Práctica 2

Apellidos: López Pérez
Nombre: Marta

Titulación: Grado de Ingeniería Informática
Grupo: 2ºA

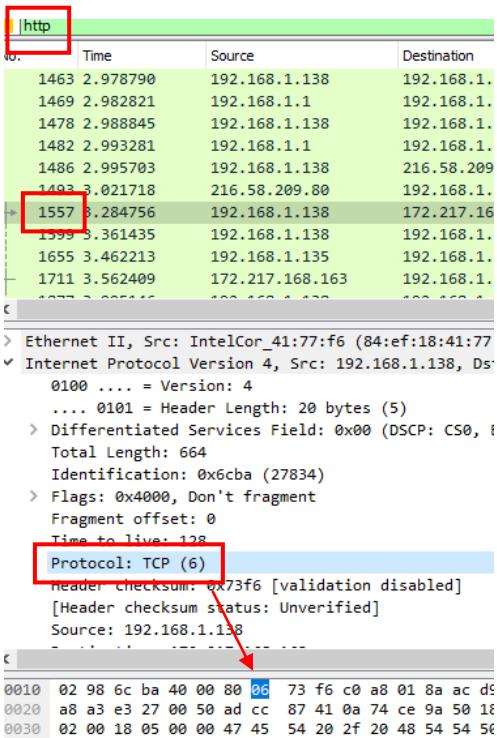
PC de la práctica: PC CASA

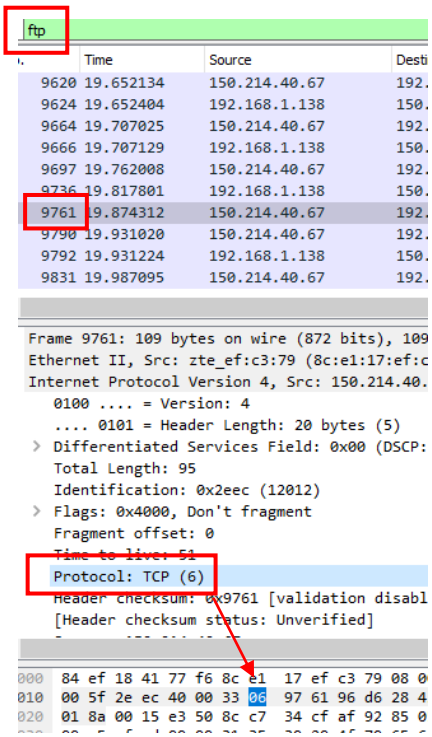
Lea el enunciado de la práctica para saber cómo generar el tráfico de cada ejercicio.

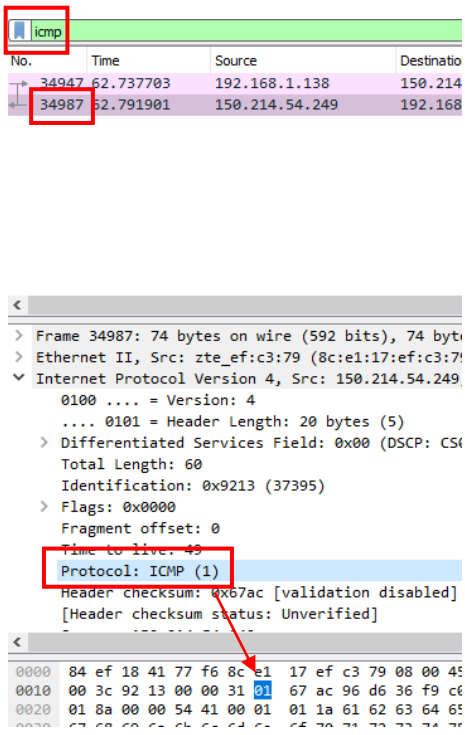
Ejercicio 1. Observe la cabecera IP de los diferentes datagramas:

- ¿Qué protocolo se indica en el campo "protocolo" en la cabecera de los datagramas que transportan mensajes ICMP, FTP y HTTP?

