Computer Networks Lab 6

Shane Cincotta

May 11, 2020

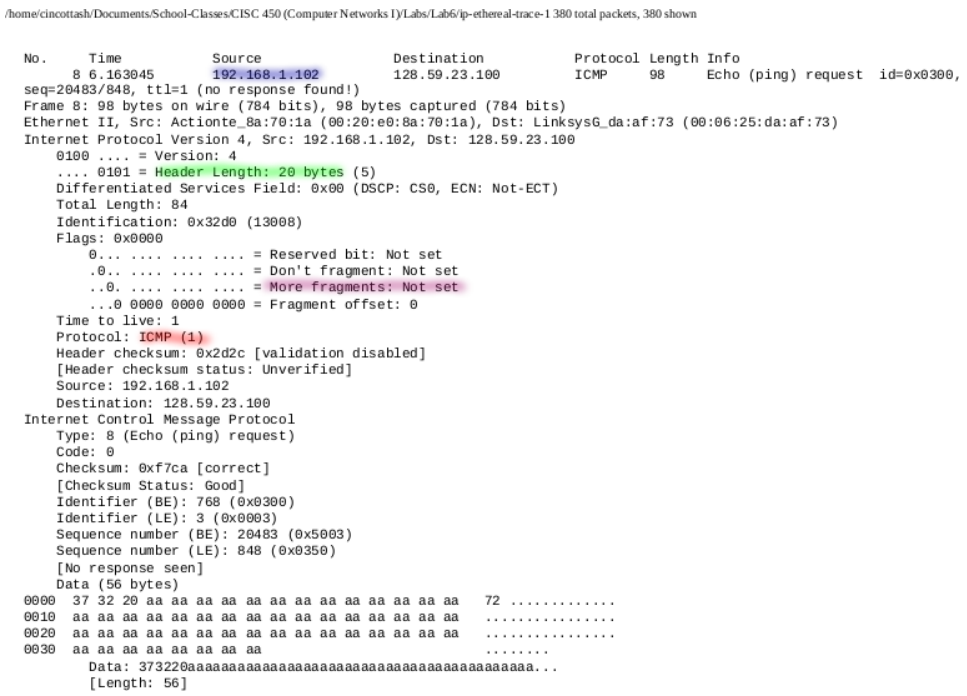


Figure 1:

What is the IP address of your computer?

According to figure 1, the IP address of my computer is 192.168.1.102.

Within the IP packet header, what is the value in the upper layer protocol field?

According to figure 1, the value in the upper layer protocol field is ICMP (1).

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.

According to figure 1, there are 20 bytes in the IP header. There are 36 bytes in the payload. This can be calculated by subtracting the IP header size (20) from the total data size (56).

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

According to figure 1, the data has not been fragmented. This can be determined by by the value of the more fragments bit, which is set to 0.

