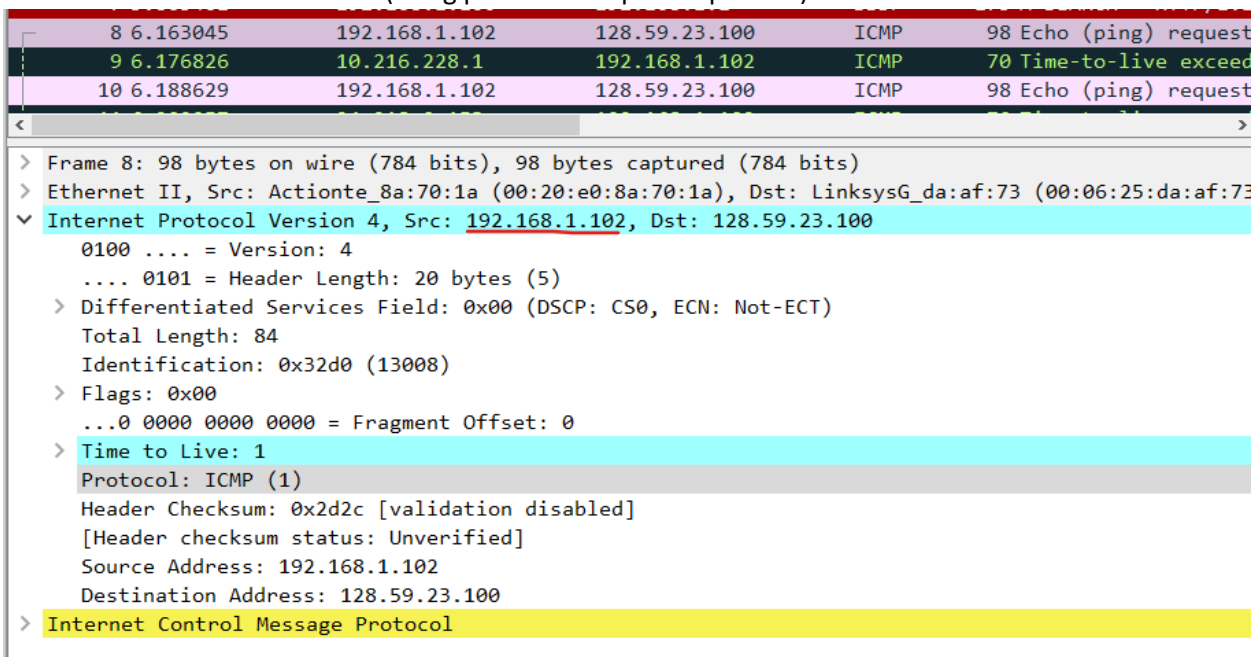
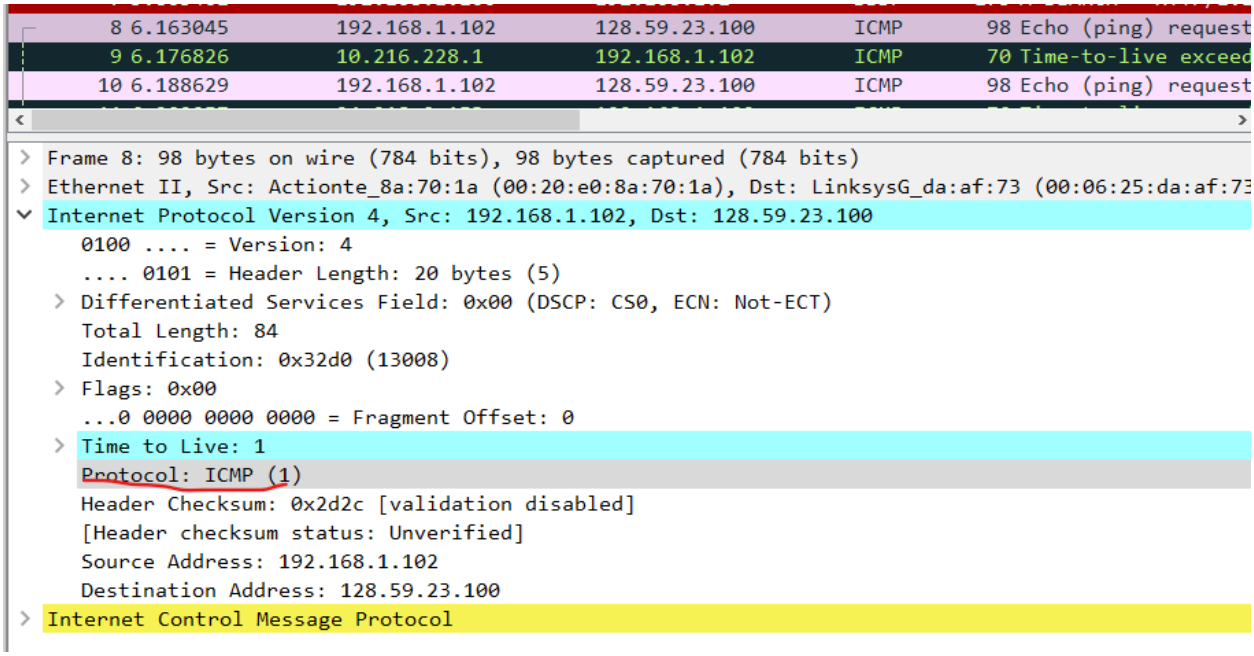
COMP 3203 Wireshark 6

