## Práctica 2

**Apellidos:** López Pérez

**Nombre:** Marta

**Titulación:** Grado de Ingeniería Informática

**Grupo:** 2ºA

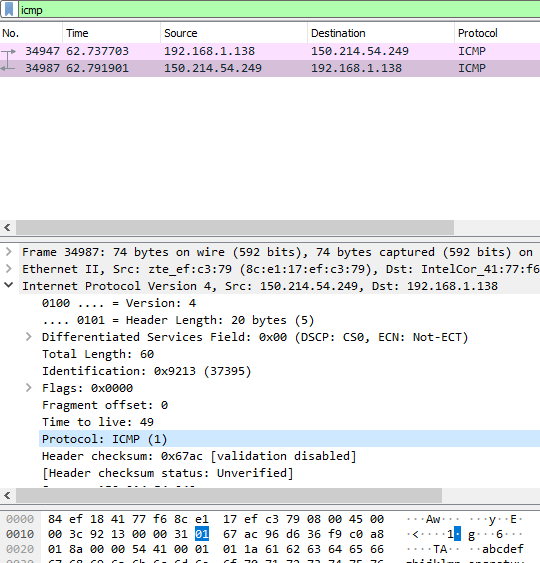
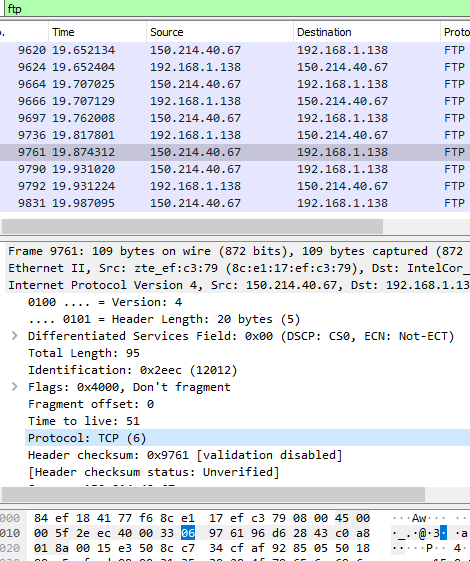
**PC de la práctica:** PC CASA

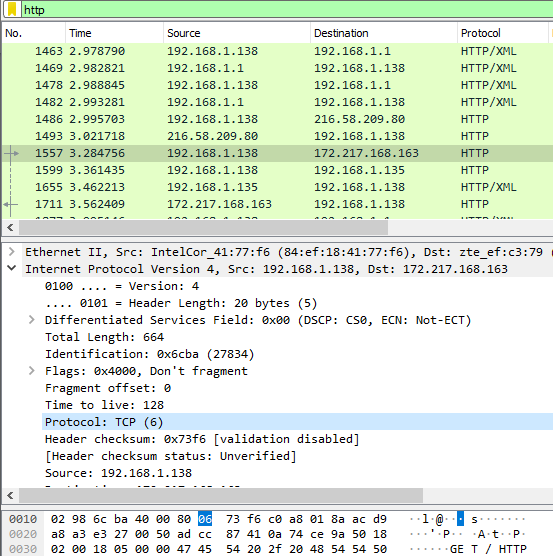
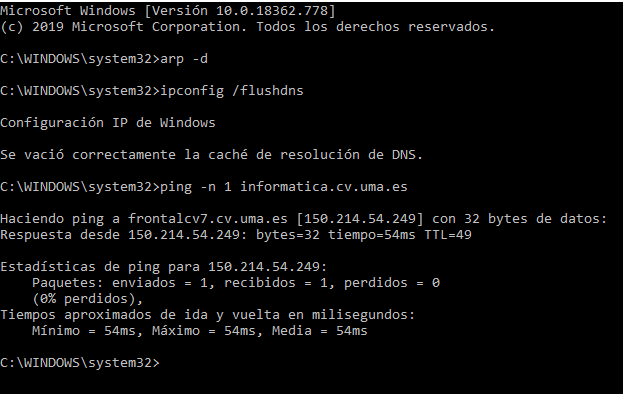
**Lea el enunciado de la práctica para saber cómo generar el tráfico de cada ejercicio.**

