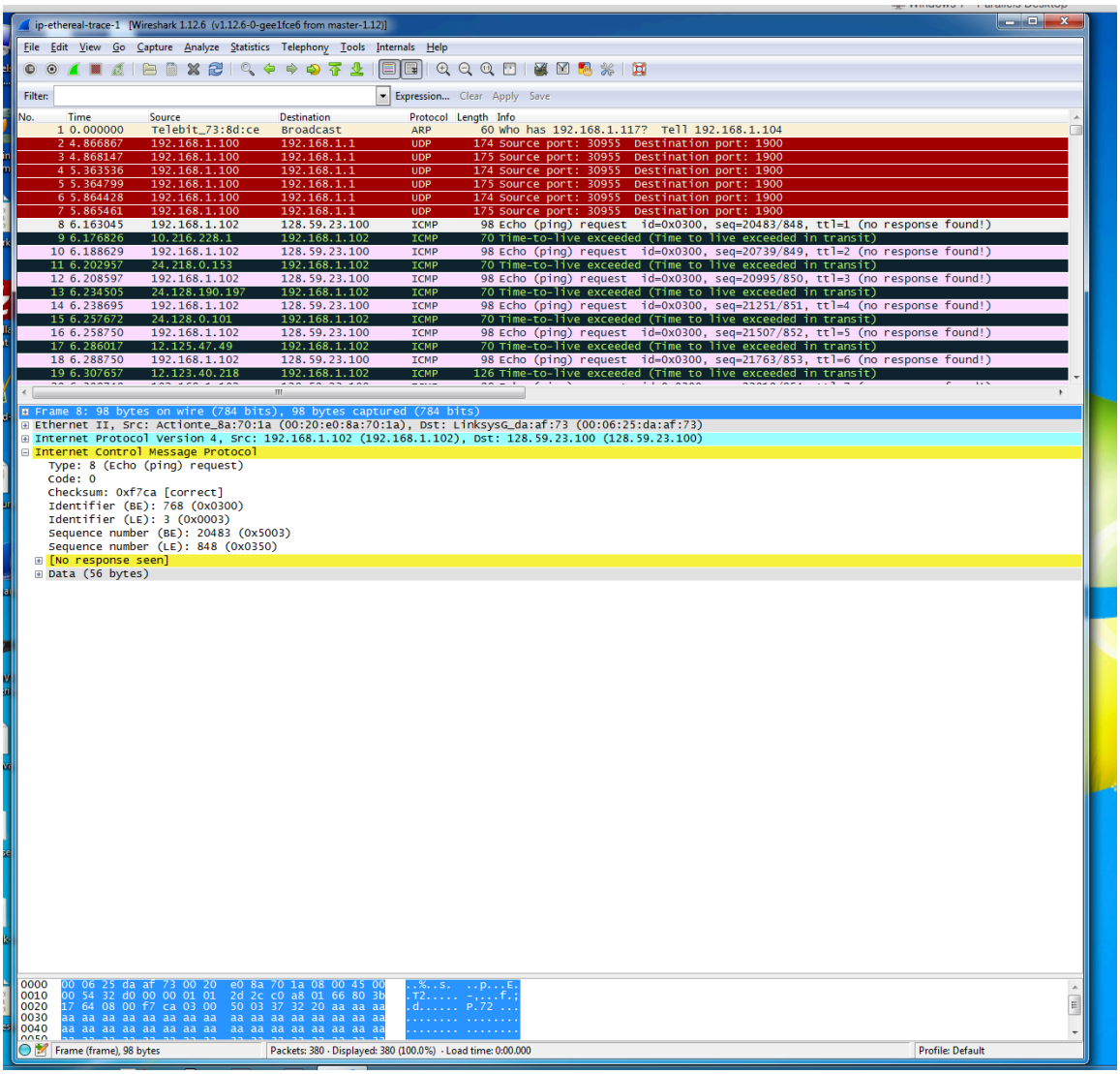
1. IP Address
- 192.168.1.102

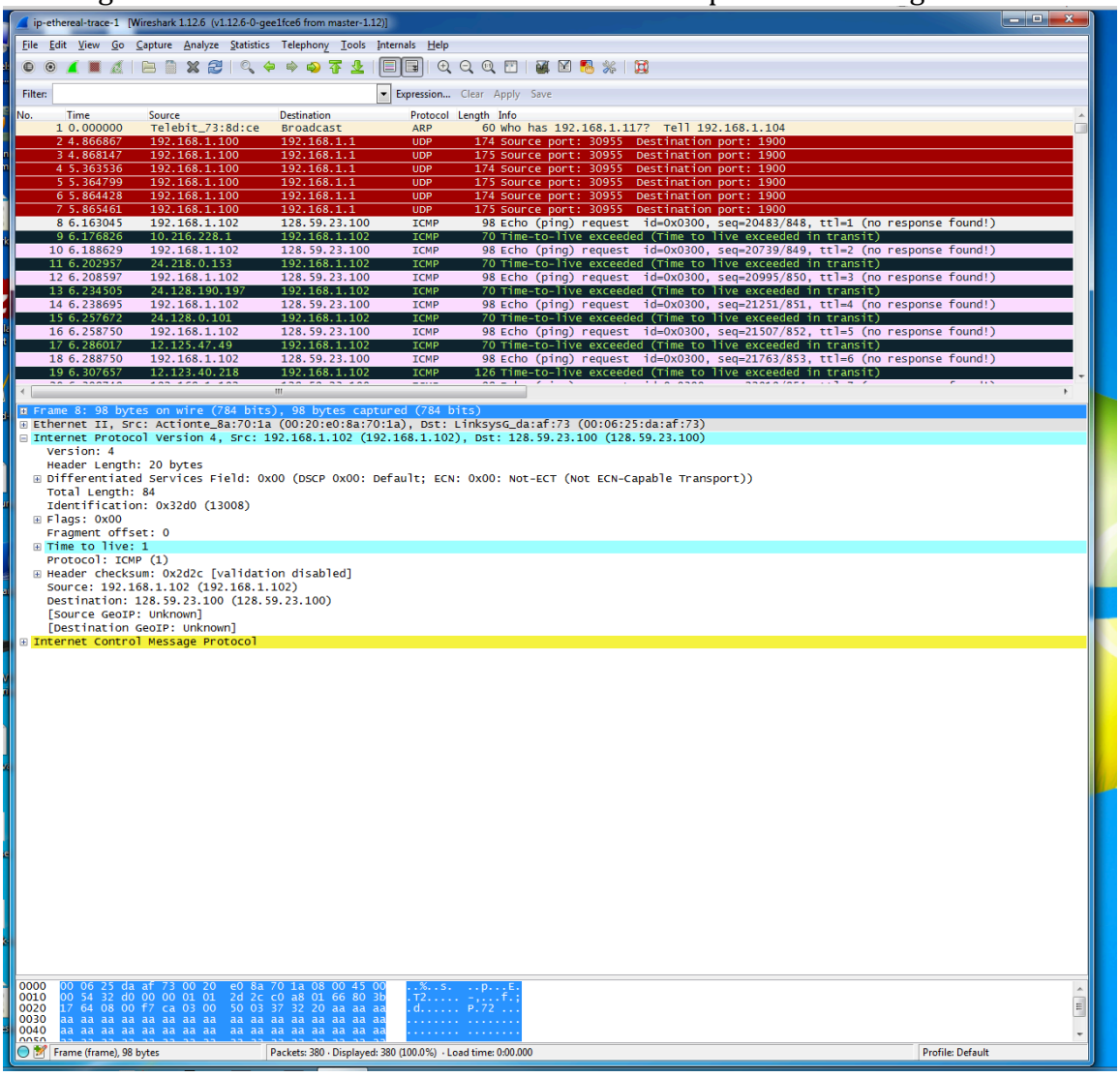
2. Within the IP packet header, what is the value in the upper layer protocol field?
The value is 768



