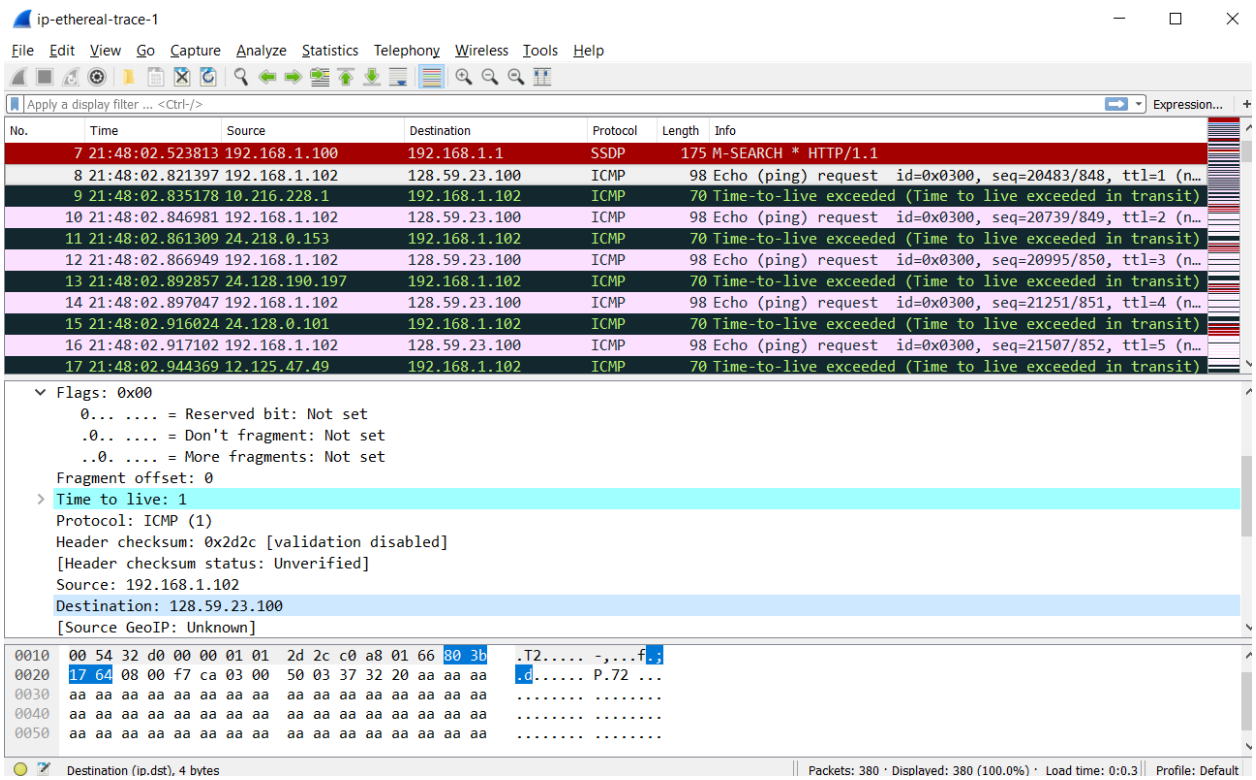
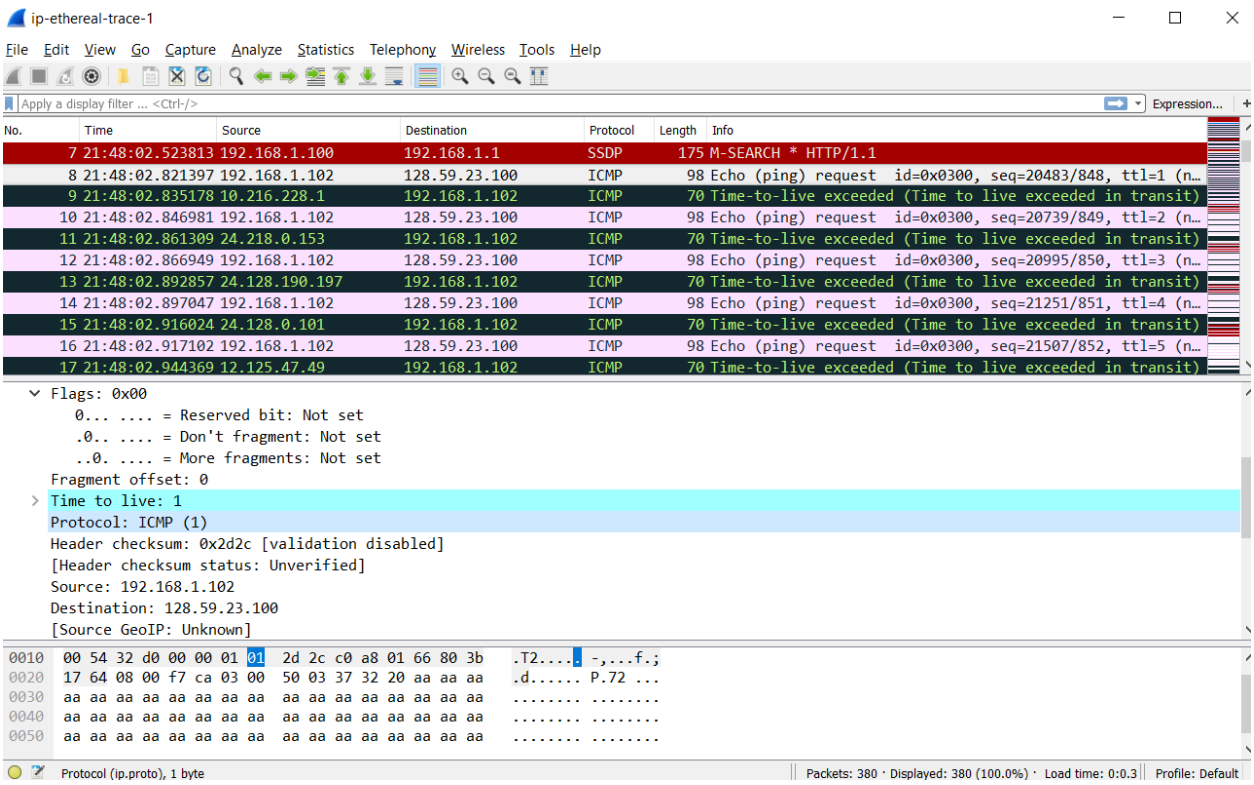
Tyler Cope

