Taller 3 Semana 3.

**Estudiante:** Paul Andrés Cuenca Macas.

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?

172.16.50.53

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

.... 0101 = Header Length: 20 bytes (5)

1. **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.**

20 bytes

58

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

Fragment offset: 0

Porque en la parte de flags no existen varios fragmentos.

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

Número, Tiempo

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

Campos constantes: Origen, Destino, Protocolo, Tamaño, Información.

Campos que deben ser constantes: Origen, Destino y Protocolo.

Campos que cambian: Número, Tiempo, Tamaño e Información.

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

Time to live: 61

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

Identification: 0x5951 (22865)

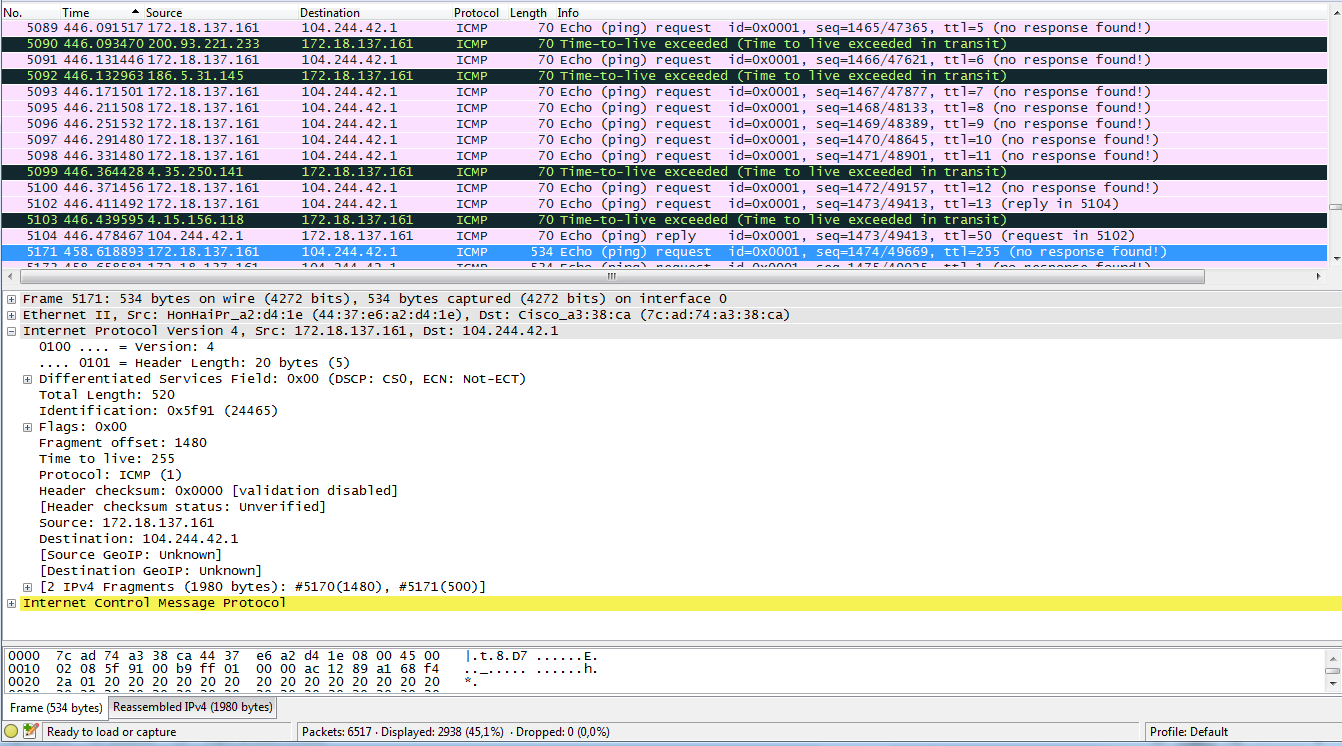
Time to live: 61

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

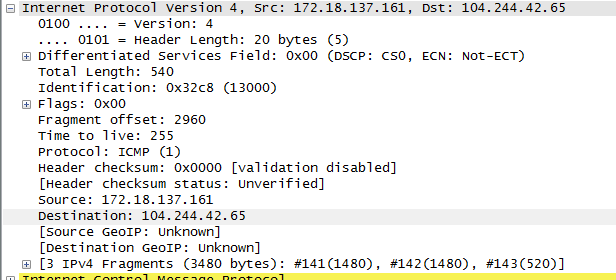
Por qué calcula el tiempo de vida y vuelta.

