Universidad Tècnica Particular de Loja

Nombre: Alex Plascencia
Jessica Dávila

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.

```
   4809 312.697585     172.16.50.53          172.17.95.132         ICMP     62     Echo (ping) request  id=0xd8a0, seq=0/0,
ttl=63 (no response found!)
Frame 4809: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: CiscoInc_b5:f8:00 (00:1c:0f:b5:f8:00), Dst: IntelCor_b1:a4:ae (00:1c:bf:b1:a4:ae)
Internet Protocol Version 4, Src: 172.16.50.53, Dst: 172.17.95.132
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x0000 (0)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 63
    Protocol: ICMP (1)
    Header checksum: 0x51f2 [validation disabled]
    Source: 172.16.50.53
    Destination: 172.17.95.132
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

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

172.16.50.53

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

ICMP1 62

3. How many bytes are in the IP header? 20
How many bytes are in the payload of the IP datagram? 28
Explain how you determined the number of payload bytes.
Se resta del tamaño total del paquete ip menos el tamaño de la cabecera.

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

No està fragmentado dado que los paquetes se fragmenta automáticamente cuando exceda 1500 bytes y este no excede.

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

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?

- Identificaciòn
- Suma de comprobación de la cabecera
- Source
- Desplazamiento del fragmento.
- Time to live
- Destino
- Tamaño total

6. Which fields stay constant?

- Protocolo
- Versión
- Tamaño de cabecera
- Campo de servicio diferenciado

Which of the fields must stay constant?

- Protocolo
- versión
- Tamaño de cabecera.

Which fields must change? Why?

El origen y el destino dado que se intercambian entre las solicitud y la respuesta.

7. Describe the pattern you see in the values in the Identification field of the IP datagram Next (with the packets still sorted by source address) find the series of ICMP TTL- exceeded replies sent to your computer by the nearest (first hop) router.

Los valores de identificación de cada paquete mientras llegan a uno de los routers varia ligeramente pero al cambiar a otro router la identificar identificaciòn varía aún más.

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

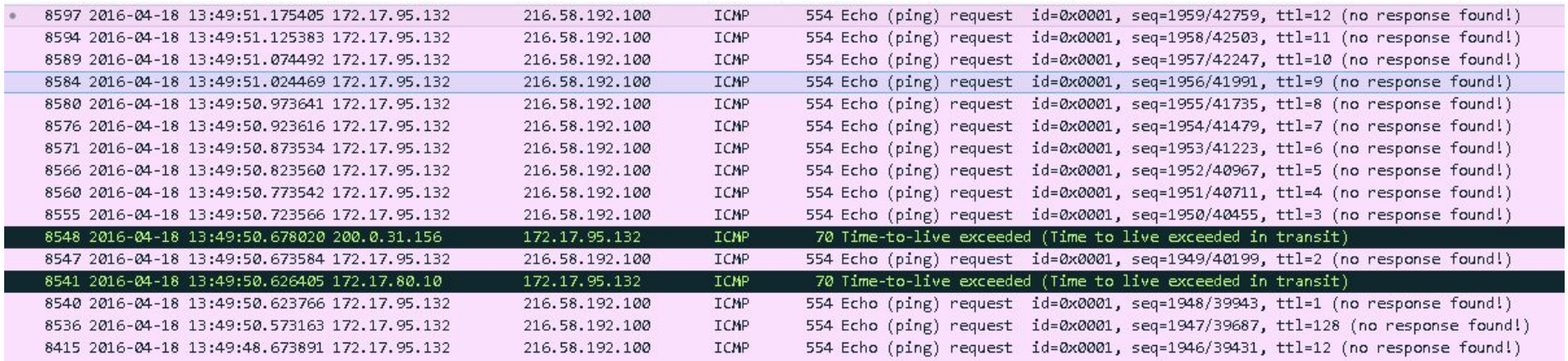
Identificaciòn:	0x0000
Time to live:	63

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?

El ttl se mantiene igual dado que indica el límite de nodos por los que del paquete pasará antes de ser rechazado pero la identificaciòn cambia.