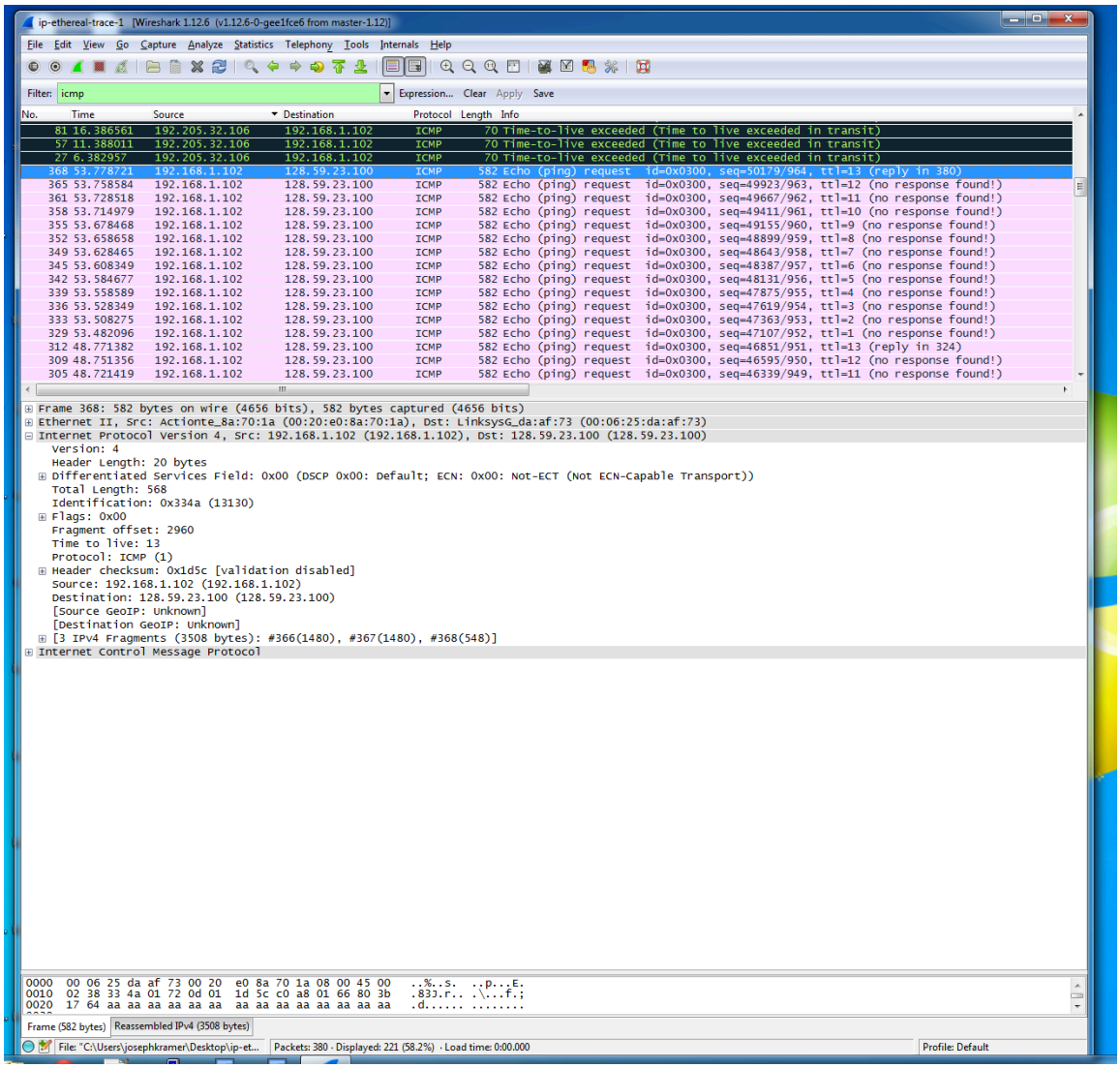
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
There are 20 bytes in the IP header.
There are 36 bytes in the payload.
There were 56 bytes sent, and 56-20=36

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

The fragment offset is set to 0. This indicates that the packet is no fragmented.



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?
Identification, Checksum, Time To Live



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

Constant:

Version – because IPv4 is used for the packets
Header Length – because of ICMP packets
Source IP – always sending from the same source.
Destination IP – always sending to the same destination.
Differentiated Services Filed – All packets are ICMP, therefore they use the same type of service class.
Upper Layer Protocol – Because these are ICMP packets

Fields That Must State Constant:

