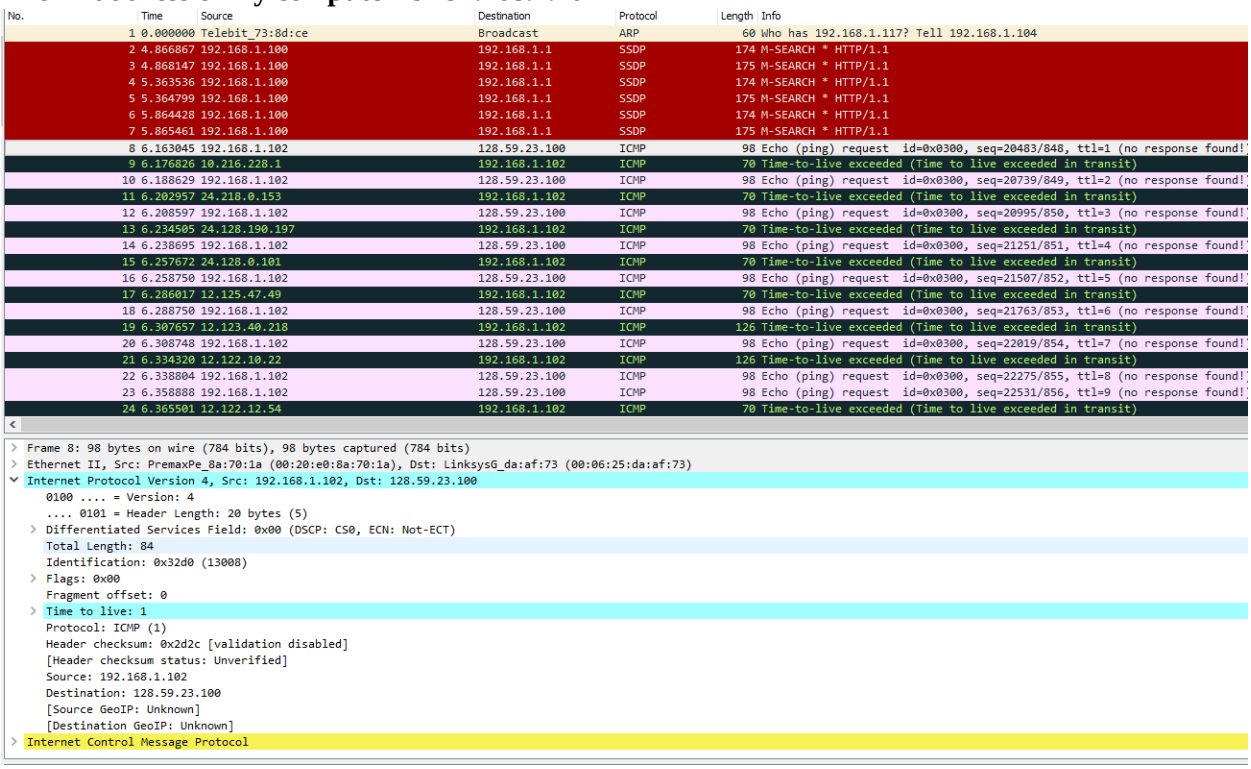
Brandon Lo
CS372 Lab 4
11/19/17

1. What is the IP address of your computer?

The IP address of my computer is 192.168.1.102



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	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
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	24.128.190.197	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	12.123.40.218	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
20	6.308748	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
22	6.338804	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!
23	6.358888	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22531/856, ttl=9 (no response found!
24	6.365501	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```
> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: PremaxPe_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: 0x32d0 (13008)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> Internet Control Message Protocol
```

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

ICMP is in the upper layer protocol field

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.

Based off the datagram, the header is 20 bytes and the total length is 84 bytes. Thus the payload is 64 bytes since 84-20 = 64.

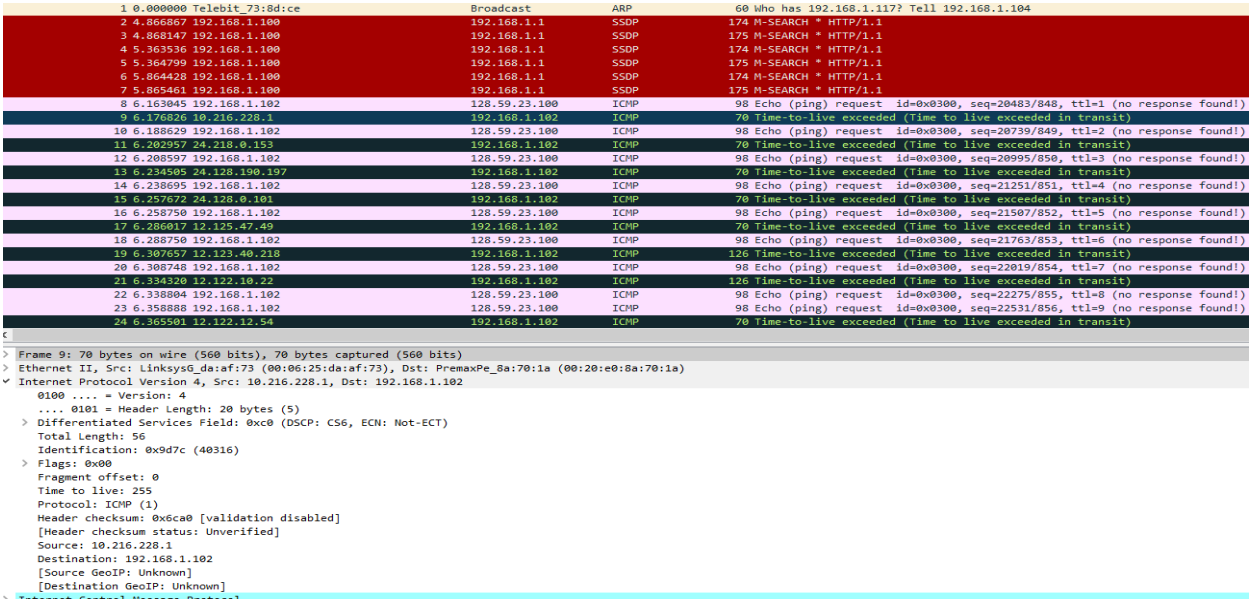
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

No the datagram has not been fragmented since the More fragments flag has not been set.

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, Time to live, and header checksum changes between thus series of datagrams

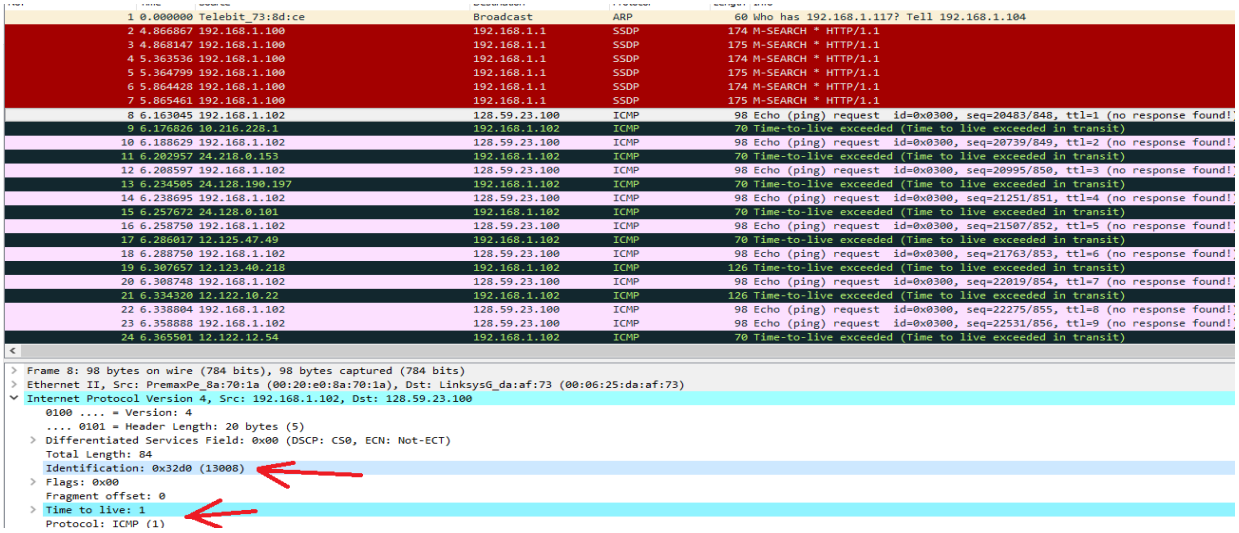
Brandon Lo
CS372 Lab 4
11/19/17



6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
   The Version, Header Length, Total Length, Flags, Fragment Offset, Protocol, Source, and Destination stay the same (everything but Identification, Time to Live and Header checksum).
   The protocol, source, destination and flags never change since it is the same data that being sent between devices.
   The identification and time to live must change since those are unique information that is important to identify between packets and is independent of the data.
   The header checksum changes because the header changes, therefore the checksum is different.
7. Describe the pattern you see in the values in the Identification field of the IP Datagram
   The pattern I see in the values in the Identification field is that it increments by 1 everytime.
8. What is the value in the Identification field and the TTL field?

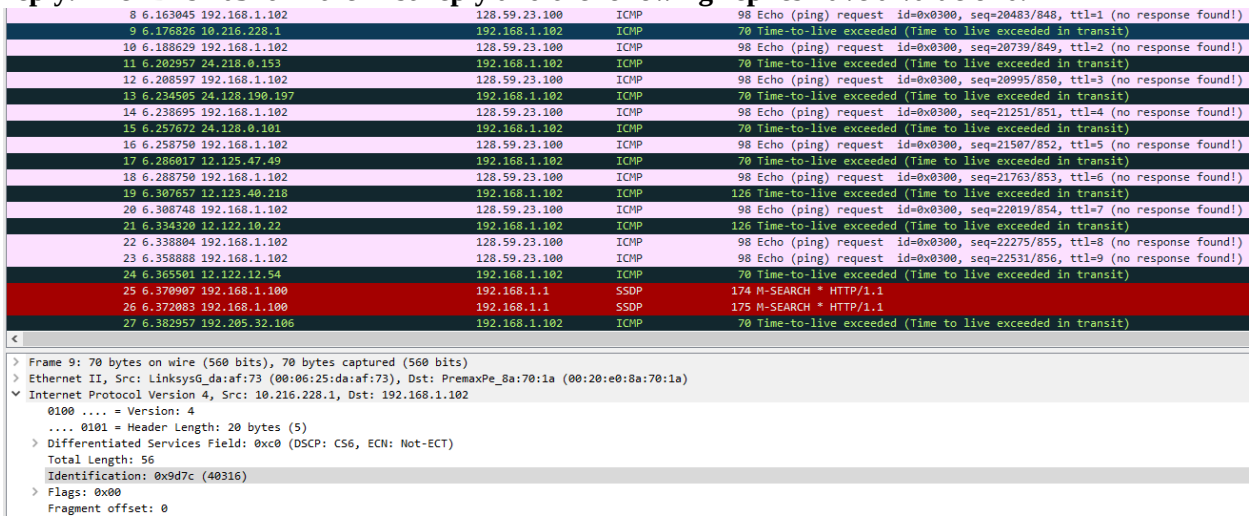
   The identification field is 13008 and the TLL is 1.

Brandon Lo
CS372 Lab 4
11/19/17

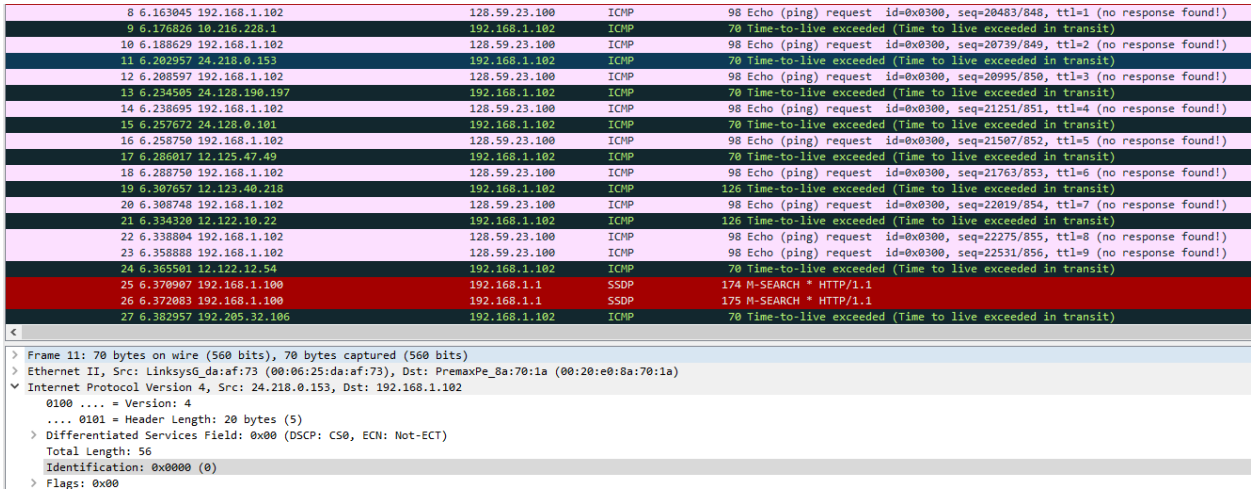


9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

No the values do not remain unchanged, the TTL decrements starting at 255 with each reply. The ID is 40316 in the first reply and the following replies have a value of 0.

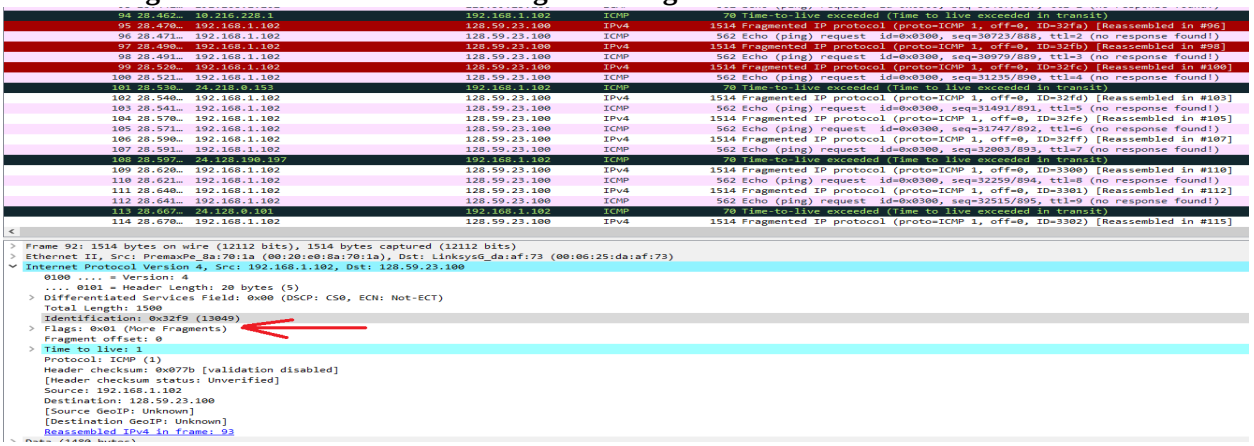


Brandon Lo
CS372 Lab 4
11/19/17



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?

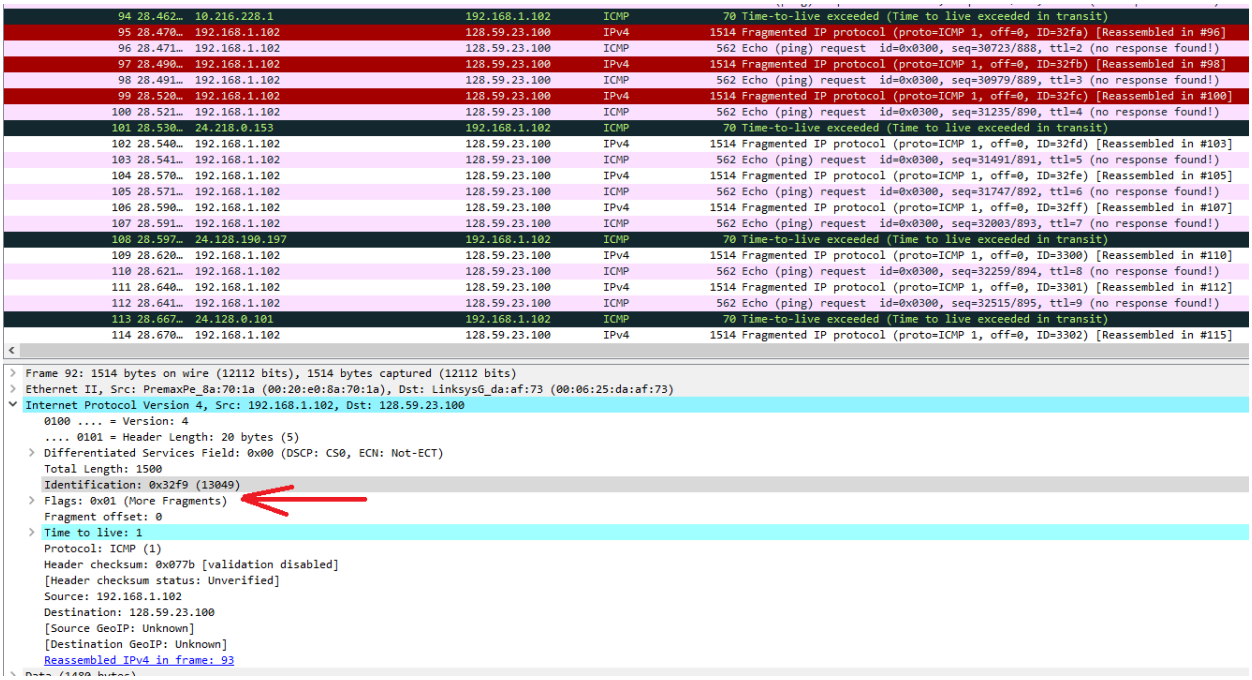
Yes it is fragmented because the More Fragments flag is set.



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?

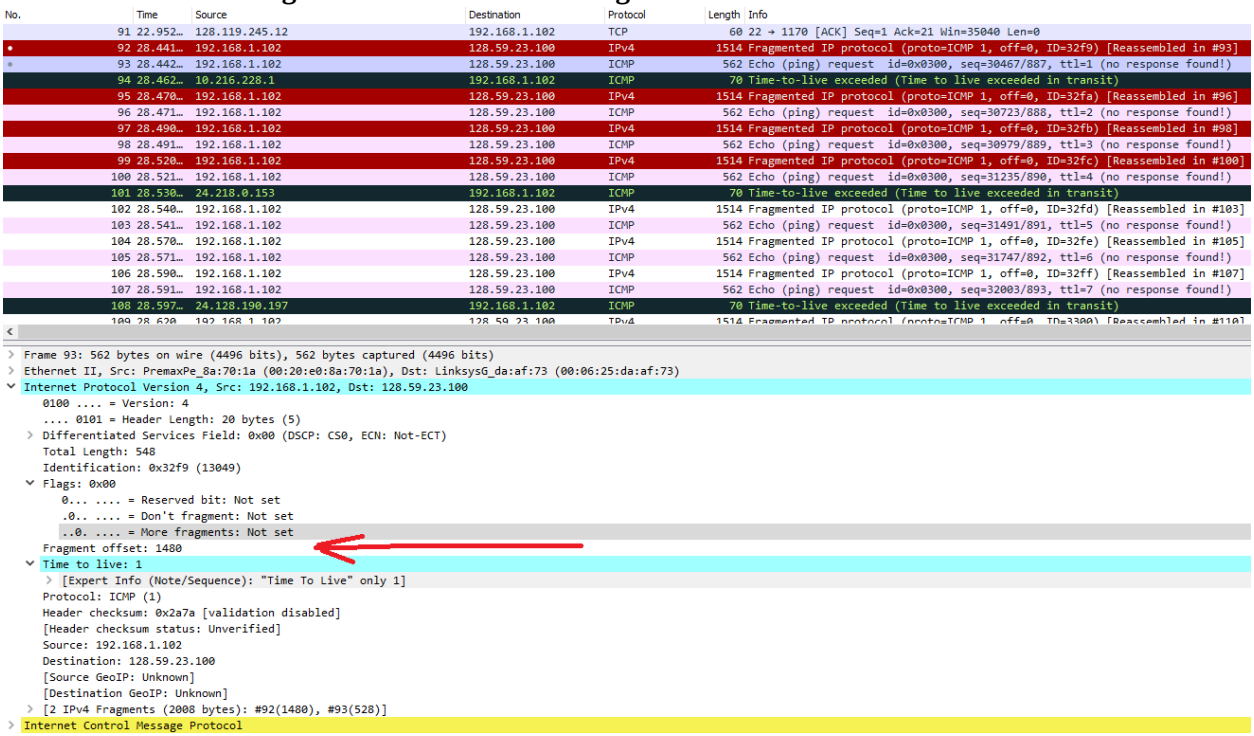
The More Fragments flag being set indicates that the datagram is fragemented. From the information you know that it is the beginning of the fragment because Fragment offset is 0. The entire datagram is 2008 bytes. There are 2 fragments with the first being 1500 bytes (+20 byte header) and the second is 546 bytes (20 byte header). From the second fragment offset being 1480, 1480+580 (total size)-20(header) = 2008 bytes

Brandon Lo
CS372 Lab 4
11/19/17



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

You know that it is the second fragment of the IP datagram since there is a nonzero number in the fragment offset.
There are no more fragments since the More Fragments is not set.



Brandon Lo
CS372 Lab 4
11/19/17

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

    The fields that changed were the Total Length, More Segments Flag, Fragment Offset, and Header Checksum.
14. How many fragments were created from the original datagram?

    2 Fragments were created form the original datagram
15. What fields change in the IP header among the fragments?

    The fields that changed were the Total Length, More Segments Flag, Fragment Offset, and Header Checksum. The length changes because there is max size of 1500 bytes (+20 byte header), so all fragments will have a size of 1500 until the final fragments which will have the remainder.
    The More Segments Flag changes to indicate there is more information to be sent. Thus the final fragment will not have the More Segments Flag set, shown by the second fragment.
    The Fragment Offset differs to indicate how the fragments will be set.
    The Header Checksum differs since the data within the header changes.