CS372 Lab 3

1. IP address of my computer: 192.168.1.102

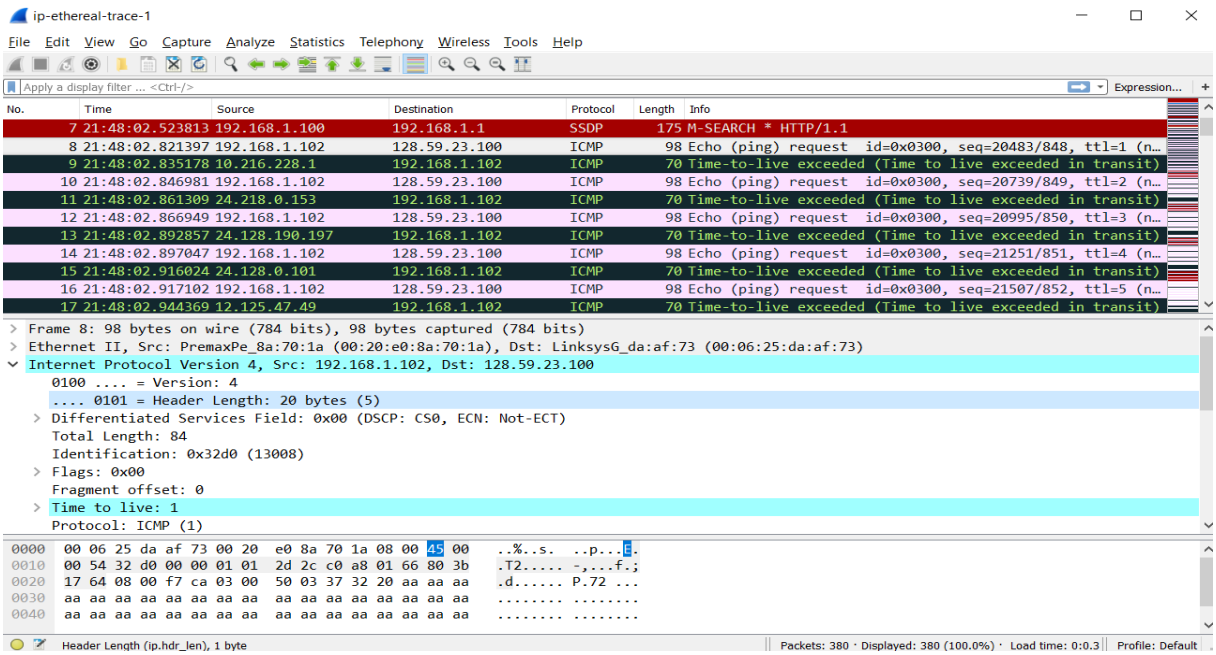


2. The value is 1.

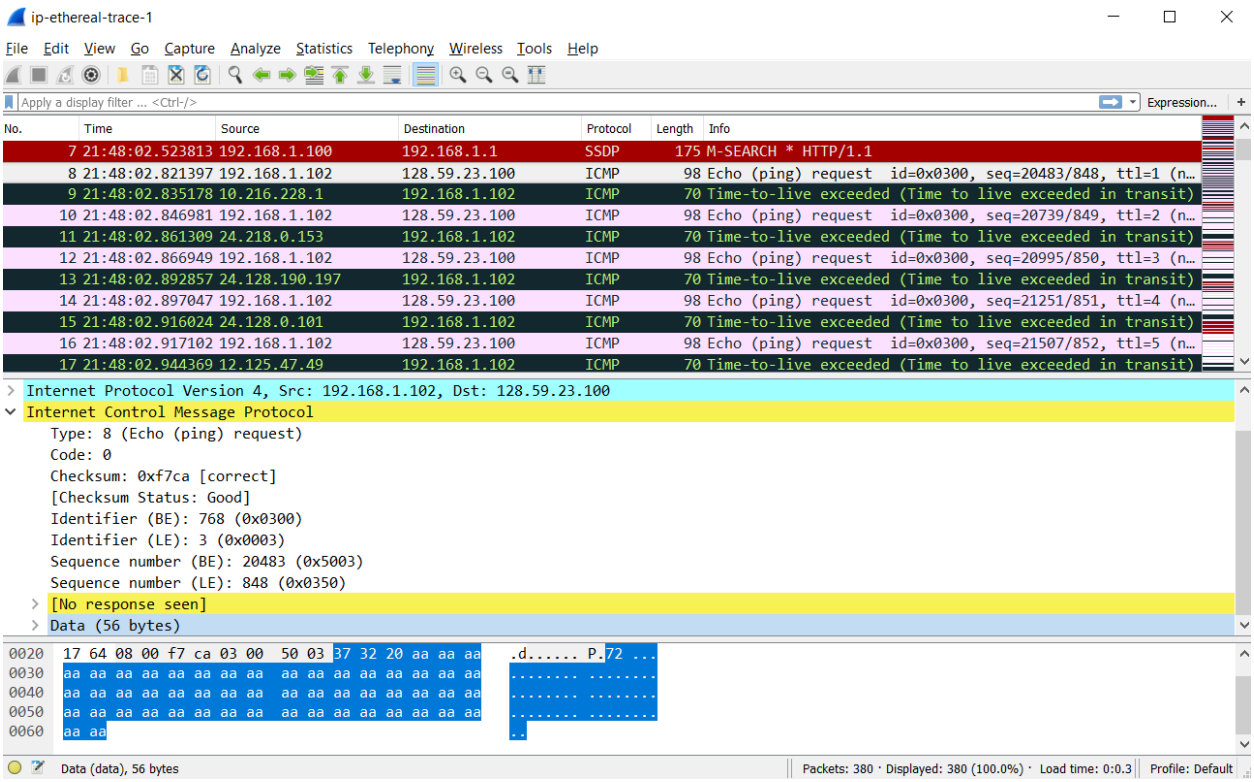


3.

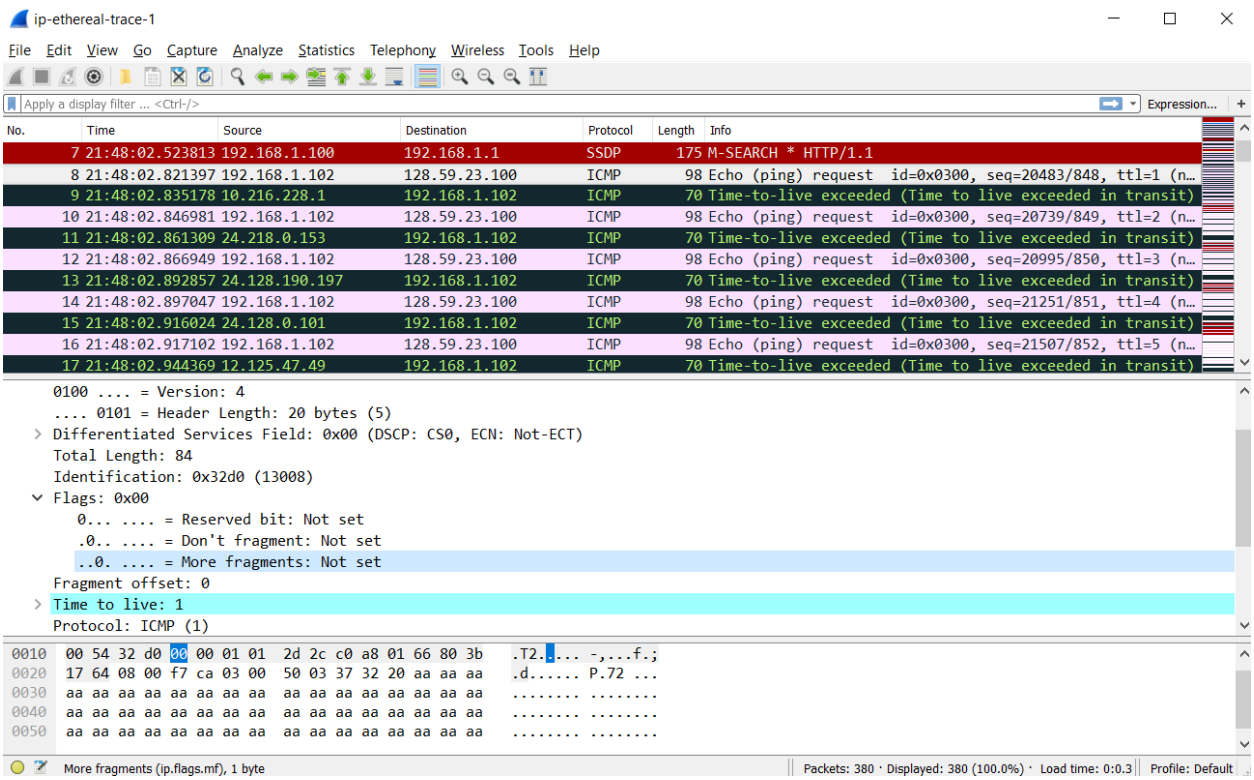
a. There are 20 bytes in the header.