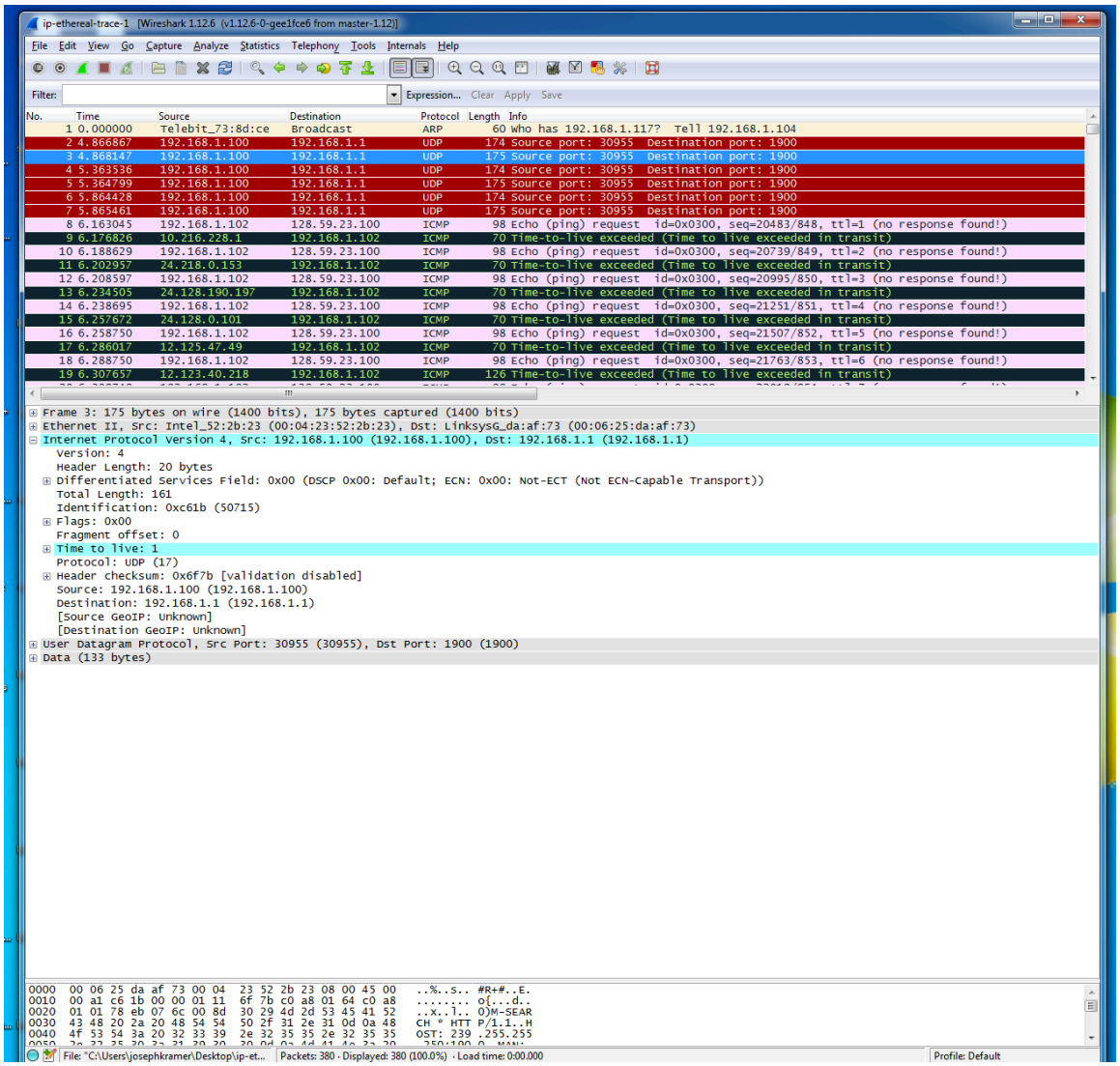
** Same As Above **

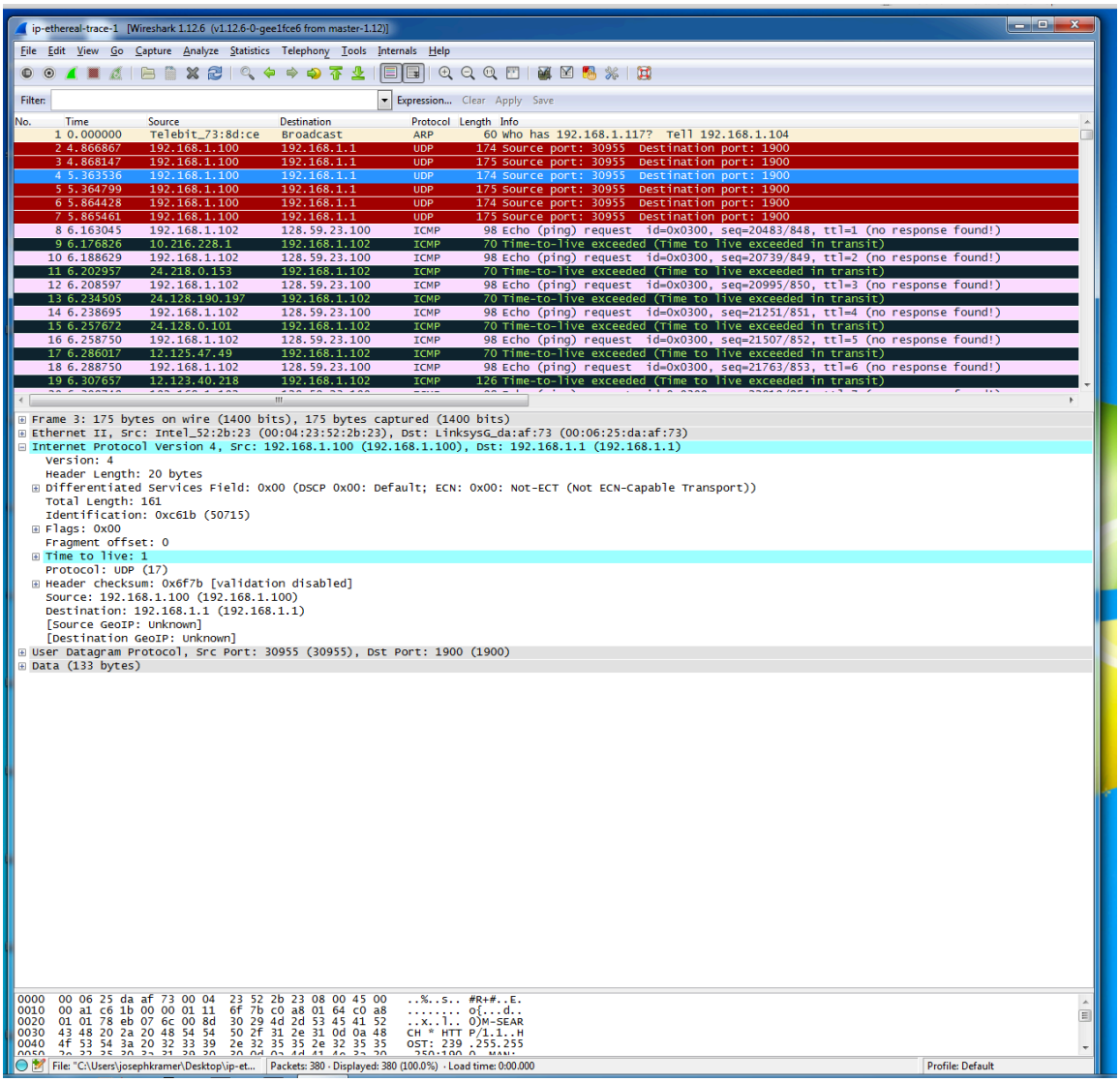
Fields That Must Change:

Time to live – The IP packets must have different ID's
Header checksum – When the header changes, so does the checksum
Identification – The IP packets must have different ID's

