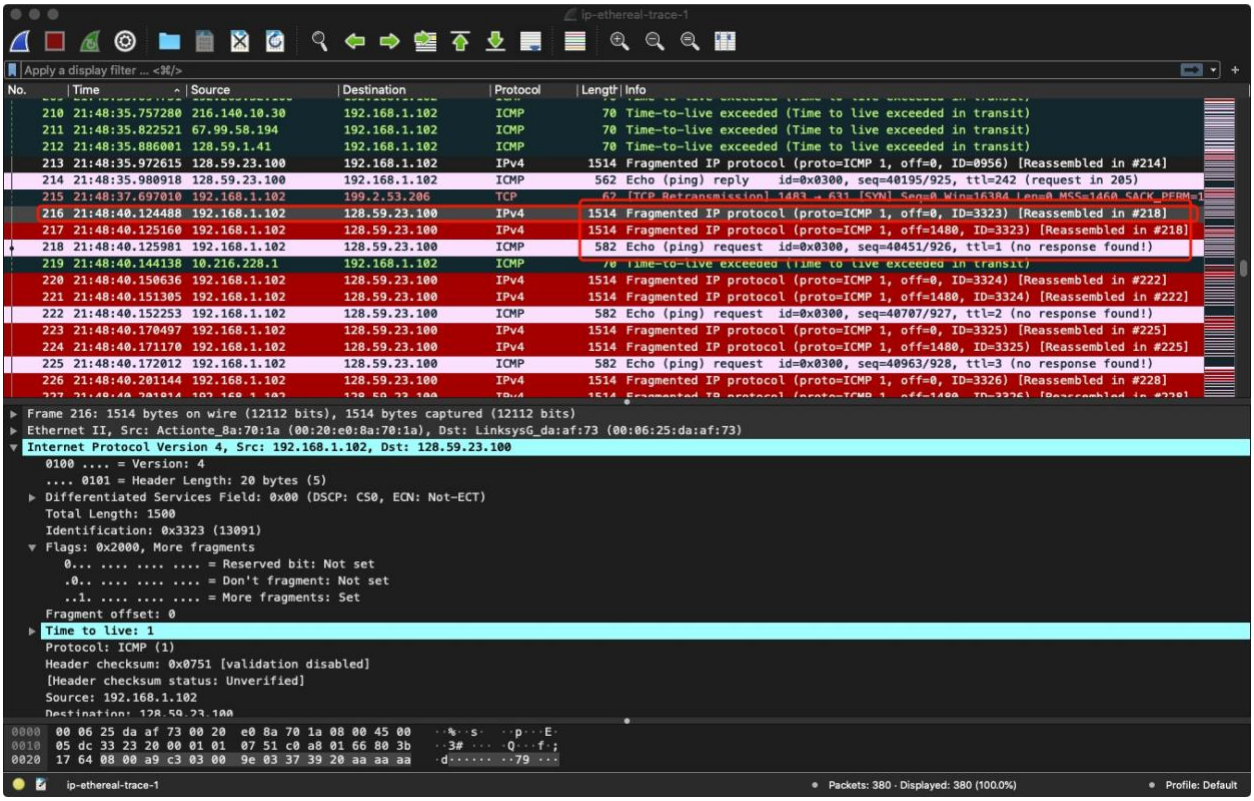
No. Time Source Destination Protocol Length Info
93 21:48:25.100537 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping)
request id=0x0300, seq=30467/887, ttl=1 (no response found!)
Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:
73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 548
Identification: 0x32f9 (13049)
Flags: 0x00b9
0... .... = Reserved bit: Not set

.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 1480
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)]

Q13. What fields change in the IP header between the first and second fragment?
Answer: As shown in the screenshot above, the "Fragment offset", "Total length", "Header checksum" ,"Flag" and "More fragments" flag are changed.

Field	Fragment 1	Fragment 2
Fragment offset	0	1480
Header checksum	0x077b	0x2a7a
Total length	1500	548
More fragment Flags	Set	Not set
Flag	0x077b	0x00b9

Q14. 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. How many fragments were created from the original datagram?
Answer: As shown in the screenshot below, the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500 is No.216 packet. And as we can see, it said that it will be reassembled in No.218, which means that there are 3 fragments were created from the original datagram, they are No.216,No.217,No.218 packets.