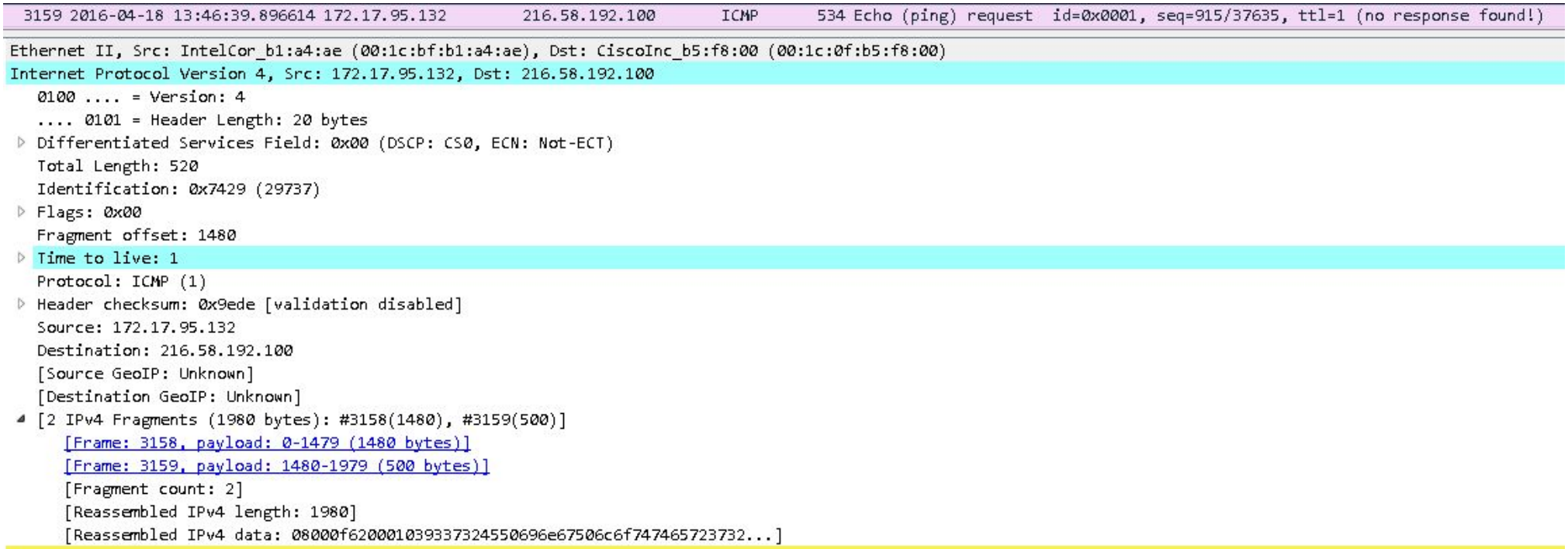
Fragmentation

Sort the packet listing according to time again by clicking on the Time column



8597	2016-04-18 13:49:51.175405	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1959/42759, ttl=12 (no response found!)
8594	2016-04-18 13:49:51.125383	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1958/42503, ttl=11 (no response found!)
8589	2016-04-18 13:49:51.074492	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1957/42247, ttl=10 (no response found!)
8584	2016-04-18 13:49:51.024469	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1956/41991, ttl=9 (no response found!)
8580	2016-04-18 13:49:50.973641	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1955/41735, ttl=8 (no response found!)
8576	2016-04-18 13:49:50.923616	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1954/41479, ttl=7 (no response found!)
8571	2016-04-18 13:49:50.873534	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1953/41223, ttl=6 (no response found!)
8566	2016-04-18 13:49:50.823560	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1952/40967, ttl=5 (no response found!)
8560	2016-04-18 13:49:50.773542	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1951/40711, ttl=4 (no response found!)
8555	2016-04-18 13:49:50.723566	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1950/40455, ttl=3 (no response found!)
8548	2016-04-18 13:49:50.678020	200.0.31.156	172.17.95.132	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
8547	2016-04-18 13:49:50.673584	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1949/40199, ttl=2 (no response found!)
8541	2016-04-18 13:49:50.626405	172.17.80.10	172.17.95.132	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
8540	2016-04-18 13:49:50.623766	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1948/39943, ttl=1 (no response found!)
8536	2016-04-18 13:49:50.573163	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1947/39687, ttl=128 (no response found!)
8415	2016-04-18 13:49:48.673891	172.17.95.132	216.58.192.100	ICMP	554 Echo (ping) request id=0x0001, seq=1946/39431, ttl=12 (no response found!)

