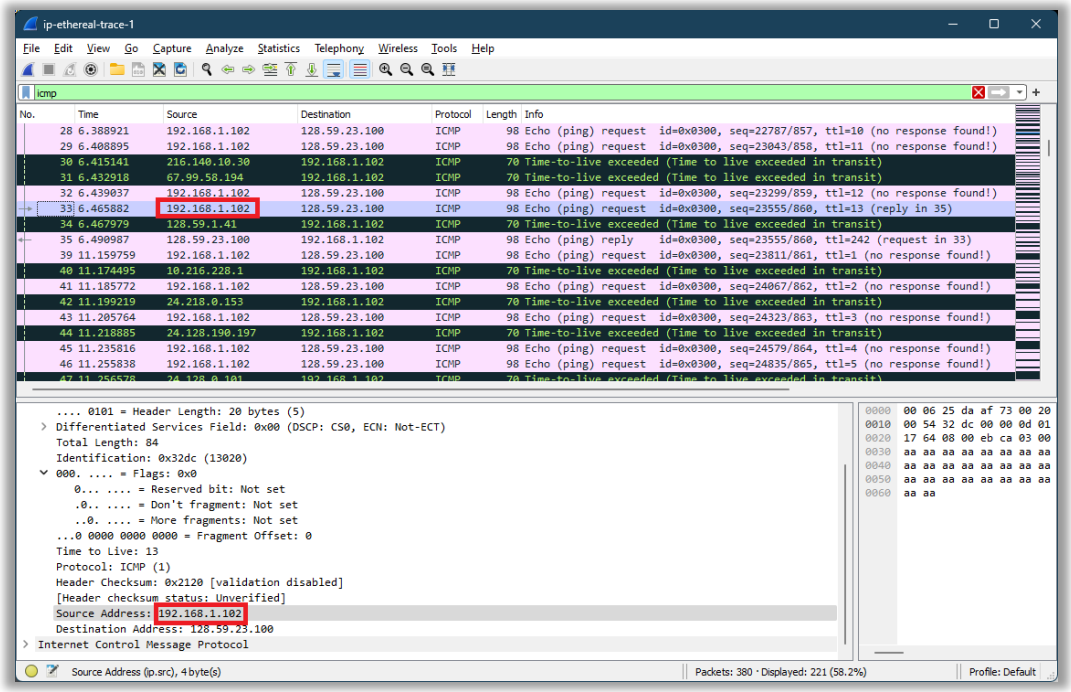
WireShark Lab 06 - IP v7.0

Igor Augusto Reis Gomes – 12011BSI290 – igor.augusto@ufu.br

Heitor Guimarães Da Fonseca Filho – 12011BSI203 – heitor.filho@ufu.br

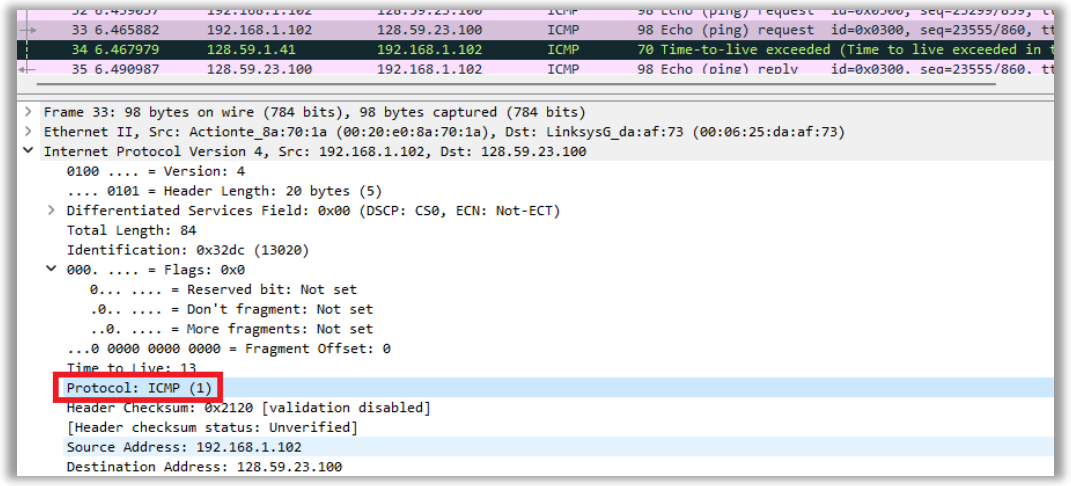
1) Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

O endereço de IP do arquivo de exemplo é 192.168.1.102, o meu é 192.168.12.1.