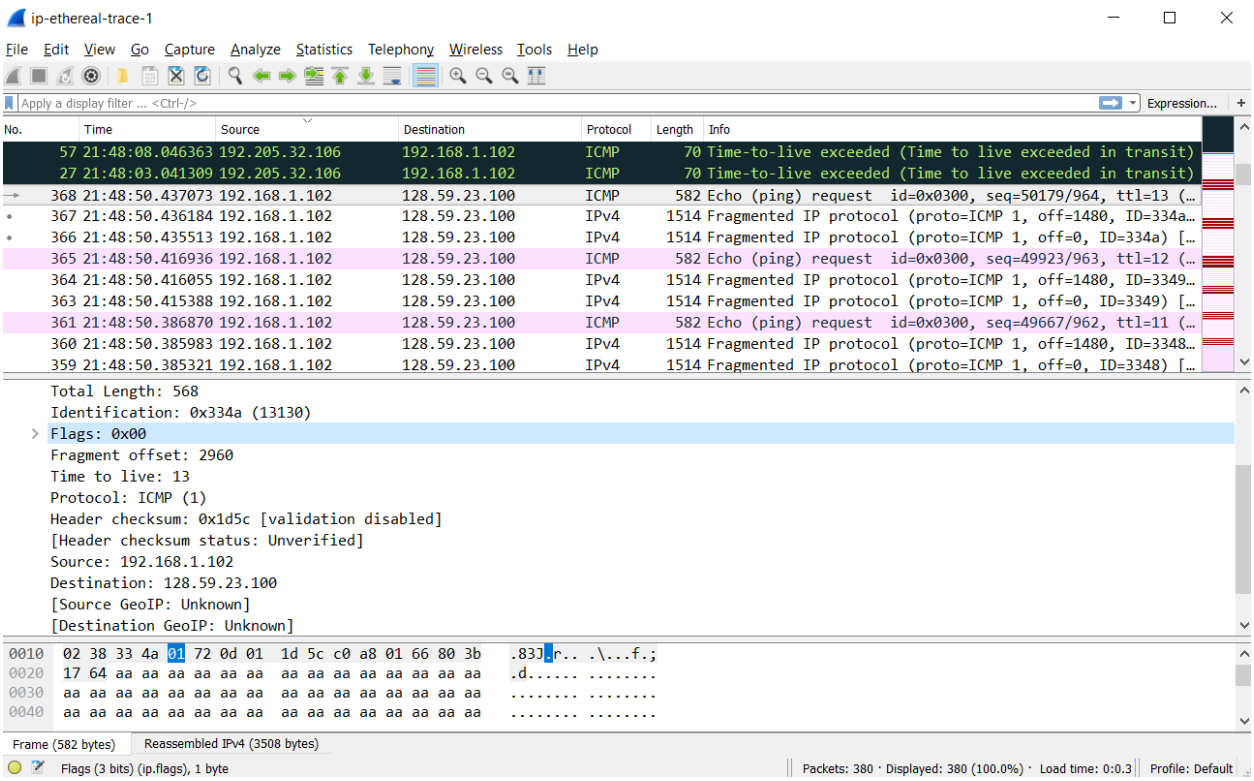
b. There are 36 bytes in the payload. This was determined because the next screenshot shows there were 56 bytes sent and 20 were for the header.



4. This IP datagram has not been fragmented. We can tell because the “More fragments” flag is not set.



5. Time to live, Header checksum, and Identification always change from one datagram to the next.



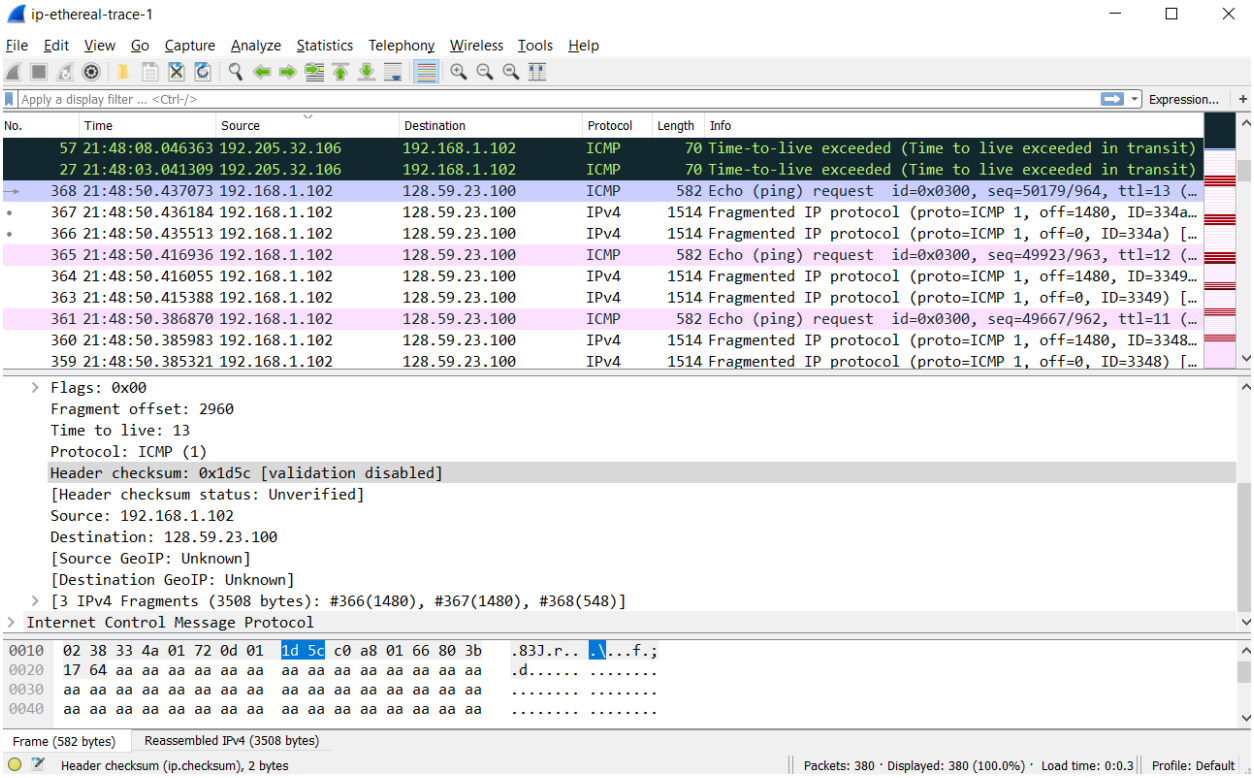
6.

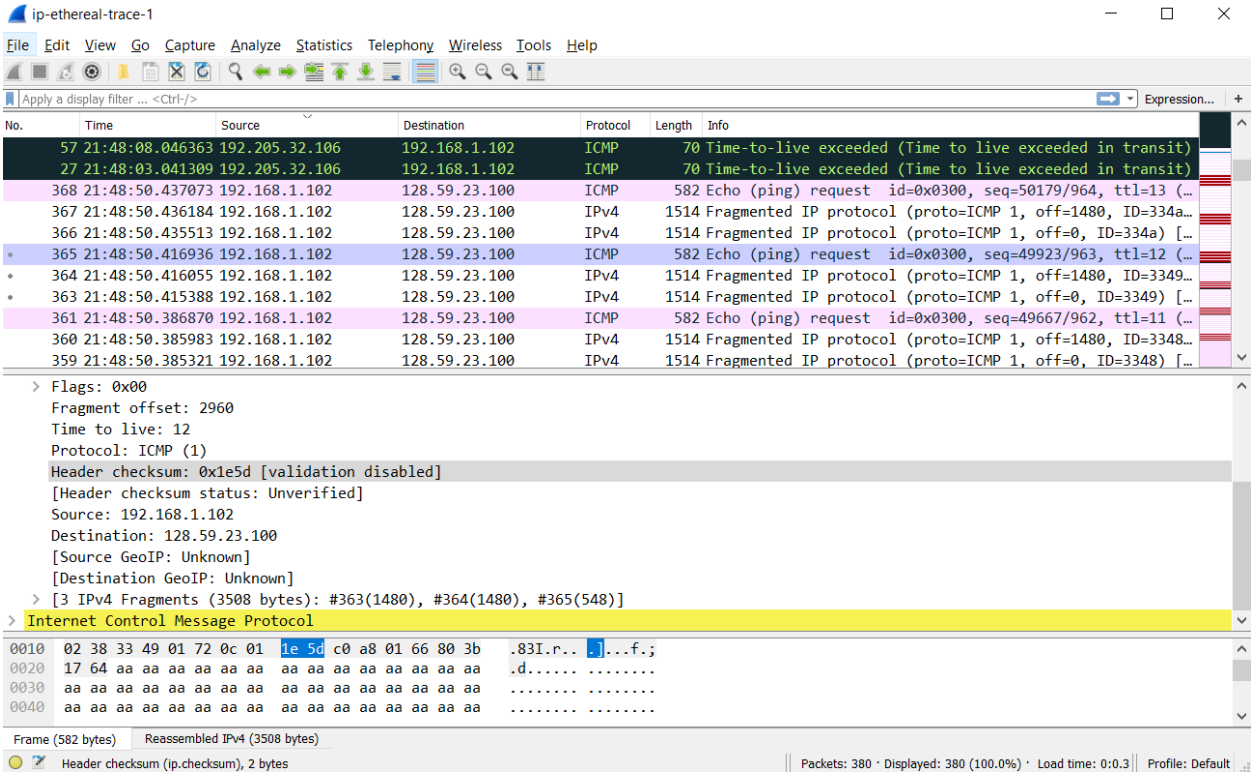
a. The fields that stay constant: Version, Header Length, Differentiated Services Field, Source, Destination, Protocol

b. The fields that must stay constant are the same as the fields that do stay constant.

