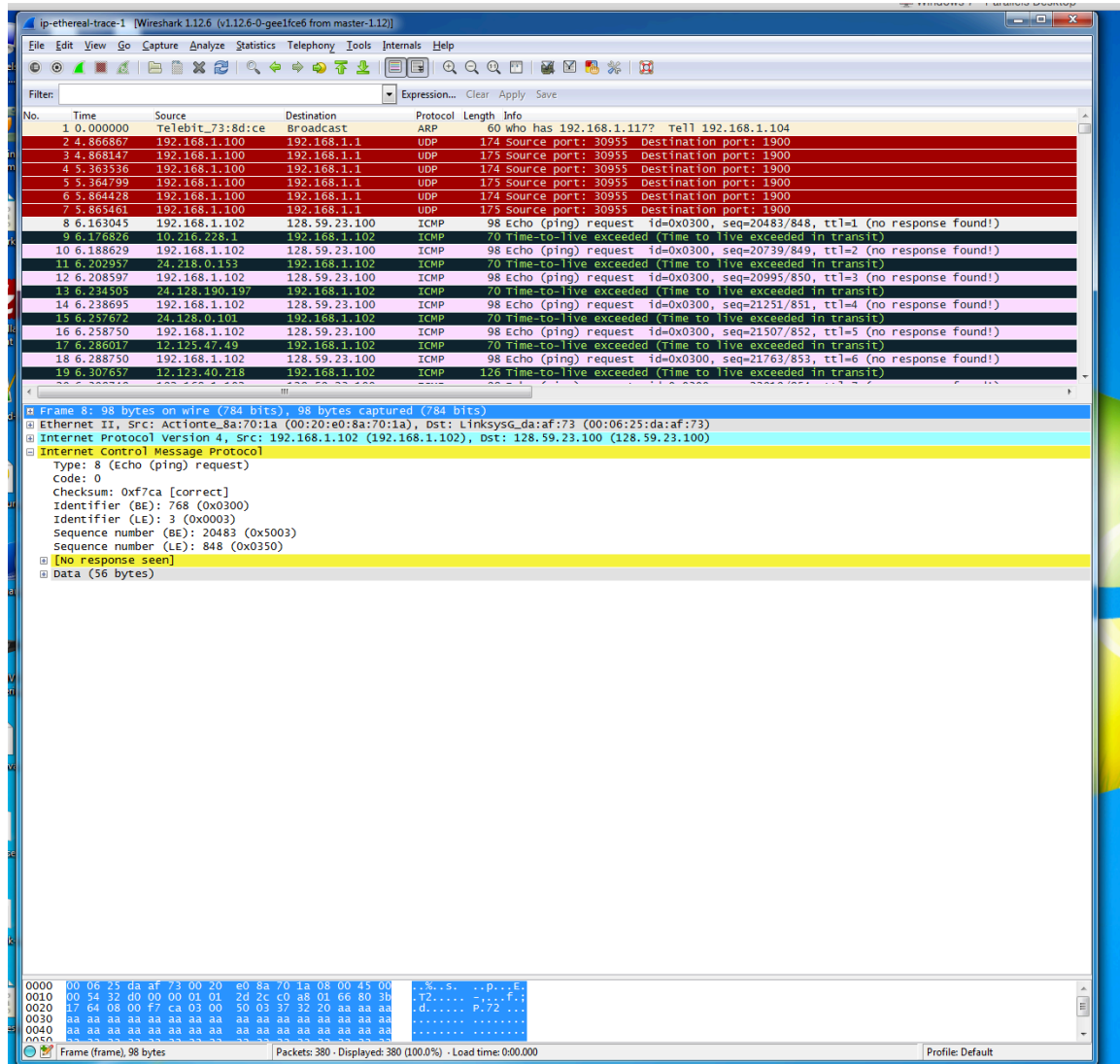


1. IP Address
- 192.168.1.102

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 not fragmented.

