Índice

Arquitectura de protocolos TCP/IP

Área de Arquitectura y Tecnología de Computadores – Versión 1.0.915, 24/03/2022

Objetivos

En esta sesión se van a estudiar cómo se construye una arquitectura de protocolos en capas y, con más detalle, la arquitectura de capas de los protocolos TCP/IP. Para capturar las tramas se va a utilizar el analizador de paquetes de red de licencia libre *Wireshark*. Con esta herramienta se puede determinar el estado de las redes de computadores a partir del estudio de los paquetes que viajan a través de ellas.

Esta herramienta presenta varias formas de uso. Así, un administrador de sistemas puede utilizarla para buscar problemas de congestión en la red; un administrador de seguridad, para encontrar posibles fallos de seguridad; un desarrollador de protocolos, para realizar tareas de depuración; o, en nuestro caso, un estudiante, para la comprensión y estudio de los distintos protocolos de red.

Conocimientos y materiales necesarios

Antes de comenzar esta práctica el alumno debe:

- Conocer las herramientas fundamentales de diagnóstico y configuración de la red.
- Acudir al laboratorio de prácticas con el libro de apuntes de la asignatura.
- Durante la sesión se plantearán una serie de preguntas que puedes responder en el correspondiente cuestionario en el Campus Virtual. Puedes abrir el cuestionario en otra pestaña del navegador pinchando en el enlace mientras mantienes pulsada la tecla `Ctrl`.

1. El analizador de protocolos *Wireshark*

Inicia el programa *Wireshark* para analizar tramas [1] y paquetes [2] de red.

En la pantalla de presentación se muestran las diferentes opciones de trabajo y configuración del programa. La sección inferior muestra la lista de interfaces de red disponibles en nuestra máquina y a los que *Wireshark* tiene acceso [3]. La opción **Open** permite acceder a un archivo que contenga una captura realizada con el programa.

- En el menú, selecciona la opción **Edit › Preferences › Name Resolution** y desactiva la opción `Resolve MAC addresses`.
- Selecciona la opción **Open**. Abre el archivo `6-captura.cap`, que se ha suministrado con el material de la práctica.

El programa mostrará un aspecto similar al de la figura 1 [4]. En el caso de que la pantalla inicial no sea igual a la mostrada en dicha figura se puede ir a **Edit › Preferences › User Interface › Layout** y seleccionar las opciones que se muestran en la figura 2. Como podemos comprobar en la figura, en el panel superior se muestra el listado de las tramas de red o paquetes que contiene el archivo, en el segundo panel se muestran los detalles, a nivel de protocolo, de la trama que seleccionemos y, en el tercer panel, tenemos los bytes concretos que conforman dicha trama.