Name: Nirmith Victor D'Almeida
Number: 101160124

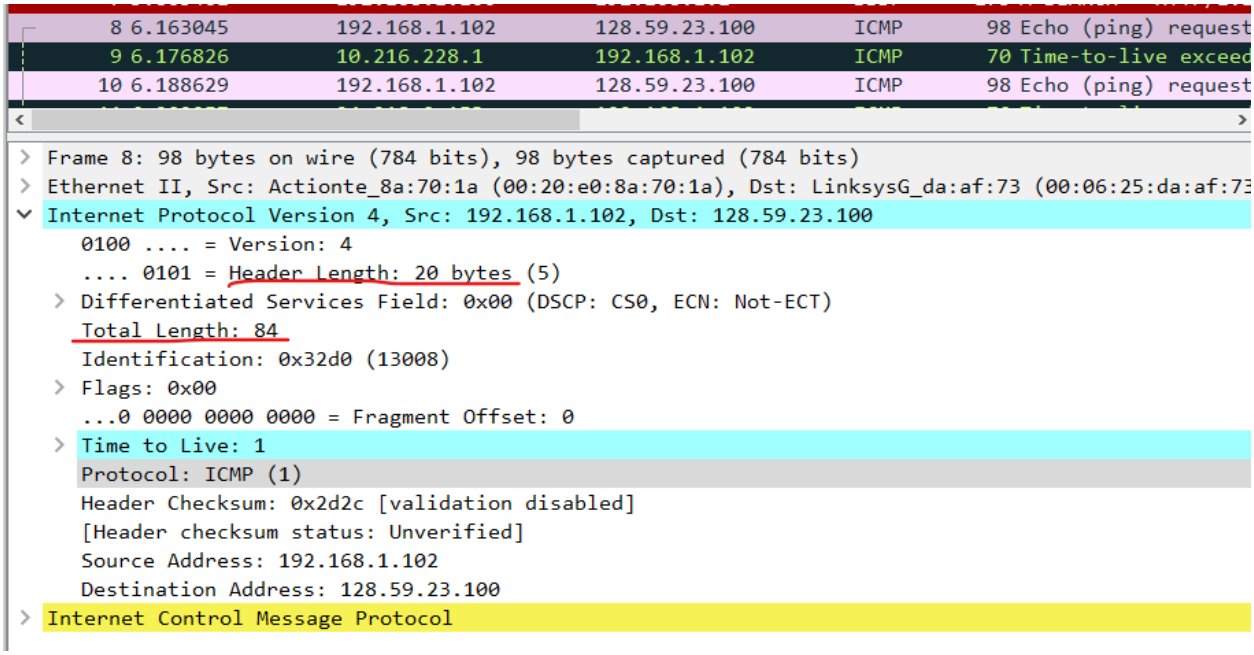
1. The IP address is 192.168.1.102 (using professors captured packets)



