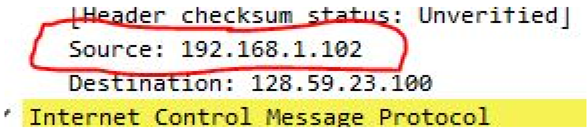
Joel Huffman
CS372-400 Spring 2019

**NOTE: Due to pingplotter no longer working on Windows, all results for this lab were pulled from the provided ip-ethereal-trace-1 file.*

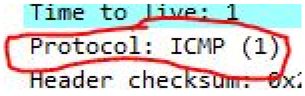
1. **Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?**



```
 [Header checksum status: Unverified]
 Source: 192.168.1.102
 Destination: 128.59.23.100
Internet Control Message Protocol
```

IP address: 192.168.1.102

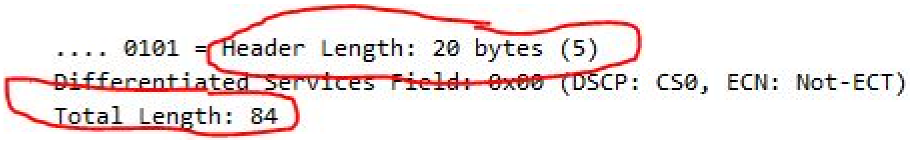
2. **Within the IP packet header, what is the value in the upper layer protocol field?**



```
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x
```

Protocol: ICMP (1)

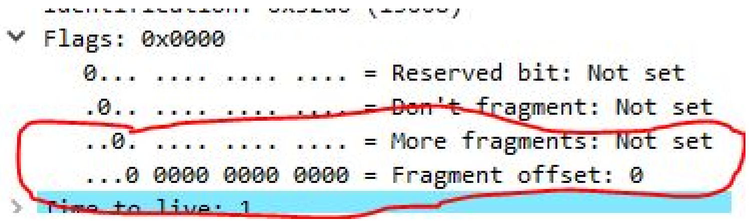
3. **How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.**



```
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
```

IP header: 20 bytes
IP Payload: 64 bytes
Total Length - Header Length = Payload Length
84 bytes - 20 bytes = 64 bytes

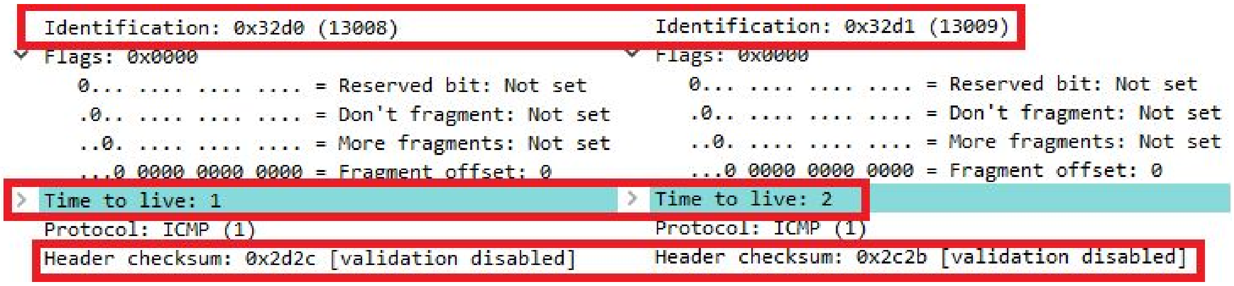
4. **Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.**



```
Flags: 0x0000
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not set
   ..0. .... .... .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 1
```

The datagram hasn't been fragmented. We know the datagram hasn't been fragmented because both the More fragments flag and Fragment offset field are 0. If either were non-zero values then we would know this datagram is a fragment.

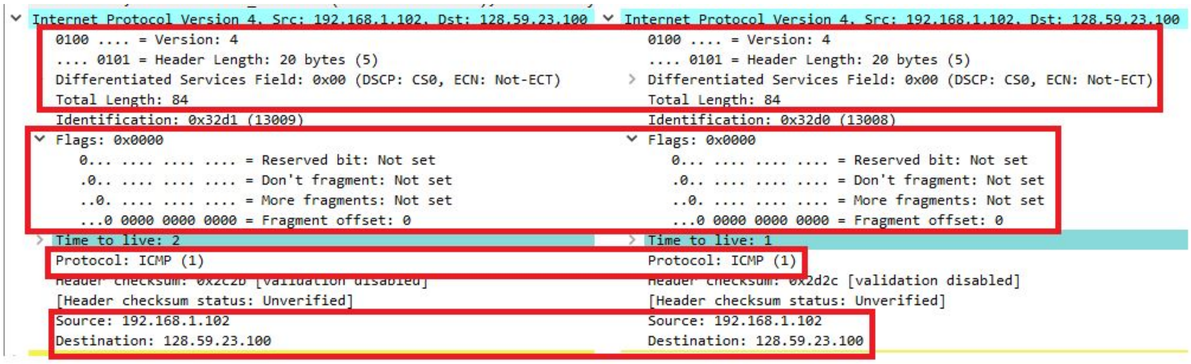
5. **Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?**



```
Identification: 0x32d0 (13008)                          Identification: 0x32d1 (13009)
Flags: 0x0000                                           Flags: 0x0000
   0... .... .... .... = Reserved bit: Not set             0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not set           .0.. .... .... .... = Don't fragment: Not set
   ..0. .... .... .... = More fragments: Not set           ..0. .... .... .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment offset: 0                ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 1                                         Time to live: 2
Protocol: ICMP (1)                                      Protocol: ICMP (1)
Header checksum: 0x2d2c [validation disabled]           Header checksum: 0x2c2b [validation disabled]
```