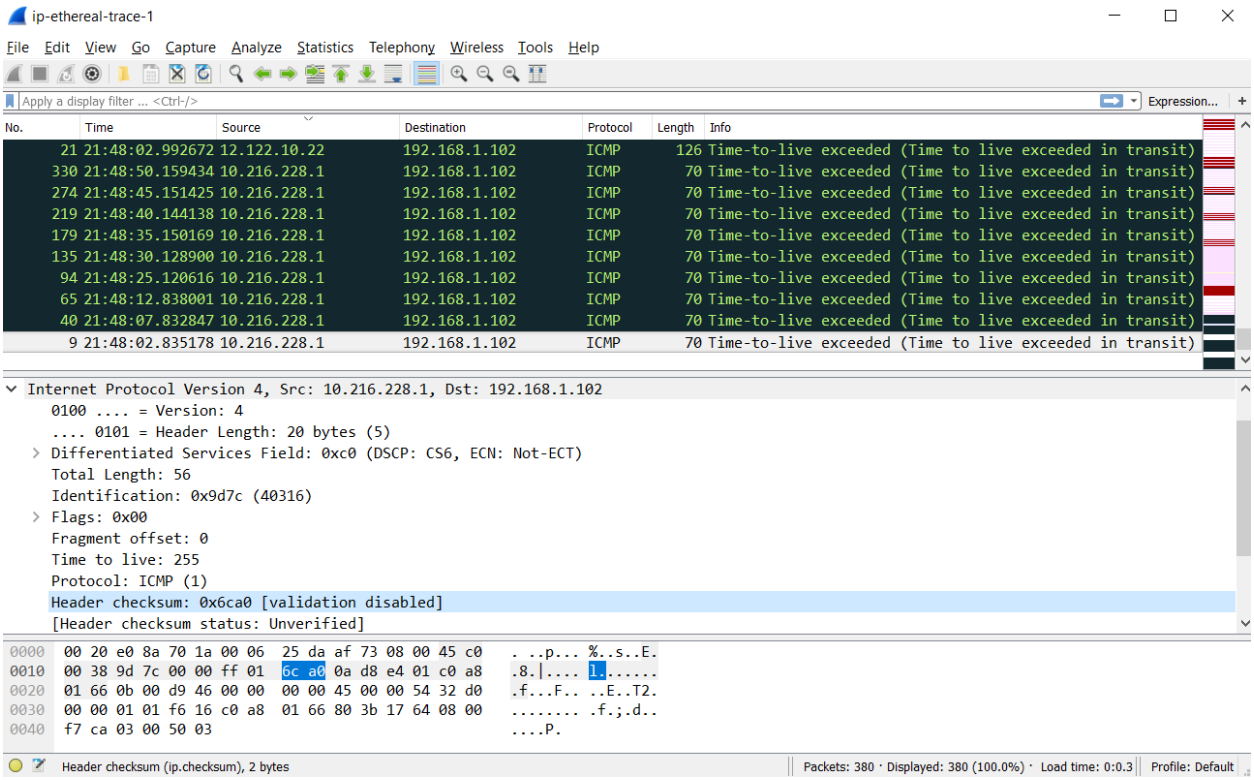
c. Same answer as #5. Time to live, header checksum, and indemnification must change.

7. I notice that the header is incrementing from each request as well as the Time to live.


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
57 21:48:08.046363 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
27 21:48:03.041309 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
368 21:48:50.437073 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (...
367 21:48:50.436184 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a...
366 21:48:50.435513 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [...
365 21:48:50.416936 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (...
364 21:48:50.416055 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349...
363 21:48:50.415388 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [...
361 21:48:50.386870 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (...
360 21:48:50.385983 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348...
359 21:48:50.385321 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3348) [...
Flags: 0x00
Fragment offset: 2960
Time to live: 13
Protocol: ICMP (1)
Header checksum: 0x1d5c [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
[3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]
Internet Control Message Protocol
0010 02 38 33 4a 01 72 0d 01 1d 5c c0 a8 01 66 80 3b .83J.r.. .\...f.;
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa .d...... ....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Header checksum (ip.checksum), 2 bytes
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3
Profile: Default


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
57 21:48:08.046363 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
27 21:48:03.041309 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
368 21:48:50.437073 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (...
367 21:48:50.436184 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a...
366 21:48:50.435513 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [...
365 21:48:50.416936 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (...
364 21:48:50.416055 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349...
363 21:48:50.415388 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [...
361 21:48:50.386870 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (...
360 21:48:50.385983 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348...
359 21:48:50.385321 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3348) [...
Flags: 0x00
Fragment offset: 2960
Time to live: 12
Protocol: ICMP (1)
Header checksum: 0x1e5d [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
[3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
Internet Control Message Protocol
0010 02 38 33 49 01 72 0c 01 1e 5d c0 a8 01 66 80 3b .83I.r.. .]...f.;
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa .d...... ....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
Frame (582 bytes)
Reassembled IPv4 (3508 bytes)
Header checksum (ip.checksum), 2 bytes
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3
Profile: Default

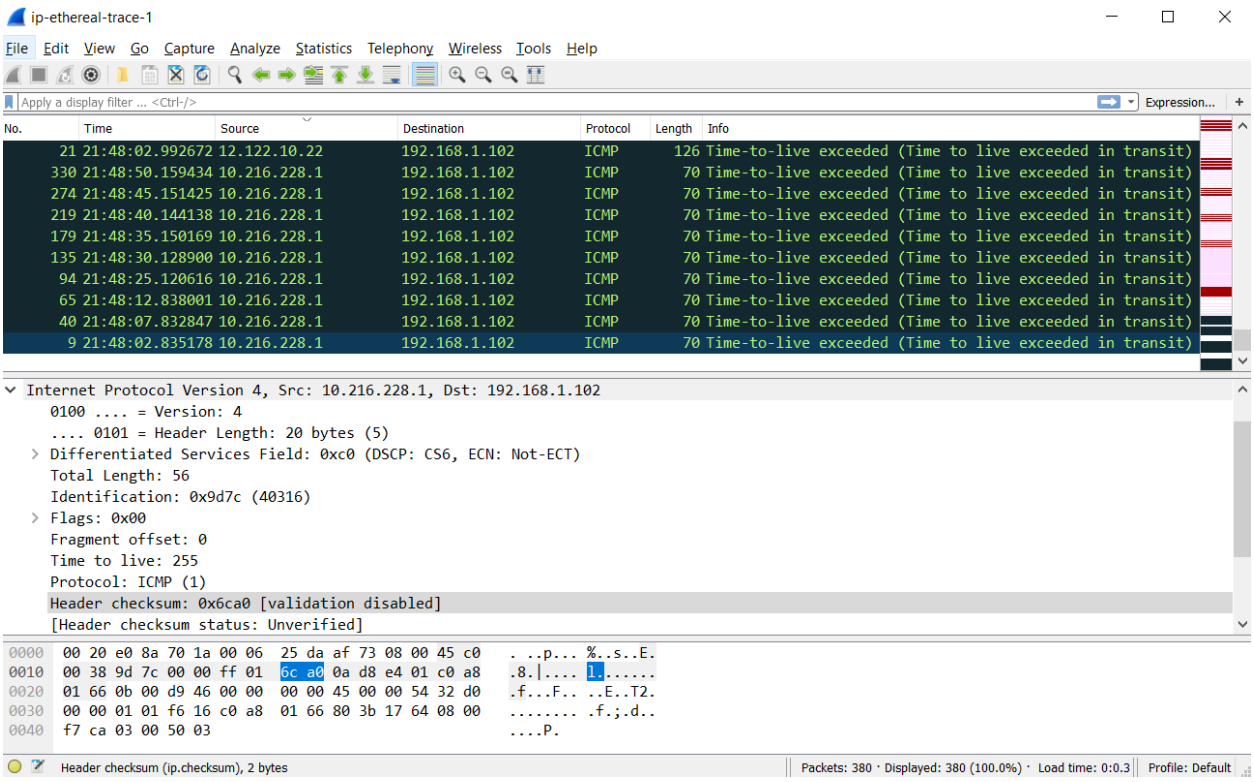
8. The identification is 0x927C (40316) and the TTL is 255.