**FRAGMENTACIÓN**

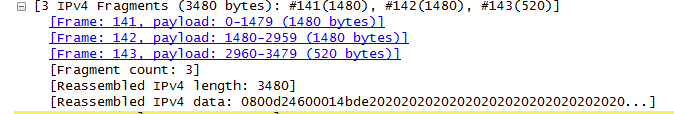
1. **Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file** [**http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip*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



1. **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?**



1. **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?**



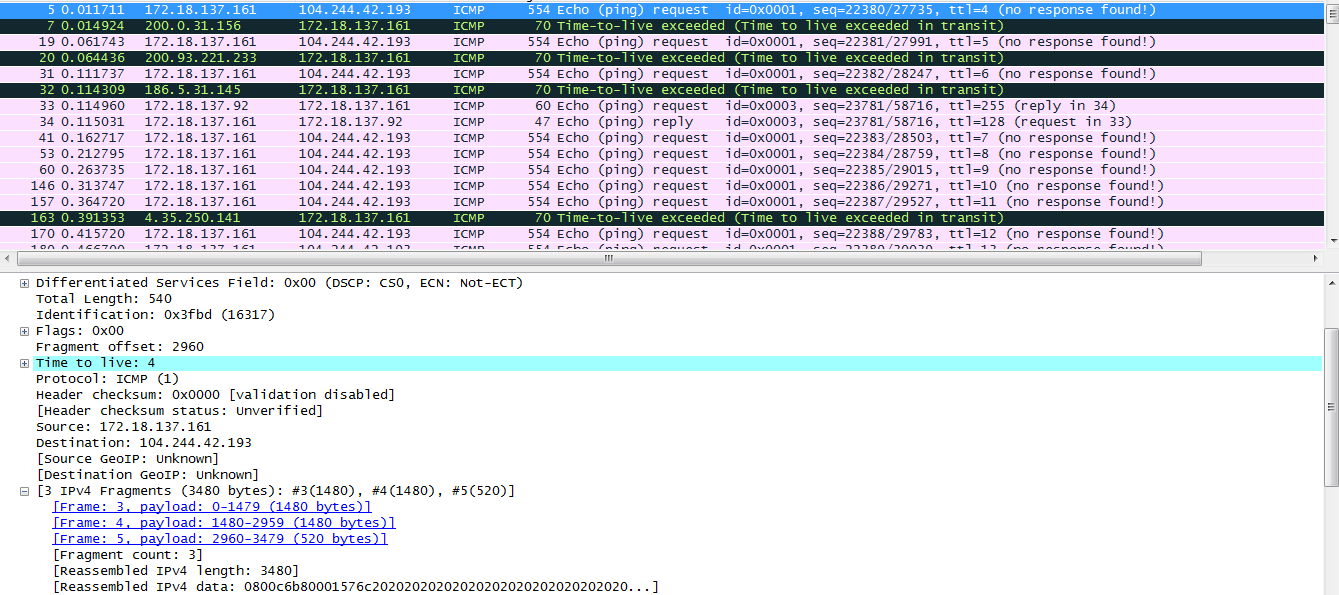
1. **What fields change in the IP header between the first and second fragment?**

Tamaño total, Identificación, Fragmento offset, Checksun, Sequence number BE, Sequence number LE, Data (bytes).

**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.**

1. **How many fragments were created from the original datagram?**

Son 3 fragmentos



1. **What fields change in the IP header among the fragments?**
   * Tamaño total
   * Identificación
   * Fragmento offset
   * Checksun
   * Sequence number BE
   * Sequence number LE
   * Data (bytes).

1. [↑](#footnote-ref-1)