Protocolo	Valor Campo protocolo	Valor (HEX)	Número de trama
ICMP	ICMP (1)	01	34987
HTTP	TCP (6)	06	1557
FTP	TCP (6)	06	9761







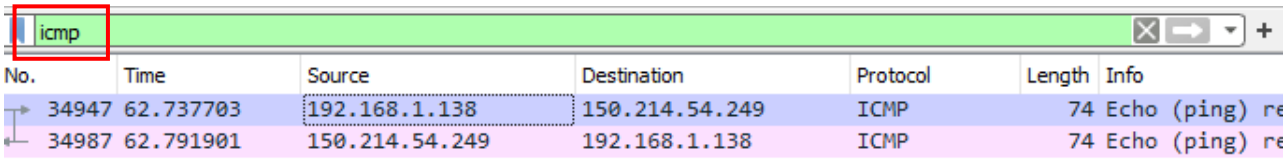
- ¿Qué indica este campo?

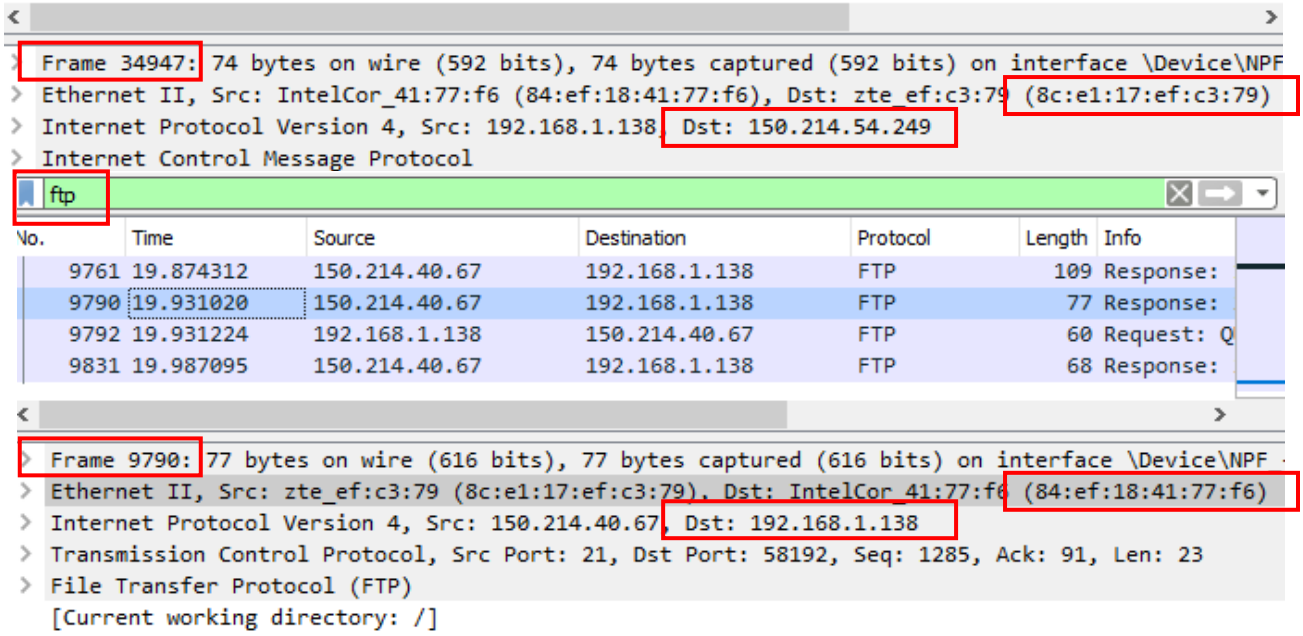
  El protocolo que se utiliza en cada trama.

```
Microsoft Windows [Versión 10.0.18362.778]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 150.214.54.249: bytes=32 tiempo=54ms TTL=49

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 54ms, Máximo = 54ms, Media = 54ms

C:\WINDOWS\system32>
```

Ejercicio 2. Seleccione una petición de ICMP de su equipo (el mensaje *echo request*) y complete la siguiente tabla indicando la dirección IP destino (en la cabecera IP) y la dirección MAC destino (en la cabecera Ethernet). Repita el proceso con una petición FTP (en *Info* poner *request*).