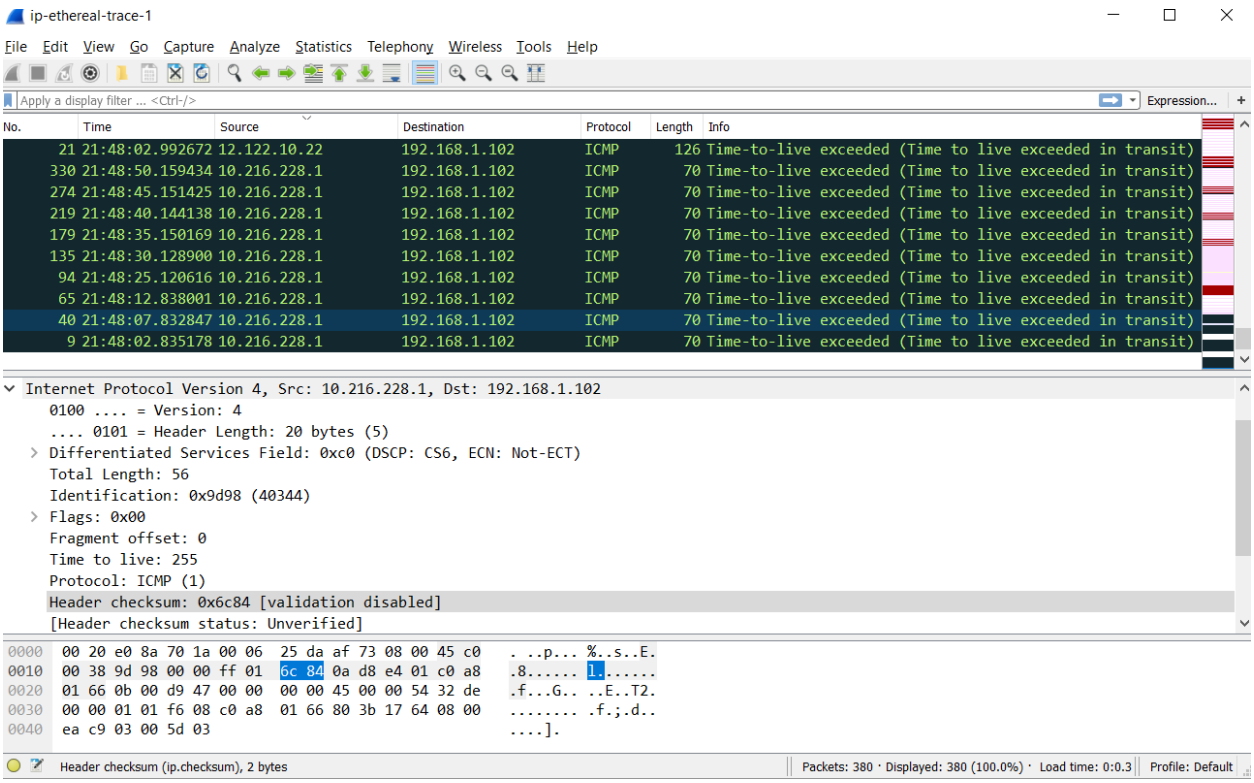


9.

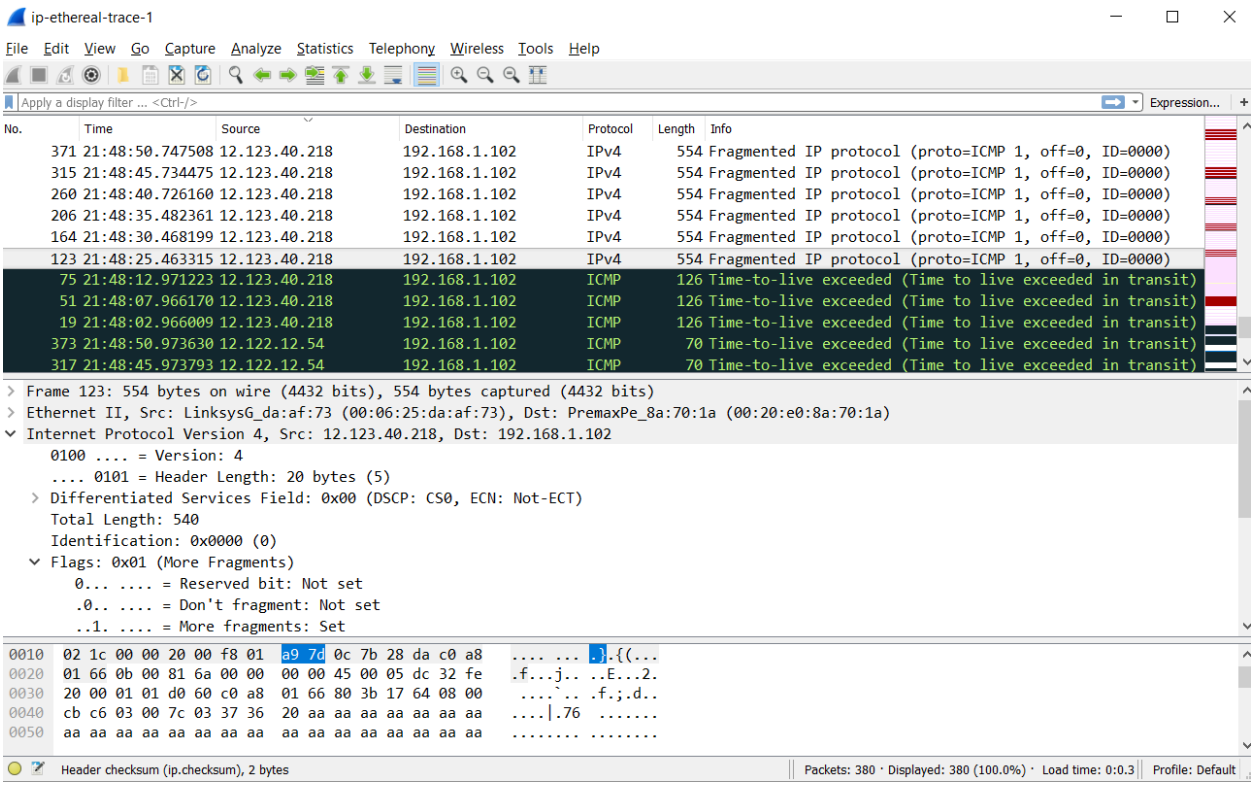
a. The identification field will change for all of the ICMP TTL-exceeded replies sent to my computer by the nearest (first hop) router. This is because the identification for each request must be unique. If datagrams had the same identification, it just means they're fragmented parts of the same datagram.

b. The TTL will not change because the TTL for the nearest router is always the same.