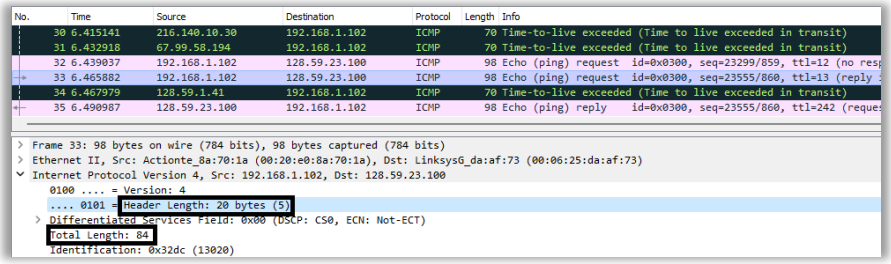
2) Within the IP packet header, what is the value in the upper layer protocol field?

O valor no campo de protocolo da camada superior é: ICMP (1).



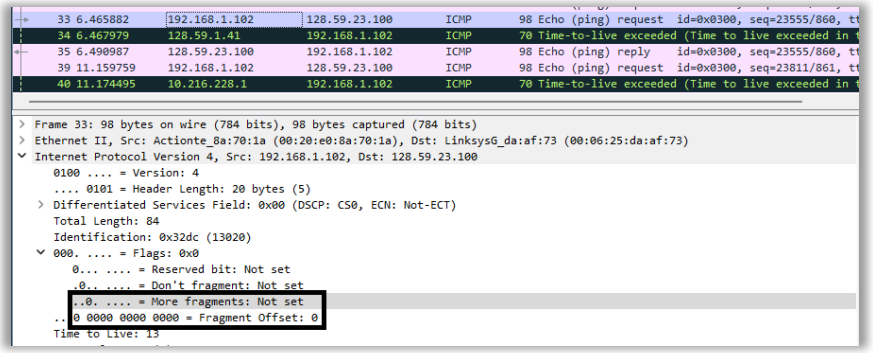
3) How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

O cabeçalho IP tem tamanho de 20 bytes, e 84 de tamanho total, resultando em uma carga útil (payload) de 64 bytes do datagrama IP, ou seja, Total Length – Header Length.



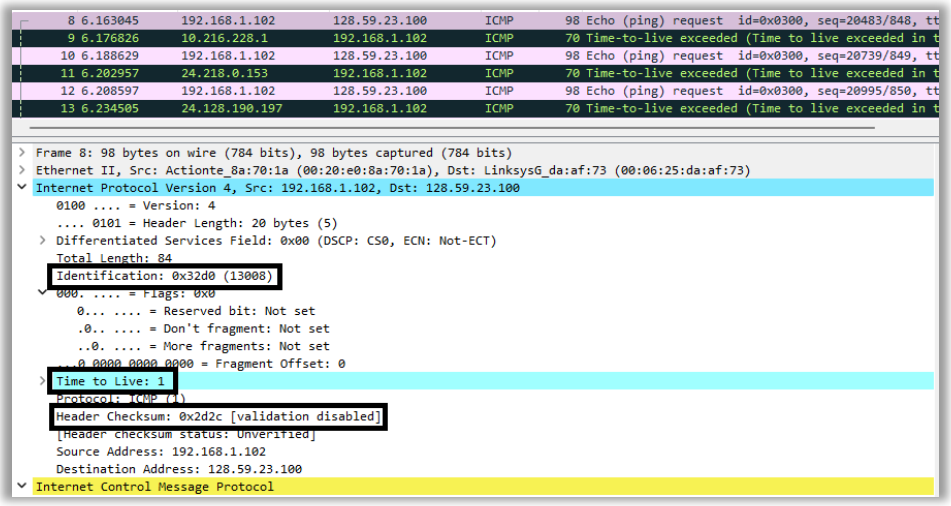
4) Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