The screenshot shows a Wireshark packet capture of an ICMP Echo request. The packet list pane displays the following information:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Telebit_73:8d:cce	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	6.208937	212.213.041.133	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	12.125.40.215	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)

The packet details pane for the selected packet (No. 9) shows the following structure:

- 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: Linksys6_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: 84
 - Identification: 0x32d0 (13008)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 1
 - Protocol: ICMP (1)
 - Header checksum: 0x2d2c [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]
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and ICMP header.

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

The image shows a Wireshark packet capture of ICMP Echo (ping) messages. The packet list at the top shows several ICMP Echo (ping) requests from 192.168.1.102 to 128.59.23.100. The packet details pane for the selected packet (No. 368) shows the structure of an ICMP Echo (ping) request, including the Identification field (0x334a), Checksum (0x00), and Time to Live (13). The packet bytes pane shows the raw data of the ICMP Echo (ping) request.

No.	Time	Source	Destination	Protocol	Length	Info
81	16.386561	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	11.388011	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	53.726221	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
369	53.758584	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
361	53.728518	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49411/961, ttl=10 (no response found!)
358	53.714979	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49155/960, ttl=9 (no response found!)
355	53.678468	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48899/959, ttl=8 (no response found!)
352	53.658658	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48643/958, ttl=7 (no response found!)
349	53.628465	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48387/957, ttl=6 (no response found!)
345	53.608349	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=48131/956, ttl=5 (no response found!)
342	53.584677	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=47875/955, ttl=4 (no response found!)
339	53.558589	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=47619/954, ttl=3 (no response found!)
336	53.528349	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=47363/953, ttl=2 (no response found!)
333	53.508275	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=47107/952, ttl=1 (no response found!)
329	53.482096	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=46851/951, ttl=13 (reply in 324)
312	48.771382	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=46595/950, ttl=12 (no response found!)
309	48.751356	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=46339/949, ttl=11 (no response found!)
305	48.721419	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=46079/948, ttl=10 (no response found!)

Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:12:5d: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: 568
Identification: 0x334a (13130)
Flags: 0x00
Fragment offset: 2960
Time to live: 13
Protocol: ICMP (1)
Header checksum: 0x1d5c [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]
[3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]
Internet Control Message Protocol

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. ..p...E.
0010 02 38 33 4a 01 72 0d 01 1d 5c c0 a8 01 66 80 3b .833.r.. \...f.
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa .d.....

Frame [582 bytes] Reassembled IPv4 (3508 bytes)

File: C:\Users\josephkramer\Desktop\ip-et... Packets: 380 - Displayed: 221 (58.2%) - Load time: 0:00:00

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

The screenshot displays a Wireshark packet capture of network traffic. The packet list at the top shows a series of ICMP Echo (ping) requests from source 192.168.1.100 to destination 192.168.1.1. The packet details pane for the selected packet (No. 19) shows the following structure:

- 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)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The ASCII column shows the text "P/1..H" and "OST: 239 .255.255".

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	5.389336	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	24.228.1008.197	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: Linksys_gd: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.. O]M-SEAR