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
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)
330 21:48:50.159434 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
274 21:48:45.151425 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
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)
179 21:48:35.150169 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
135 21:48:30.128900 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
94 21:48:25.120616 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
65 21:48:12.838001 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
40 21:48:07.832847 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
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)
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: 0x00
Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x6ca0 [validation disabled]
[Header checksum status: Unverified]
0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 c0 . ..p... %..s..E.
0010 00 38 9d 7c 00 00 ff 01 6c a0 0a d8 e4 01 c0 a8 .8.|.... l.......
0020 01 66 0b 00 d9 46 00 00 00 00 45 00 00 54 32 d0 .f...F.. ..E..T2.
0030 00 00 01 01 f6 16 c0 a8 01 66 80 3b 17 64 08 00 .... .f.;.d..
0040 f7 ca 03 00 50 03 ....P.
Header checksum (ip.checksum), 2 bytes
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3
Profile: Default


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
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)
330 21:48:50.159434 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
274 21:48:45.151425 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
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)
179 21:48:35.150169 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
135 21:48:30.128900 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
94 21:48:25.120616 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
65 21:48:12.838001 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
40 21:48:07.832847 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
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)
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: 0x9d98 (40344)
Flags: 0x00
Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x6c84 [validation disabled]
[Header checksum status: Unverified]
0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 c0 . ..p... %..s..E.
0010 00 38 9d 98 00 00 ff 01 6c 84 0a d8 e4 01 c0 a8 .8...... l.......
0020 01 66 0b 00 d9 47 00 00 00 00 45 00 00 54 32 de .f...G.. ..E..T2.
0030 00 00 01 01 f6 08 c0 a8 01 66 80 3b 17 64 08 00 .... .f.;.d..
0040 ea c9 03 00 5d 03 ....].
Header checksum (ip.checksum), 2 bytes
Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.3
Profile: Default

10. The message has been fragmented across more than one IP datagram.

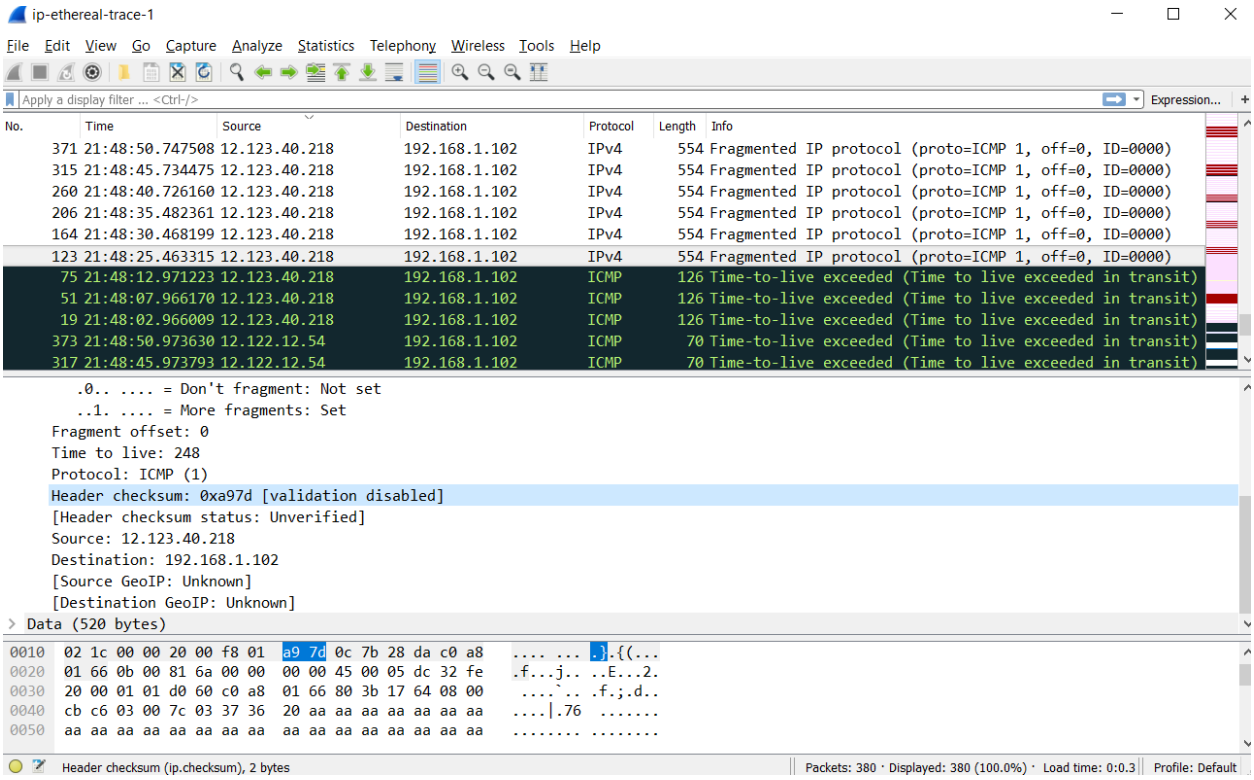


11.

a. You can see in the header that More fragments is set so that tells us that it is fragmented.

b. We know it's the first fragment because the offset is 0.

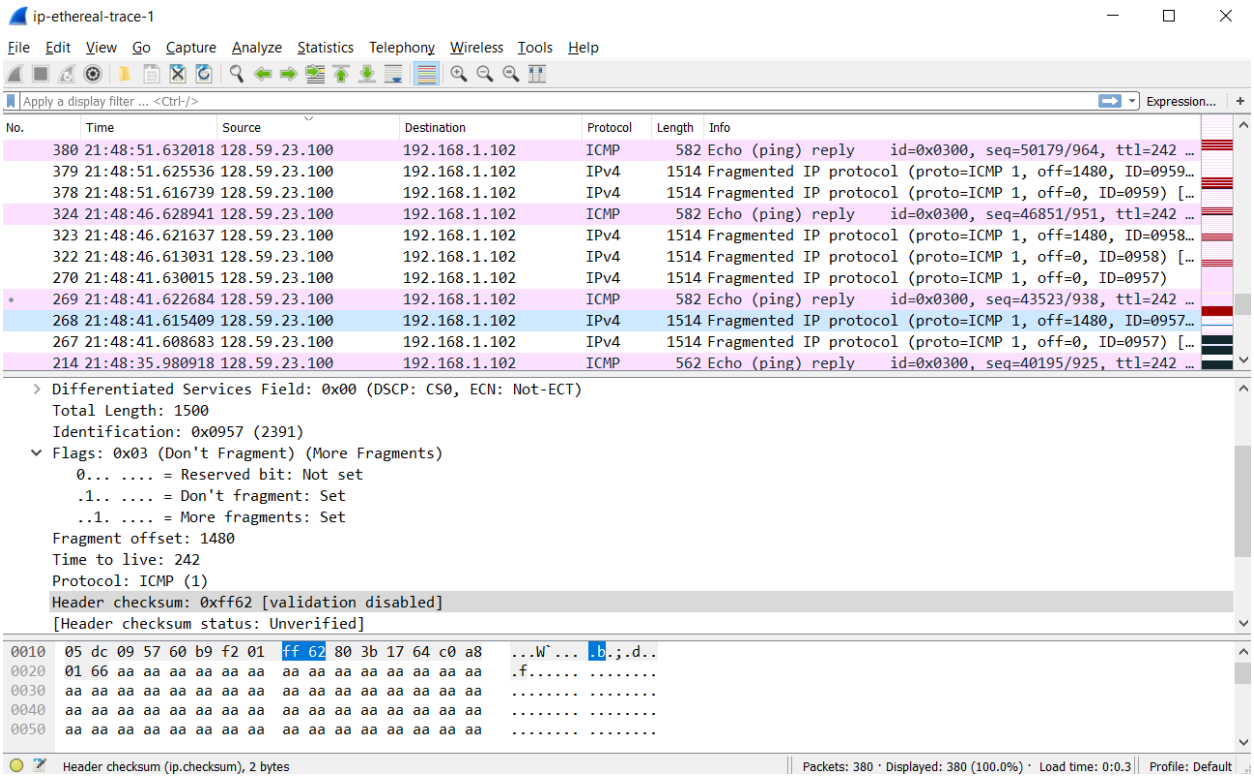
c. The total length is 540 bytes. You can see under Data that 520 bytes were sent so you just add the 20-byte header.