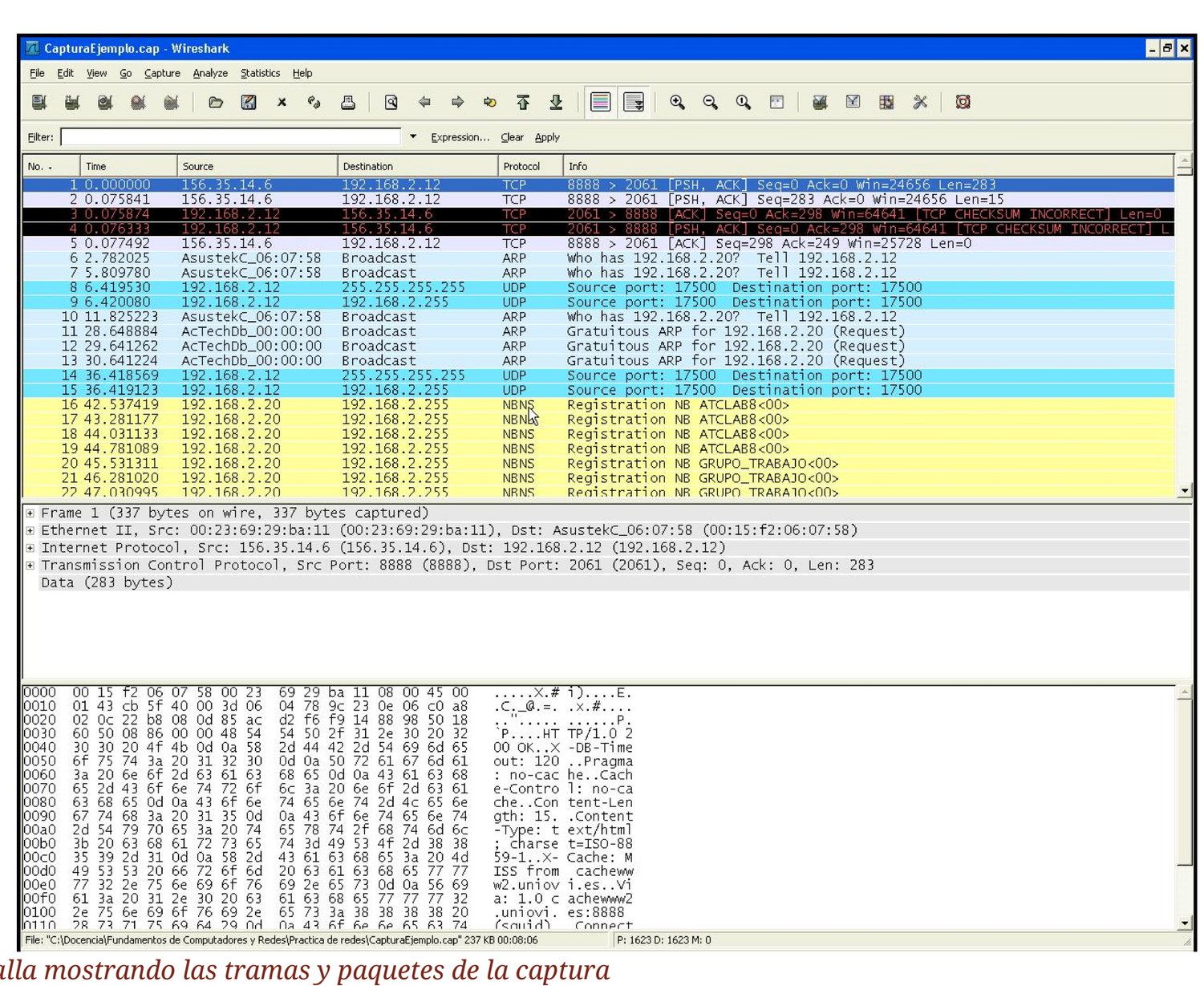

Figura 1. Pantalla mostrando las tramas y paquetes de la captura

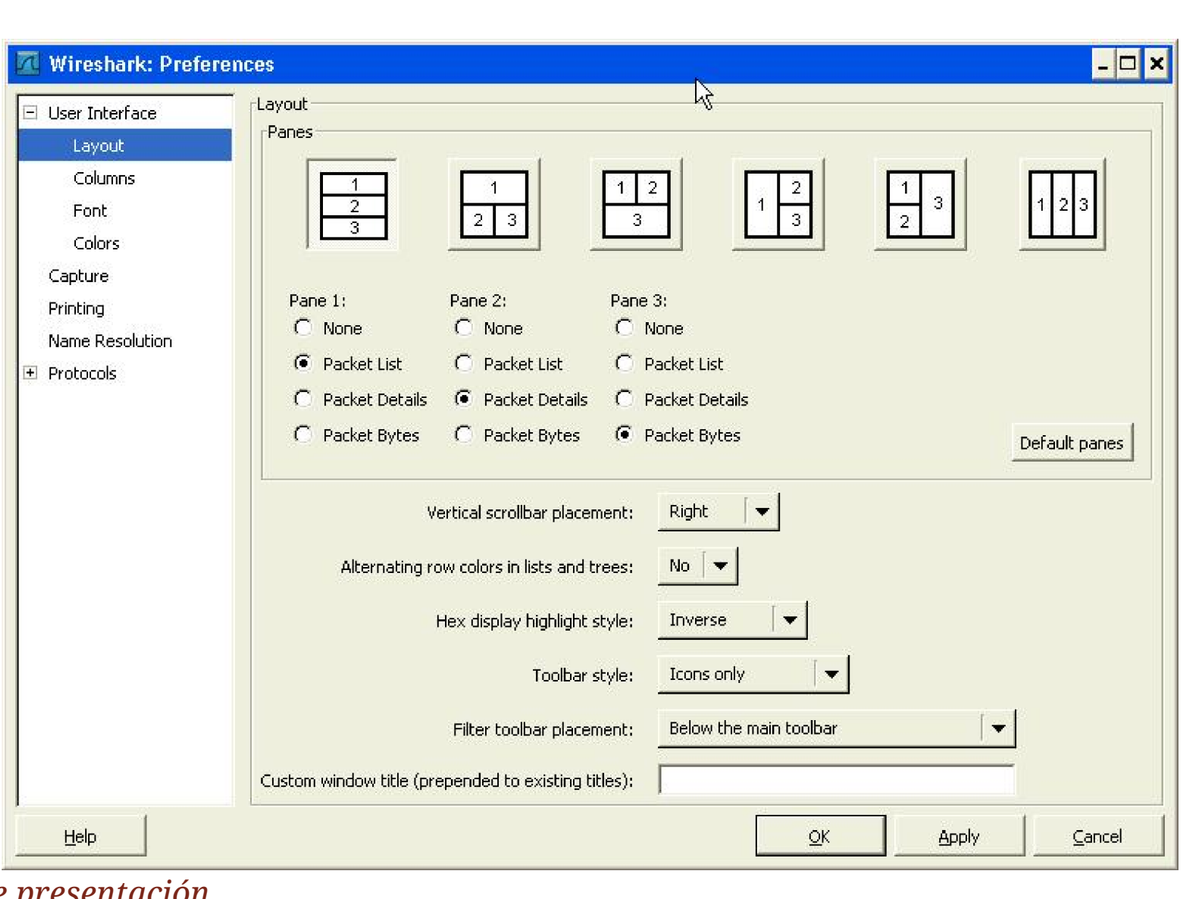

Figura 2. Configuración de presentación

1.1. Opciones de presentación

En el panel superior la información está organizada en columnas, las cuales tienen las siguientes etiquetas:

No. Es el número de orden de la trama. La primera trama que se capturó tiene el número 1, la siguiente el 2, y así sucesivamente.