Identification, TTL and Header checksum always change from datagram to datagram.

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



```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100    Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
   0100 .... = Version: 4                                                 0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)                                .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)          Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 84                                                       Total Length: 84
   Identification: 0x32d1 (13009)                                         Identification: 0x32d0 (13008)
   Flags: 0x0000                                                          Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set                            0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set                          .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set                          ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0                               ...0 0000 0000 0000 = Fragment offset: 0
   Time to live: 2                                                        Time to live: 1
   Protocol: ICMP (1)                                                     Protocol: ICMP (1)
   Header checksum: 0x2c2b [validation disabled]                          Header checksum: 0x2d2c [validation disabled]
   [Header checksum status: Unverified]                                   [Header checksum status: Unverified]
   Source: 192.168.1.102                                                  Source: 192.168.1.102
   Destination: 128.59.23.100                                             Destination: 128.59.23.100
```

IP Version, Header Length, Differentiated Service Field, Total Length, Flags, Protocol, Source and Destination all remain constant. Of these, the following must remain constant for their provided reason:

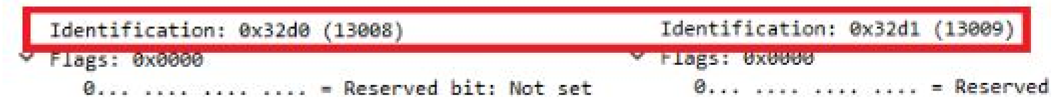
- IP Version
  - We aren't going to switch to IPv6 mid-way through sending data.
- Header Length
  - All of these datagrams are ICMP packets, thus the same header size
- Protocol
  - All of these datagrams are ICMP packets and will list as so
- Source
  - All of these datagrams are coming from the same place
- Destination
  - All of these datagrams are going to the same place

The fields listed in question 5 (Identification, TTL and Header checksum) are all required to change for each datagram for the following reasons:

- Identification
  - Each packet needs a unique identifier, otherwise we can't distinguish between different packets
- TTL
  - Increases to test for great number of hops between source and destination

- Header checksum
    - The checksum for the header changes because the header contents is changing for each datagram

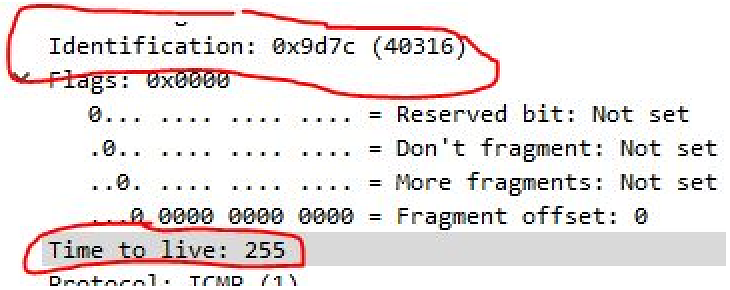
7. **Describe the pattern you see in the values in the Identification field of the IP datagram**



```
Identification: 0x32d0 (13008)                          Identification: 0x32d1 (13009)
Flags: 0x0000                                           Flags: 0x0000
  0... .... .... .... = Reserved bit: Not set             0... .... .... .... = Reserved
```

The identification field is one greater than the previous datagram.