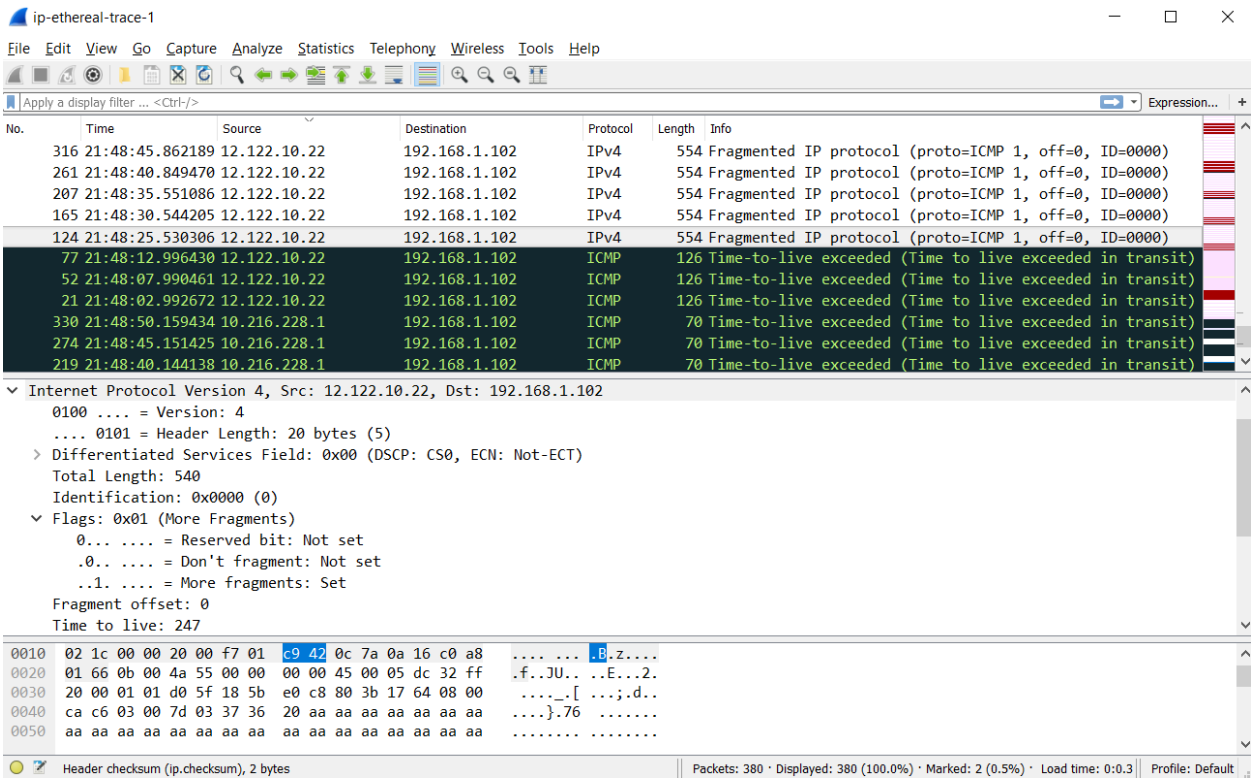
12.

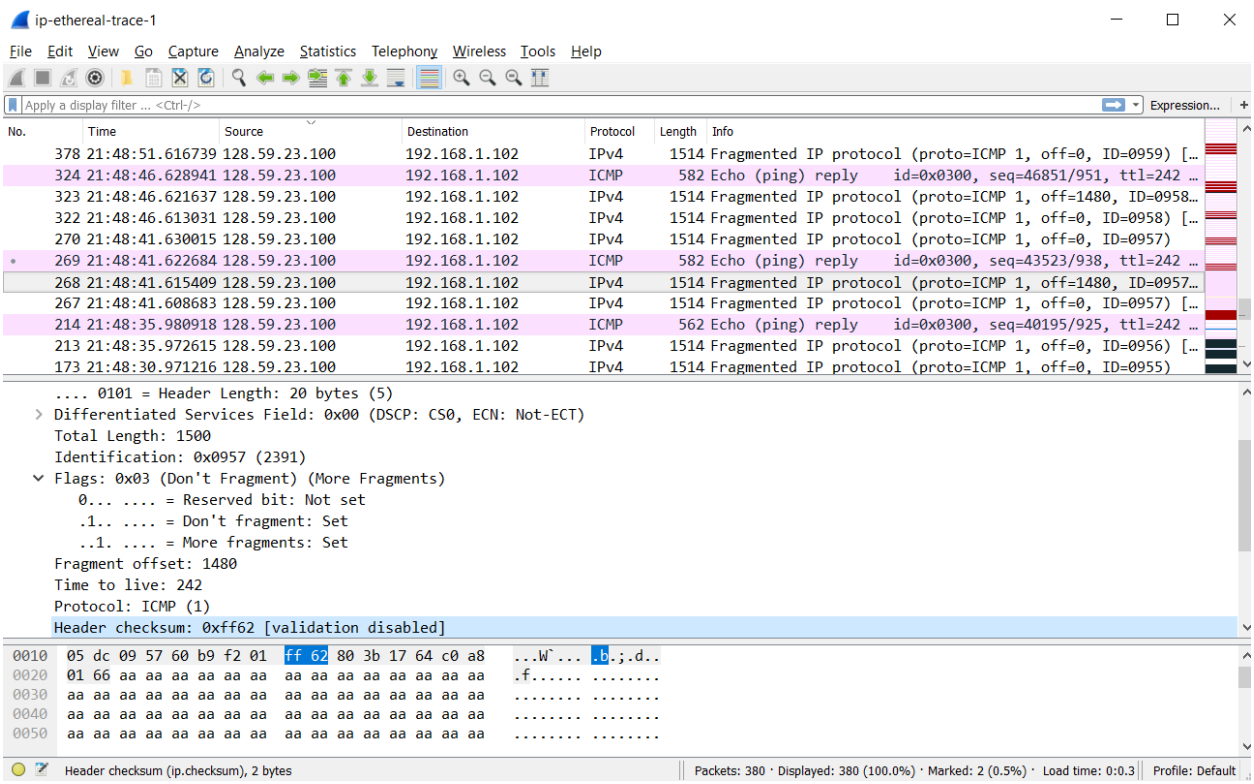
a. The header has offset 1480 so we know it’s not the first datagram fragment.

b. There are more fragments because the More fragments flag is set.



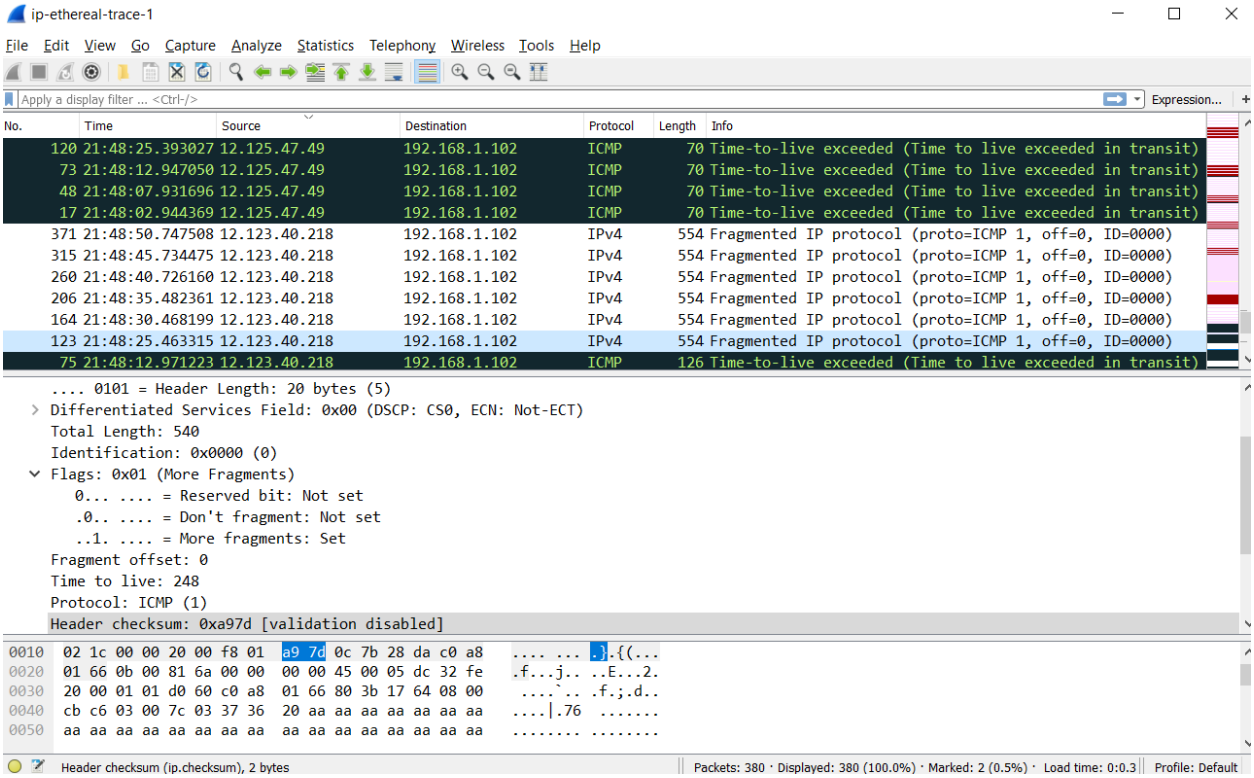
13. The checksum, total length, fragment offset, and flags change between the first and second fragment.