Time Es una referencia al instante en el que se capturó la trama.

Source Dirección de origen de la trama. En este campo el aspecto de la información mostrada depende del tipo de trama.

Destination Dirección de destino de la trama. Como en el caso anterior, la información mostrada va a depender del tipo de trama.

Protocol Protocolo que contiene la trama capturada. *Wireshark* muestra el protocolo de más alto nivel que logra identificar. Así, por ejemplo, aunque todos los paquetes TCP o UDP tienen que ir dentro de un datagrama IP, la información que se muestra en este campo no es IP sino UDP o TCP, según corresponda.

Info Información que contiene la trama. Cuando son datos de usuario, muestra unos pocos bytes nada más.

Las cabeceras de las columnas son botones que nos permiten alterar la forma de presentación de los datos. Cada vez que pulsamos sobre una de ellas nos permite cambiar la ordenación de los datos de mayor a menor, y viceversa.

- Pulsa dos veces sobre la cabecera de la columna `No.`. Observa los cambios.
- Selecciona la trama número 11. Fíjate que la primera dirección mostrada está formada por 12 dígitos hexadecimales agrupados de dos en dos separados por el carácter ":". Se trata de una dirección de la capa de enlace, en concreto del protocolo Ethernet.
- Selecciona ahora la trama número 1. Fíjate que la primera dirección mostrada está formada por cuatro números separados por puntos. Se trata de una dirección de la capa de red, en concreto del protocolo IP.
- Fíjate en la columna `Protocol`. Desplaza hacia arriba y hacia abajo para ver los distintos protocolos que hay en las tramas capturadas que contiene el archivo. Podrás comprobar que hay multitud de protocolos distintos: ARP, DCERPC, ICMP, IGMP, SMB, etc.

2. Filtrado y análisis de paquetes

Wireshark permite filtrar las tramas por cualquier valor en cualquiera de los campos que se muestran en el panel superior. Para activar un filtro en una columna con un valor que nos interese, si este ya está presente y visible, simplemente nos tenemos que colocar sobre el valor y pulsar el botón derecho del ratón. Aparecerá un menú emergente como el de la figura 3 que permite definir con más precisión el filtro.

