

PRÁCTICA

Introducción a Wireshark

Objetivo: Aprender a analizar paquetes capturados con la herramienta Wireshark.

Conocimientos previos: Dominar el concepto de encapsulación.

Desarrollo:

Parte 1: Vamos a analizar el **frame1** que aparece en el fichero Captura1.pcapng.

1. ¿Qué IP tiene el equipo encargado de encapsular el mensaje del frame1?
2. ¿Cuál es la dirección física destino? ¿Tiene algún significado especial la dirección? ¿En qué encabezado podemos encontrar esa dirección? Es importante que lo verifiques en Wireshark.
3. ¿Qué valor contiene el campo Target IP Address? ¿Qué significa?
4. ¿Qué valor contiene el campo Target MAC Address? ¿Por qué tiene ese valor?
5. ¿Qué IP tiene el equipo encargado de desencapsular el mensaje del frame1?
6. Como podrás comprobar en la captura, los bytes que conforman el frame 1 son los mostrados en la figura 1.

```
ff ff ff ff ff ff 3c 97 0e 06 08 2a 08 06 00 01
08 00 06 04 00 01 3c 97 0e 06 08 2a c0 a8 00 68
00 00 00 00 00 00 c0 a8 00 02
```

Figura 1: Bytes del Frame 1

Cumplimenta la siguiente tabla. Para realizar esta cuestión adecuadamente necesitarás analizar previamente la figura 2.

Capa del Modelo OSI	PDU	Bytes del encabezado ¹	Bytes del campo datos	Protocolo
7. Aplicación				
6. Presentación				
5. Sesión				
4. Transporte				
3. Red				
2. Enlace				

Tabla 1: proceso de encapsulación

7. ¿Cuál es el puerto origen del frame1? ¿y el puerto destino? ¿por qué?

¹ Por simplificar, para especificar los bytes generados por cada capa, escribe los 4 primeros dígitos hexadecimales y la longitud de la secuencia en bytes.

Parte 2: Vamos a analizar el frame2 que aparece en Captura1.pcapng.

1. ¿Qué IP tiene el equipo encargado de encapsular el mensaje del frame2?
2. ¿Cuál es la dirección física destino del frame2?
3. ¿Qué contiene el campo Target MAC Address? Contrasta este valor con el del frame1.
4. ¿Qué IP tiene el equipo encargado de desencapsular el mensaje del frame2?

Parte 3: Vamos a analizar el frame3 que aparece en Captura1.pcapng.

1. ¿Qué IP tiene el equipo encargado de encapsular el mensaje del frame3?
2. ¿Qué IP tiene el equipo encargado de desencapsular el mensaje del frame3.
3. Cumplimenta la tabla 1. Para realizar esta cuestión adecuadamente necesitarás analizar previamente la figura

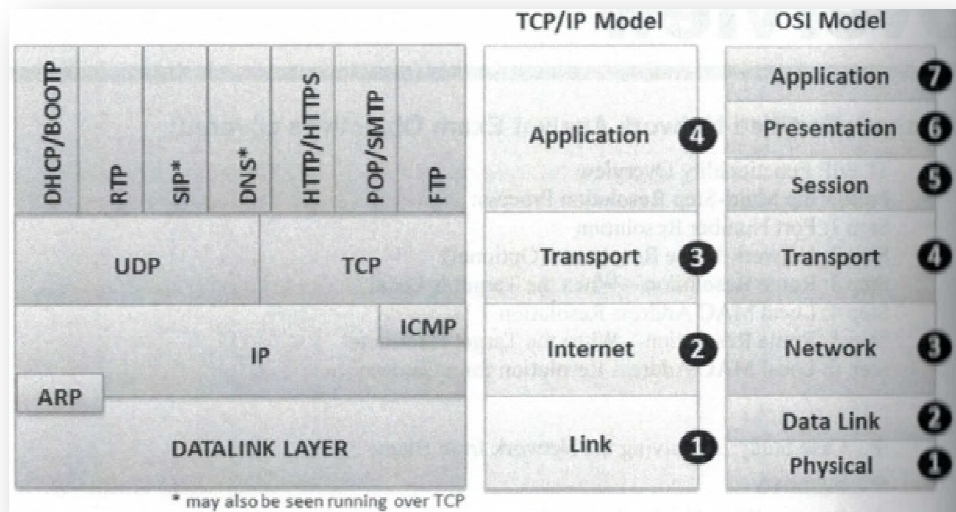


Figura 2: TCP/IP stack. Fuente imagen: Laura Chappell. Wireshark Network Analysis. Chappell University, 2012

4. ¿En qué encabezado están los campos IP origen, IP destino? Es importante que lo verifiques en wireshark.
5. ¿Qué es Internet Control Message Protocol? ¿Por qué hay más frames en la captura que utilizan este protocolo? Analízalo en detalle.
6. ¿A qué se debe que los mensajes ARP aparezcan antes que los ICMP?