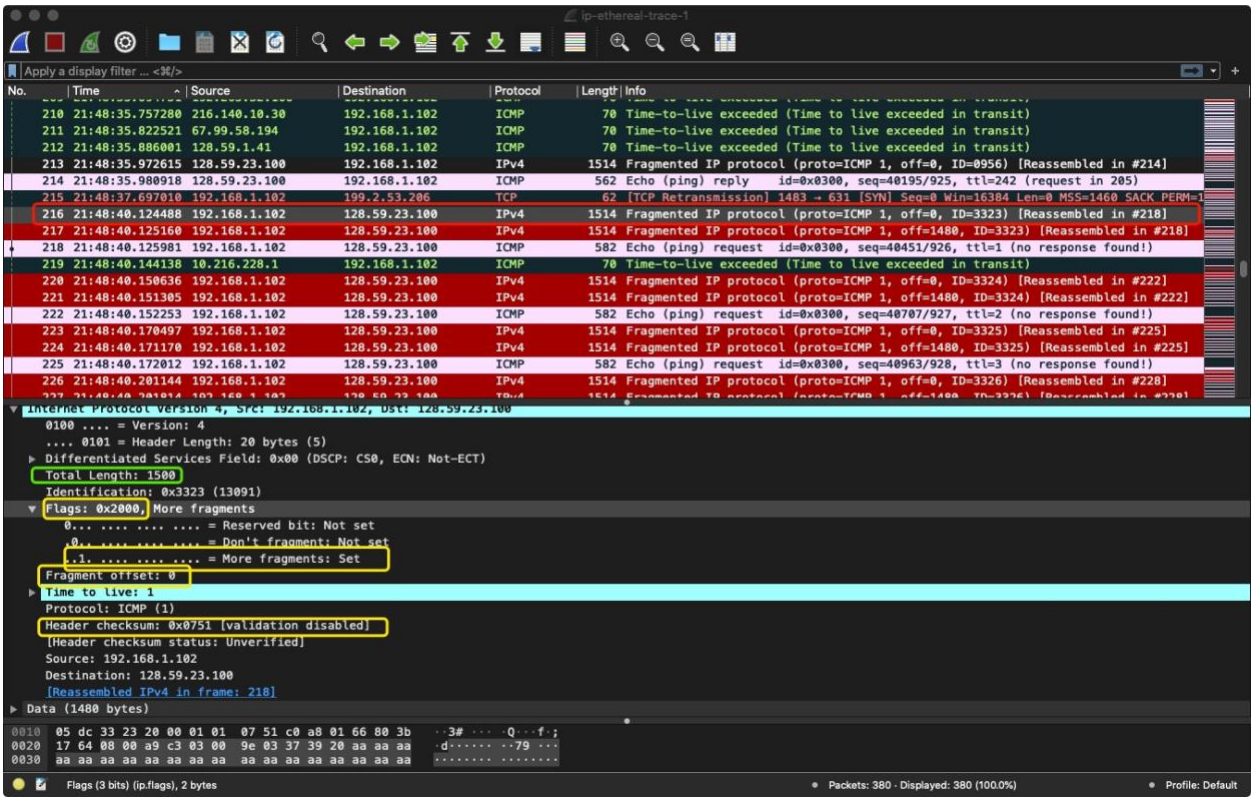


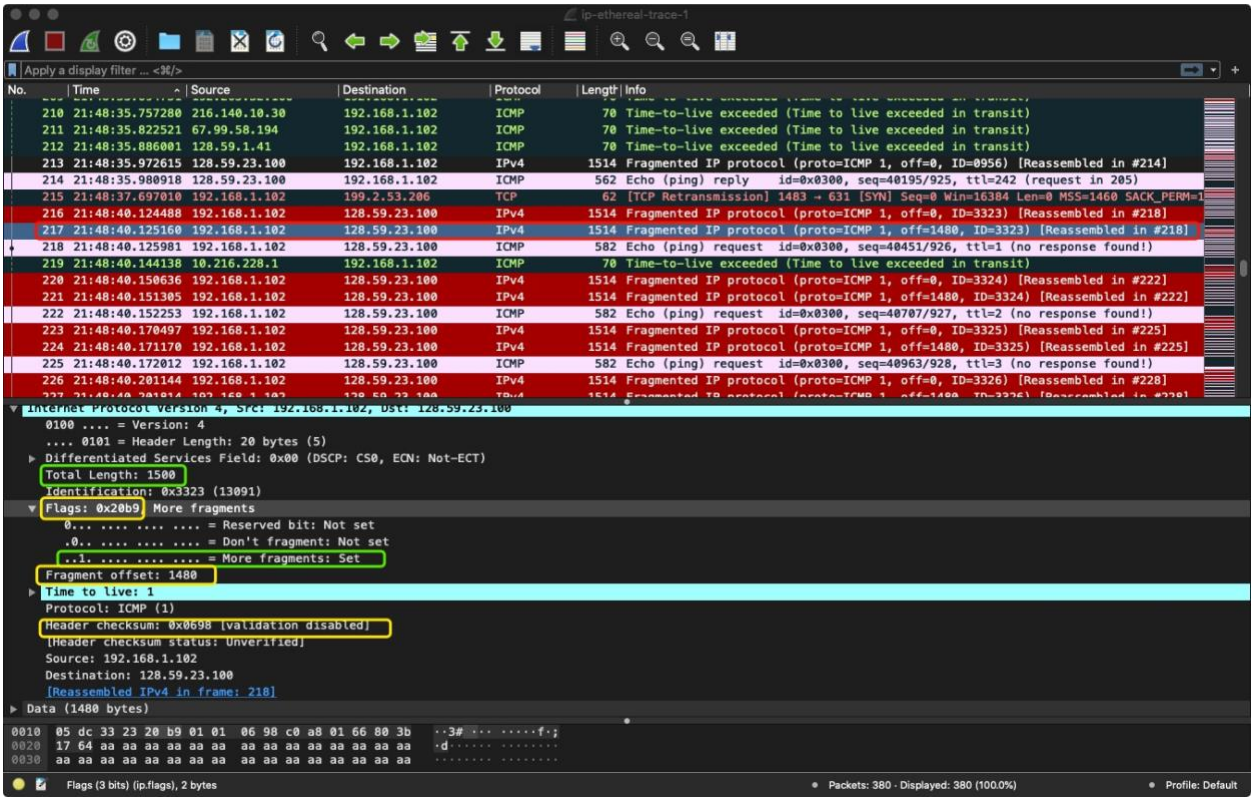
The first fragment of 3500 datagram:

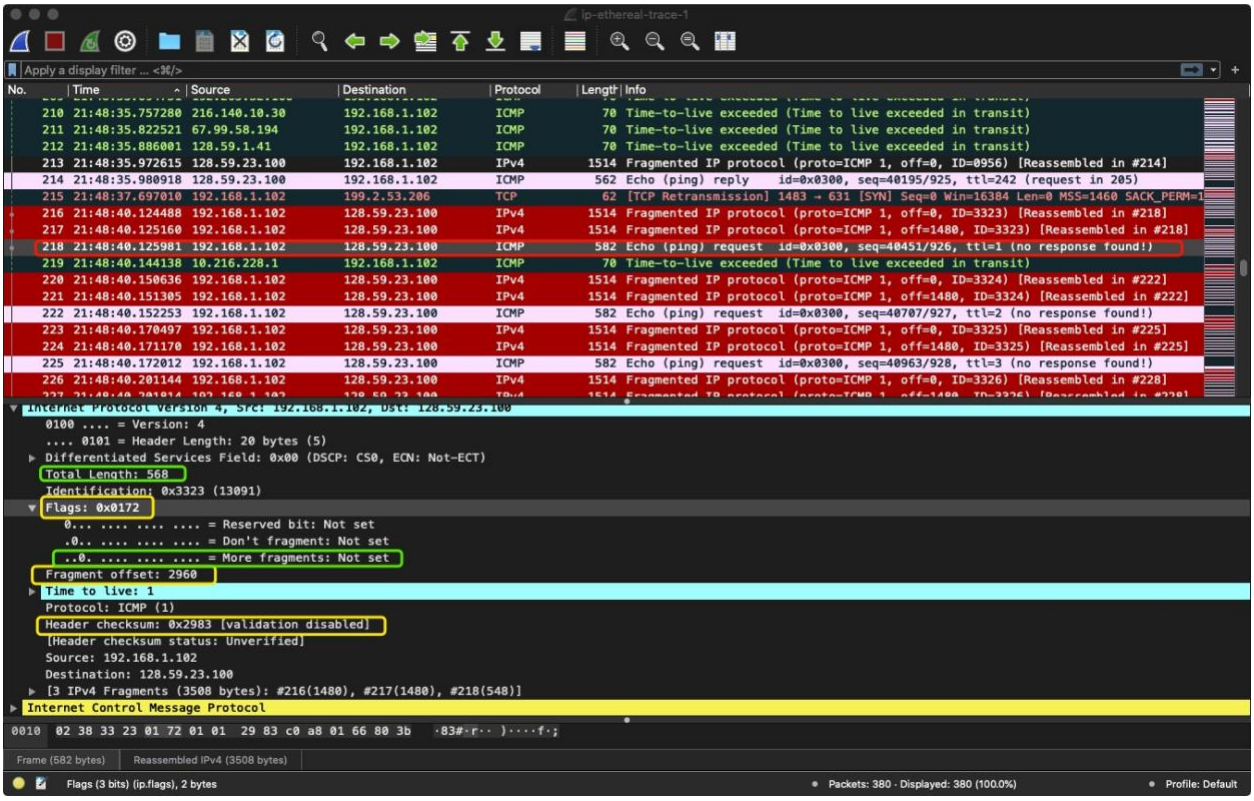
No. Time Source Destination Protocol Length Info
216 21:48:40.124488 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented
IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:
73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x2000, More fragments
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0751 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[Reassembled IPv4 in frame: 218]
Data (1480 bytes)