0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1..H

0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255

0050 7a 31 35 30 3a 31 30 30 30 0d 05 4d 41 4e 3a 30 750-1900.0-NAU

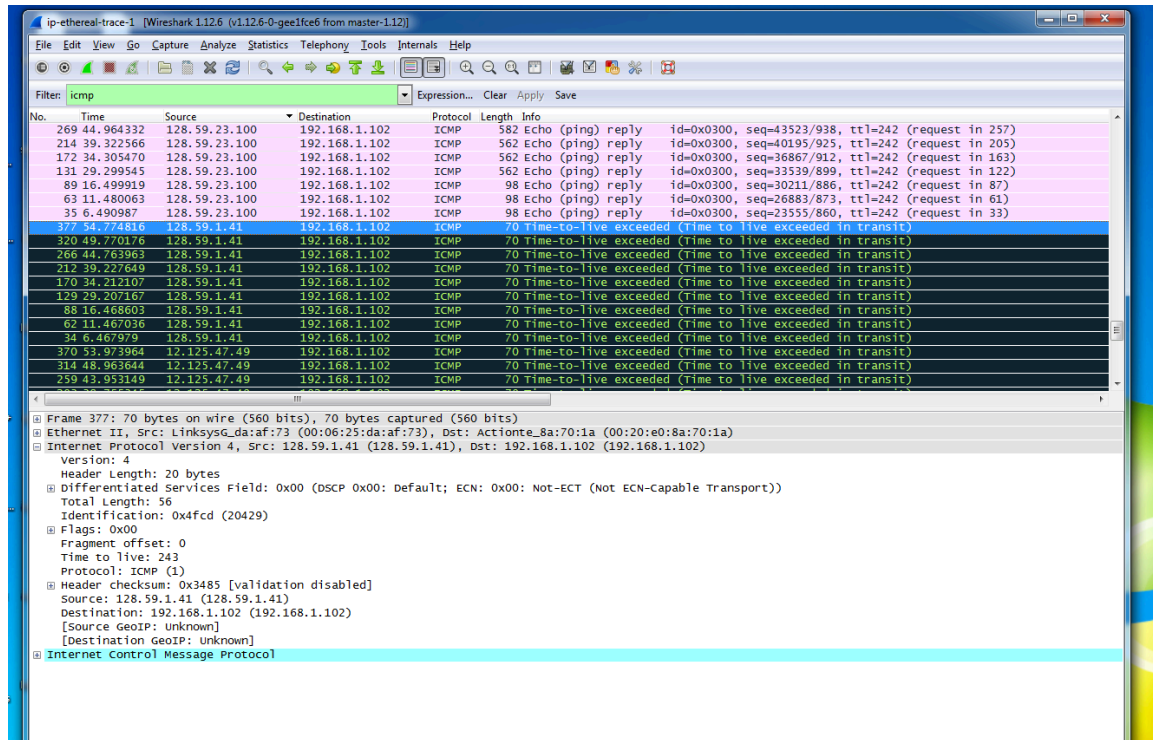
File: C:\Users\josephkramer\Desktop\ip-et... Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:00:000

Profile: Default

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

Identification: 0x4fcd (20429)

Time to live: 243



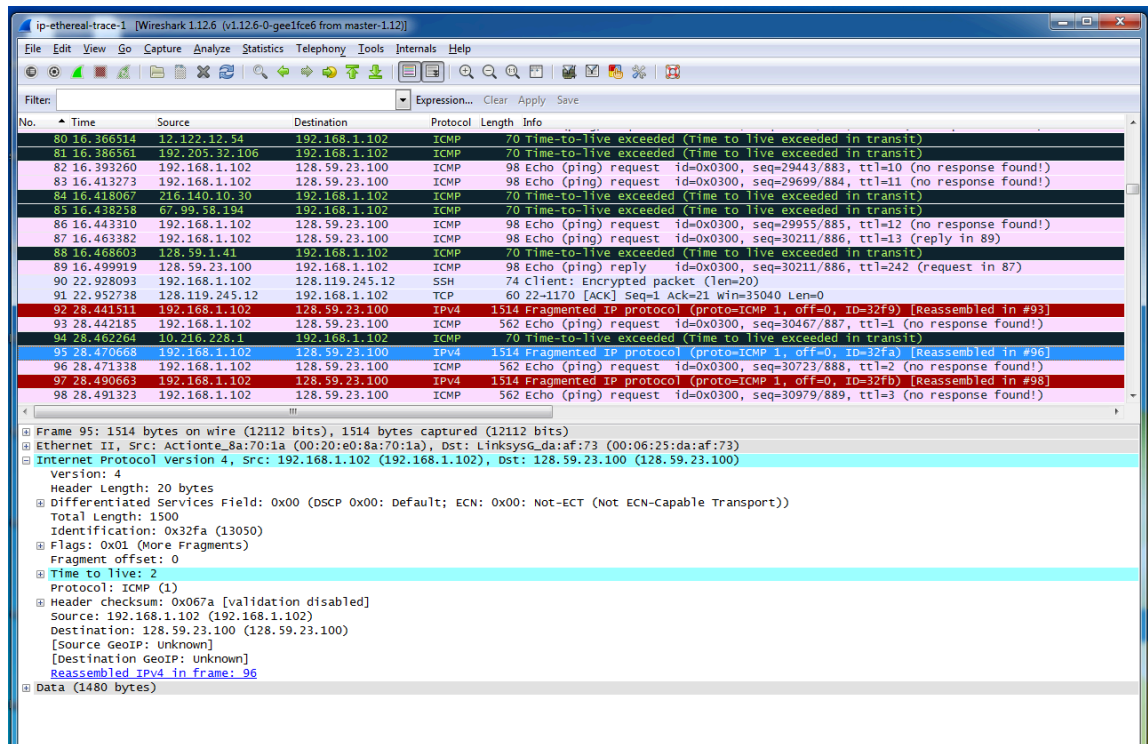
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