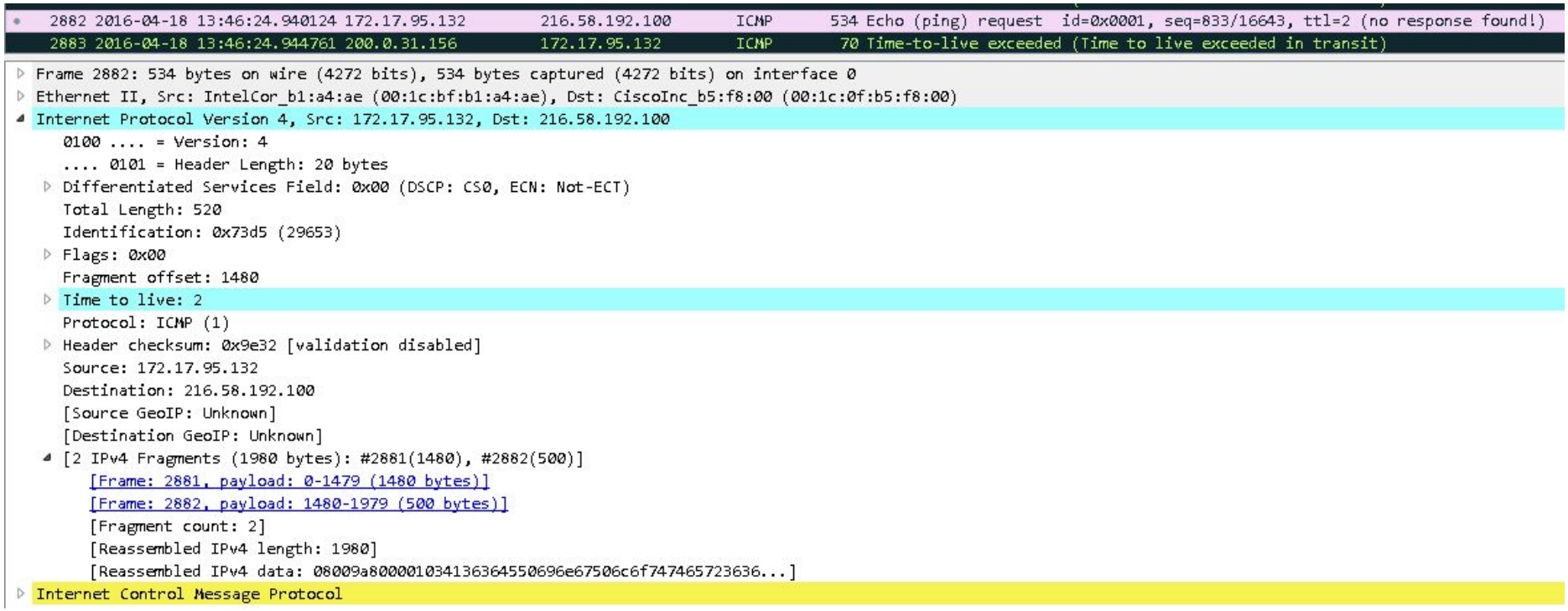
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark- traces.zip and extract the ip-ethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]



Se fragmentó dos veces.

11. Print out the first fragment of the fragmented IP datagram.
What information in tP header indicates that the datagram been fragmented?
Fragment count