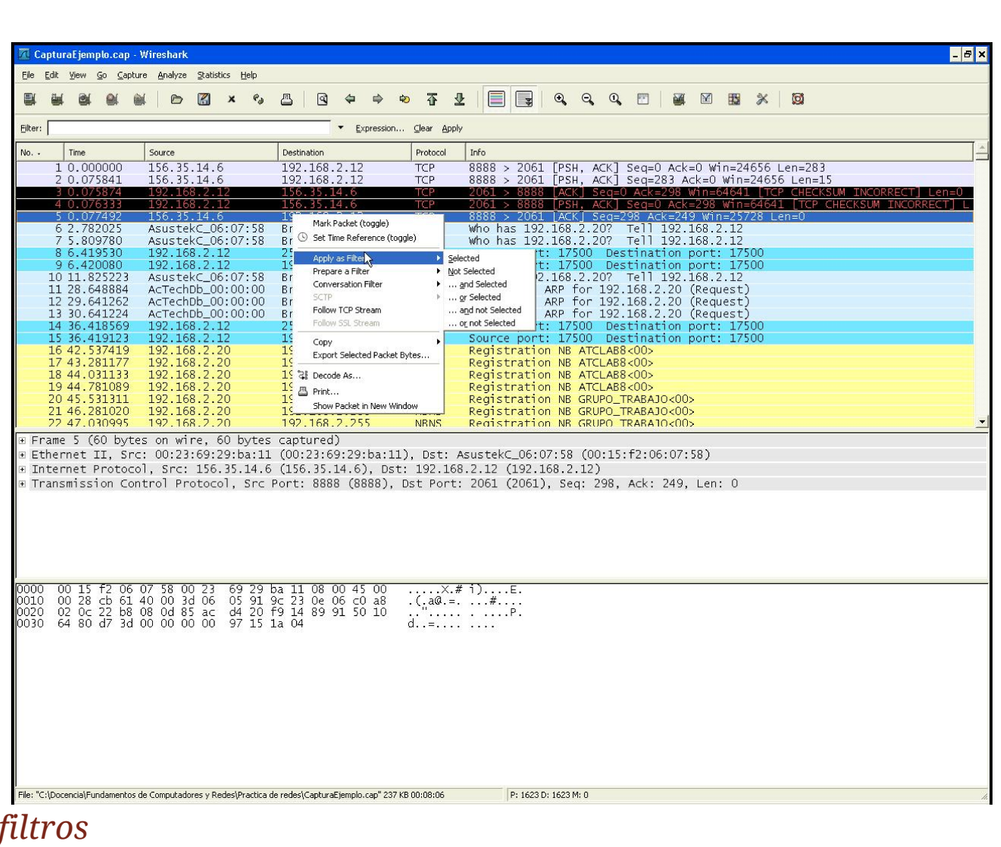

Figura 3. Menú de definición de filtros

Las posibilidades del menú emergente para definir filtros son tres: **Apply as Filter**, **Prepare a Filter** y **Conversation Filter**. Las dos primeras se diferencian en que la primera prepara y aplica inmediatamente el filtro a las tramas del archivo de captura. Por su parte, la segunda solo lo prepara, apareciendo en el cuadro de texto **Filter** del programa el código necesario para que el filtro tenga efecto, pero sin aplicarlo hasta que se pulse sobre la flecha en la caja de filtrado.

La opción **Conversation Filter** permite extraer del archivo aquellos paquetes que se intercambian las máquinas que hayamos seleccionado. Veamos como funciona:

- Haz click sobre la columna **Source** del paquete número 5 y pulsa el botón derecho del ratón.
- Selecciona la opción **Conversation Filter › IPv4**. A partir de ese momento en el panel superior solo se muestran los paquetes IP que se han intercambiado las máquinas de direcciones 156.35.14.6 y 192.168.2.12, que son las máquinas que se intercambiaron el paquete número 5 que hemos seleccionado en el paso anterior. Fíjate que ambas máquinas pueden ser tanto origen como destino de los paquetes.
- Observa el cuadro de la ventana **Filter** en el que se encuentra la expresión que selecciona los paquetes a mostrar. Colócate en el cuadro de texto y vete hasta el final para ver la expresión completa. Intenta comprender la expresión.
- Arregla la expresión del filtro para que se muestren los paquetes IP que se han intercambiado entre las máquinas 192.168.2.20 y 192.168.2.12.
- Limpia la expresión del filtro pulsando el botón `x` y vuelve a las primeras tramas del archivo usando la barra de desplazamiento vertical.

Apply as Filter y **Prepare a Filter** presentan las mismas posibilidades para construir un filtro permitiendo hacer operaciones lógicas entre varias condiciones. Veamos un ejemplo:

- Pulsa con el botón derecho en el campo **Source** del paquete número 16. Selecciona **Prepare a Filter › Selected**. Observa lo que ha aparecido en la ventana **Filter**. Observa también que no se ha aplicado aún el filtro.
- Pulsa con el botón derecho en el campo **Destination** del paquete número 5. Selecciona **Prepare a filter › …and Selected**. Observa lo que ha aparecido en la ventana **Filter**.
- Pulsa el botón con la flecha en la caja del filtro para aplicarlo. ¿Qué ha ocurrido?
- Pulsa el botón `x` en la caja de filtro y vuelve a la cabecera del archivo.

3. La arquitectura de protocolos en capas

Cuando queremos enviar una nota a una persona en otra ciudad metemos la nota en un sobre, escribimos la dirección de la persona en el exterior, hacemos llegar el sobre al servicio de correos, el cual lo transporta a la otra ciudad y allí un servicio de reparto lo entrega a la persona deseada. No se nos ocurre llevar la nota en persona y, desde luego, no esperamos que la otra persona venga a nuestro domicilio a entregarnos la nota de respuesta. De la misma manera cuando un programa que está ejecutándose en una máquina quiere enviar un dato a otro programa que está ejecutándose en otra máquina, no lo hace directamente sino que utiliza distintos servicios intermedios para hacerlo. En la sección 8.2 del libro de teoría se explica que estos servicios de transporte intermedios configuran una **arquitectura de protocolos** en capas y que, como podemos comprobar en la figura 4, cada capa por la que atraviesa el dato, añade una cierta cantidad de bytes al paquete para poder realizar su trabajo (en el ejemplo del correo es el equivalente al sobre, la dirección, el remite, el código postal, el sello, etc.).