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.

ip-ethereal-trace-1 [Wireshark 1.12.6 (v1.12.6-0-gee1c66 from master-112)]

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
80	16.366514	192.168.1.102	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	16.386561	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
82	16.393260	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29443/883, ttl=10 (no response found!)
83	16.413273	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29699/884, ttl=11 (no response found!)
84	16.418067	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.438258	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.443310	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	16.463382	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	16.468603	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.499919	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	22.928093	192.168.1.102	128.119.245.12	SSH	74	Client: encrypted packet (len=20)
91	22.952738	128.119.245.12	192.168.1.102	TCP	60	22->1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [reassembled in #93]
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [reassembled in #96]
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [reassembled in #98]
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)

Frame 95: 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: 0x32fa (13050)

Flags: 0x01 (More Fragments)

Fragment offset: 0

Time to live: 2

Protocol: ICMP (1)

Header checksum: 0x067a [validation disabled]

Source: 192.168.1.102 (192.168.1.102)

Destination: 128.59.23.100 (128.59.23.100)

[Source GeoIP: Unknown]

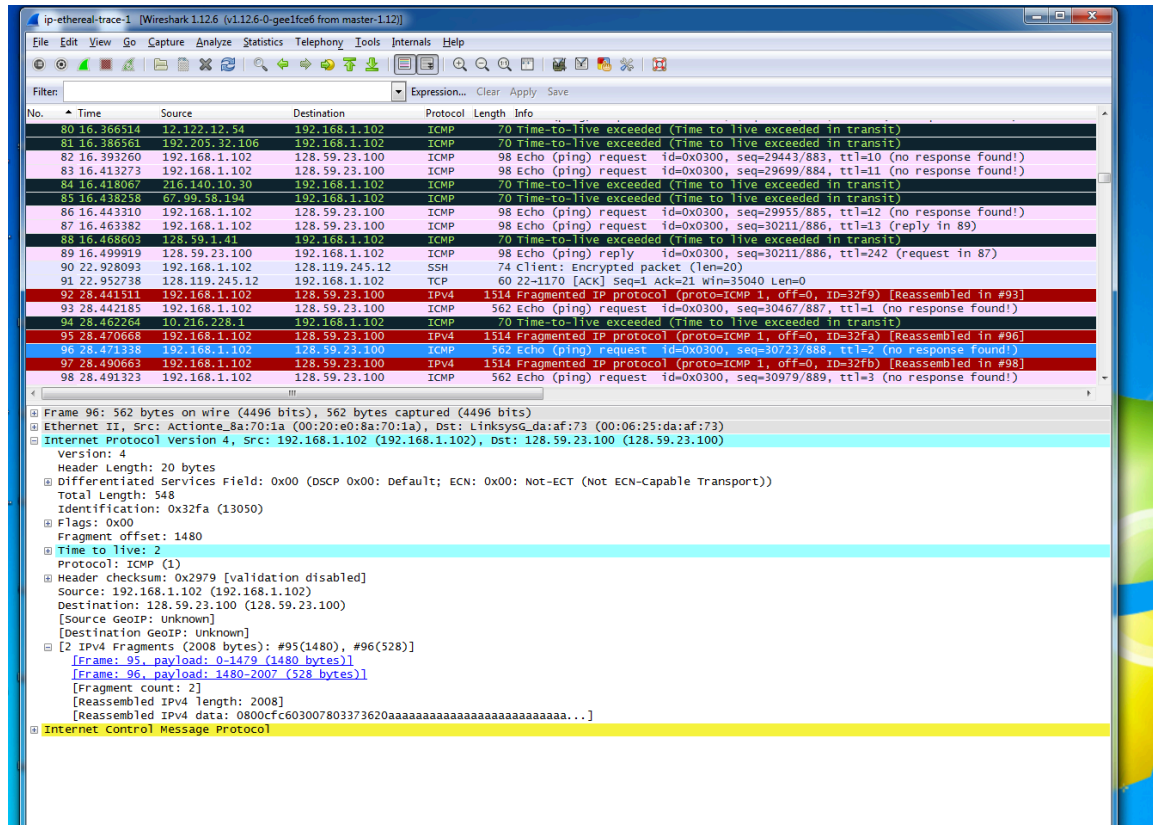
[Destination GeoIP: Unknown]

Reassembled IPv4 in frame: 96

Data (1480 bytes)

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 there 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 created after switching to 3500.

The top screenshot shows a packet capture in Wireshark. The packet list pane shows a packet of type ICMP Echo (ping) request. The packet details pane shows the following information:

- Frame 96: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0:00:00:00:00:00
- Ethernet II, Src: Axiomtek (08:00:00:00:00:00), Dst: Linksys (08:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 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: 548
- Identification: 0x32fa (13050)