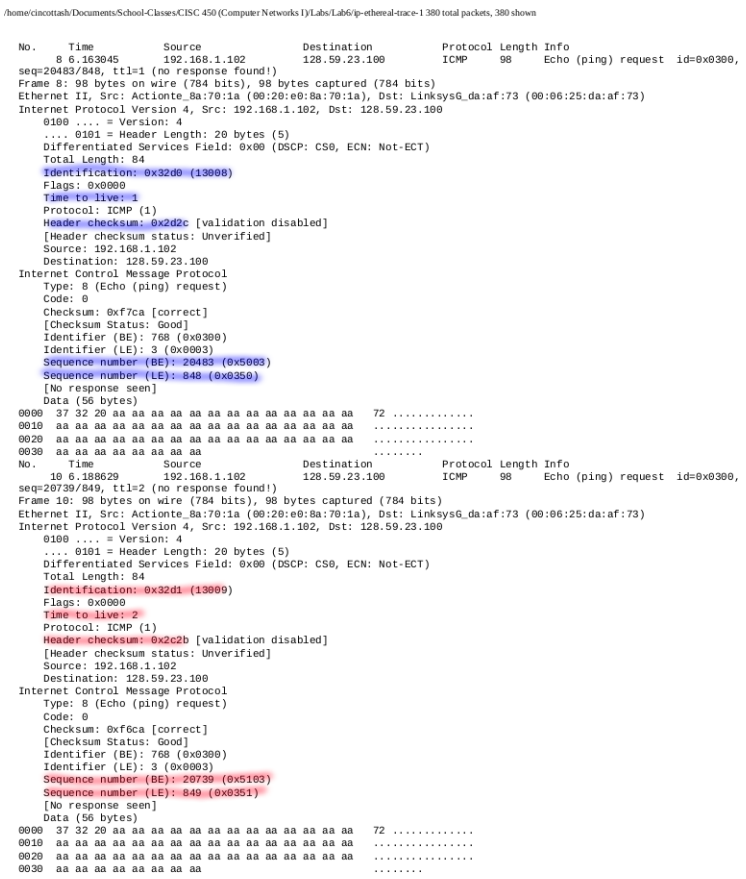


Figure 2:

Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

According to figure 2, the Identification, Time to live, Header checksum and sequence number never change.

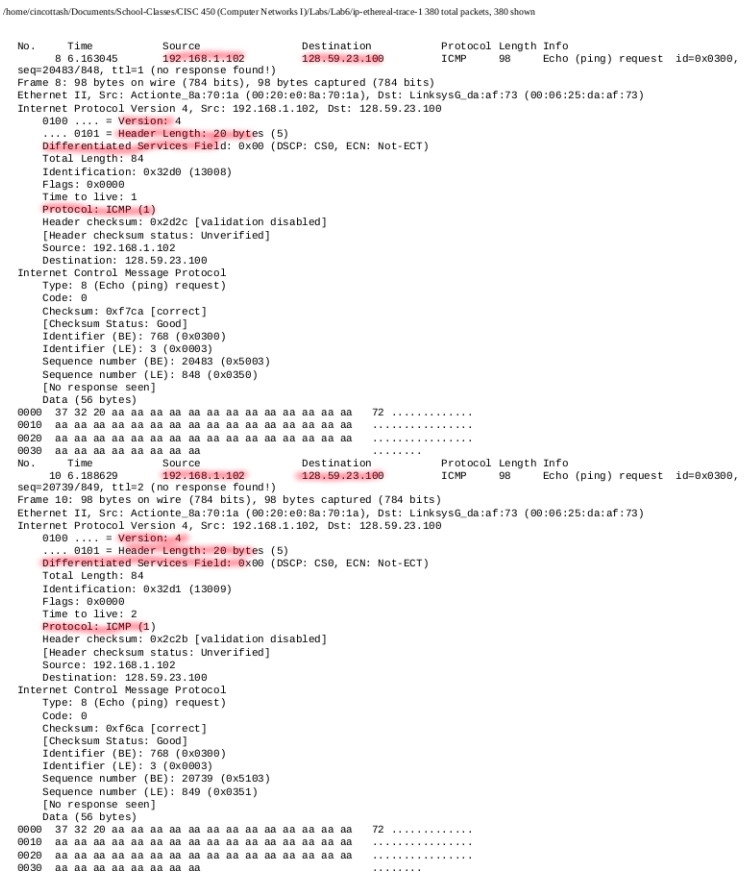


Figure 3:

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

According to figure 3: version, header length, source IP, destination IP differentiated services and upper layer protocol all remain constant.

The fields that must stay constant are: version (because we are using IPv4), header length (because each packet is ICMP), source IP (because we are sending from the same source PC), destination IP (because we are sending to the same source PC), differentiated services (because each packet is ICMP thus they use the same type of service) and upper layer protocol (because each packet is ICMP).

The fields that must change are: identification (because each packet has a different ID), time to live (because each TTL is incremented after each packet) and header checksum (because the checksum changes along with the header).

