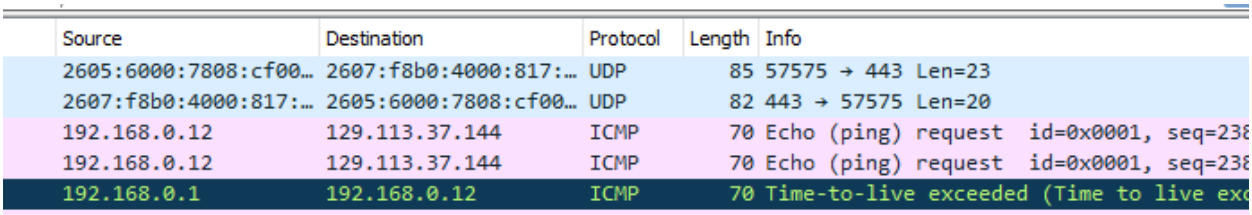
Juan Bermudez
12/6/18
CMPE 4345
#20158030

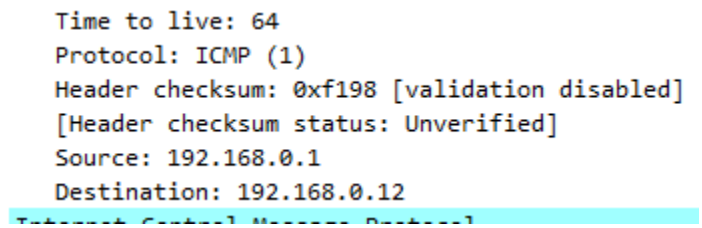
Lab 05: IP

1.What is the IP address of your computer?
192.168.0.12



| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 2605:6000:7808:cf00… | 2607:f8b0:4000:817:… | UDP | 85 | 57575 → 443 Len=23 |
| 2607:f8b0:4000:817:… | 2605:6000:7808:cf00… | UDP | 82 | 443 → 57575 Len=20 |
| 192.168.0.12 | 129.113.37.144 | ICMP | 70 | Echo (ping) request id=0x0001, seq=238 |
| 192.168.0.12 | 129.113.37.144 | ICMP | 70 | Echo (ping) request id=0x0001, seq=238 |
| 192.168.0.1 | 192.168.0.12 | ICMP | 70 | Time-to-live exceeded (Time to live exc |

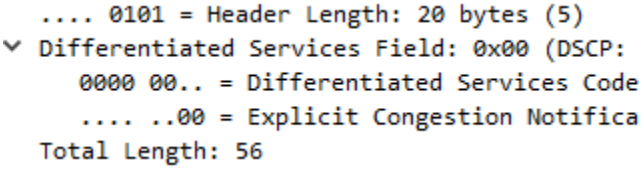
2. Within the IP packet header, what is the value in the upper layer protocol field?
ICMP(1)



```
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xf198 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.1
Destination: 192.168.0.12
```

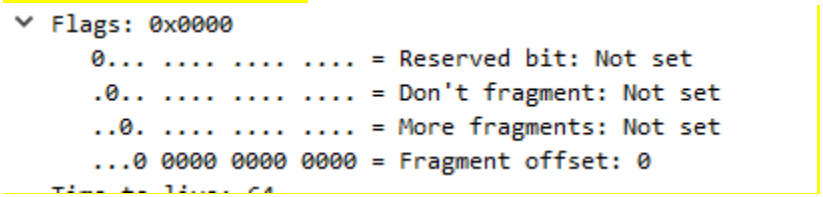
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

The header length is 20 bytes
The payload bytes are 36, by subtracting 56 total length – 20 header length



```
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP:
    0000 00.. = Differentiated Services Code
    .... ..00 = Explicit Congestion Notifica
Total Length: 56
```

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
No, according to the flags



```
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
```

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?

The checksum, identification, and sequence number always change

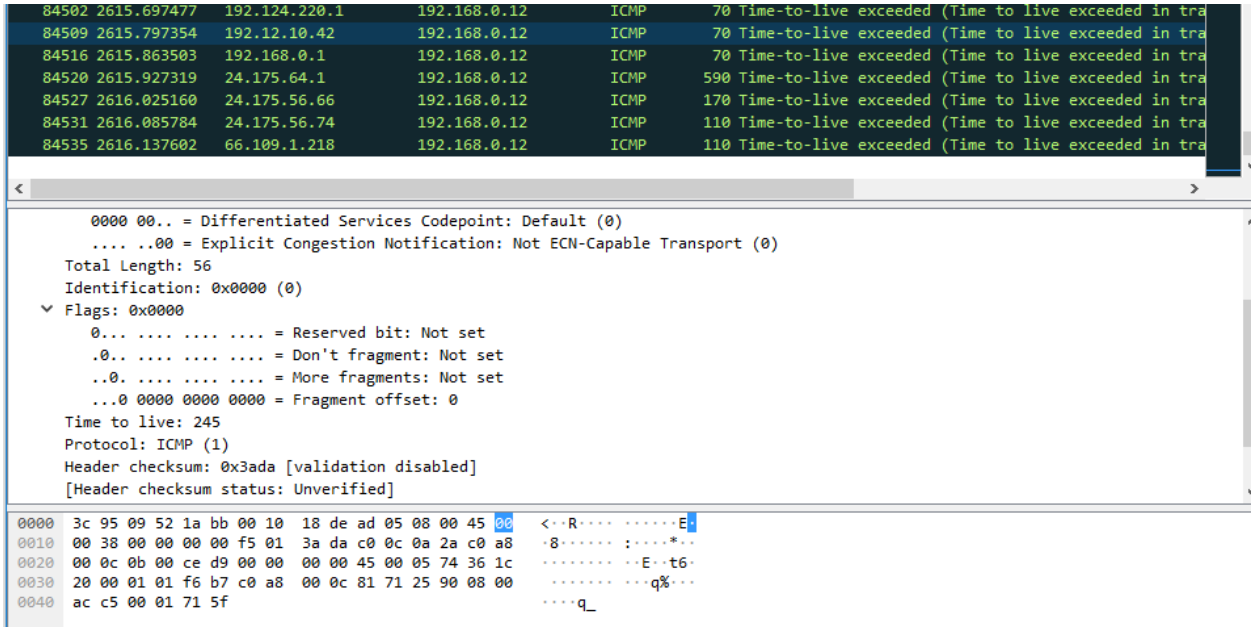
6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