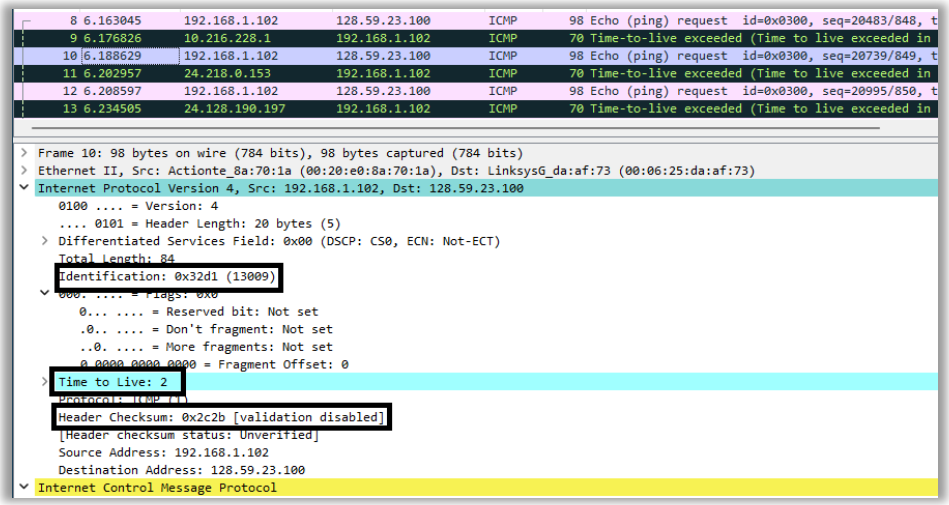
Esse datagrama IP não está fragmentado. É possível determinar com o sinalizador (flag) "*More fragments*", se não estiver definido, o datagrama não será fragmentado, caso contrário, será fragmentado.



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?

Os campos os quais sempre mudam são: identificação (*Identification*), tempo de vida (*Time to live*) e verificação de soma de cabeçalho (*Header checksum*).

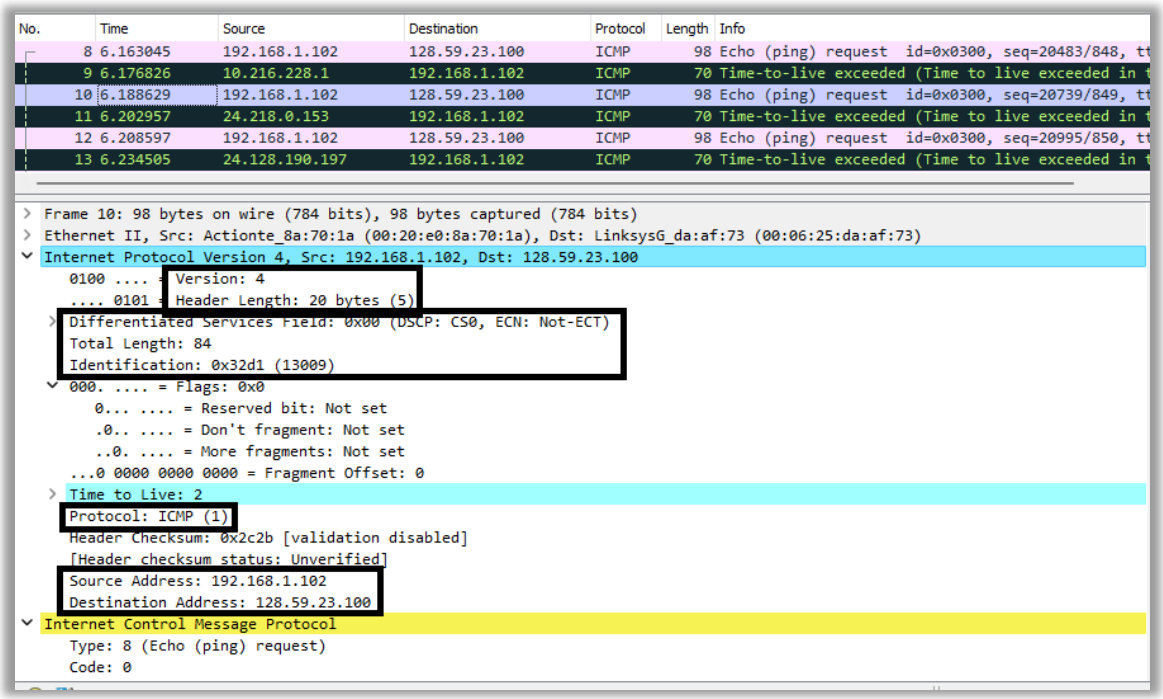




6) Which fields stay constant? Which of the fields must stay constant? Why?