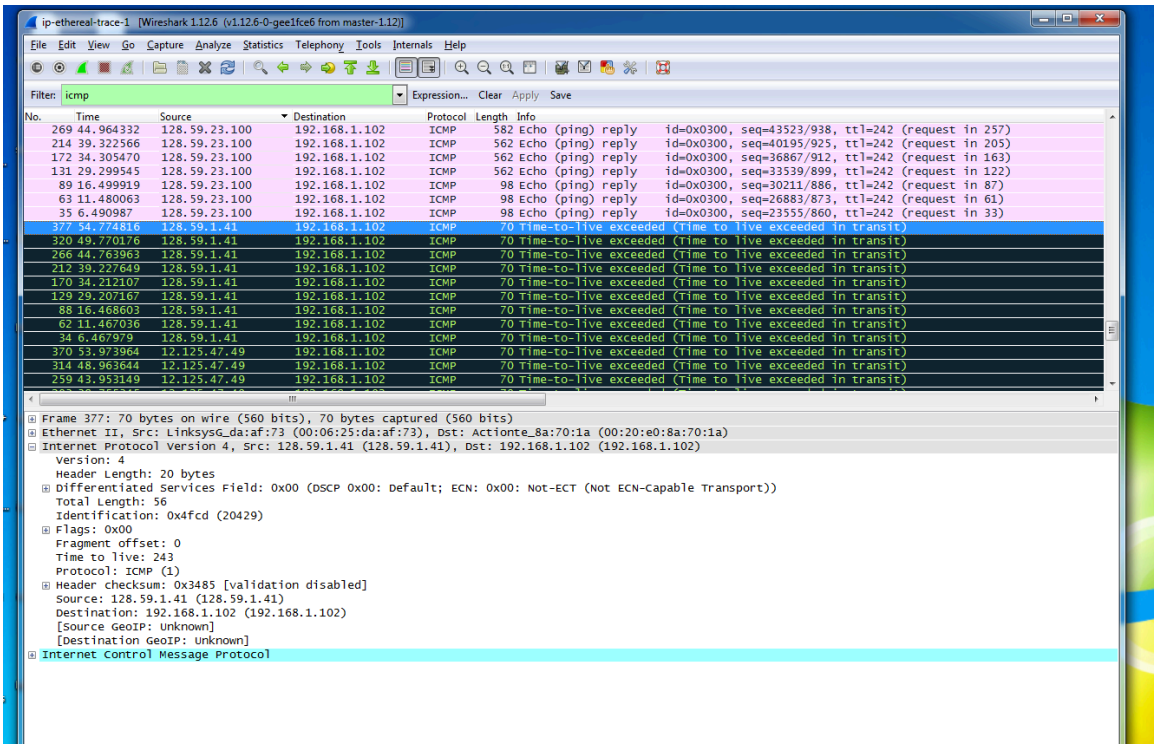
7. Describe the pattern you see in the values in the Identification field of the IP datagram

The IP header ID fields' increment with each ICMP echo




ip-ethereal-trace-1 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 Telebit_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 UDP 174 Source port: 30955 Destination port: 1900
3 4.868147 192.168.1.100 192.168.1.1 UDP 175 Source port: 30955 Destination port: 1900
4 5.363536 192.168.1.100 192.168.1.1 UDP 174 Source port: 30955 Destination port: 1900
5 5.364799 192.168.1.100 192.168.1.1 UDP 175 Source port: 30955 Destination port: 1900
6 5.864428 192.168.1.100 192.168.1.1 UDP 174 Source port: 30955 Destination port: 1900
7 5.865461 192.168.1.100 192.168.1.1 UDP 175 Source port: 30955 Destination port: 1900
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!)
13 6.234505 24.128.190.197 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
14 6.238695 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15 6.257672 24.128.0.101 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
16 6.258750 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17 6.286017 12.125.47.49 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
18 6.288750 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19 6.307657 12.123.40.218 192.168.1.102 ICMP 126 Time-to-live exceeded (Time to live exceeded in transit)
Frame 3: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits)
Ethernet II, Src: Intel_52:2b:23 (00:04:23:52:2b:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.1 (192.168.1.1)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 161
Identification: 0xc61b (50715)
Flags: 0x00
Fragment offset: 0
Time to live: 1
Protocol: UDP (17)
Header checksum: 0x6f7b [validation disabled]
Source: 192.168.1.100 (192.168.1.100)
Destination: 192.168.1.1 (192.168.1.1)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 30955 (30955), Dst Port: 1900 (1900)
Data (133 bytes)
0000 00 06 25 da af 73 00 04 23 52 2b 23 08 00 45 00 ..%..s.. #R+#..E.
0010 00 a1 c6 1b 00 00 01 11 6f 7b c0 a8 01 64 c0 a8 .... o{...d..
0020 01 01 78 eb 07 6c 00 8d 30 29 4d 2d 53 45 41 52 ..x..l.. 0)M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
File: "C:\Users\josephkramer\Desktop\ip-et... Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:00.000
Profile: Default

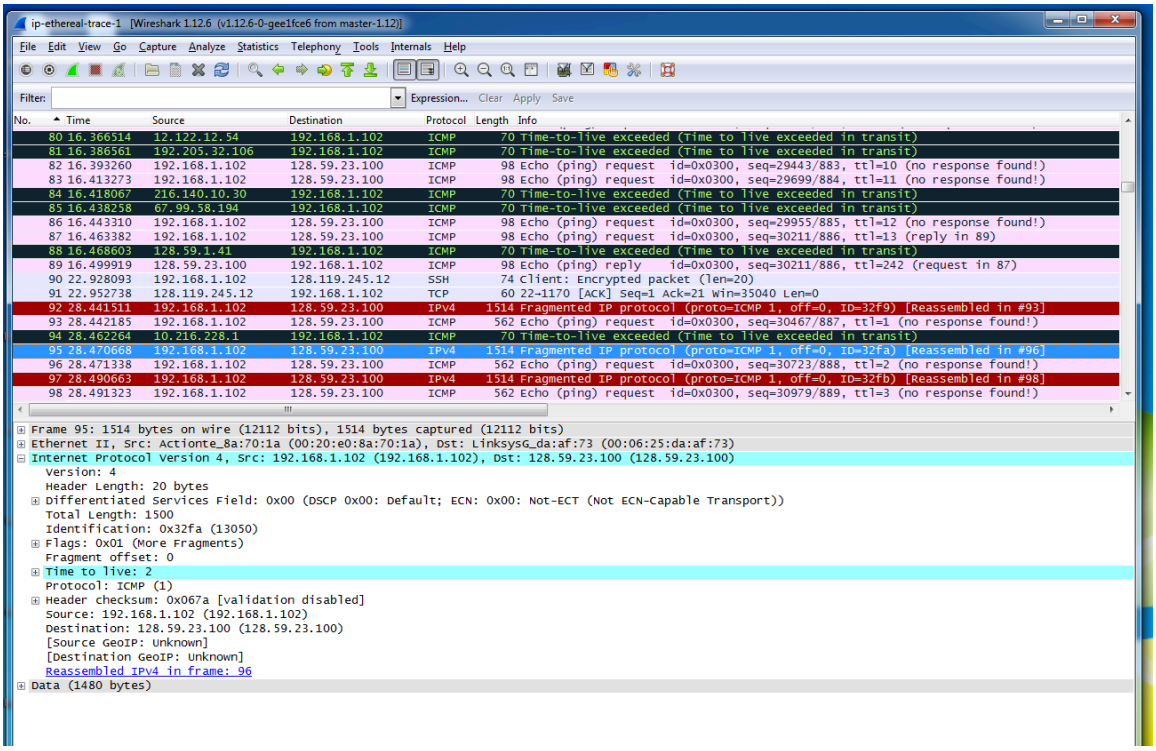
8. What is the value in the Identification field and the TTL field?
Identification: 0x4fcd (20429)
Time to live: 243



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 identification field changes from every reply, because the field must remain unique. If the ID fields have the same value then the replies are fragments of a bigger packet.
The time to live field is unchanged, because the time to live for the first hop router is always the same.