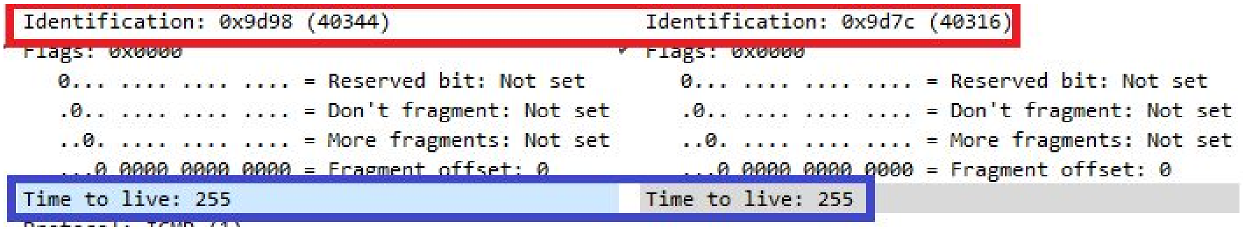
8. **What is the value in the Identification field and the TTL field?**



```
Identification: 0x9d7c (40316)
Flags: 0x0000
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not set
   ..0. .... .... .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
```

Identification: 40316
TTL: 255

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?**

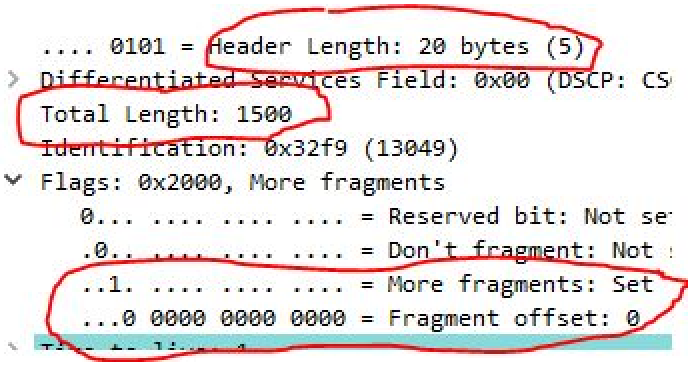


```
Identification: 0x9d98 (40344)                        Identification: 0x9d7c (40316)
Flags: 0x0000                                         Flags: 0x0000
   0... .... .... .... = Reserved bit: Not set           0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not set         .0.. .... .... .... = Don't fragment: Not set
   ..0. .... .... .... = More fragments: Not set         ..0. .... .... .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment offset: 0              ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255                                     Time to live: 255
```

The Identification field changes so the datagrams can still be uniquely identified, but the TTL field remains constant because these are all jumps to the same router.

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? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]**

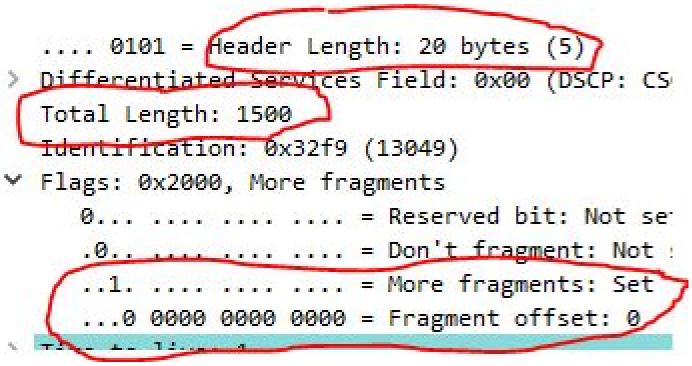
Joel Huffman
CS372-400 Spring 2019



```
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS
  Total Length: 1500
  Identification: 0x32f9 (13049)
v Flags: 0x2000, More fragments
    0... .... .... .... = Reserved bit: Not se
    .0.. .... .... .... = Don't fragment: Not
    ..1. .... .... .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment offset: 0
```

Yes, this message has been fragmented as seen by the More fragments flag being set.

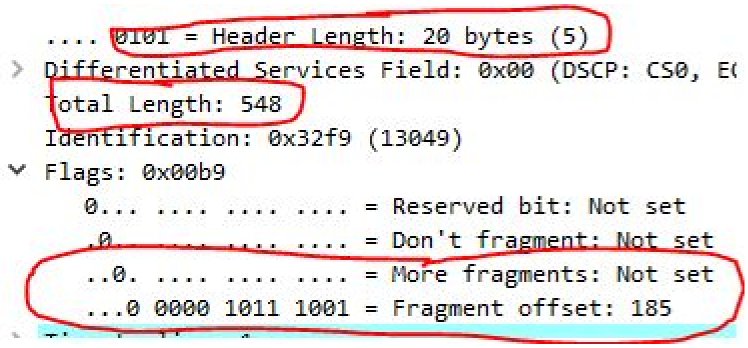
11. **Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?**



```
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS
  Total Length: 1500
  Identification: 0x32f9 (13049)
v Flags: 0x2000, More fragments
    0... .... .... .... = Reserved bit: Not se
    .0.. .... .... .... = Don't fragment: Not
    ..1. .... .... .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment offset: 0
```

The More fragments flag being set shows that this datagram is fragmented. The Fragment offset of 0 shows that this is the first fragment of the fragmented message. If the offset was greater than one it would be the second or greater fragment. This datagram is 1500 bytes including the body and header. The payload is 1480 bytes (Total Length - Header Length).