Os campos que permanecem e devem permanecer constantes são:

- Version, pois estamos usando IPv4 para todos os pacotes.
- Header Length, pois esses pacotes são ICMP.
- Source Address (IP), pois estamos mandando da mesma origem.
- Destination Address (IP), pois estamos mandando para o mesmo destino.
- Differentiated Services, pois dado que todos os pacotes são since all packets are ICMP eles usam a mesma classe Type of Service).
- Upper Layer Protocol, pois esses pacotes são ICMP.



Which fields must change? Why?

Os campos que devem mudar são:

- Identification, pois os pacotes devem ter ids diferentes.
- Time to live, pois o traceroute incrementa cada pacote subsequente.
- Header checksum, pois a verificação de soma do cabeçalho deve mudar à medida que o cabeçalho é alterado.

*economizando print, pois o da questão 5 já serve para essa parte.

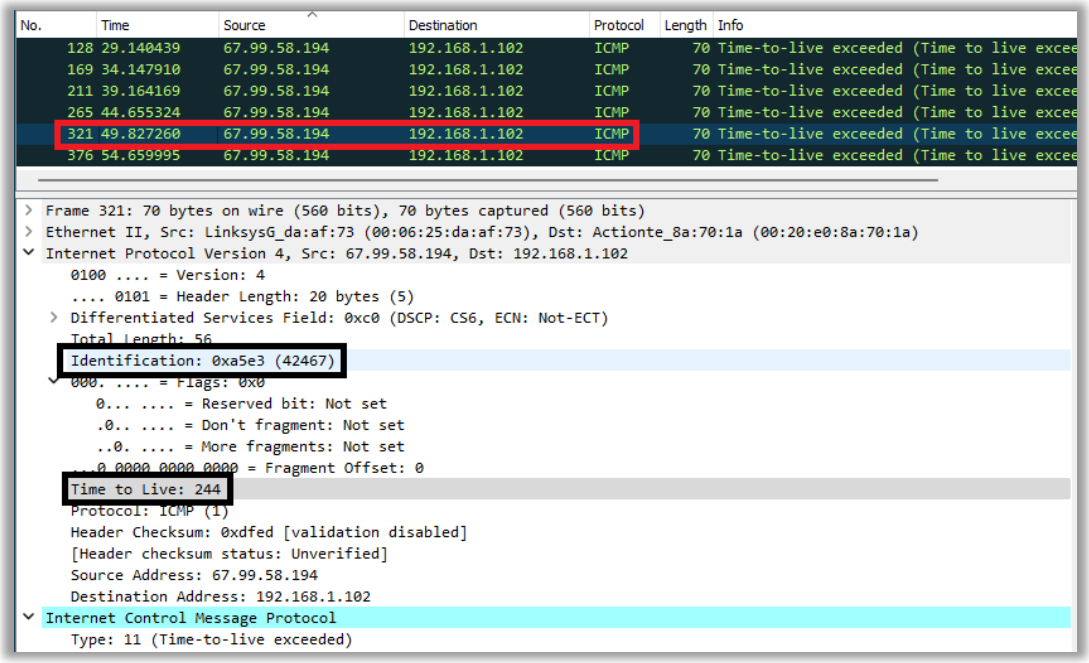
7) Describe the pattern you see in the values in the Identification field of the IP datagram

Percebo que valor deste campo é incrementado por 1 (um) a cada ICMP Echo (ping) request:

Pacote 8: Identification: 0x32d0 (13008)
Pacote 9: Identification: 0x32d1 (13009)
Pacote 10: Identification: 0x32d2 (13010)