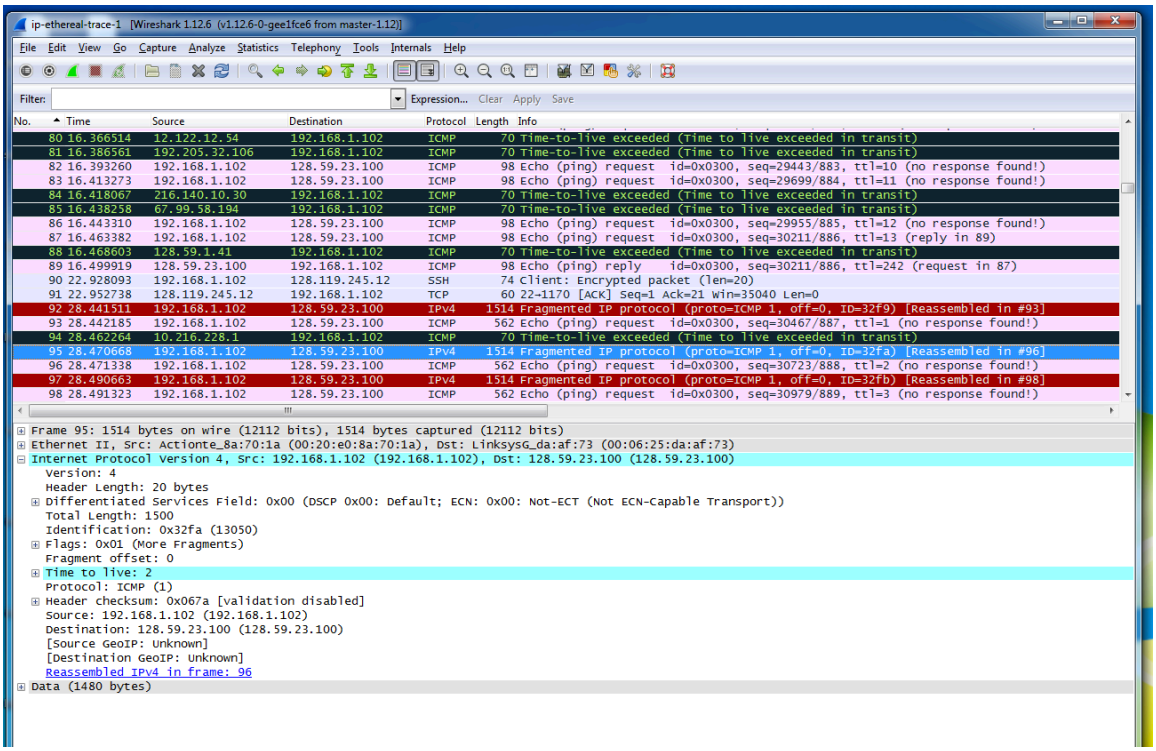
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Yes the message has been fragmented across more than one IP Datagram.



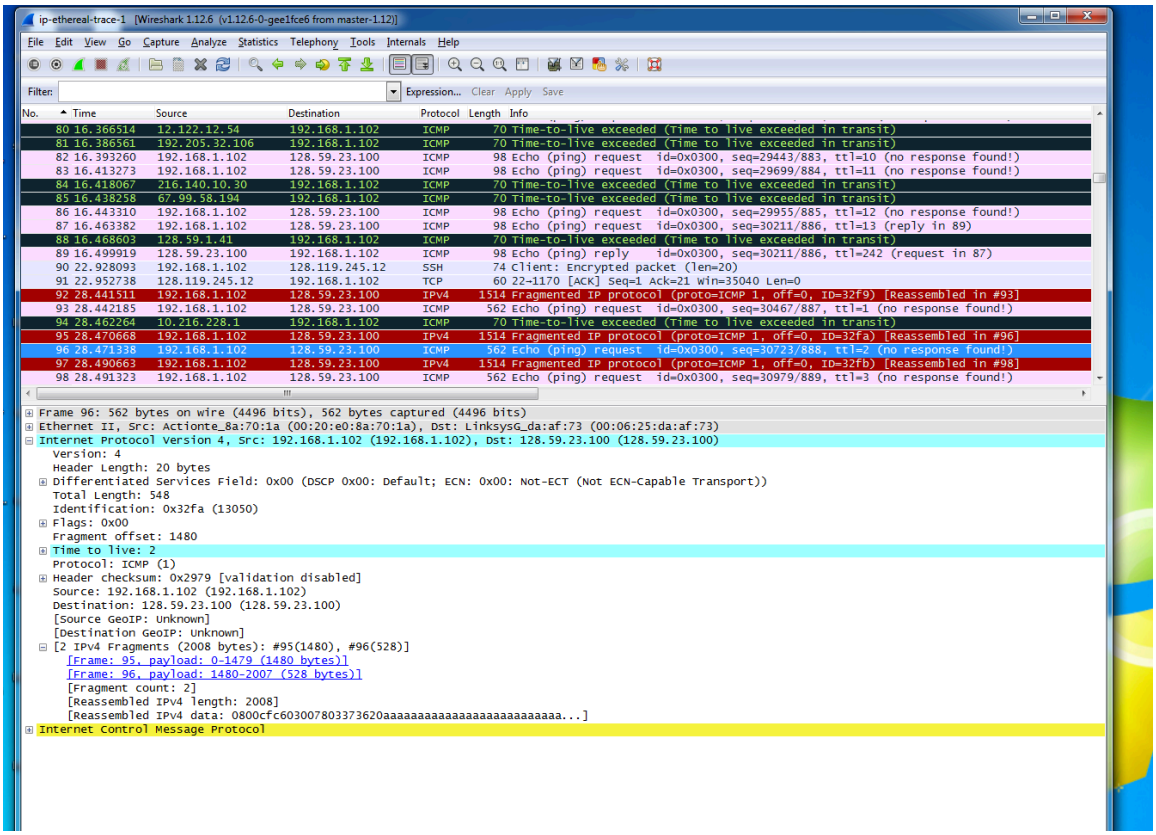
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

The flag bit is set, which indicates that the datagram is fragmented. The fragment offset is 0, therefore this is the first fragment. The length is a total of 1500, header + offset.