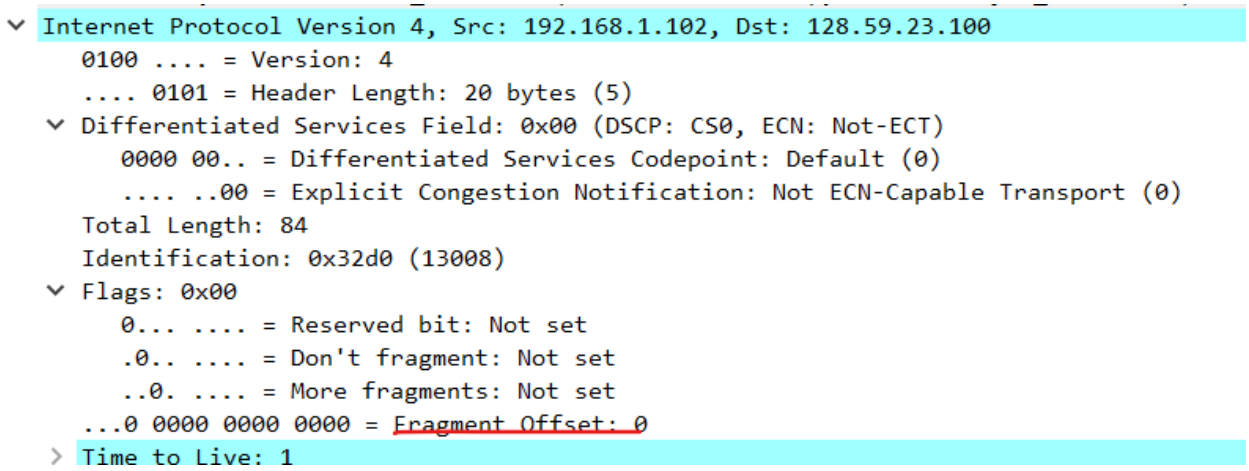
2. ICMP (0 X 01)



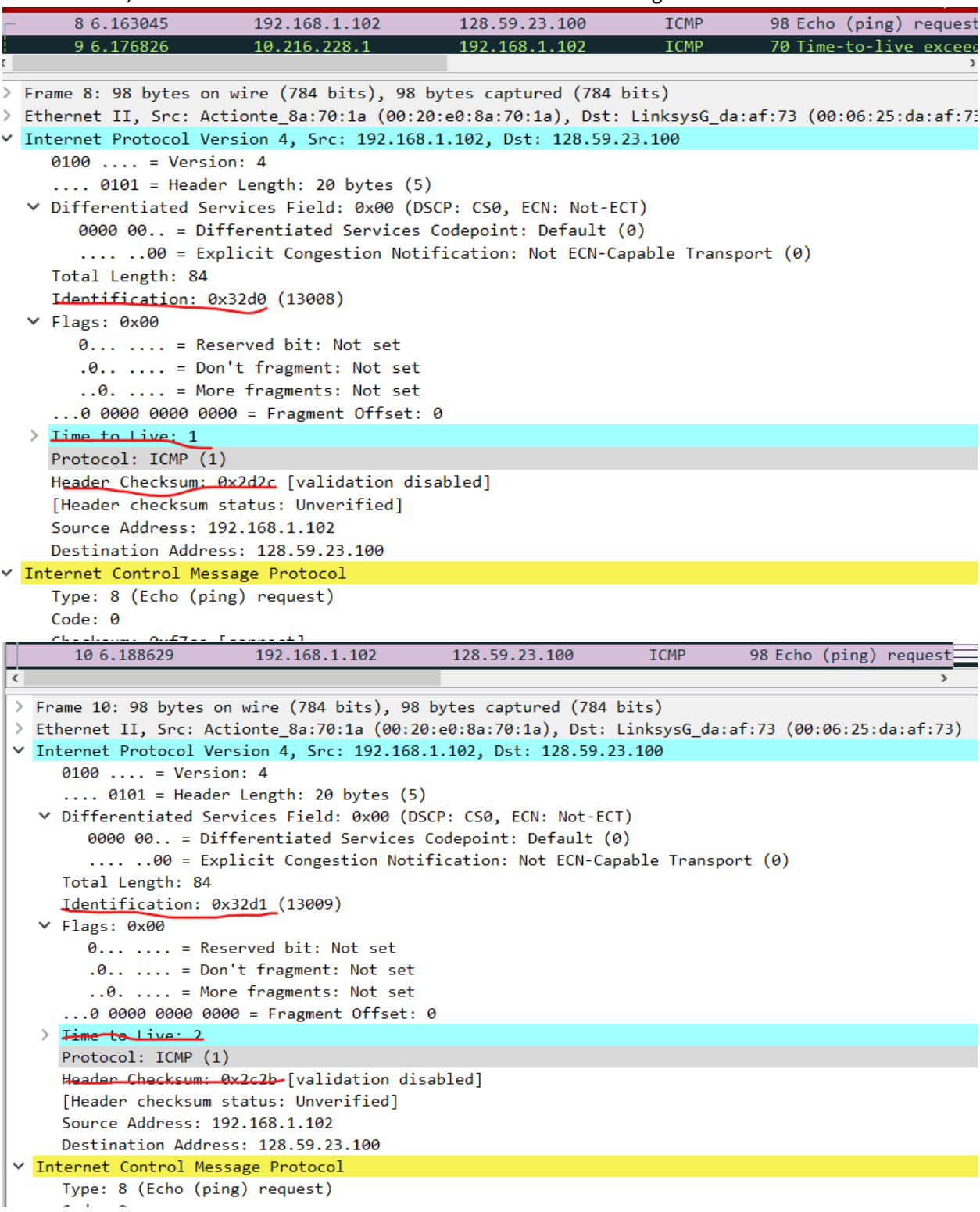
3. There are 20 bytes in the header with a total length of 84 bytes this gives us 64 bytes in the payload of the IP datagram.