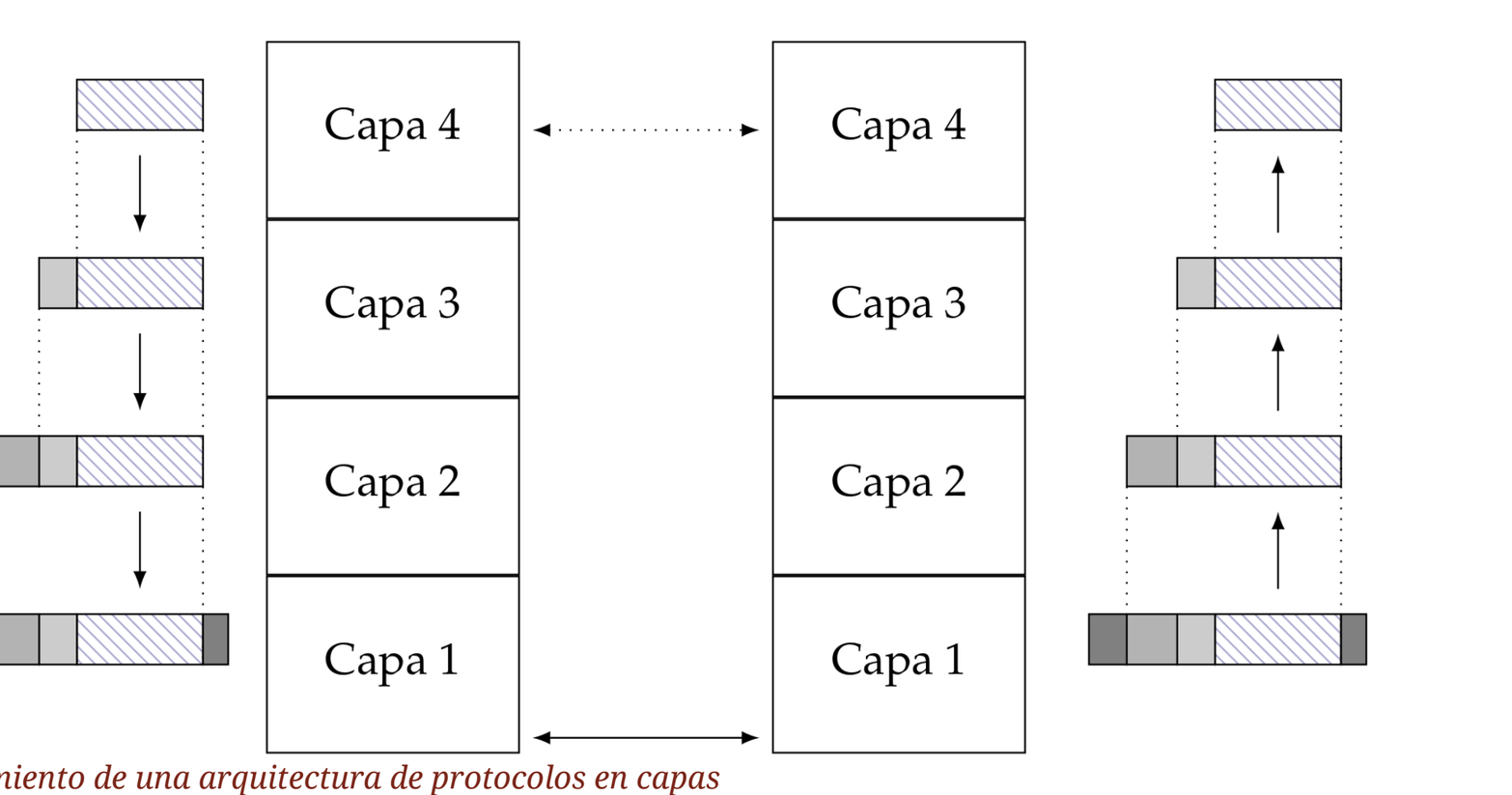

Figura 4. Funcionamiento de una arquitectura de protocolos en capas

Vamos a utilizar el programa *Wireshark* para analizar las distintas capas y cuáles son los bytes que añade cada capa cuando dos aplicaciones quieren transferir información a través de una red de telecomunicaciones basada en TCP/IP. Vamos a utilizar como ejemplo de aplicaciones un servidor *Web* y un navegador que le solicita una página.

El archivo `6-peticionHTTPcorta.pcap` contiene la captura de una sesión de comunicaciones entre el navegador y el servidor web. La sesión consiste en el envío, por parte del navegador, de una petición de un archivo al servidor web y de la respuesta de éste con el envío del archivo.