12. 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?

The fragment offset is 1480 and that is what indicates this is not the first datagram fragment. There are no more fragments, because the flag is not set

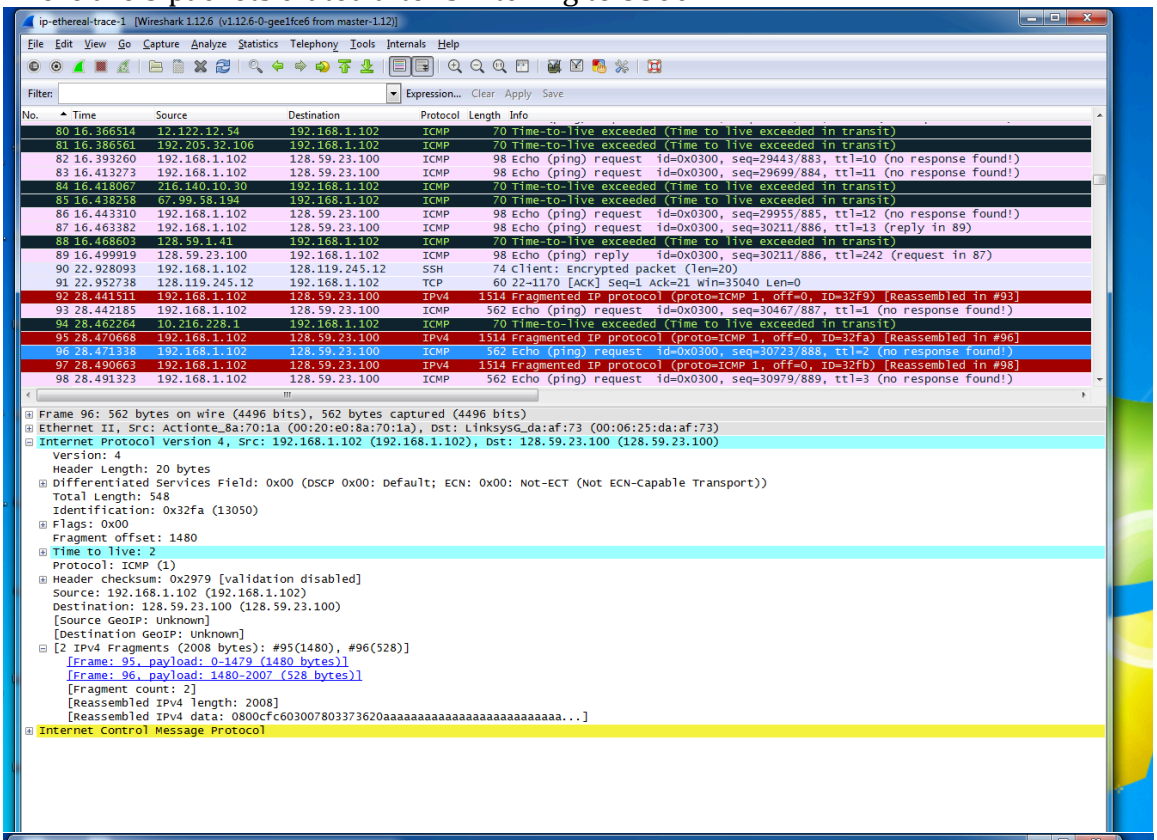


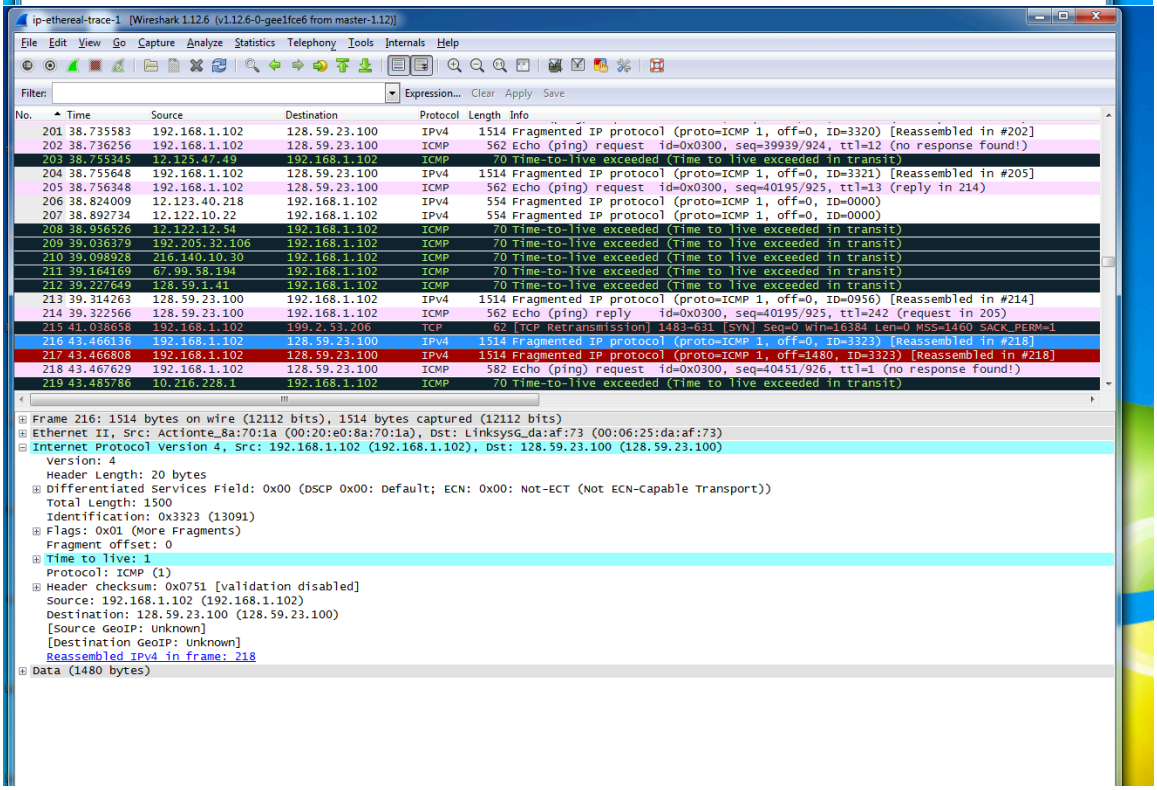
13. What fields change in the IP header between the first and second fragment?