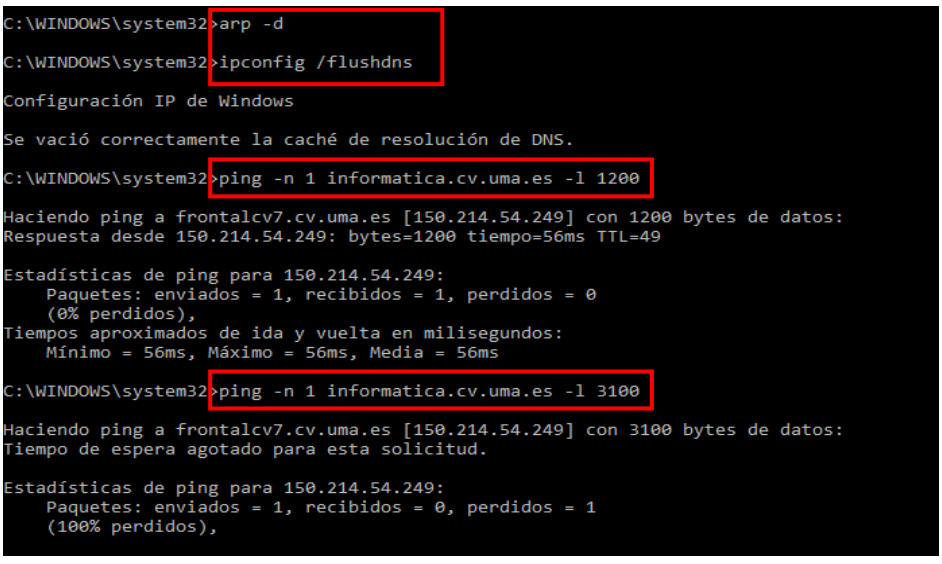
	ICMP	FTP
Dirección IP destino (cab IP)	150.214.54.249	192.168.1.138
Dirección MAC destino (cab Ethernet)	8c:e1:17:ef:c3:79	84:ef:18:41:77:f6
Número de trama	34947	9790





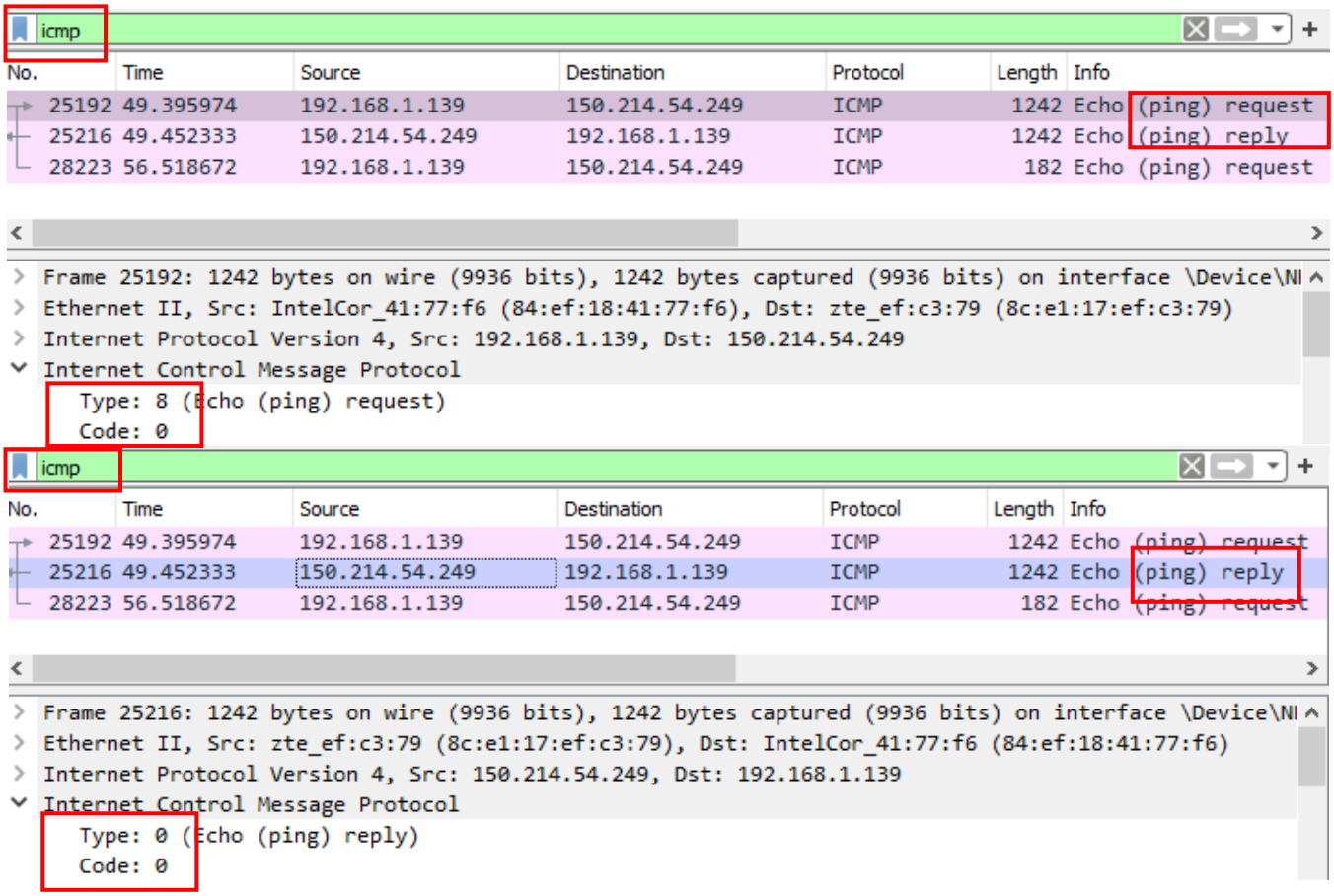
- ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