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

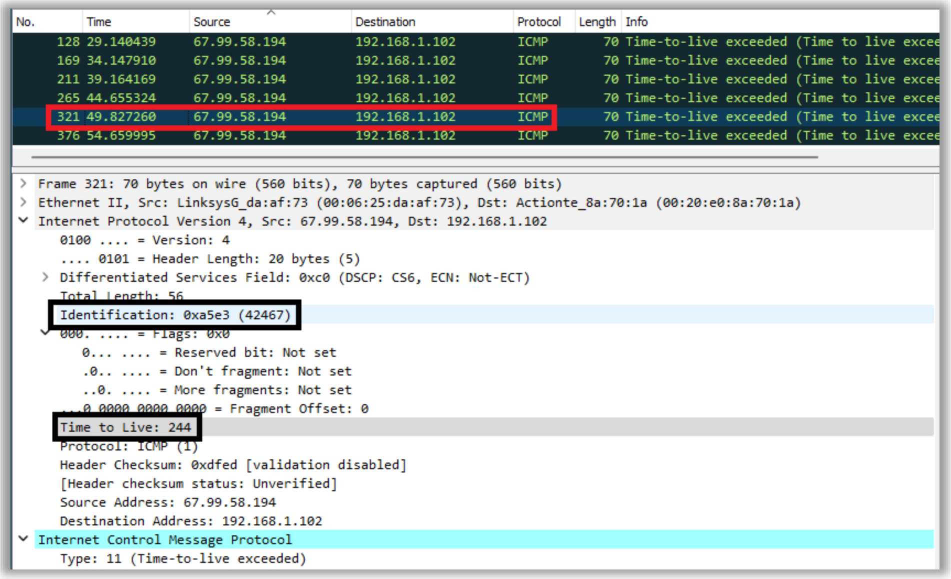
Identification: 0xa60b (42507)
Time to Live: 244



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?

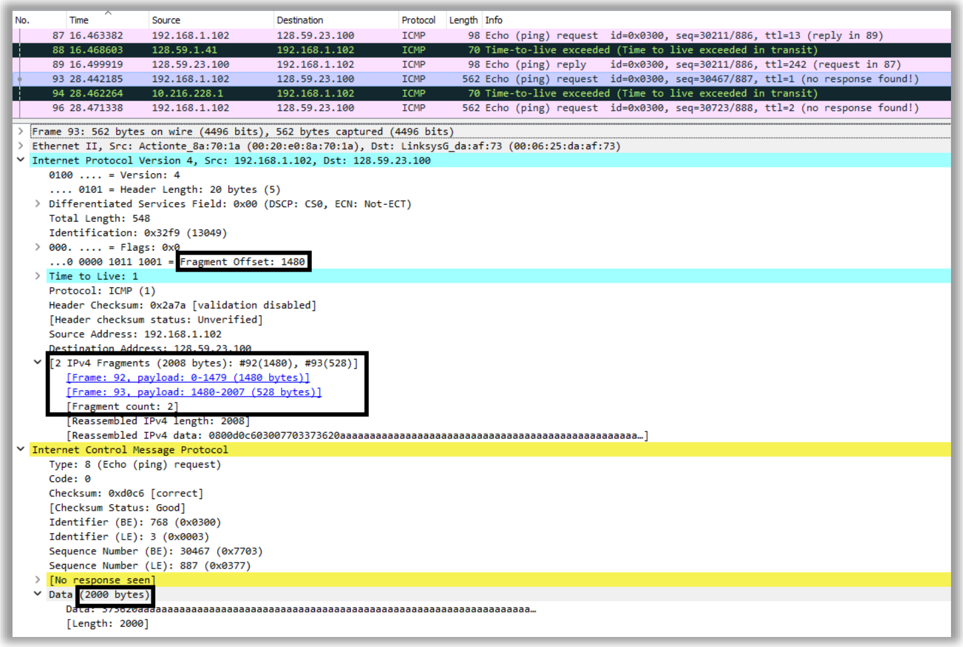
Como é possível observar na captura de tela abaixo, o campo de identificação muda para todas as respostas ICMP TTL excedidas porque o campo de identificação é um valor exclusivo. Dessa forma, quando dois ou mais datagramas IP têm o mesmo valor de identificação, isso significa que esses datagramas IP são fragmentos de um único datagrama IP grande.

O campo TTL permanece inalterado porque o TTL do roteador de primeiro salto (first hop) é sempre o mesmo.