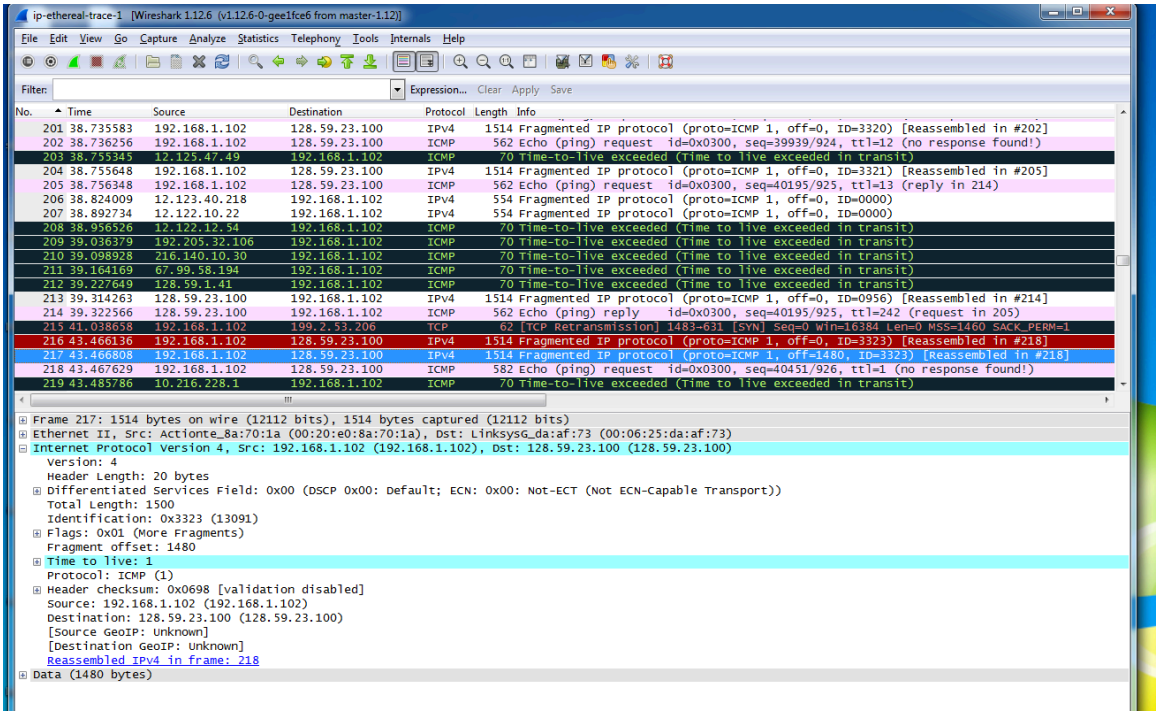
Length, Flag Set, Fragment Offset, Header Checksum

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

There are 3 packets crated after switching to 3500.