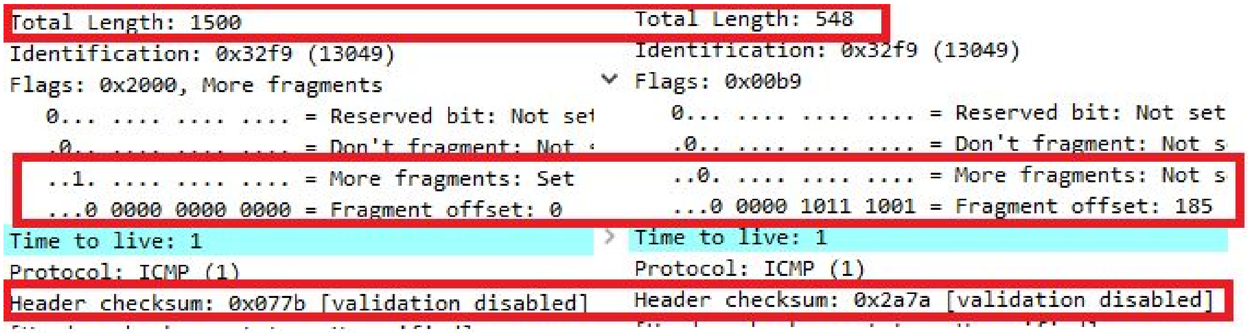
12. **Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?**



```
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, E(
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
```

We know this isn't the first fragment because the Fragment offset is not 0. There are no more fragments to this message because the More fragments flag is not set.

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

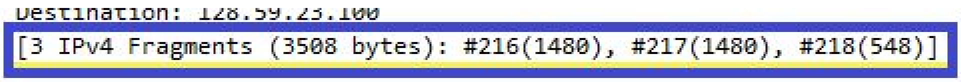


```
Total Length: 1500
Identification: 0x32f9 (13049)
Flags: 0x2000, More fragments
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not s
   ..1. .... .... .... = More fragments: Set
   ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x077b [validation disabled]
```

```
Total Length: 548
Identification: 0x32f9 (13049)
Flags: 0x00b9
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not s
   ..0. .... .... .... = More fragments: Not s
   ...0 0000 1011 1001 = Fragment offset: 185
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2a7a [validation disabled]
```

Total Length, More fragments flag, Fragment offset and Header checksum.

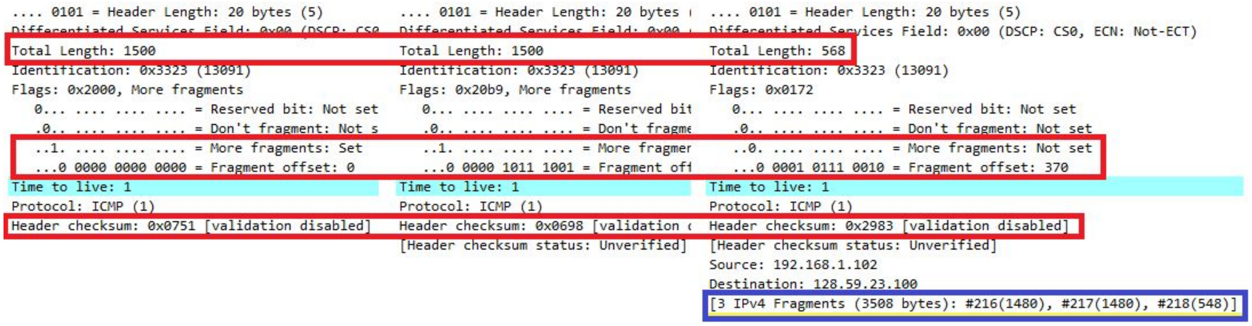
14. How many fragments were created from the original datagram?



```
Destination: 128.59.23.100
[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
```

Three fragments were created.

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



```
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x2000, More fragments
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not s
   ..1. .... .... .... = More fragments: Set
   ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0751 [validation disabled]
```

```
.... 0101 = Header Length: 20 bytes (
Differentiated Services Field: 0x00 (
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x20b9, More fragments
   0... .... .... .... = Reserved bit
   .0.. .... .... .... = Don't fragme
   ..1. .... .... .... = More fragmer
   ...0 0000 1011 1001 = Fragment off
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0698 [validation (
[Header checksum status: Unverified]
```

```
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 568
Identification: 0x3323 (13091)
Flags: 0x0172
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not set
   ..0. .... .... .... = More fragments: Not set
   ...0 0001 0111 0010 = Fragment offset: 370
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2983 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.102
Destination: 128.59.23.100
[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
```

Total Length was different for the last fragment. The More fragments flag was changed for the last fragment. The Fragment offset was different for each fragment. The header checksum changed for each fragment.