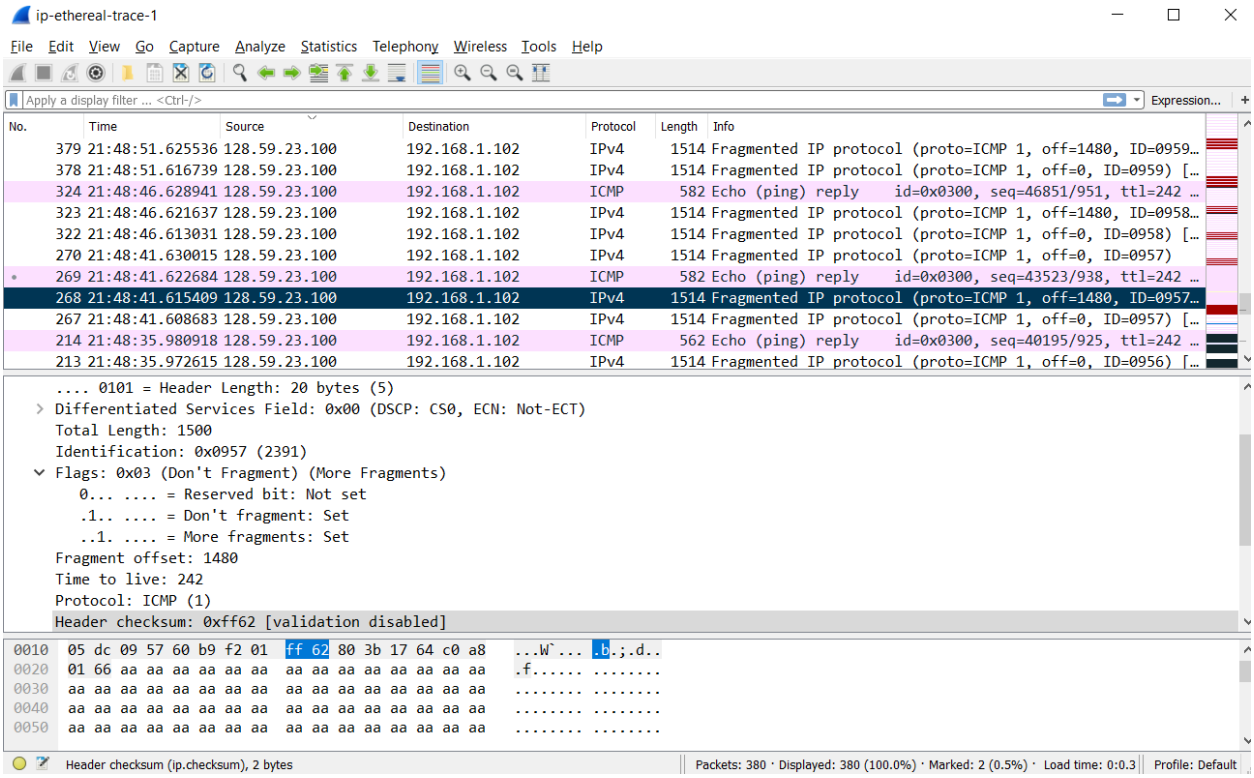

ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
316 21:48:45.862189 12.122.10.22 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
261 21:48:40.849470 12.122.10.22 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
207 21:48:35.551086 12.122.10.22 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
165 21:48:30.544205 12.122.10.22 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
124 21:48:25.530306 12.122.10.22 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
77 21:48:12.996430 12.122.10.22 192.168.1.102 ICMP 126 Time-to-live exceeded (Time to live exceeded in transit)
52 21:48:07.990461 12.122.10.22 192.168.1.102 ICMP 126 Time-to-live exceeded (Time to live exceeded in transit)
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)
330 21:48:50.159434 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
274 21:48:45.151425 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
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)
Internet Protocol Version 4, Src: 12.122.10.22, 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: 540
Identification: 0x0000 (0)
Flags: 0x01 (More Fragments)
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
Fragment offset: 0
Time to live: 247
0010 02 1c 00 00 20 00 f7 01 c9 42 0c 7a 0a 16 c0 a8 .... .B.z....
0020 01 66 0b 00 4a 55 00 00 00 00 45 00 05 dc 32 ff .f..JU.. ..E...2.
0030 20 00 01 01 d0 5f 18 5b e0 c8 80 3b 17 64 08 00 ....._.[...;.d..
0040 ca c6 03 00 7d 03 37 36 20 aa aa aa aa aa aa aa ....}.76 ....
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
Header checksum (ip.checksum), 2 bytes
Packets: 380 · Displayed: 380 (100.0%) · Marked: 2 (0.5%) · Load time: 0:0.3
Profile: Default


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
378 21:48:51.616739 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0959) [...
324 21:48:46.628941 128.59.23.100 192.168.1.102 ICMP 582 Echo (ping) reply id=0x0300, seq=46851/951, ttl=242 ...
323 21:48:46.621637 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0958...
322 21:48:46.613031 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0958) [...
270 21:48:41.630015 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957)
269 21:48:41.622684 128.59.23.100 192.168.1.102 ICMP 582 Echo (ping) reply id=0x0300, seq=43523/938, ttl=242 ...
268 21:48:41.615409 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0957...
267 21:48:41.608683 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957) [...
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 ...
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) [...
173 21:48:30.971216 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0955)
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x0957 (2391)
Flags: 0x03 (Don't Fragment) (More Fragments)
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..1. .... = More fragments: Set
Fragment offset: 1480
Time to live: 242
Protocol: ICMP (1)
Header checksum: 0xff62 [validation disabled]
0010 05 dc 09 57 60 b9 f2 01 ff 62 80 3b 17 64 c0 a8 ...W`... .b.;.d..
0020 01 66 aa aa aa aa aa aa aa aa aa aa aa aa aa aa .f...... ....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
Header checksum (ip.checksum), 2 bytes
Packets: 380 · Displayed: 380 (100.0%) · Marked: 2 (0.5%) · Load time: 0:0.3
Profile: Default

14. There are three fragments created after changing the Packet Size to 3500.

15. It looks like the checksum and the offset change between each header. The length and the flags also has variation.




ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
379 21:48:51.625536 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0959…
378 21:48:51.616739 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0959) […
324 21:48:46.628941 128.59.23.100 192.168.1.102 ICMP 582 Echo (ping) reply id=0x0300, seq=46851/951, ttl=242 …
323 21:48:46.621637 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0958…
322 21:48:46.613031 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0958) […
270 21:48:41.630015 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957)
269 21:48:41.622684 128.59.23.100 192.168.1.102 ICMP 582 Echo (ping) reply id=0x0300, seq=43523/938, ttl=242 …
268 21:48:41.615409 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0957…
267 21:48:41.608683 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957) […
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 …
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) […
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x0957 (2391)
Flags: 0x03 (Don't Fragment) (More Fragments)
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..1. .... = More fragments: Set
Fragment offset: 1480
Time to live: 242
Protocol: ICMP (1)
Header checksum: 0xff62 [validation disabled]
0010 05 dc 09 57 60 b9 f2 01 ff 62 80 3b 17 64 c0 a8 ...W`... .b.;.d..
0020 01 66 aa aa aa aa aa aa aa aa aa aa aa aa aa aa .f...... ....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa ....
Header checksum (ip.checksum), 2 bytes
Packets: 380 · Displayed: 380 (100.0%) · Marked: 2 (0.5%) · Load time: 0:0.3
Profile: Default