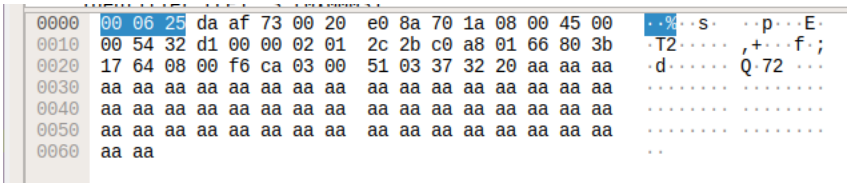


Figure 4:

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

According to figure 4, the pattern I observe is that the IP header Identification fields increment after each ICMP Echo.

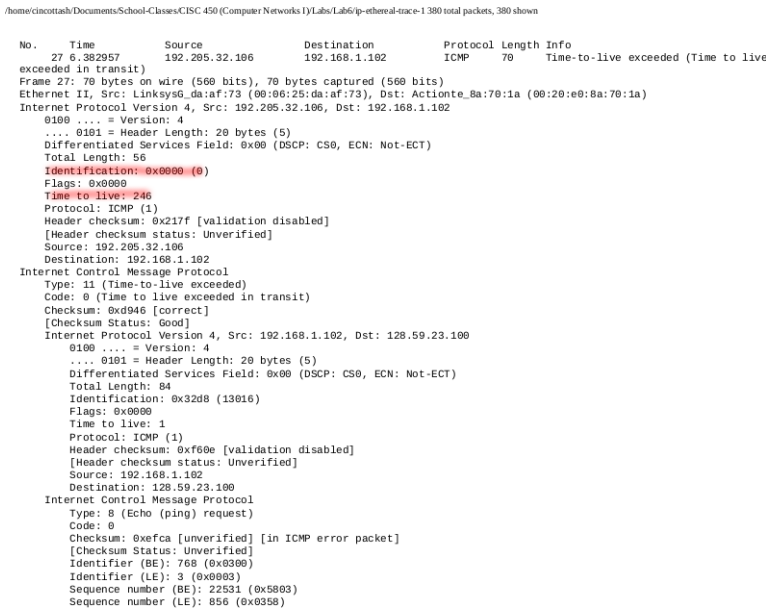


Figure 5:

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

According to figure 5, the value of the indentification field is 0 and the value of the TTL field is 246.

Figure 6:

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

According to figure 6, the identification field does not change. The reason for this is when two or more IP datagrams have the same ID value, they are fragments of a larger IP datagram.

According to figure 6, the TTL fields remains unchanged because the TTL for the first hop router is always the same.

```
92 28.441511    192.168.1.102    128.59.23.100    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #
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
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 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=32fb) [Reassembled in #
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
99 28.520729    192.168.1.102    128.59.23.100    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #
```

Figure 7:

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?

According to figure 7, this packet has been fragmented across more than one IP diagram.

```
/home/cincottash/Documents/School-Classes/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-trace-1 380 total packets, 380 shown

No.     Time           Source                Destination           Protocol Length Info
     92 28.441511      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)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    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
        ...0 0000 0000 0000 = 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)
```

Figure 8:

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?

According to figure 8, the flags bit for more fragments is set, this tells us that the datagram is fragmented. Also, since the fragment offset is 0, we know that this is the first fragment. This datagram has a total length of 1500 (1480 + header size).

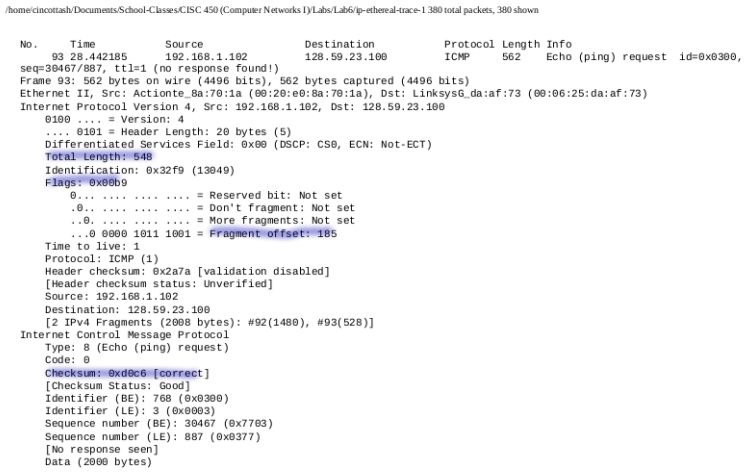
```
/home/cincottash/Documents/School-Classes/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-trace-1 380 total packets, 380 shown

No.     Time           Source                Destination           Protocol Length Info
     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!)
Frame 96: 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: 0x32fa (13050)
    Flags: 0x00b9
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 1011 1001 = Fragment offset: 185
    Time to live: 2
    Protocol: ICMP (1)
    Header checksum: 0x2979 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [2 IPv4 Fragments (2008 bytes): #95(1480), #96(528)]
Internet Control Message Protocol
```