Q15. What fields change in the IP header among the fragments?
Answer: As shown in the screenshots above, the first screenshot is the first fragment, and the second screenshot is the second fragment, and the third screenshots is the last fragment. The “fragment offset” ,“checksum” and “Flag” change.
And the value of “Total length” and “More fragment” of fragment 3 are different from Fragment1 and Fragment2.

Field	Fragment 1	Fragment 2	Fragment 3
Fragment offset	0	1480	2960
Header checksum	0x0751	0x0698	0x2983
Total length	1500	1500	568
More fragment Flags	Set	Set	Not set
Flag	0x2000	0x20b9	0x0172




ip-ethereal-trace-1
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
210 21:48:35.757280 216.140.10.30 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
211 21:48:35.822521 67.99.58.194 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
212 21:48:35.886001 128.59.1.41 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
213 21:48:35.972615 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214 21:48:35.980918 128.59.23.100 192.168.1.102 ICMP 562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215 21:48:37.697010 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 21:48:40.124488 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 21:48:40.125160 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 21:48:40.125981 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219 21:48:40.144138 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
220 21:48:40.150636 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221 21:48:40.151305 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222 21:48:40.152253 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223 21:48:40.170497 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224 21:48:40.171170 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225 21:48:40.172012 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)
226 21:48:40.201144 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled in #228]
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x20b9 More fragments
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
Fragment offset: 1480
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0698 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[Reassembled IPv4 in frame: 218]
Data (1480 bytes)
0010 05 dc 33 23 20 b9 01 01 06 98 c0 a8 01 66 80 3b
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
Flags (3 bits) (ip.flags), 2 bytes
Packets: 380 · Displayed: 380 (100.0%)
Profile: Default


ip-ethereal-trace-1
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
210 21:48:35.757280 216.140.10.30 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
211 21:48:35.822521 67.99.58.194 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
212 21:48:35.886001 128.59.1.41 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
213 21:48:35.972615 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214 21:48:35.980918 128.59.23.100 192.168.1.102 ICMP 562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215 21:48:37.697010 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 21:48:40.124488 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 21:48:40.125160 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 21:48:40.125981 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219 21:48:40.144138 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
220 21:48:40.150636 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221 21:48:40.151305 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222 21:48:40.152253 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223 21:48:40.170497 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224 21:48:40.171170 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225 21:48:40.172012 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)
226 21:48:40.201144 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled in #228]
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 (13091)
Flags: 0x0172
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 2960
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
0010 02 38 33 23 01 72 01 01 29 83 c0 a8 01 66 80 3b
Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Flags (3 bits) (ip.flags), 2 bytes
Packets: 380 · Displayed: 380 (100.0%)
Profile: Default