- Abre el archivo `6-peticionHTTPcorta.pcap` que se ha suministrado con el material de la práctica. Lo que ves en el primer panel son las 13 tramas de datos que se han tenido que intercambiar entre la máquina del navegador y la máquina del servidor web para que el navegador reciba el archivo.
- Escribe `http` en el campo **Filter** y pulsa la flecha en la caja de filtro para aplicar un filtro que sólo muestre los paquetes relacionados con el protocolo HTTP ("*Hyper Text Transfer Protocol*"), que es el que utilizan los navegadores y los servidores web para comunicarse entre sí. Los dos paquetes que han quedado en el primer panel son los únicos que contienen la información que se intercambiaron directamente el navegador y el servidor web. El intercambio entre el navegador y el servidor se inicia con el envío por parte del navegador de una petición `GET` al servidor con el nombre del archivo que desea. A esa petición responde el servidor con `OK` y el archivo, si lo tiene, o con `ERROR` si no lo tiene. En este caso, ha enviado el archivo.
- En el panel superior de *Wireshark* marca el primer paquete. En el panel intermedio se muestra, interpretado, lo que contiene el paquete. Cada una de las líneas del panel intermedio (excepto la primera, que da información general) representa una capa en la arquitectura de protocolos que ha atravesado la información en su camino entre el navegador y el servidor web. En el panel inferior vemos los bytes que conforman realmente ese paquete. En cada fila se muestran 16 bytes. La columna de la izquierda muestra la dirección (desplazamiento con respecto al inicio del paquete) del primer byte mostrado en esa fila, las dos columnas del centro muestran los bytes del paquete en hexadecimal y la columna de la derecha muestra su interpretación como ASCII.
- Pulsa sobre las palabras **Hypertext Transfer Protocol** en el panel intermedio. Verás que en el panel inferior se han marcado de azul una serie de bytes: son los que forman parte del protocolo HTTP. Son fáciles de reconocer porque los primeros bytes son los códigos ASCII de la petición del navegador `GET /hola.html`.
- Mueve la barra de desplazamiento del panel inferior hacia arriba y hacia abajo. Comprobarás que hay bytes que no están seleccionados en azul. Eso significa que el paquete contiene más bytes que los correspondientes al protocolo HTTP. Son los bytes que han añadido las demás capas de protocolo. Aunque en el panel intermedio **HyperText Transfer Protocol** se encuentra en la línea inferior, su posición en la arquitectura de protocolos es la más alta, la más cercana a los programas de usuario, es la correspondiente a la capa de aplicación en la figura 5.
- Pulsa ahora sobre las palabras **Transmission Control Protocol** en el panel intermedio. Acabas de descender un nivel en la arquitectura de protocolos y te has colocado en la capa de transporte. Verás que en el tercer panel se han seleccionado un conjunto diferente de bytes (mueve la barra de desplazamiento si lo necesitas) que son la cabecera del protocolo TCP. Comprueba, alternando la selección entre **HyperText Transfer Protocol** y **Transmission Control Protocol**, que los bytes de HTTP están justo a continuación de los correspondientes a la cabecera del protocolo TCP. Esto significa que los bytes de HTTP son los datos que transporta TCP.
- Pulsa ahora sobre las palabras **Internet Protocol** en el panel intermedio. Nuevamente, en el tercer panel se han seleccionado un conjunto diferente de bytes (mueve la barra de desplazamiento si lo necesitas). Has vuelto a descender un nivel en la arquitectura de protocolos y ahora te has colocado en la capa de red o internet (Capas TCP/IP). Comprueba, alternando la selección entre **Internet Protocol** y **Transmission Control Protocol**, que los bytes de la cabecera de TCP están también a continuación de los correspondientes a la cabecera del protocolo IP. De nuevo eso significa que los bytes de TCP son los datos que transporta IP.
- Pulsa ahora sobre **Ethernet II** en el panel intermedio. Como era de esperar, en el tercer panel se ha seleccionado un conjunto diferente de bytes (mueve la barra de desplazamiento si lo necesitas). Lo has hecho otra vez. Has descendido un nivel en la arquitectura de protocolos y ahora te has colocado en la capa de enlace. Como antes has hecho, comprueba, alternando la selección entre **Internet Protocol** y **Ethernet II**, que los bytes de IP están a continuación de los correspondientes a la cabecera de la trama de Ethernet. Como en los casos anteriores, eso significa que los bytes de IP son los datos que transporta Ethernet.

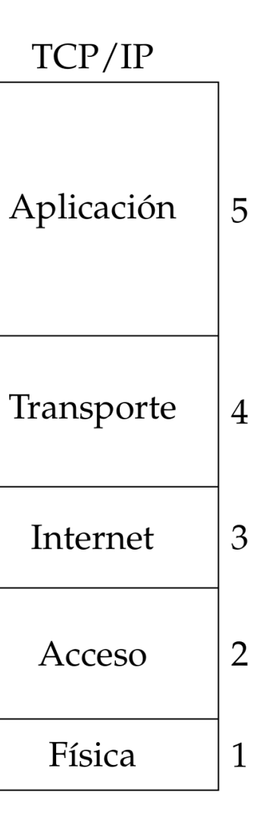

Figura 5. Capas TCP/IP

Si repasamos todos los pasos anteriores podemos ver que en el nivel más bajo tenemos una trama Ethernet que, en su campo de datos, transporta un datagrama IP. A su vez, el datagrama IP, en su campo de datos, transporta un segmento TCP que, en su campo de datos, lleva unas instrucciones del protocolo HTTP. Esas instrucciones HTTP son la información que quería enviar el navegador al servidor web. Esta encapsulación de unos datos dentro de otros es es el resultado de organizar los protocolos en una arquitectura en capas.

- Alterna la pulsación sobre los distintos niveles de protocolo en el panel intermedio para ver la selección de los bytes en el tercer panel hasta que te quede claro el concepto.
- En la figura 6 se muestra un esquema del encapsulamiento de protocolos en el interior de la trama. Rellena, en los huecos de la fila etiquetada con `BYTE`, el valor del primer y último byte de cada protocolo implicado. En la fila de abajo, indica en qué posición de la trama se encuentra cada uno de los bytes de la fila superior. La posición escríbela también en hexadecimal ya que es así como la obtienes de *Wireshark*.