Figure 9:

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?

According to figure 9, we can tell that this is not the first fragment because the fragment offset is 185, also we know it is the last fragment because the more fragments flag is not set.



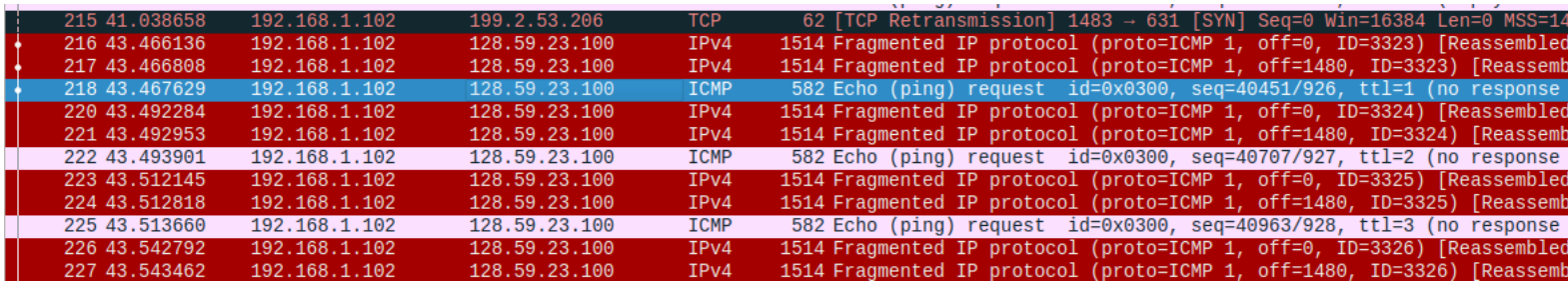
```
/home/cincottash/Documents/School-Classes/CISC 450 (Computer Networks I)/Labs/Lab6/ip-ethereal-trace-1 380 total packets, 380 shown

No.     Time           Source                Destination           Protocol Length Info
     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!)
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
        ...0 0000 1011 1001 = Fragment offset: 185
    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)]
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd0c6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
    Identifier (LE): 3 (0x0003)
    Sequence number (BE): 30467 (0x7703)
    Sequence number (LE): 887 (0x0377)
    [No response seen]
    Data (2000 bytes)
```

Figure 10:

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

According to figure 10, we can see that the total length, checksum, flags and dragment offset are changed.



```
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=14
216 43.466136   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled
217 43.466808   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassemb
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
220 43.492284   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled
221 43.492953   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassemb
222 43.493901   192.168.1.102   128.59.23.100   ICMP   582 Echo (ping) request  id=0x0300, seq=40707/927, ttl=2 (no response
223 43.512145   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled
224 43.512818   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassemb
225 43.513660   192.168.1.102   128.59.23.100   ICMP   582 Echo (ping) request  id=0x0300, seq=40963/928, ttl=3 (no response
226 43.542792   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3326) [Reassembled
227 43.543462   192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3326) [Reassemb
```

Figure 11:

How many fragments were created from the original datagram?

According to figure 11, after switching to 3500, there are 3 packets created.

Figure 12:

What fields change in the IP header among the fragments?

According to figure 12, the fragment offset and checksum change among the fragments.