La dirección MAC es la dirección física del dispositivo y por eso no cambia, mientras que la dirección IP cambia dependiendo del protocolo, por eso es distinta.



Ejercicio 3. Responda las siguientes preguntas:

- ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)?



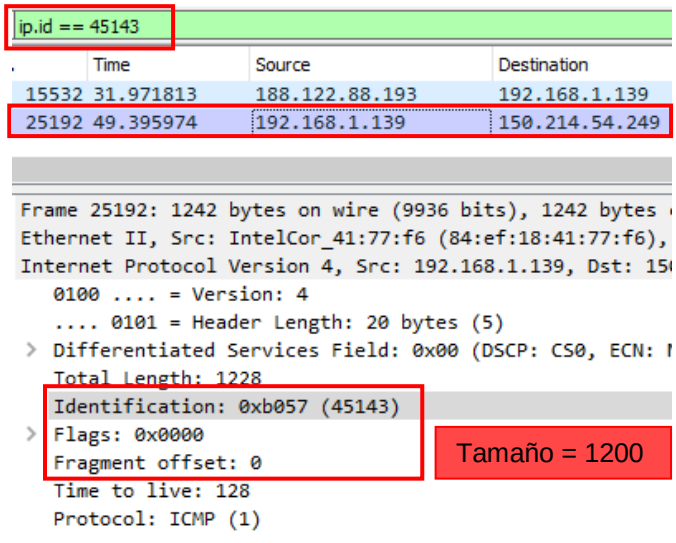
Para el resto de preguntas y rellenar la tabla considere solo las peticiones.

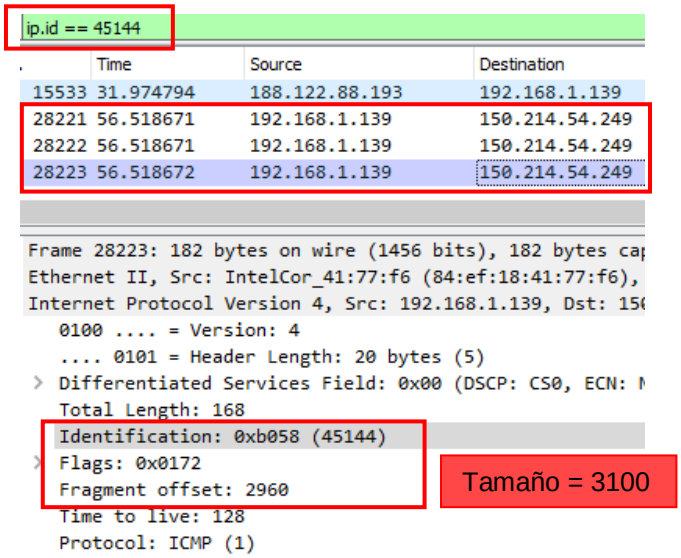
- ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto?