- Flags: 0x00
- Fragment offset: 1480
- Time to live: 2
- Protocol: ICMP (1)
- Header checksum: 0x2979 [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]
- [2 IPv4 Fragments (2008 bytes): #95(1480), #96(528)]
- [Frame 95, payload: 0-1479 (1480 bytes)]
- [Frame 96, payload: 1480-2007 (528 bytes)]
- [Fragment count: 2]
- [Reassembled IPv4 length: 2008]
- [Reassembled IPv4 data: 0800fc603007803373620aaaaaaaaaaaaaaaaaaaaaaaaaaaa...]
- Internet Control Message Protocol

The bottom screenshot shows a packet capture in Wireshark. The packet list pane shows a packet of type ICMP Echo (ping) request. The packet details pane shows the following information:

- Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0:00:00:00:00:00
- Ethernet II, Src: Axiomtek (08:00:00:00:00:00), Dst: Linksys (08:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 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: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x0751 [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)

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	38.936326	12.122.12.94	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	39.083658	192.168.1.102	192.233.206	ICP	62	ICP Retransmission 1482=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=3322) [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: Actifone_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.

The top screenshot shows a list of packets in Wireshark. The packets are filtered by 'Filter:'. The list includes various protocols such as ICMP, SSH, TCP, and IPv4. The bottom screenshot shows a detailed view of a specific packet (Frame 216) which is an IPv4 packet. The packet details are as follows:

- 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: Linksys_gd: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: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x0751 [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)

ip-ethereal-trace-1 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-112)]

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	38.936326	12.122.12.34	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	41.038058	192.168.1.102	199.2.53.206	TCP	62	[TCP Retransmission] 1483-831 [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=0, 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: Linksys_G: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)