**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 |



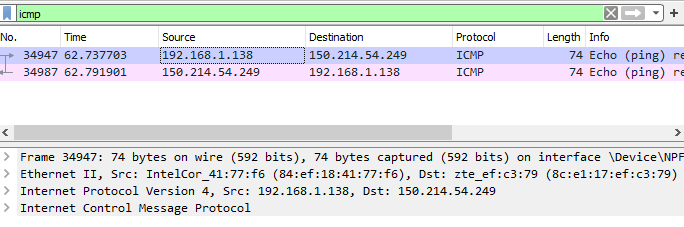
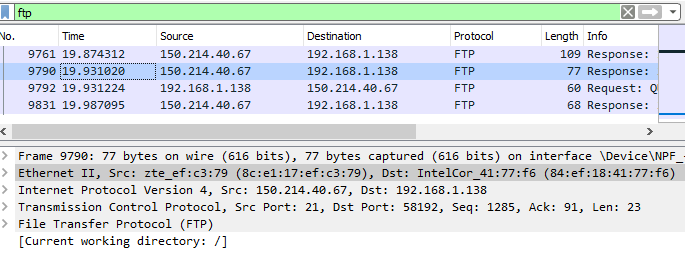


* ¿Qué indica este campo?

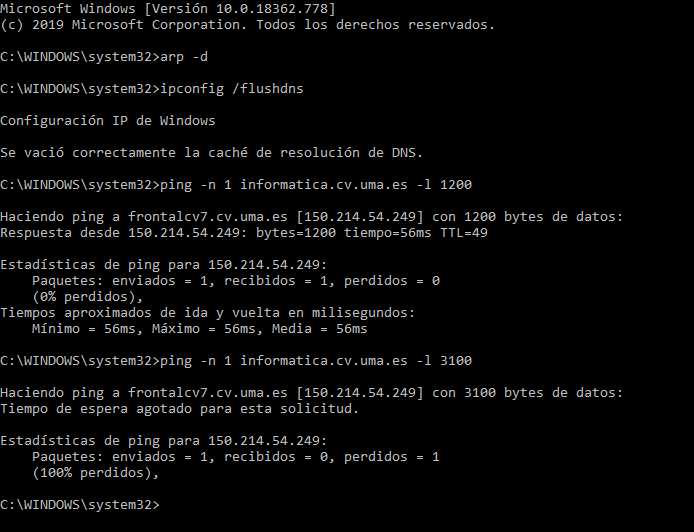
El protocolo que se utiliza en cada trama.

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*).

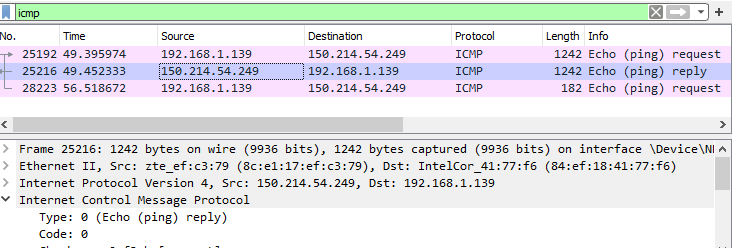
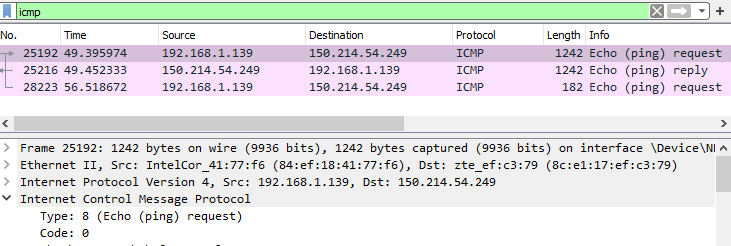
|  |  |  |
| --- | --- | --- |
|  | ICMP | FTP |
| Dirección IP destino (cab IP) | 150.214.54.249 | 192.168.1.138 |
| Dirección MAC destino (cab Ethernet) | 8c:e1:17:ef:c3:79 | 84:ef:18:41:77:f6 |
| Número de trama | 34947 | 9790 |



* ¿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)?

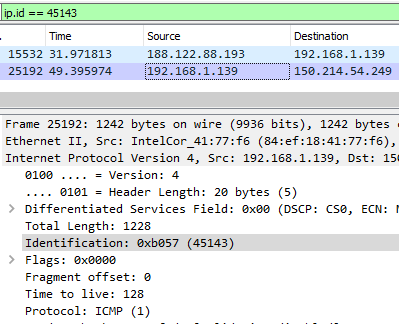
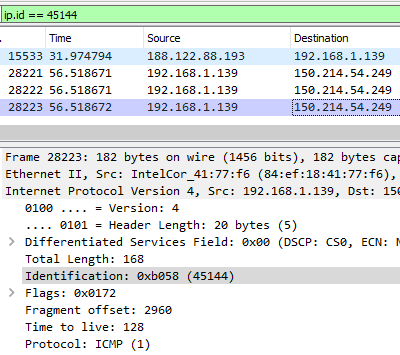
Para el resto de preguntas y rellenar la tabla considere solo las peticiones.