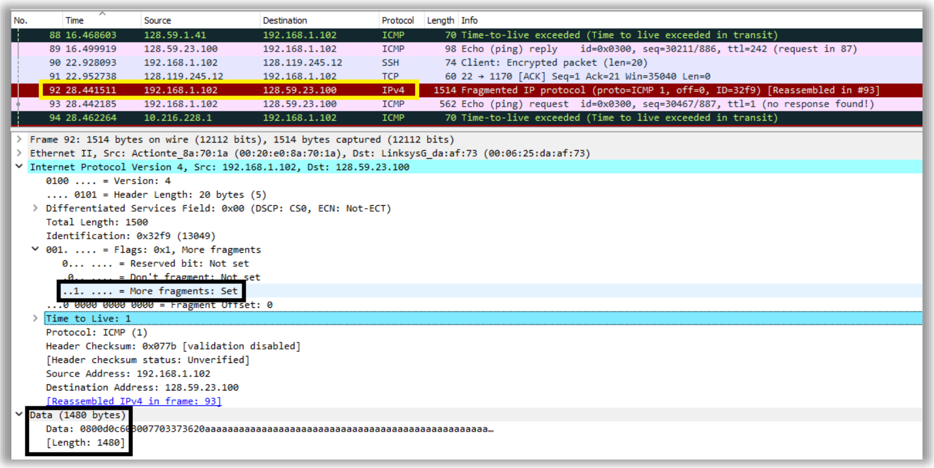


10) Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Sim, esse pacote foi fragmentado em mais de um datagrama IP.



11) Print out the first fragment of the fragmented IP datagram.



What information in the IP header indicates that the datagram been fragmented?

O sinalizador (flag) *more fragments* indica se o datagrama foi fragmentado ou não, sendo que neste caso está com valor 1 de bit definido, isto é, está fragmentado.

What information in the IP header indicates whether this is the first fragment versus a latter fragment?

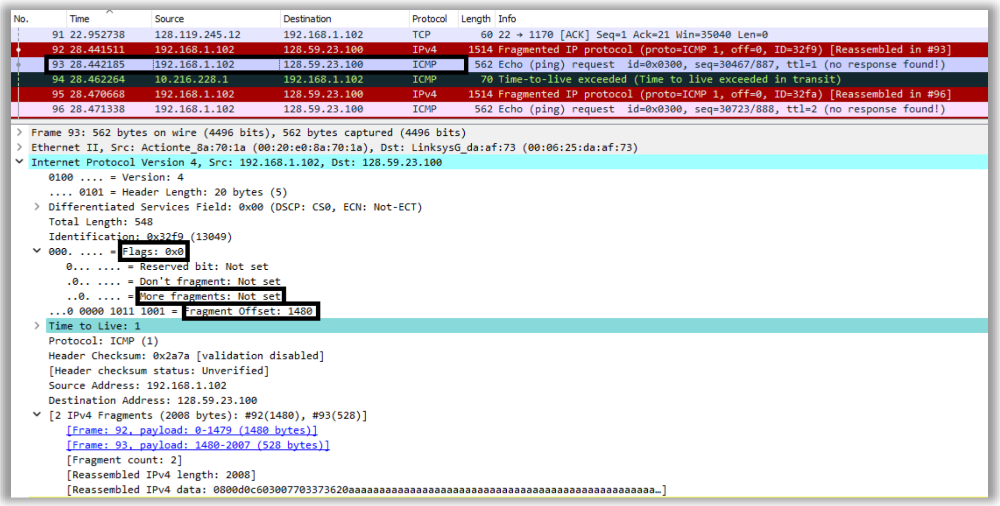
É indicado pelo campo *Fragment offset*, sendo que está definido como 0, indicando que este é o primeiro fragmento.

How long is this IP datagram?

O datagrama IP tem tamanho de 1480 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? Are the more fragments? How can you tell?

É possível afirmar que este não é o primeiro fragmento dado já que o deslocamento do fragmento (*Fragment offset*) é 1480. É o último fragmento, já que o sinalizador (*flag*) de mais fragmentos (*More fragments*) não está definido.