  ip.id == identificador

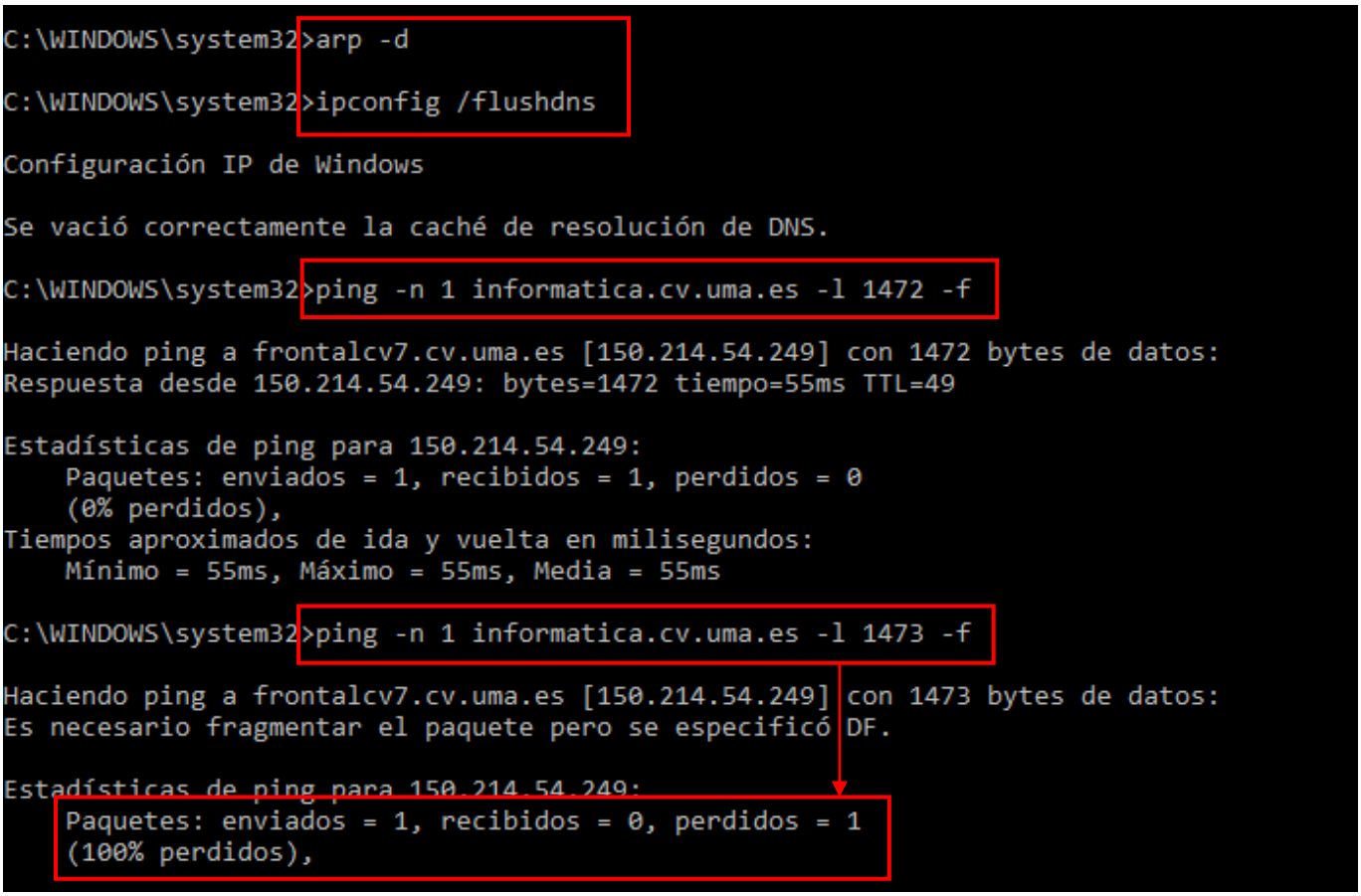
- Completa la siguiente tabla, indicando los flags que tiene activo cada fragmento, su identificador y su desplazamiento (para cada tamaño escribe un valor por cada fragmento, separados por comas (,) cuando hay varios fragmentos).