* ¿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).

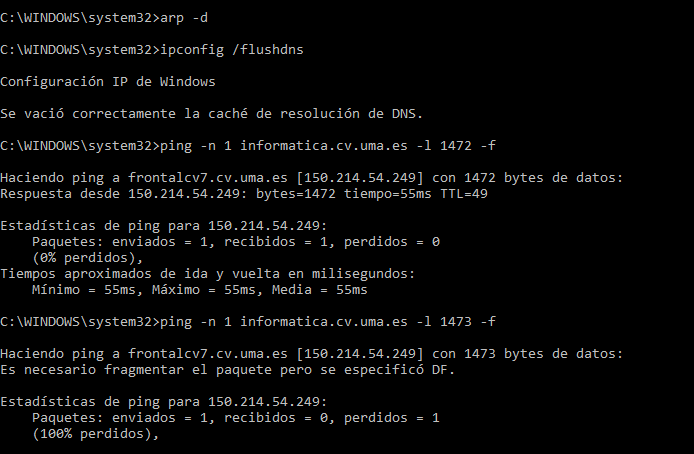
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Tamaño | Número de tramas | Identificadores | Flags | Desplazamientos | |
| 1200 | 1 | 0xb057 | 0x0000 | 0 | |
| 3100 | 3 | 0xb058 | 0x0172 | 2960 |



Tamaño = 3100

Tamaño = 1200

**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?

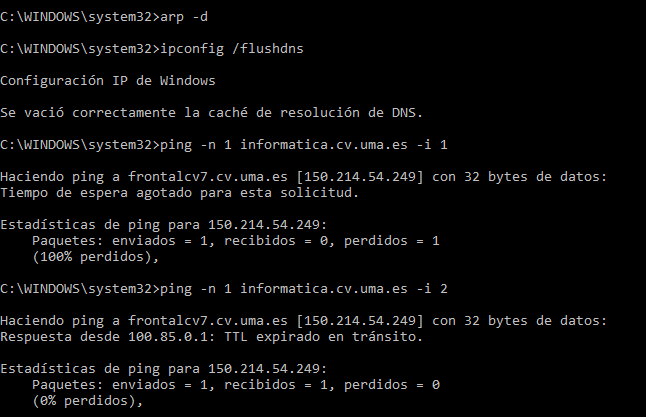
Para calcular ese número tenemos que coger y al valor máximo de la MTU que es 1500 bytes le tenemos que restar 20 bytes de la cabecera del protocolo IP y 8 bytes de la cabecera de ICMP.

1500-20-8 = 1472.

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

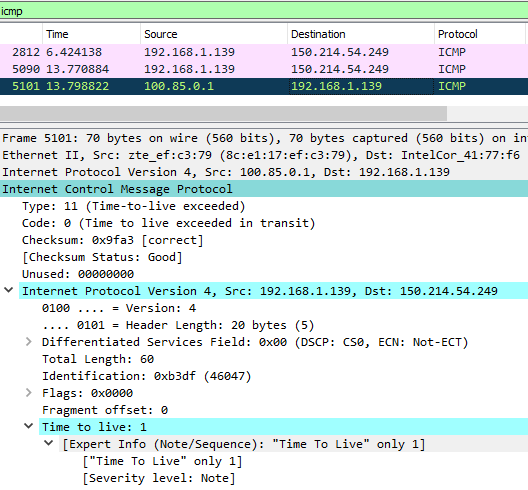
No aparece, porque si observamos la terminal, aparece que se pierde el paquete, ya que no se puede fragmentar y no puede mandar todos sus bytes.