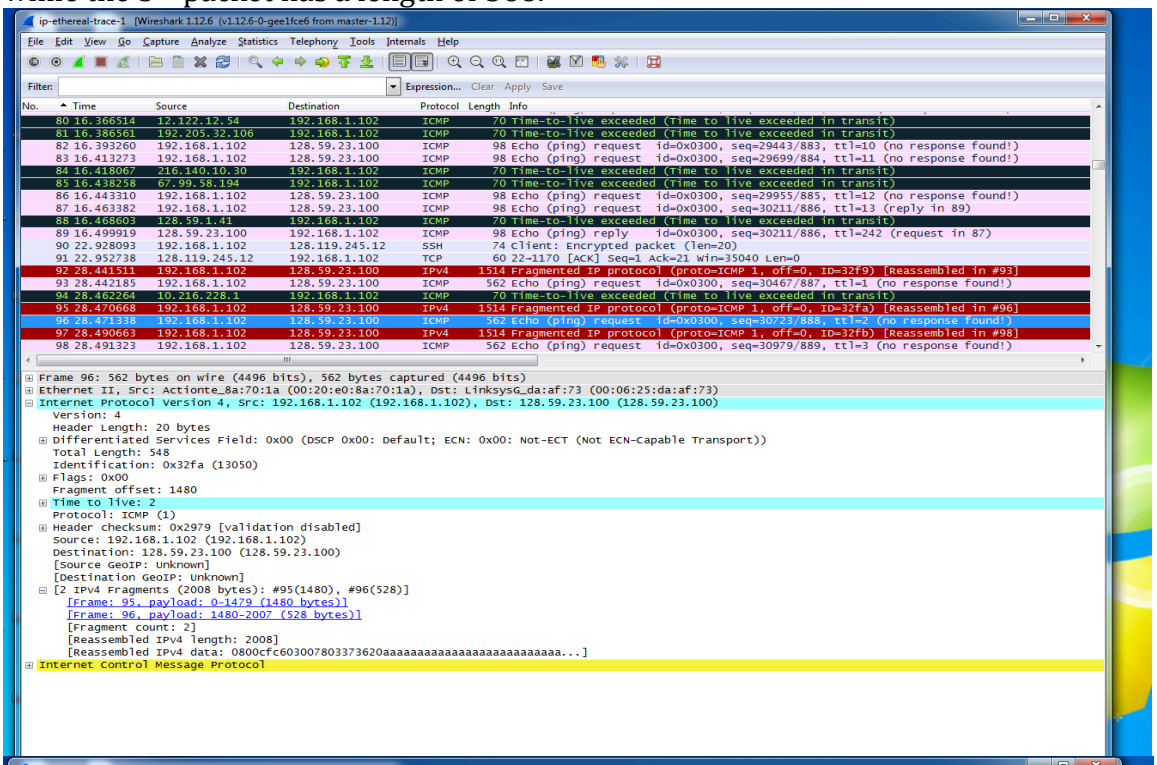


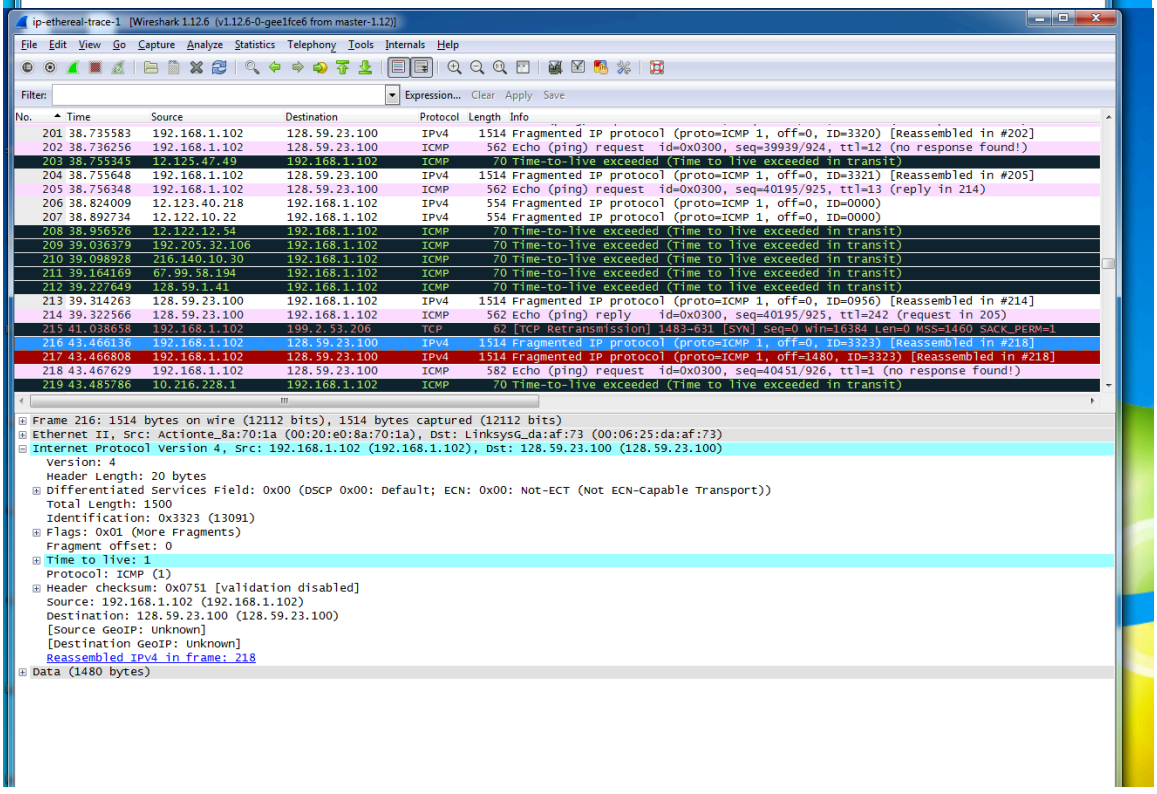


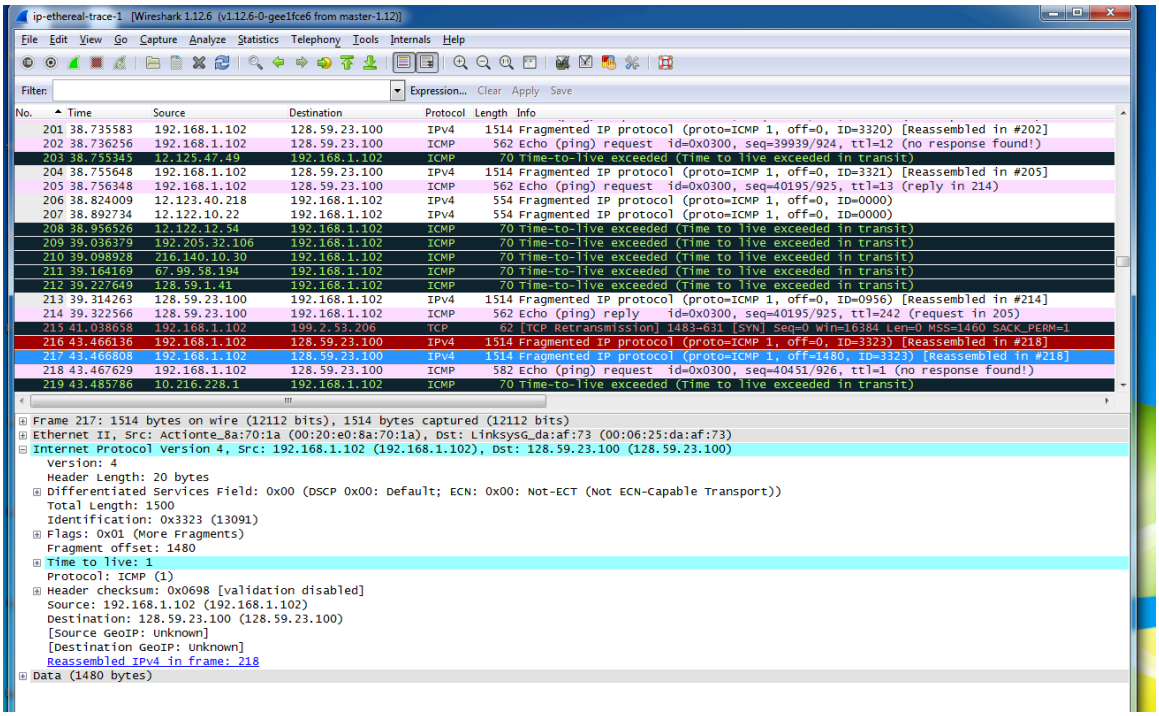

ip-ethereal-trace-1 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
201 38.735583 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3320) [Reassembled in #202]
202 38.736256 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=39939/924, ttl=12 (no response found!)
203 38.755345 12.125.47.49 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
204 38.755648 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3321) [Reassembled in #205]
205 38.756348 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=40195/925, ttl=13 (reply in 214)
206 38.824009 12.123.40.218 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
207 38.892734 12.122.10.22 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
208 38.956526 12.122.12.54 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
209 39.036379 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
210 39.098928 216.140.10.30 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
211 39.164169 67.99.58.194 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
212 39.227649 128.59.1.41 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
213 39.314263 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214 39.322566 128.59.23.100 192.168.1.102 ICMP 562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215 41.038658 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 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219 43.485786 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Frame 217: 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 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x01 (More Fragments)
Fragment offset: 1480
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0698 [validation disabled]
Source: 192.168.1.102 (192.168.1.102)
Destination: 128.59.23.100 (128.59.23.100)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Reassembled IPv4 in frame: 218
Data (1480 bytes)

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

Between all packets the IP header fields that changed are checksum and fragment offset. For all three packets there is a change in the total length. There is a change in the flag for the 3rd packet from 1 to 0. The first two packets have a length of 1500, while the 3rd packet has a length of 568.






ip-ethereal-trace-1 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
201 38.735583 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3320) [Reassembled in #202]
202 38.736256 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=39939/924, ttl=12 (no response found!)
203 38.755345 12.125.47.49 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
204 38.755648 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3321) [Reassembled in #205]
205 38.756348 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=40195/925, ttl=13 (reply in 214)
206 38.824009 12.123.40.218 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
207 38.892734 12.122.10.22 192.168.1.102 IPv4 554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
208 38.956526 12.122.12.54 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
209 39.036379 192.205.32.106 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
210 39.098928 216.140.10.30 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
211 39.164169 67.99.58.194 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
212 39.227649 128.59.1.41 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
213 39.314263 128.59.23.100 192.168.1.102 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214 39.322566 128.59.23.100 192.168.1.102 ICMP 562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215 41.038658 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 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219 43.485786 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Frame 217: 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 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x01 (More Fragments)
Fragment offset: 1480
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0698 [validation disabled]
Source: 192.168.1.102 (192.168.1.102)
Destination: 128.59.23.100 (128.59.23.100)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Reassembled IPv4 in frame: 218
Data (1480 bytes)