Tamaño	Número de tramas	Identificadores	Flags	Desplazamientos
1200	1	0xb057	0x0000	0
3100	3	0xb058	0x0172	2960





Ejercicio 4. Realice dos pings a **informatica.cv.uma.es** con tamaños MAX y MAX+1 y el bit DF activo (MAX es el tamaño máximo calculado). Añada una captura de pantalla.



- ¿Cuál es el valor máximo?

  1472

- ¿Por qué es ese tamaño?

  Para calcular ese número tenemos que coger y al valor máximo de la MTU que es 1500 bytes le tenemos que restar 20 bytes de la cabecera del protocolo IP y 8 bytes de la cabecera de ICMP.

  1500-20-8 = 1472.

- ¿En la traza de wireshark aparece el segundo ping? ¿Por qué?

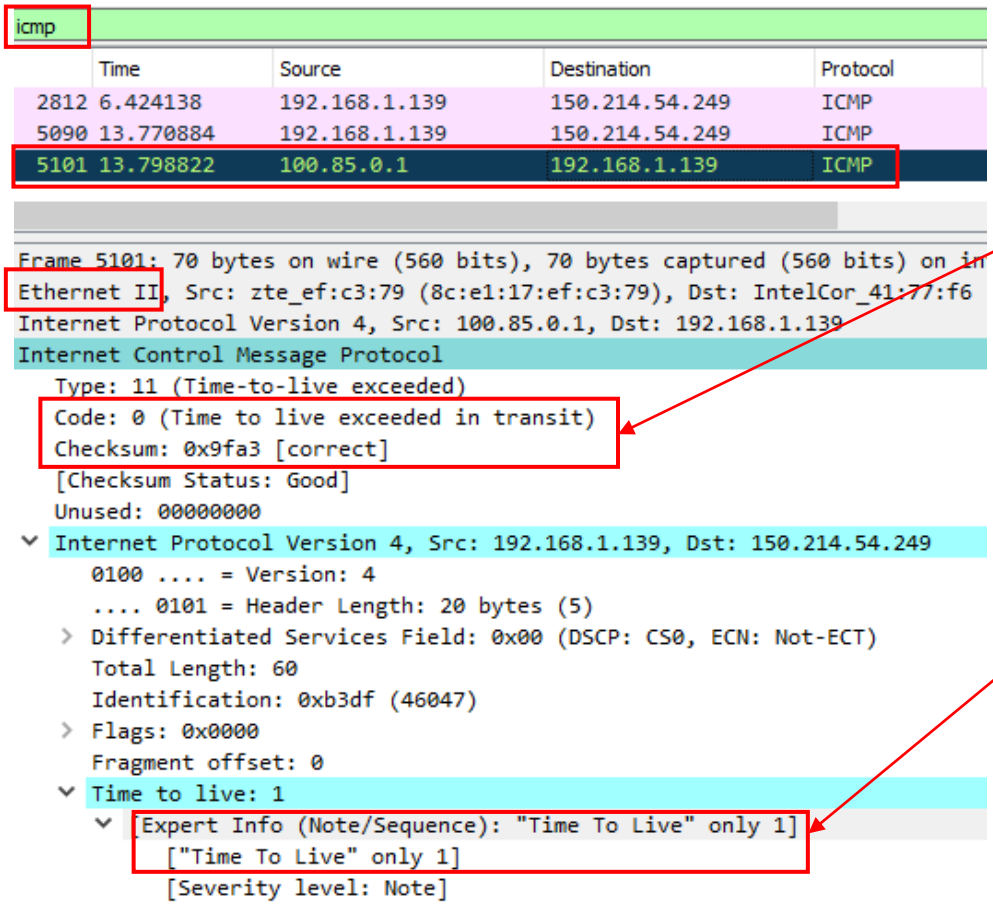
  No aparece, porque si observamos la terminal, aparece que se pierde el paquete, ya que no se puede fragmentar y no puede mandar todos sus bytes.