**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.

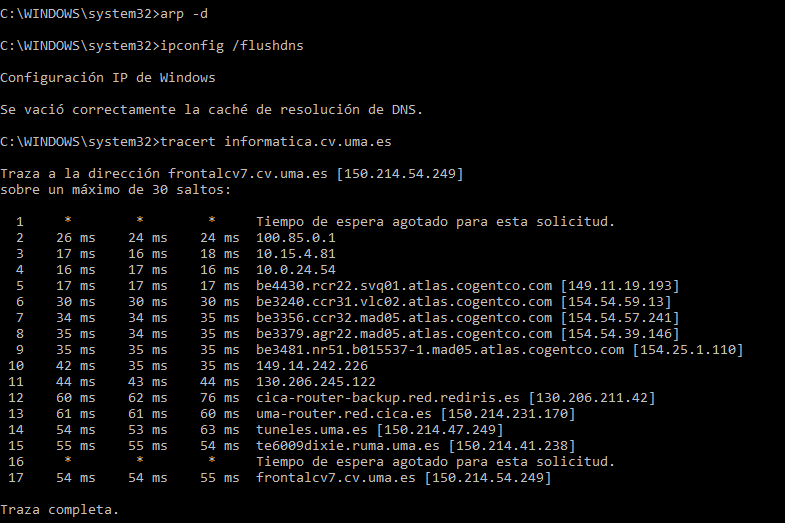


* Número de trama analizado

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?

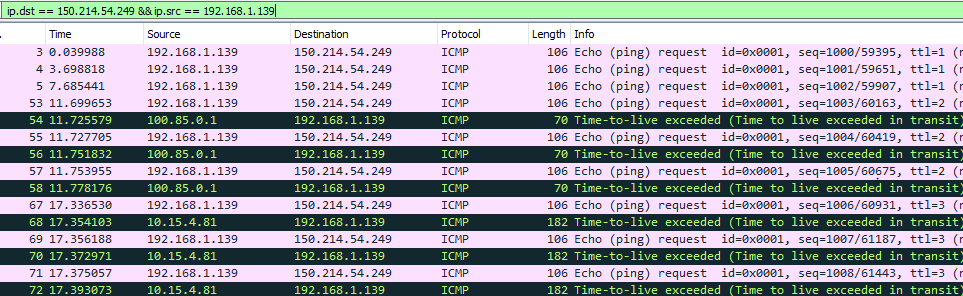
**Ejercicio 6.** Responda a las siguientes preguntas:

* 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?

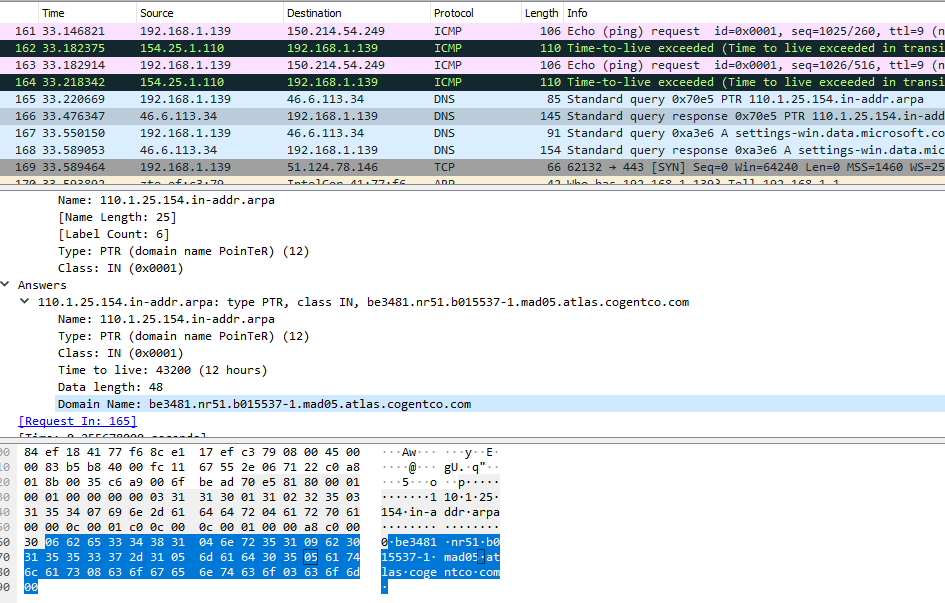
Los de tipo ICMP. Paquetes 3,4,5,53,54,55,56… hay 93 en total que se usan al hacer el tracert.



* 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.



Si nos fijamos en la captura de la consola de este ejercicio en el ttl 9, observamos que esta trama DNS le devuelve la IP del nodo intermedio para que se vaya moviendo, pero esta IP está invertida.

* ¿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.