constant – the fragmentation is constant because it is fixed to 56 bytes as well the time to live. The header length will also remain at 20 bytes. The flags change if there is a fragment, and the sequence number changes per packet

Changing- the fragmentation number changes so it is in sequence with the next chunk. The checksum changes as it passes through a router.

7. Describe the pattern you see in the values in the Identification field of the IP datagram
The identification numbers increase going up the wireshark packet list, and decrease as they go down the list

8. What is the value in the Identification field and the TTL field?
TTL exceed: 245
identification: 0

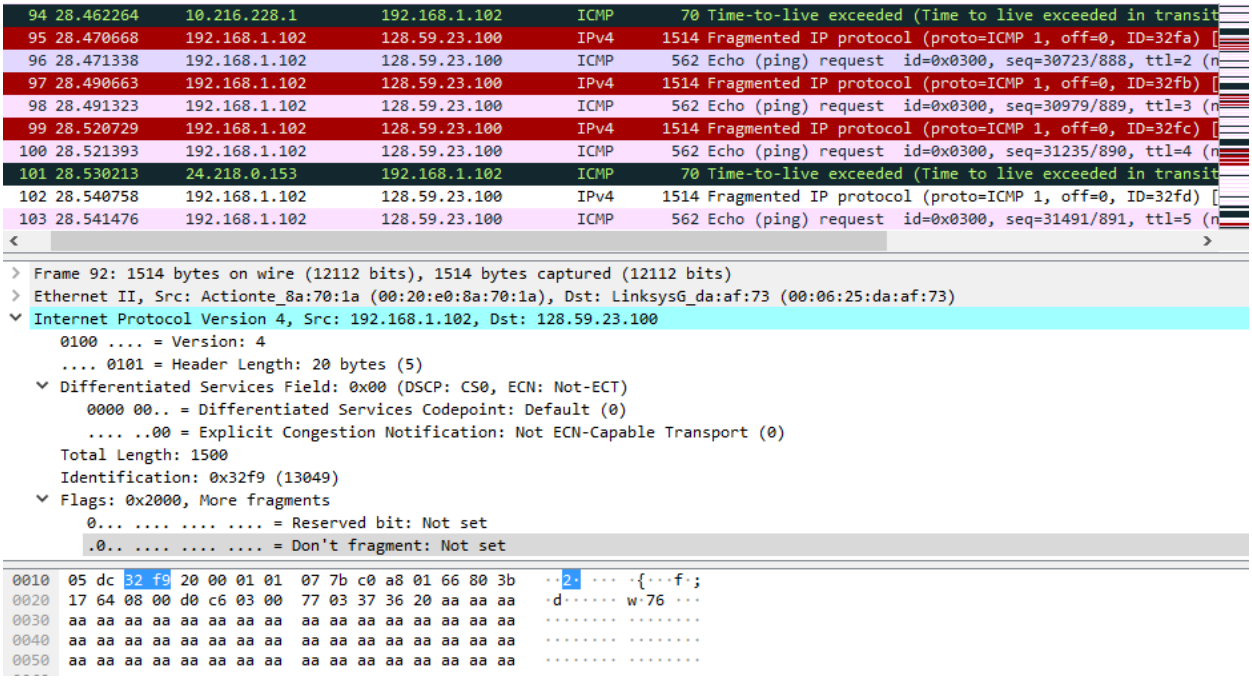



9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The TTL remains constant, but the identification will change per hop

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 was fragmented across more than one 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 more fragment flag  bit is set to 1 -indicates datagram is fragmented.
The fragment offset is set to 0 - indicates that this is the first fragment.
The datagram's total length is set to 1500

```
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
```

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 IP header has fragment offset to 1480 which shows it is the second part of the incoming first fragment. The fragment flag is set, which means there is an incoming fragment.

```
221 43.492953   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324)
220 43.492284   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [R
218 43.467629   192.168.1.102   128.59.23.100   ICMP    582 Echo (ping) request  id=0x0300, seq=40451/926, ttl=1 (no
217 43.466808   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323)
216 43.466136   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [R
215 41.038658   192.168.1.102   199.2.53.206    TCP      62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Le
205 38.756348   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=40195/925, ttl=13 (r
```

```
  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: 0x3324 (13092)
  Flags: 0x20b9, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
      ...0 0000 1011 1001 = Fragment offset: 185
  > Time to live: 2
    Protocol: ICMP (1)
    Header checksum: 0x0597 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    Reassembled IPv4 in frame: 222
  Data (1480 bytes)
```

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

The fragment offset flag changes and the header checksum

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

I was not able to find the packets with length 3500 bytes in the IPthereal trace 1

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

Some fields that may have changed are the fragment offset, the time to live, checksum, sequence number, and the fragment sizes