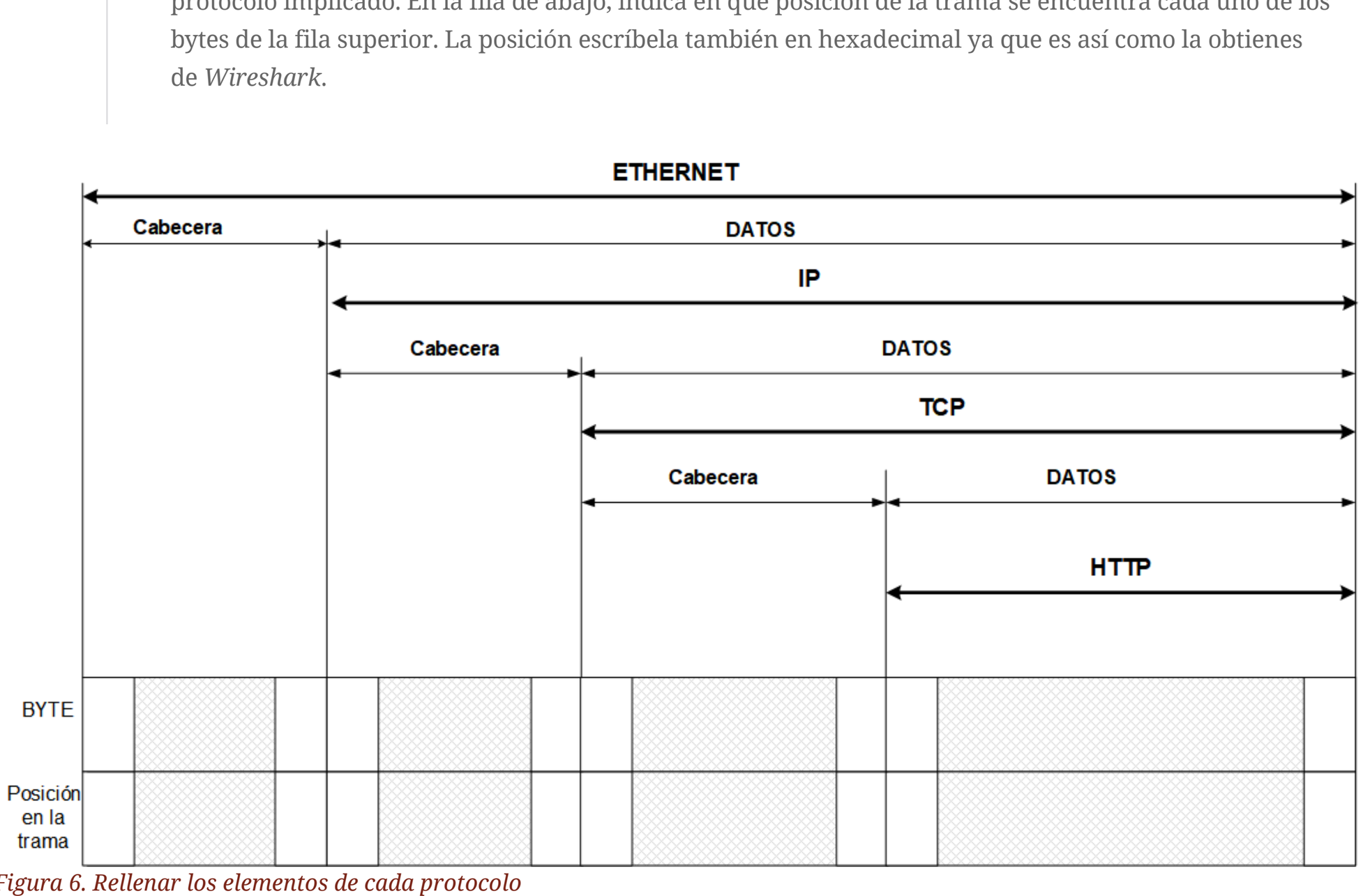

Figura 6. Rellenar los elementos de cada protocolo

4. Ejercicios adicionales

4.1. Elementos del medio físico

Vamos a identificar los elementos del hardware que configuran nuestra red.

- Accede a la parte trasera del computador en el que te encuentras, identifica el cable de red y desconéctalo del computador. Fíjate en el conector, ¿sabrías decir de qué tipo es? Responde en el cuestionario: pregunta 1. (Puedes consultar a tu profesor en el caso de que no lo recuerdes). El tipo de cable que tienes en la mano se denomina "par trenzado". ¿Cuántos cables hay en su interior? Responde en el cuestionario: pregunta 2. (Si tienes dificultad con los cables, puedes contar los contactos del conector).
- Es posible que el cable tenga impresas unas letras que indiquen sus propiedades físicas. ¿De qué categoría es el cable? Responde en el cuestionario: pregunta 3. La categoría del cable está relacionada con la máxima velocidad de transferencia que soporta dicho cable ¿Cuál es la máxima velocidad de trasferencia en ese cable? Responde en el cuestionario: pregunta 4.

4.2. Captura en tiempo real

Es posible que la copia de *Wireshark* instalada en el laboratorio de prácticas te permita realizar la captura en tiempo real de las tramas que circulan por la subred del laboratorio. En ese caso, puedes realizar lo siguiente:

✓ Cierra el archivo actual con **File › Close**.