What information in the IP header indicates whether this is the first fragment versus a latter fragment?
El valor de las flags
How long is this IP datagram?
1980 bytes

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?

La flag.

Are the more fragments?

Solo dos

How can you tell?

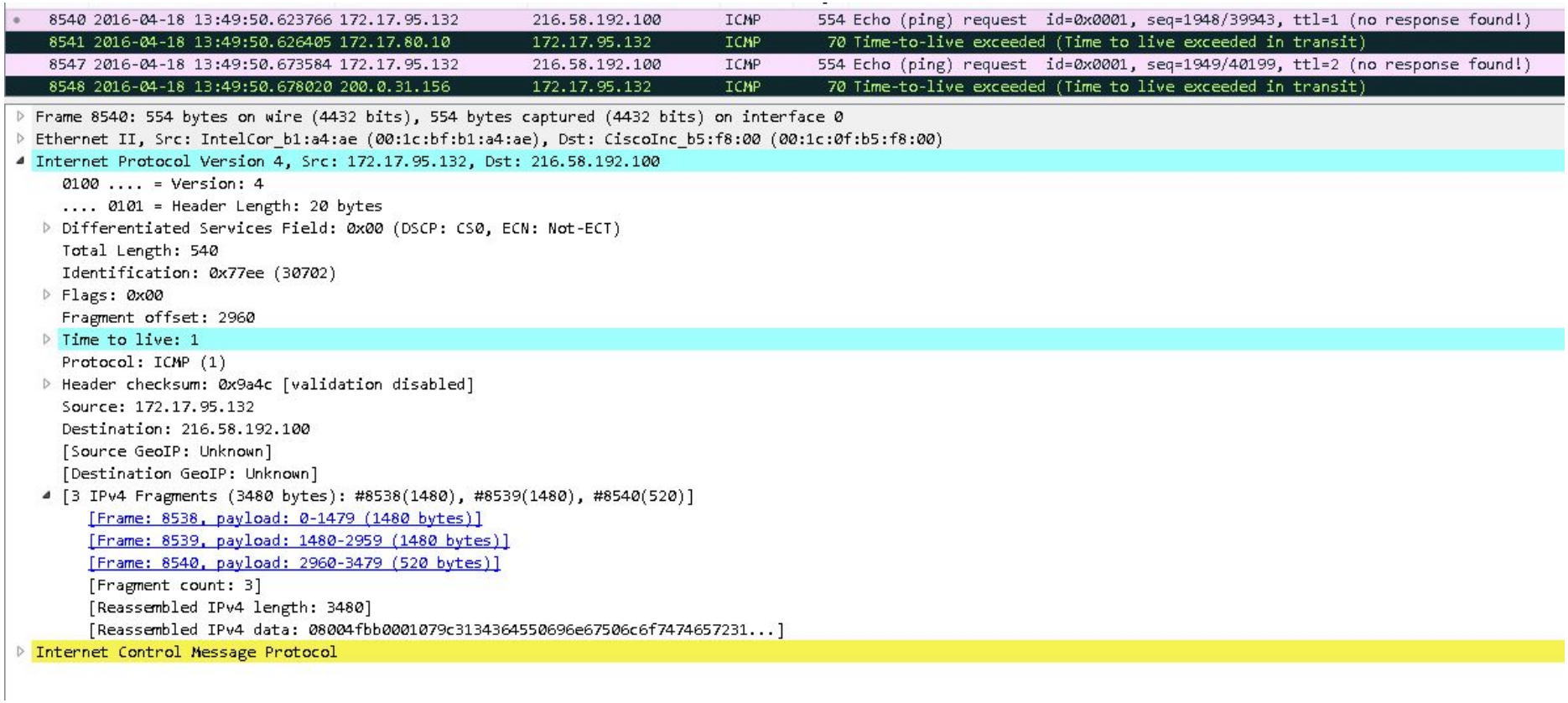
Están listados en el apartado ipv4 fragments.

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

El time to live.y la identificación.

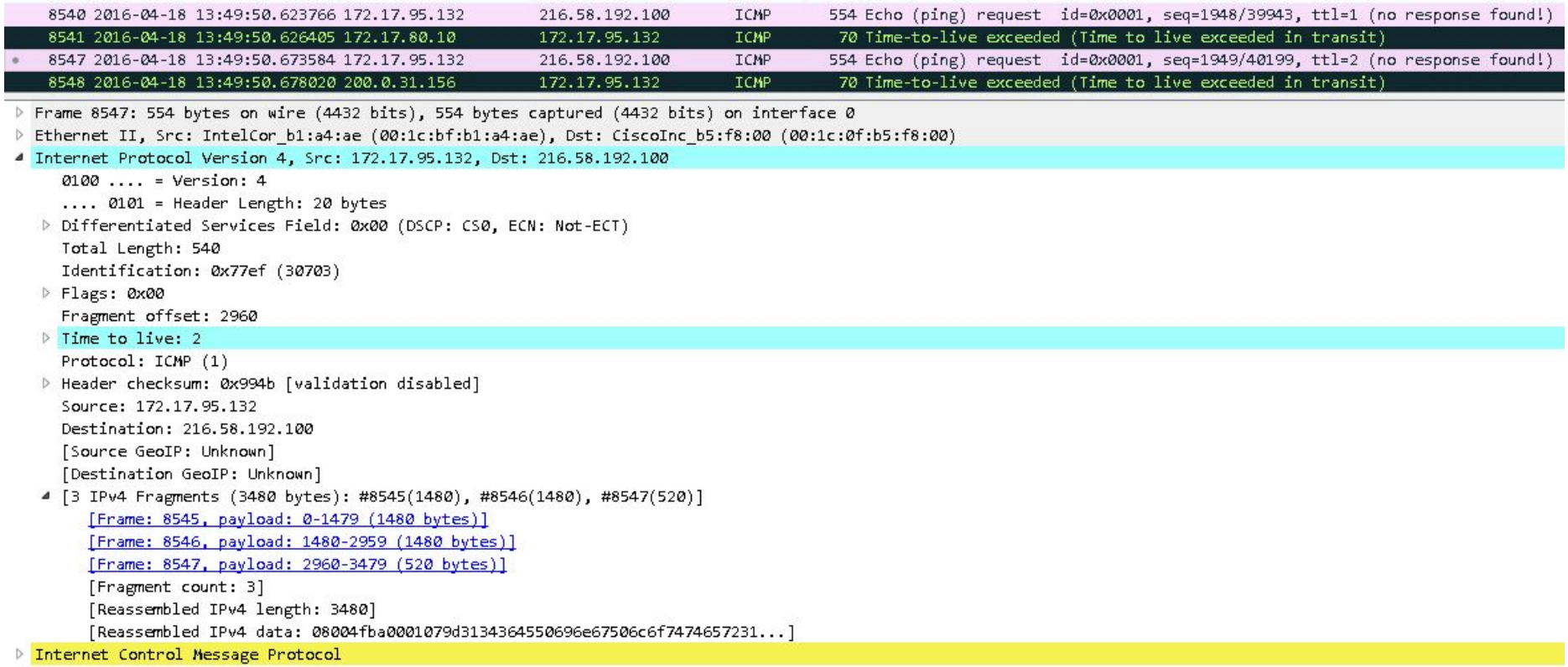
Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

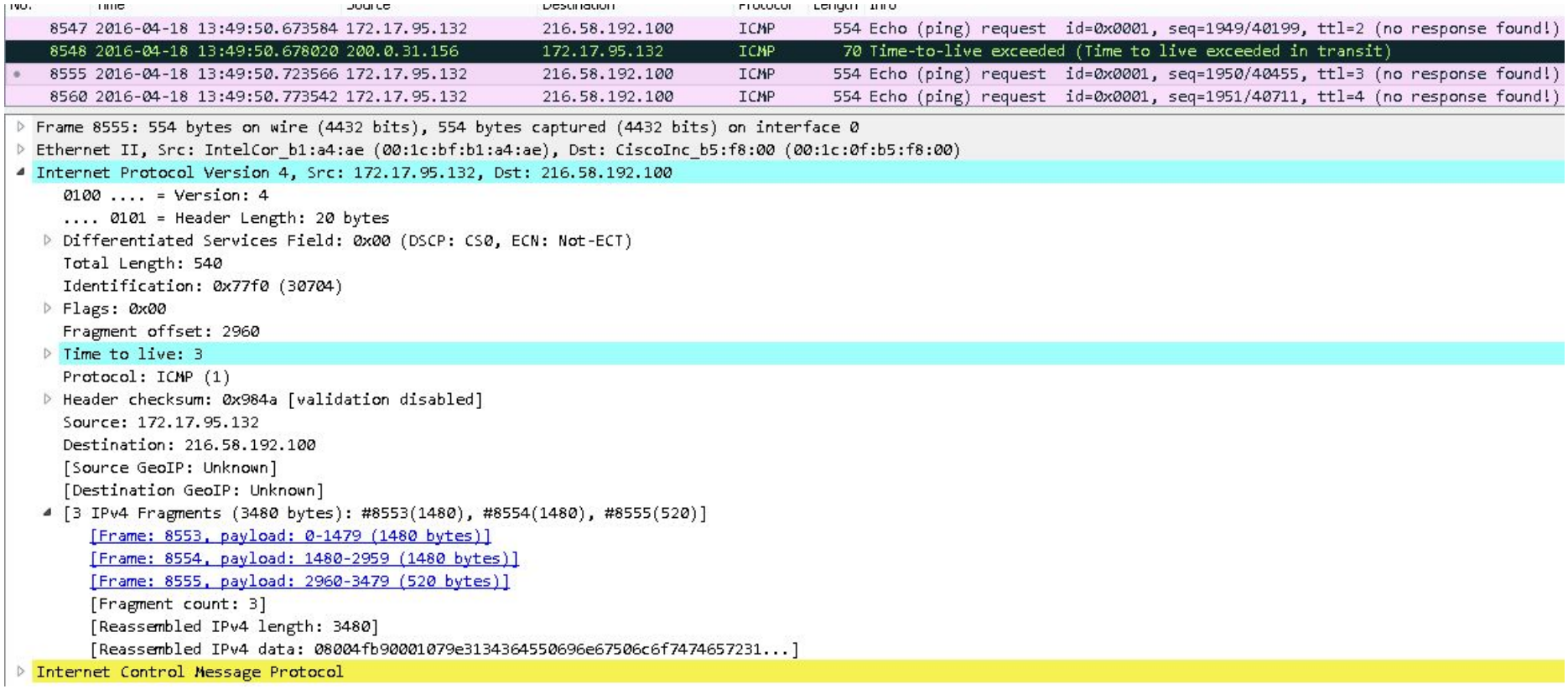
14. How many fragments were created from the original datagram?



3 fragmentos

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





La identificaciòn y el ttl.