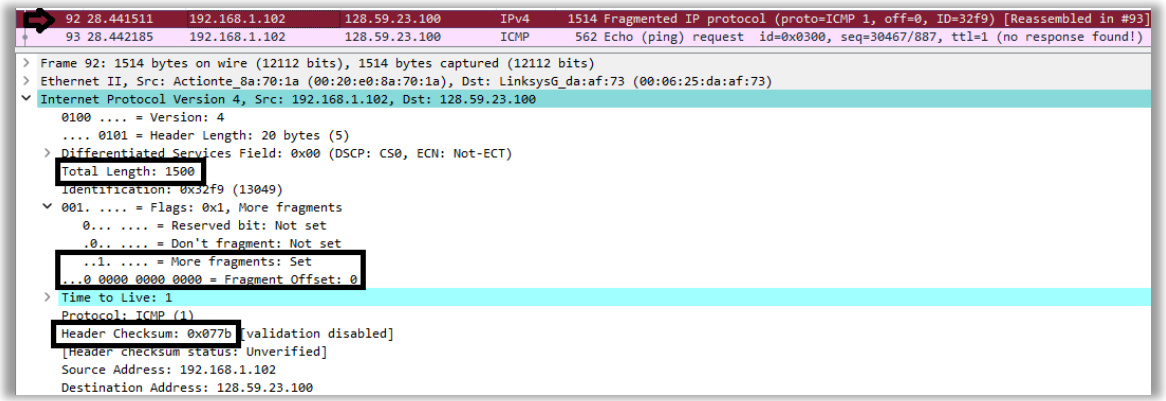


13) What fields change in the IP header between the first and second fragment?

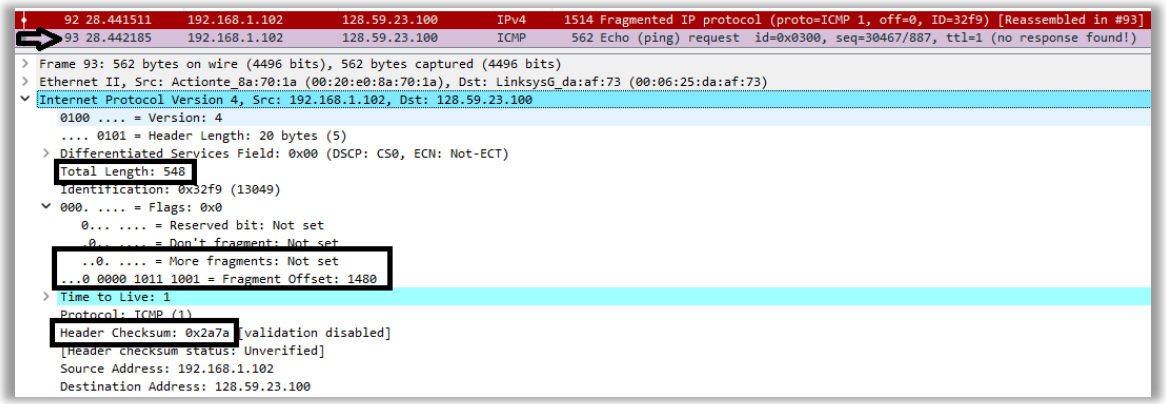
Os campos que mudam entre o primeiro e segundo fragmento são:

- Total length.
- Flags (*More fragments*).
- Fragment offset
- Checksum.

Primeiro pacote:

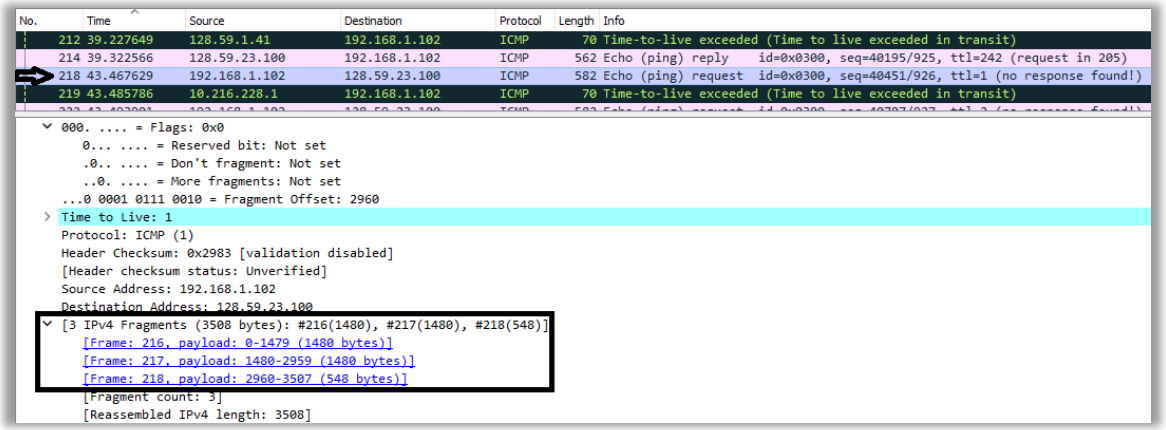


Segundo pacote:



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

Ao usar tamanho de pacote 3500, foram criados 3 fragmentos a partir do datagrama original.