Parte 4: Vamos a analizar la conexión HTTP que aparece en Captura2.pcapng.

1. ¿Qué web se está solicitando? ¿Qué frame nos da esa información?
2. ¿Qué IP tiene el equipo cliente?
3. ¿Qué IP tiene el servidor web?
4. Cumplimenta la tabla 1.

Trabajo en casa: Ahora ya puedes realizar tus propias capturas en casa y empezar a analizarlas. Los siguientes anexos podrás utilizarlos como información de apoyo.

Anexo I: Instalación de Wireshark

Wireshark es una herramienta gratuita y puede descargarse en <https://www.wireshark.org/>

Si tu sistema operativo es Windows, es necesario que aceptes la instalación de WinPcap. Esta librería aportará la funcionalidad de captura de paquetes. Los usuarios de Linux utilizan la librería LibPcap y esta ya viene integrada en el propio sistema operativo.

Anexo II: Antes de lanzar una captura con Wireshark

Antes de empezar, es necesario averiguar cuál es la interfaz de red² de nuestro equipo que utilizaremos para efectuar la captura. ¿Cómo podrías averiguarlo?

Anexo III: Lanzando una captura con Wireshark

En la ventana principal pinchamos en Capture Options (Figura 3).

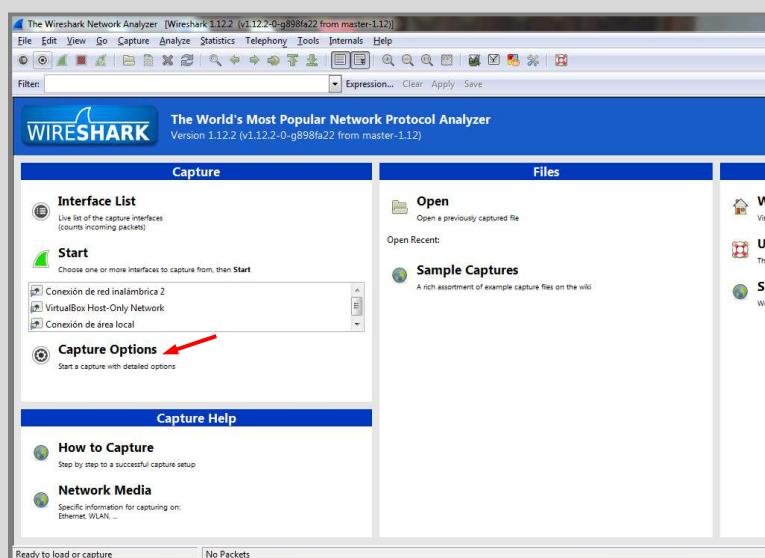


Figura 3: Ventana inicial de Wireshark

Wireshark mostrará la ventana de la figura 4. Como podéis ver, esta venta lista todas las interfaces de red que posee nuestro ordenador. Debemos elegir la que obtuvimos en anexo II.

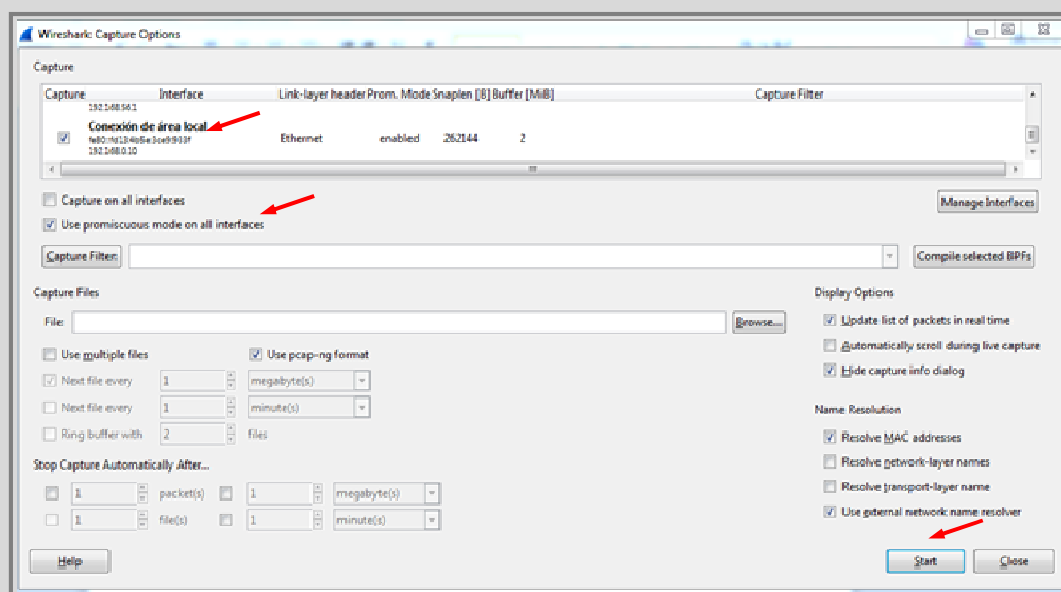


Figura 4: Ventana opciones de captura de Wireshark

² También conocida como tarjeta de red, adaptador de red, NIC.

