

1/

No.	Time	Source	Destination	Protocol	Length	Info
10	2004-08-22 08:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	2004-08-22 08:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	2004-08-22 08:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	2004-08-22 08:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	2004-08-22 08:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	2004-08-22 08:48:02.916024	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	2004-08-22 08:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	2004-08-22 08:48:02.944369	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	2004-08-22 08:48:02.947102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19	2004-08-22 08:48:02.966009	12.123.40.218	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
20	2004-08-22 08:48:02.967100	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
21	2004-08-22 08:48:02.992672	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 10: 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)
v 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: 0x32d1 (13009)
 > Flags: 0x00
 Fragment Offset: 0
 > Time to Live: 2
 Protocol: ICMP (1)
 Header Checksum: 0x2c2b [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.102
 Destination Address: 128.59.23.100
 > Internet Control Message Protocol

According to the figure, the IP address of my computer is 192.168.1.102

2/ICMP (1)

3/

Header bytes: 20 (as seen in screenshot)

Payload bytes: 64 (total length 84 minus the 20 header bytes = 64)

4/

Fragment offset: 0

From the previous screenshot, we do not see any IPv4 fragments. We will see these later when we transmit longer ICMP echo requests.

5/

Identification field and time to live is incrementing

6/The following fields remain constant:

- version (IPv4 always used)
- header length (doesn't change since we are always using IPv4)
- source IP (my computer's IP address doesn't change)
- destination IP (usc.edu's IP address doesn't change)

- differentiated services (same protocol every time)
- upper layer protocol (same protocol every time)
- header checksum (verification disabled in my tests)

The following fields change:

- Identification field is incrementing (each IP datagram has a different ID)
- Time to live is also incrementing (this is how trace route works, as discussed in the assignment)

7/

They are incrementing with each datagram.

8/

No.	Time	Source	Destination	Protocol	Length	Info
7	2004-08-22 08:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	2004-08-22 08:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response)
9	2004-08-22 08:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	2004-08-22 08:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response)
11	2004-08-22 08:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	2004-08-22 08:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response)
13	2004-08-22 08:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	2004-08-22 08:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response)
15	2004-08-22 08:48:02.916024	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	2004-08-22 08:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response)
17	2004-08-22 08:48:02.944369	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	2004-08-22 08:48:02.947102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response)

> Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
 > Ethernet II, Src: Linksys_Gda: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)
 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]
 Source Address: 10.216.228.1
 Destination Address: 192.168.1.102
 > Internet Control Message Protocol

Identification: 40316

TTL: 255

9/

The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

The TTL field remains unchanged because the TTL for the first hop router is always the same.

10/

92	2004-08-22 08:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	2004-08-22 08:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	2004-08-22 08:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	2004-08-22 08:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	2004-08-22 08:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	2004-08-22 08:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	2004-08-22 08:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	2004-08-22 08:48:25.179081	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	2004-08-22 08:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!)
101	2004-08-22 08:48:25.188565	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> 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: 0x20, More fragments
Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x077b [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[\[Reassembled IPv4 in frame: 93\]](#)

> Data (1480 bytes)

0010 05 dc 32 f9 20 00 01 01 07 7b c0 a8 01 66 80 3b ..2.{...f.;

Yes, this packet has been fragmented across more than one IP datagram.

11/

The Flags bit for more fragments is set, indicating that the datagram has been fragmented. Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 1500, including the header.

12/

92	2004-08-22 08:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	2004-08-22 08:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	2004-08-22 08:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	2004-08-22 08:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	2004-08-22 08:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	2004-08-22 08:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	2004-08-22 08:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	2004-08-22 08:48:25.179081	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	2004-08-22 08:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!)
101	2004-08-22 08:48:25.188565	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> 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: 0x00
Fragment Offset: 1480
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0xa27a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]

> Internet Control Message Protocol

We can tell that this is not the first fragment, since the fragment offset is 1480. It is the last fragment, since the more fragments flag is not set.

13/

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

14/

216	2004-08-22 08:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	2004-08-22 08:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	2004-08-22 08:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	2004-08-22 08:48:40.144138	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	2004-08-22 08:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	2004-08-22 08:48:40.151305	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]

> 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: 0x20, More fragments

Fragment Offset: 0

> Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x0751 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

[Reassembled IPv4 in frame: 218]

> Data (1480 bytes)

After switching to 3500, there are 3 packets created from the original datagram.

15/

The IP header fields that changed between all of the packets are: fragment offset, and checksum. Between the first two packets and the last packet, we see a change in total length, and also in the flags. The first two packets have a total length of 1500, with the more fragments bit set to 1, and the last packet has a total length of 540, with the more fragments bit set to 0.