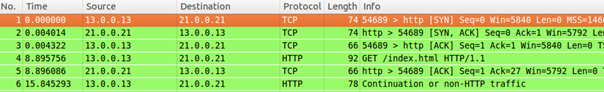
**PRÁCTICA 0**

## **1.1.** **Captura-1**



* **Columna No.**

Su número de orden dentro de la captura. El número 1 es el primer paquete capturado.

* **Columna Time**

Tiempo en segundos que ha pasado desde que se capturó el primer paquete. El primer paquete marca el origen de tiempos, por lo que el valor de tiempo es 0.000000 segundos. El segundo paquete muestra 0.004014 segundos lo que significa que el segundo paquete se capturó transcurridos 0.004014 segundos ***desde que se capturó el primer paquete***. Y así sucesivamente.

* **Columna Source**

Dirección de origen del paquete.

* **Columna Destination**

Dirección destino del paquete.

* **Columna Protocol**

Protocolo de más alto nivel reconocido dentro del paquete.

* **Columna Length**

Longitud total de la trama capturada en bytes (columna Length), sin contar el campo CRC (4 bytes).

* **Columna Info**

Resumen de la información más importante contenida en los protocolos reconocidos en el paquete.

***\*\*NOTA\*\****

*Es importante tener en cuenta que wireshark nunca nos muestra el CRC por lo que para saber la longitud real deberíamos sumar 4 bytes.*

*A todos los paquetes capturados hay que sumarles el CRC ya que wireshark comprueba que el CRC es correcto y lo descarta. Si no fuese correcto no acepta la captura.*

**El CRC** es el control de redundancia cíclica o comprobación de redundancia cíclica**.** Dicho de otra manera **es un codigo de detección de errores.**

El tamaño mínimo de una trama es 64 bytes (contando el CRC)

**Observa que wireshark interpreta el valor de Type 0x0800 como el código asociado al protocolo IP. ¿Qué significa que el valor del campo Type se corresponda con el código asociado al protocolo IP?**

****

Que el campo Tipo lleve el número 0x0800 es para indicar que los datos son del protocolo IP concretamente IPV4. Este código numérico es importante porque hay una lista de diferentes EtherTypes con códigos numéricos diferentes.

**Si la columna Length de la trama tuviera un valor igual a 60 bytes (longitud total de la trama igual a 64 bytes: 60 más 4 bytes del CRC) ¿podrias decir si dicha trama tiene o no relleno?**

Puedo afirmar que esta trama no tiene relleno ya que su longitud total incluyendo 4 bytes del CRC es de 64 bytes.

**1.2. Captura-2**

El código 0X0806 pertenece al protocolo ARP.

Observa para este paquete el campo **Padding.** ¿Que longitud tiene? ¿Qué crees que significa este campo?

El campo Padding tiene una longitud de 18 bytes.

Sabiendo que, el tamaño mínimo de una trama es de 64 bytes.

* Todos los mensajes del protocolo ARP tienen la misma longitud, 28 bytes.
* La cabecera de Ethernet ocupa 14 bytes.
* El CRC 4 bytes.

Por tanto la longitud total de la trama sería 46 bytes y habría que introducir bits de relleno.

64 - 46 = 18

El campo padding tiene una extensión de 18 bytes por lo que cuando hablamos de padding estamos hablando de byts de relleno en una trama.

**Netgui**

**Comandos**

* **ifconfig** (eth0, eth1…) para consultar las direcciones ethernet de una máquina.
* **tcpdump -i ethX -s 0 -w /hosthome/pcX.cap** para capturar tráfico de x máquina.
* **arping -c 1 00:07:e9:22:22:22** para generar tráfico.

*La dirección Ethernet que estamos utilizando (00:07:e9:22:22:22) es la dirección Ethernet destinataria de las tramas, en este caso la de pc2. La opción -c 1 hace que arping envíe un único paquete a la máquina pc2 y que esta le responda.*