✓ Selecciona **Capture › Options**. Se abrirá la ventana de opciones de la figura 7. En esa ventana nos interesa el cuadro **Interface**, en el que debemos seleccionar `local` y la interfaz de red física; el cuadro **File**, que nos permite seleccionar un fichero en el que almacenar los datos que vamos capturando; y el cuadro **Capture Filter** en el cual podemos poner una expresión que se aplicará antes de capturar la trama y, si ésta no cumple las condiciones del filtro, será rechazada.

✓ Selecciona un archivo en el que almacenar los paquetes capturados.

✓ Introduce en el cuadro del filtro, al lado del botón `Capture Filter`, la cadena `tcp port http` e inicia una captura.

✓ Abre el navegador y visita alguna página web.

✓ Detén la captura y analiza el archivo generado.

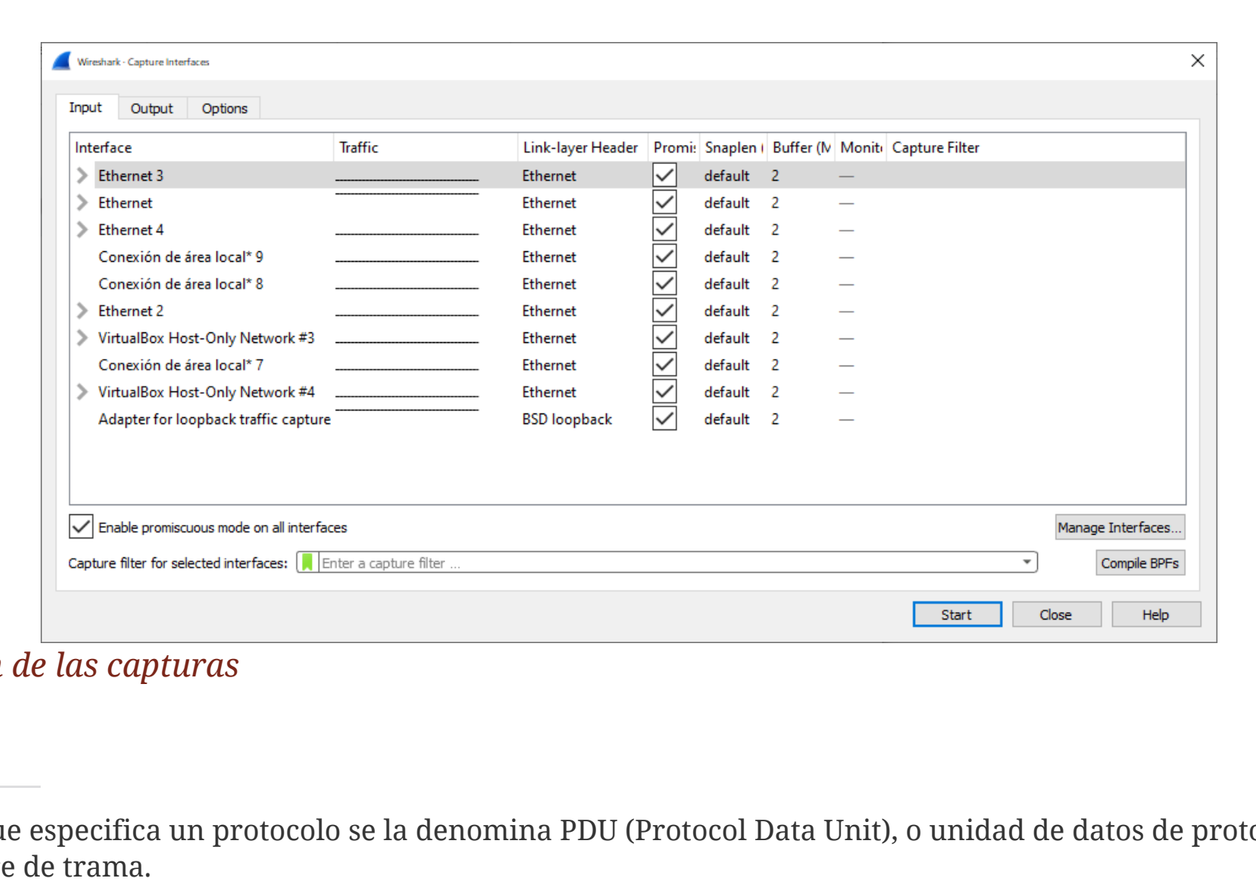

Figura 7. Configuración de las capturas

1. A la unidad de datos que especifica un protocolo se la denomina PDU (Protocol Data Unit), o unidad de datos de protocolo. A nivel de enlace, la PDU recibe el nombre de trama.
2. PDU a nivel de red. También recibe el nombre de datagrama.
3. Sin permisos de administrador es posible que no se muestren.
4. En esta figura la opción `Name Resolution` está habilitada, con lo que se puede observar el fabricante de cada interfaz de red.