Ejercicio 5. Haga un ping a **informatica.cv.uma.es** usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta del servidor. Observe en Wireshark el intercambio de paquetes que se produce.

```
C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -i 1

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -i 2

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 100.85.0.1: TTL expirado en tránsito.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
```

- Número de trama analizado

  5101



- ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)?

- ¿Qué incluye dicho mensaje ICMP como información adicional?

Ejercicio 6. Responda a las siguientes preguntas:

```
C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>tracert informatica.cv.uma.es

Traza a la dirección frontalcv7.cv.uma.es [150.214.54.249]
sobre un máximo de 30 saltos:

  1     *        *        *     Tiempo de espera agotado para esta solicitud.
  2    26 ms    24 ms    24 ms  100.85.0.1
  3    17 ms    16 ms    18 ms  10.15.4.81
  4    16 ms    17 ms    16 ms  10.0.24.54
  5    17 ms    17 ms    17 ms  be4430.rcr22.svq01.atlas.cogentco.com [149.11.19.193]
  6    30 ms    30 ms    30 ms  be3240.ccr31.vlc02.atlas.cogentco.com [154.54.59.13]
  7    34 ms    34 ms    35 ms  be3356.ccr32.mad05.atlas.cogentco.com [154.54.57.241]
  8    35 ms    34 ms    35 ms  be3379.agr22.mad05.atlas.cogentco.com [154.54.39.146]
  9    35 ms    35 ms    35 ms  be3481.nr51.b015537-1.mad05.atlas.cogentco.com [154.25.1.110]
 10    42 ms    35 ms    35 ms  149.14.242.226
 11    44 ms    43 ms    44 ms  130.206.245.122
 12    60 ms    62 ms    76 ms  cica-router-backup.red.rediris.es [130.206.211.42]
 13    61 ms    61 ms    60 ms  uma-router.red.cica.es [150.214.231.170]
 14    54 ms    53 ms    63 ms  tuneles.uma.es [150.214.47.249]
 15    55 ms    55 ms    54 ms  te6009dixie.ruma.uma.es [150.214.41.238]
 16     *        *        *     Tiempo de espera agotado para esta solicitud.
 17    54 ms    54 ms    55 ms  frontalcv7.cv.uma.es [150.214.54.249]

Traza completa.
```

- Indique el número de los paquetes utilizados para responder estas preguntas

  Números indicados en cada pregunta.

- ¿Qué tipo de paquetes (protocolo de más alto nivel) usa **tracert** para hacer su función?