4. The data is not fragmented since the fragment offset = 0



5. Identification, Time to live and header checksum are the ones to change



6.

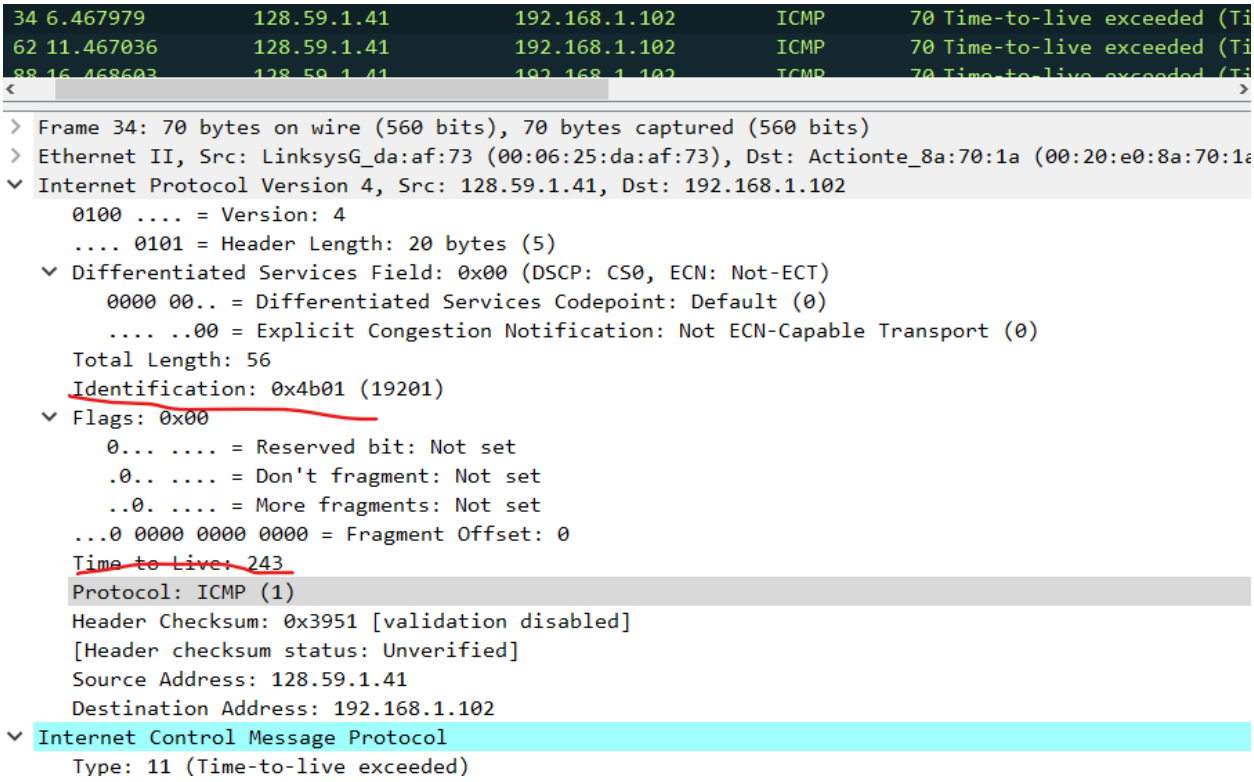
a. Version, header length, Differentiated Services Field, flags fragment offset), Source and destination address (using image referenced above for question 5)

b. Fields that must stay constant:
Version, header length, Differentiated Services Field, flags fragment offset), Source and destination address (using image referenced above for question 5)

c. Fields that must change:
Identification, Time to Live, header checksum

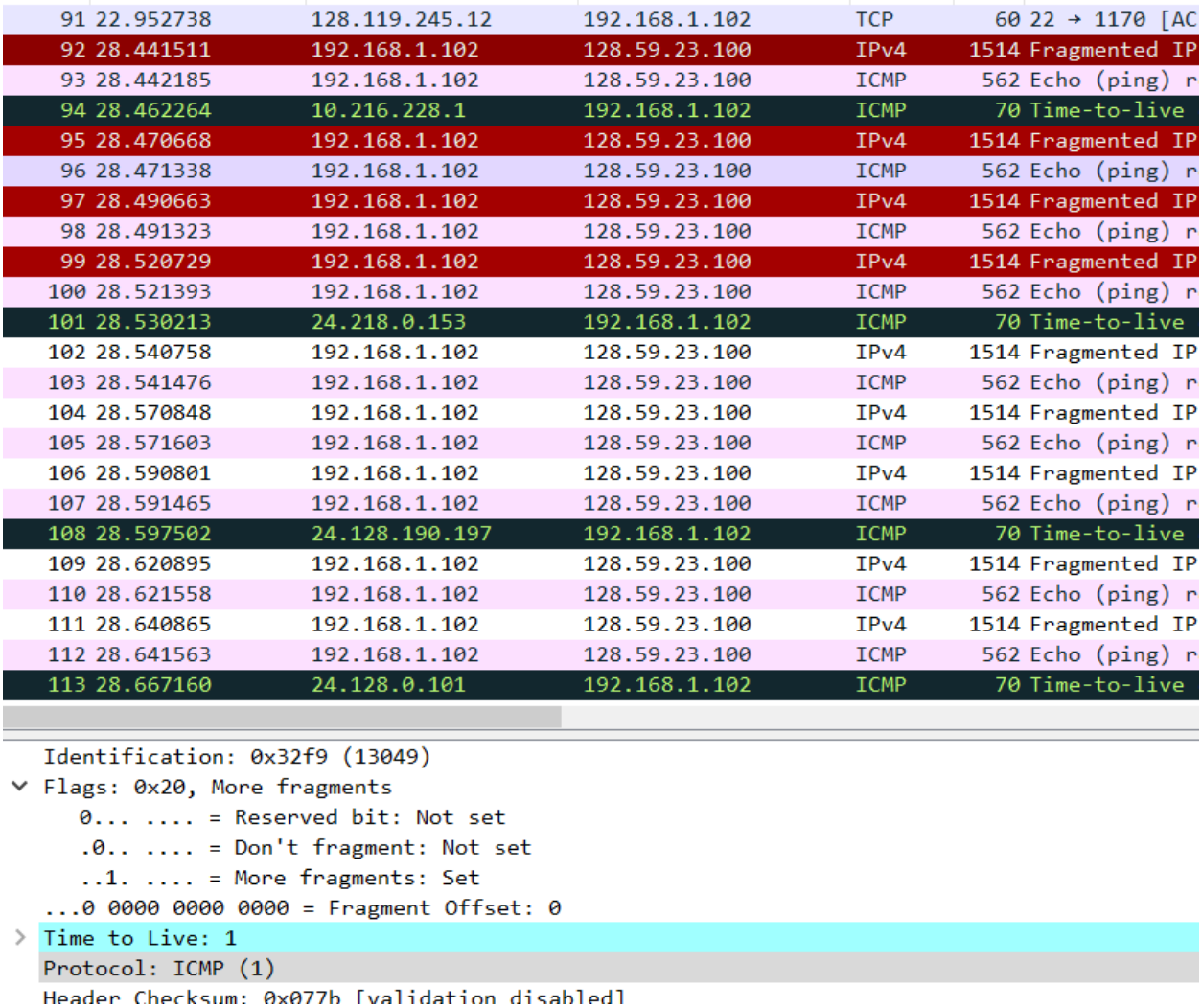
7. Increment by one number for the Identification for each ICMP message.

8. Time to live 243 and Identification is 0 X 4b01



9. Identification keeps changing but time to live remains constant (for downloaded packetts professors) The Identification changes since it is a unique value.

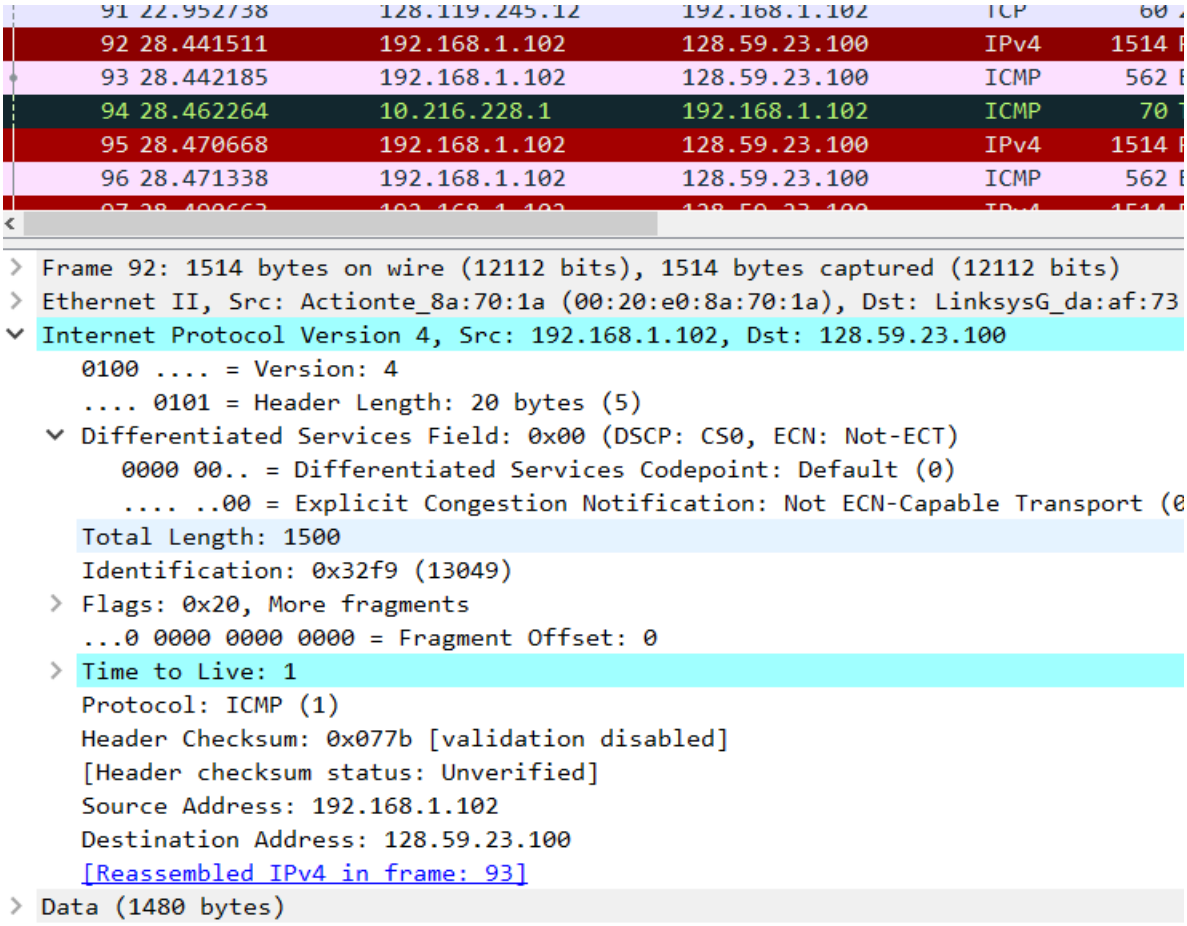
10. Yes this packet has been fragmented across more than one IP datagram.



91	22.952738	128.119.245.12	192.168.1.102	TCP	60 22 → 1170 [AC
92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
101	28.530213	24.218.0.153	192.168.1.102	ICMP	70 Time-to-live
102	28.540758	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
103	28.541476	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
104	28.570848	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
105	28.571603	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
106	28.590801	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
107	28.591465	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
108	28.597502	24.128.190.197	192.168.1.102	ICMP	70 Time-to-live
109	28.620895	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
110	28.621558	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
111	28.640865	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP
112	28.641563	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) r
113	28.667160	24.128.0.101	192.168.1.102	ICMP	70 Time-to-live

```
Identification: 0x32f9 (13049)
Flags: 0x20, 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]
```

11.



Since there is more fragments set we know that it is fragmented.
Since the fragment offset is set to 0 we find out that it is the first segment.
The IP Datagram data is 1480 not including the header (1500 inclusive of header).

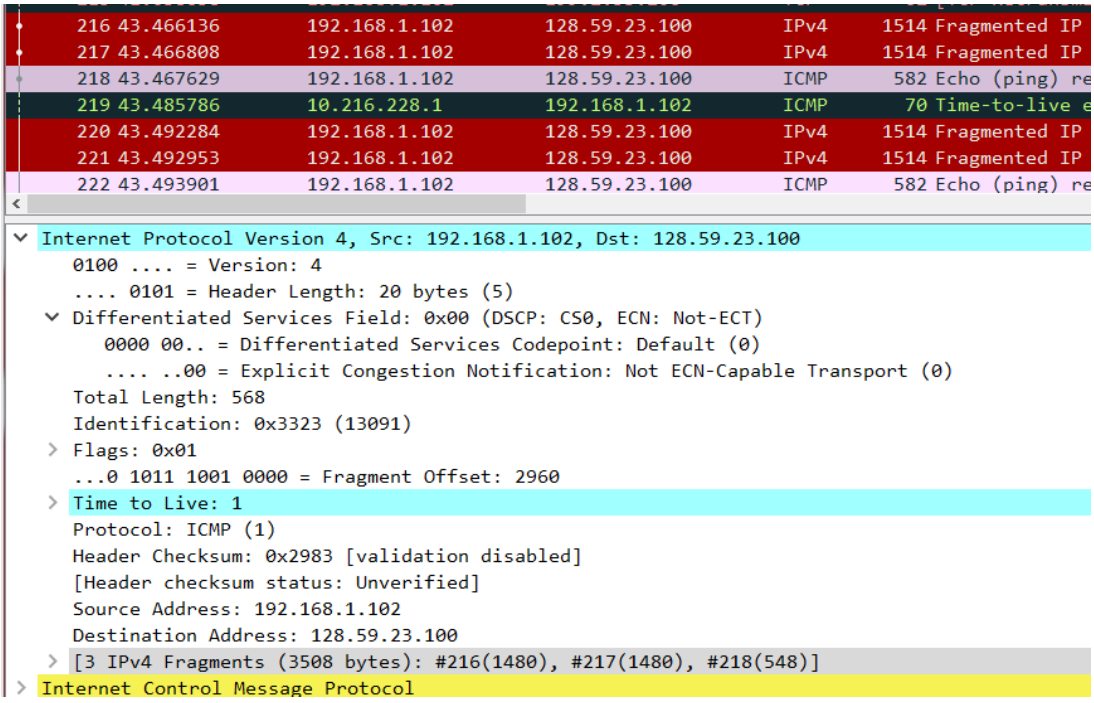
12.

```
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable T
  Total Length: 548
  Identification: 0x32f9 (13049)
▾ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment Offset: 1480
▸ Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2a7a [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)]
    [Frame: 92, payload: 0-1479 (1480 bytes)]
    [Frame: 93, payload: 1480-2007 (528 bytes)]
    [Fragment count: 2]
    [Reassembled IPv4 length: 2008]
```

More fragment is not set and Fragment offset is 1480.

13. Length, Fragment offset, checksum and flags (using q 12 and 11 image for reference)

14. There are 3 Fragments.



15. The Fragment offset changes along with header checksum and total length.