Si en la figura 4 marcamos la opción “Use promiscuous mode on all interfaces”, Wireshark capturar  todo el tr fico que circula por el medio f sico, aunque no vaya dirigido a nuestro equipo. Importante: no todas las tarjetas de red son compatibles con este modo.

Si en la figura 4 NO marcamos la opci n “Use promiscuous mode on all interfaces”, Wireshark s lo capturar  el tr fico dirigido a nuestro equipo.

Por  ltimo, pulsar el bot n Start para lanzar la captura (figura 4).

Anexo IV: Familiariz ndonos con el entorno de captura de Wireshark

Wireshark mostrar  en la ventana de la figura 5 los frames que va capturando.

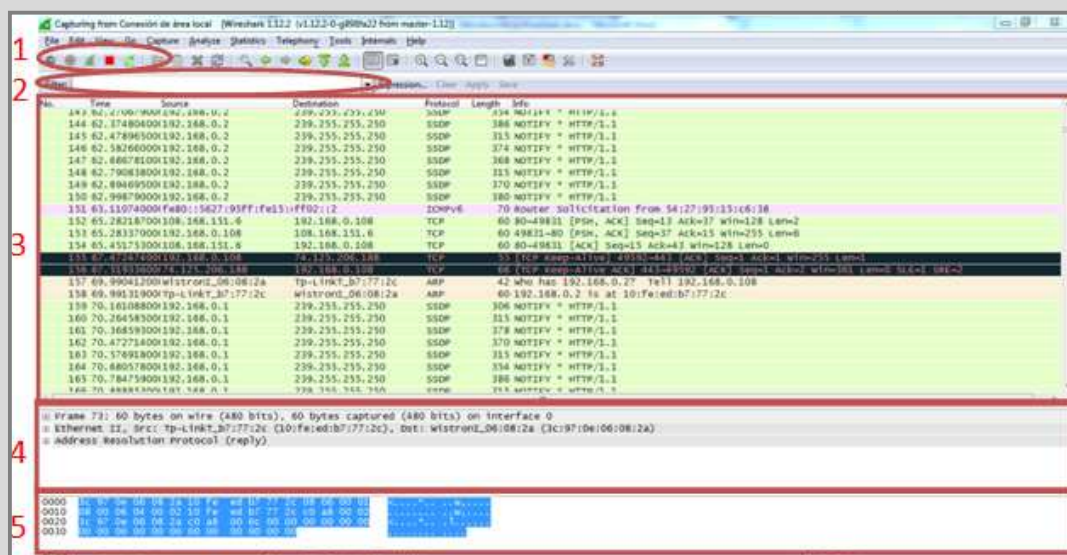







Figura 5: Ventana de captura de Wireshark

A continuaci n, se detallan las partes principales de la ventana de la Figura 5:

1.- Botones b sicos:

-  Listar las interfaces de red de nuestro equipo.
-  Ir a la ventana opciones de captura (figura 4). Bot n no disponible durante la captura.
-  Iniciar la captura.
-  Parar la captura.
-  Reiniciar la captura.

2.- En este cuadro de texto podemos introducir un filtro para mostrar s lo determinados paquetes de la captura. Es recomendable filtrar una vez hayamos parado la captura o antes de iniciarla.

3.- Este es el panel “lista de paquetes”, en  l aparecen los paquetes capturados (frames). Por columnas se puede observar el n mero del frame, direcci n del equipo origen, direcci n del equipo destino, protocolo utilizado, etc. Si hacemos click en un frame concreto, podremos ver m s detalles en los paneles “Detalles del paquete” y “Bytes del paquete”.

4.- Este es el panel “Detalles del paquete”. En este panel podemos ver los distintos encabezados del frame seleccionado. Si expandimos un encabezado, podremos ver todos sus campos.

5.- Este es el panel “Bytes del paquete”. En este panel podemos ver el paquete capturado en formato hexadecimal y Ascii. Pod is observar como marca el encabezado/campo que se ha seleccionado en el panel “Detalles del paquete”.