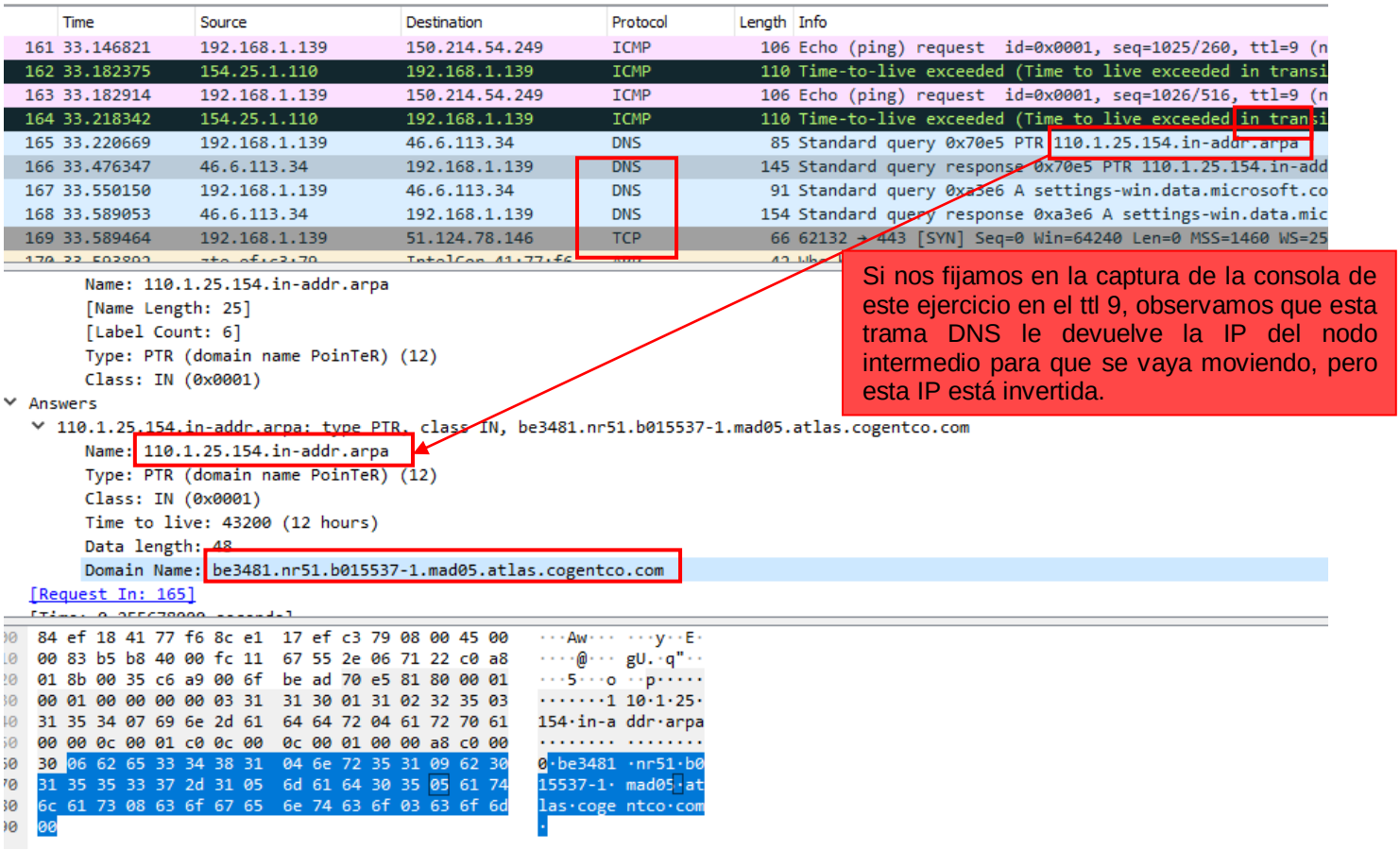
  Los de tipo ICMP. Paquetes 3,4,5,53,54,55,56… hay 93 en total que se usan al hacer el tracert.

ip.dst == 150.214.54.249 && ip.src == 192.168.1.139

	Time	Source	Destination	Protocol	Length	Info
3	0.039988	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1000/59395, ttl=1 (r
4	3.698818	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1001/59651, ttl=1 (r
5	7.685441	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1002/59907, ttl=1 (r
53	11.699653	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1003/60163, ttl=2 (r
54	11.725579	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
55	11.727705	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1004/60419, ttl=2 (r
56	11.751832	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
57	11.753955	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1005/60675, ttl=2 (r
58	11.778176	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
67	17.336530	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1006/60931, ttl=3 (r
68	17.354103	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit
69	17.356188	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1007/61187, ttl=3 (r
70	17.372971	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit
71	17.375057	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1008/61443, ttl=3 (r
72	17.393073	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit

- Además de los mensajes propios para obtener el camino, **tracert** puede provocar que se realicen otros envíos auxiliares para conseguir información o mostrar de forma más amistosa la información, ¿qué otros mensajes pueden ser necesarios?

  Podría ser necesario algunos de tipo DNS, ya que traduce las direcciones IP a las URL que les corresponde
  Tramas 163,165,166,167,168 las del siguiente ejemplo.



- ¿Qué estrategia usa **tracert** para averiguar qué máquina hay en cada salto del paquete?

  Según las diferentes tablas de encaminamiento de router a router se envían ICMP hasta que llega al destino determinado. Las tramas en negro devuelven la IP de los nodos intermedios y las tramas DNS las IPs de destino de los nodos intermedios, así es como se vé todos los pasos que hace.