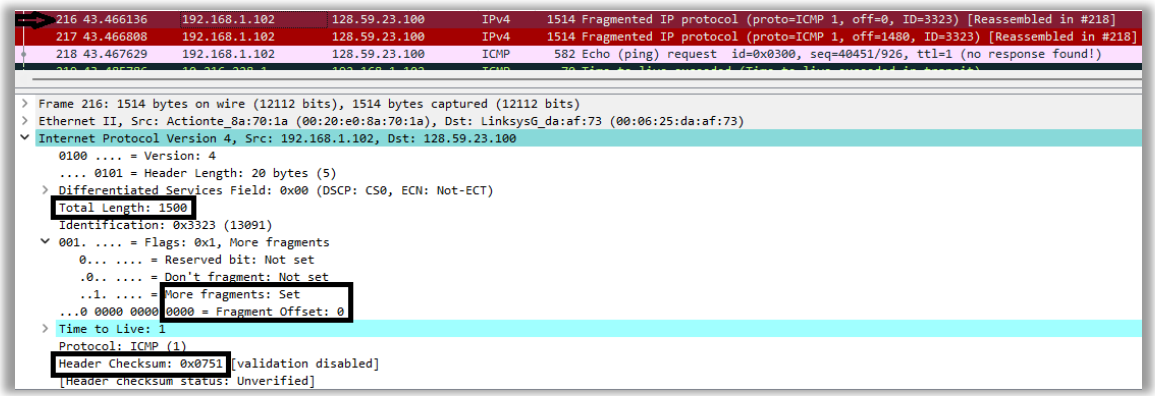


15) What fields change in the IP header among the fragments?

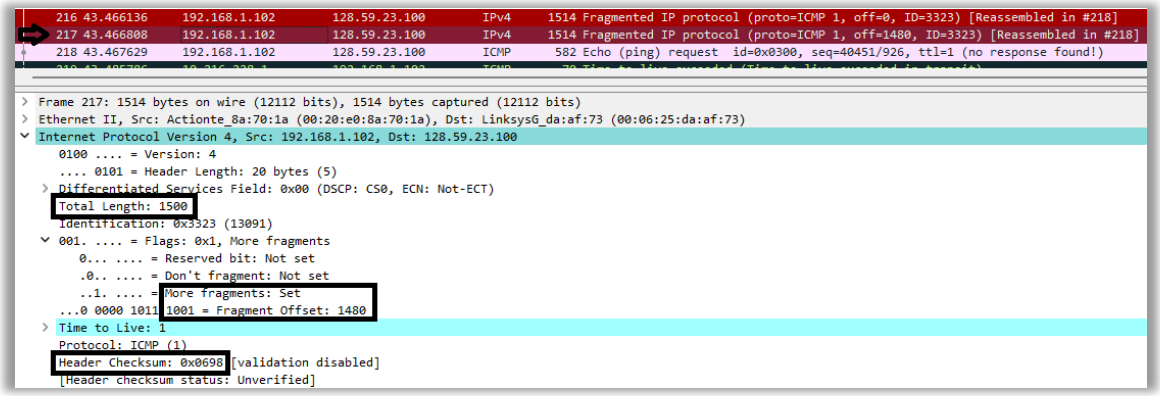
Os campos do cabeçalho IP que mudaram entre todos os três fragmentos foram:

- Total length: mudança entre os dois primeiros pacotes (dado que ambos possuem o mesmo número) e o último. Ambos possuem tamanho total de 1500, já o último é de 568.
- Flags (*More fragments*): os dois primeiros estão com valor 1, já o último está com 0.
- Fragment offset: 0, 1480 e 2960, no primeiro, segundo e terceiro, respectivamente.
- Checksum: 0x0751 (1873), 0x0698 (1688) e 0x2983 (10627), respectivamente

Primeiro pacote:



Segundo pacote:



Terceiro pacote: