REDES DE COMPUTADORES

Grado en Ingeniería en Informática
Doble Grado en Ingeniería Informática y ADE

Curso académico 2023/2024

PRACTICA 0. Metodología de trabajo en las prácticas de la asignatura

Contenidos

1. OBJETIVOS

El laboratorio de prácticas de la asignatura **Redes de Computadores** tiene como objetivo proporcionar al alumnado las destrezas y el conocimiento de herramientas tecnológicas que le permitan la comprensión del funcionamiento de las redes de comunicaciones actuales.

Dentro del marco profesional de la actividad de la Ingeniería Informática está la función de Administrador de Redes, que tendrá las responsabilidades de diseño y gestión de los sistemas de comunicaciones de una entidad. Puede definirse una **red de computadores** como el **conjunto de computadores que son capaces de intercambiar información entre ellos empleando un medio de comunicación** (cables eléctricos, fibra óptica, ondas electromagnéticas).

Una red de computadores muy sencilla es la denominada red **Ethernet de bus común**. Este tipo de red interconecta todos los computadores empleando un solo cable eléctrico, de manera que existe comunicación física entre todos ellos.

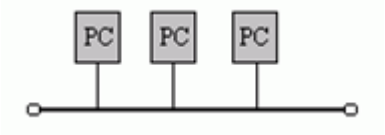

Figura 1. Estructura de de una red de computadores Ethernet de bus común.

Aunque durante décadas coexistieron diferentes tecnologías de sistemas de comunicaciones (voz analógica, fax, vídeo analógico, Internet, redes X.25, etc.) en la actualidad la inmensa mayoría de sistemas de comunicaciones emplean la **Arquitectura de Red TCP/IP**.

Una arquitectura de red define el funcionamiento de un sistema de comunicaciones: desde las aplicaciones que pueden ser utilizadas (navegadores web, clientes de correo, videoconferencias, etc.) hasta las características físicas de los medios de comunicación empleados. La Arquitectura TCP/IP tiene su origen en una red de comunicaciones de la década de 1970 (ARPANET) diseñada específicamente para computadores con sistema operativo Unix (precursor de Linux). La adopción de la Arquitectura TCP/IP, conocida popularmente como

Internet, es un fenómeno digno de estudio al haber desplazado a otras de grandes prestaciones (ATM, RDSI, etc.) y ser empleada por todos los dispositivos actuales: desde smartphones, tablets y computadores personales hasta decodificadores de vídeo y TV, terminales telefónicos o electrodomésticos.

El trabajo dedicado a la administración de redes no deja de ser como cualquier otro trabajo en ingeniería: **un trabajo fundamentado en el método científico**.

El profesional de la ingeniería deberá ser capaz de resolver problemas (pues es la esencia de esta actividad profesional) y para ello debe seguir un metódico procedimiento basado en el **conocimiento** y la **experimentación**.

Las prácticas de la asignatura "Redes de Computadores" complementan a los contenidos teóricos que se imparten en la asignatura, afianzándolos, y proporcionan un acercamiento real a la actividad profesional de la administración de redes.

1.1 Metodología de las prácticas

La resolución de problemas en ingeniería se fundamenta en el conocimiento acerca de las diferentes tecnologías y su experimentación para verificar el correcto funcionamiento de las mismas.

Así, las prácticas de la asignatura proporcionaran en los enunciados el conocimiento necesario sobre las diferentes tecnologías empleadas en las redes de Internet. Para su correcta comprensión se plantearán una serie de experimentos en las que el alumnado deberá verificar que los resultados se corresponden con la descripción de la tecnología. **Es muy importante leer detenidamente los enunciados de las prácticas ANTES de realizar los experimentos propuestos.**

Al igual que en física o química existen una serie de instrumentos de medida para verificar que el resultado de un experimento está en consonancia con las leyes asociadas, en las redes de computadores existe un instrumento de medida que se denomina **monitor de red**.

El monitor de red es una herramienta software que permite visualizar la información que está siendo intercambiada (transmitida y recibida) por un computador en una red de comunicaciones. Aunque a lo largo de la asignatura se estudiará en detalle cómo se realiza el intercambio de información, puede afirmarse de manera general que los computadores intercambian grandes volúmenes de información en bloques limitados en tamaño denominados **paquetes**.

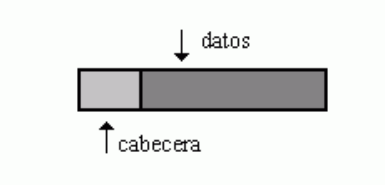

Figura 2. Estructura de un paquete transmitido en una red de comunicaciones.

Cada paquete es una secuencia de bits dividida en dos partes: una parte inicial denominada cabecera (que hace referencia al tipo de datos intercambiado, los computadores que lo intercambian, etc.) y una parte posterior que son los datos a intercambiar (contenido de una página web, contenido de un correo electrónico, vídeo, etc.)

La realización de las prácticas conlleva la elaboración de un **cuaderno de laboratorio**. Este cuaderno, de formato libre, deberá recoger las actividades experimentales llevadas a cabo en el laboratorio. Para cada experimento deberá indicarse:

a) Enunciado del experimento a realizar y acciones llevadas a cabo (comandos ejecutados en el computador).
b) Resultado del experimento indicado la información visualizada por el monitor de red (tipos de paquetes visualizados).
c) Breve conclusión que permita verificar que el resultado del experimento se corresponde con el modo de funcionamiento de la tecnología.

Para ser evaluado en la asignatura el alumnado deberá tener al día el cuaderno de laboratorio y mostrarlo al profesor de prácticas cuando lo requiera en el laboratorio.

2. INICIACIÓN AL MONITOR DE RED

El monitor de red que se empleará en las prácticas de la asignatura es **Wireshark** que permitirá, empleando una interfaz gráfica, visualizar los paquetes que circulan por el medio físico (lo que se denomina realizar una **captura de paquetes**).

Wireshark es un software multiplataforma de captura de paquetes en redes muy extendido y de libre distribución. Al igual que un gran número de herramientas utilizadas en la administración de redes, se basa en unas librerías comunes conocidas como 'pcap' o 'winpcap' dependiendo de la plataforma utilizada.

El formato de los ficheros de captura que **Wireshark** utiliza es compatible con otras herramientas tales como **tcpdump**, **tcptrace**, **tcpflow**, **snort**, **ntop** y un largo etc., todas ellas especializadas en el tratamiento de capturas de paquetes.

Se podrían enumerar las siguientes ventajas:

- Interfaz gráfica de usuario.
- Compatible en lectura y escritura con capturas realizadas mediante otros monitores de red como *tcpdump.*
- Sintaxis de filtrado de paquetes muy flexible y potente.
- Funciona tanto en entornos Linux como en Windows.
- Se pueden intercambiar las capturas realizadas en máquinas Windows y Linux.

Para realizar una captura y exploración de la información que circula por la red pueden seguirse los pasos básicos que se comentan en sucesivos apartados.

2.1 Inicio de una captura de paquetes que circulan por la red

Al iniciar el programa, en la parte central se indica la opción **'Capturar'** donde aparece un listado de interfaces de red (conexiones a redes) disponibles en el computador. En el laboratorio de prácticas el interfaz de red a emplear es el **Ethernet**, pues es el que conecta el PC a la red Ethernet del aula.

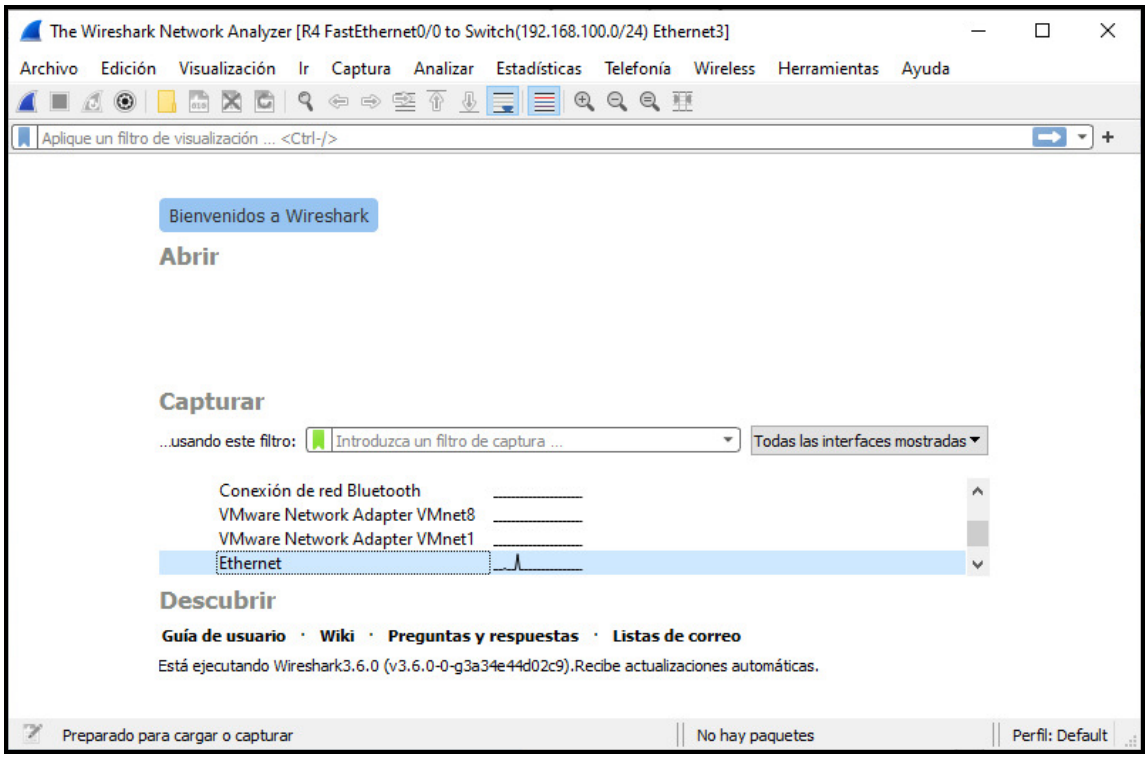

Figura 3. Ventana principal del software Wireshark.

Una vez seleccionado el interfaz Ethernet con el ratón (quedará sombreado el texto Ethernet) se debe pulsar en el icono de la '**Aleta Azul**' en la parte izquierda de la barra de iconos de menú para iniciar una captura de paquetes.

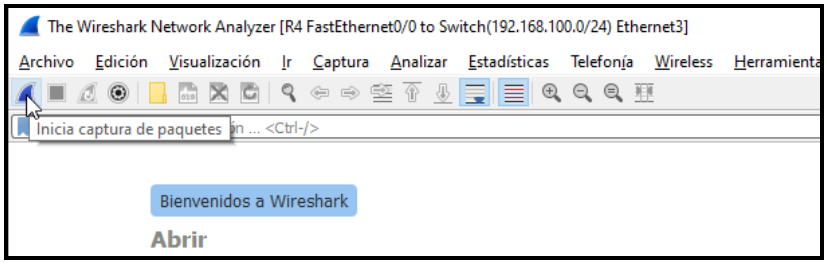

Figura 4. Botón de inicio de captura de paquetes.

A partir de este momento, el monitor de red captura y visualiza TODOS los paquetes que el interfaz de red Ethernet del equipo del aula **transmite o recibe**.

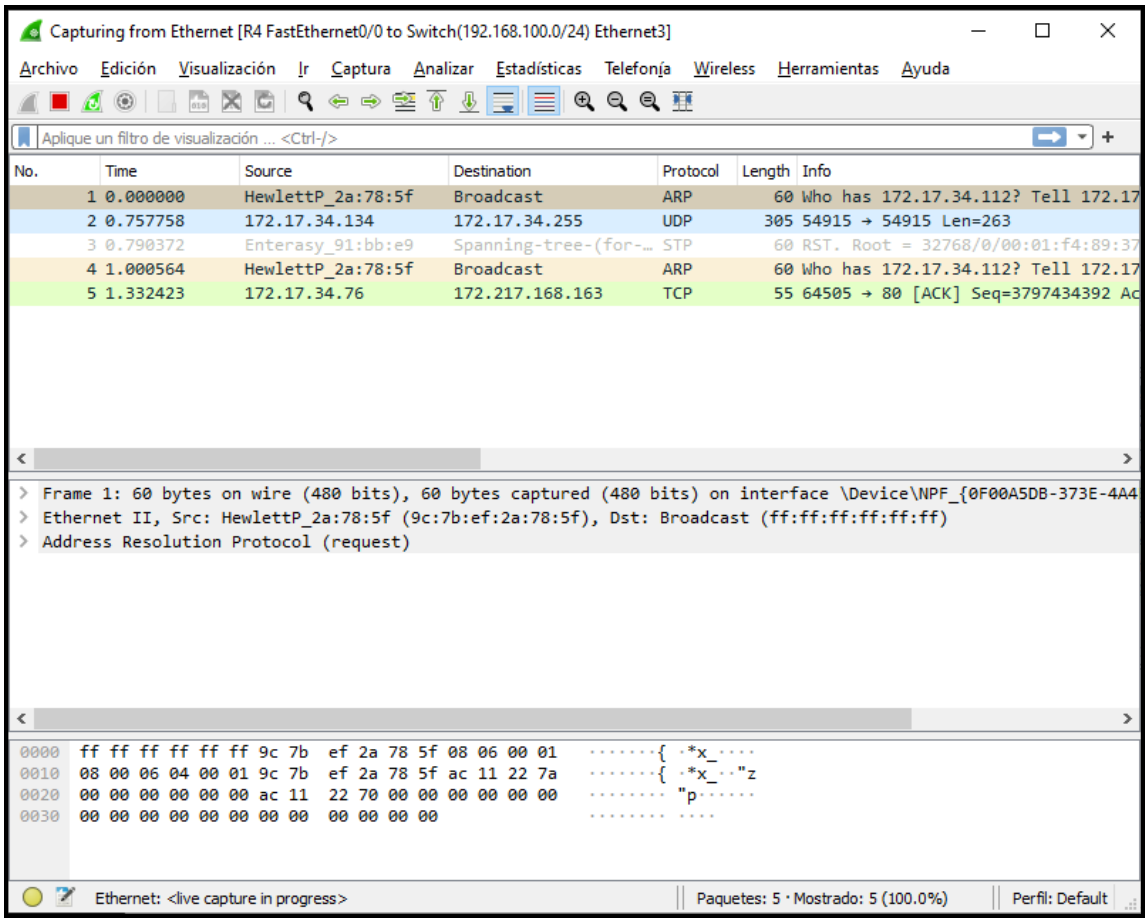

Figura 5. Proceso de captura de paquetes con Wireshark.

Al iniciarse la captura, el monitor de red mostrará **3 secciones** en la ventana principal.

La **sección superior** mostrará un listado de paquetes capturados indicando su orden de captura (estos paquetes pueden haber sido transmitidos por el PC o recibidos por el PC). Para cada paquete se muestra información general acerca de los mismos, algo que se abordará en las prácticas de la asignatura.

La **sección media** hace referencia al contenido del paquete que se haya seleccionado en la sección superior. Mostrará la estructura de la información del paquete, lo que se conoce como cabeceras de protocolos y que se estudiará en la asignatura. Para cada protocolo se visualiza una línea que puede desplegarse pinchando en el símbolo **'+'** de la izquierda y acceder al contenido de los campos de la cabecera del protocolo.

La **sección inferior** muestra la secuencia de bits del paquete que se haya seleccionado en la sección superior. La secuencia de bits del paquete se muestra en formato hexadecimal y ASCII. Cuando en la sección horizontal central se selecciona alguna cabecera de protocolo o algún campo de las cabeceras, se sombrea la porción del paquete al que se corresponde en la sección inferior. De esta forma es posible identificar la posición de las cabeceras de los protocolos en el paquete capturado.

La captura de paquetes continúa hasta que es detenida por parte del usuario. Esto es posible realizarlo desde la barra de menús con el icono del '**Cuadro Rojo**'.

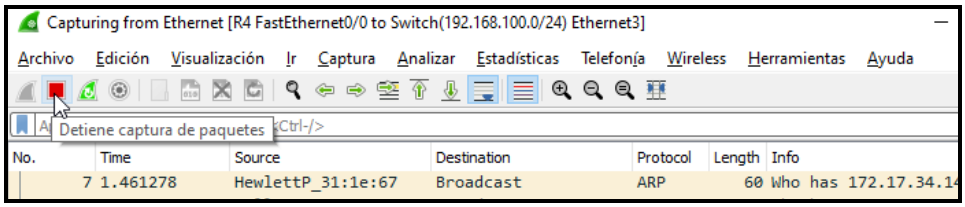

Figura 6. Botón de finalización de captura de paquetes.

Una vez finalizada la captura, se puede analizar seleccionando los paquetes deseados y también almacenarla empleando el menú '**Archivo → Guardar como**'.

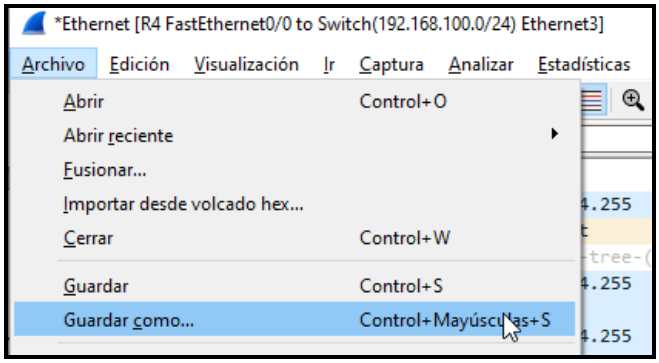

Figura 7. Almacenamiento de una captura de paquetes en un archivo.

Todas las capturas de paquetes realizadas en el laboratorio y almacenadas en un archivo pueden ser analizadas en **cualquier computador donde esté instalado el software Wireshark**. Esto permite que el alumnado pueda revisar y analizar los experimentos fuera del aula de prácticas.

Un aspecto muy importante en el uso de Wireshark es que la captura de paquetes se inicia cuando se pulsa el botón 'Aleta Azul' y finaliza con el botón 'Cuadro Rojo'. Cuando se familiariza con el uso de esta herramienta, lo primero que debe llamar la atención es la enorme cantidad de paquetes capturados (unos 300) en una fracción de tiempo pequeña (unos 60 segundos). En la actualidad, un computador conectado a cualquier de red de comunicaciones está permanentemente intercambiado paquetes, incluso sin la intervención del usuario (tareas de control de la red de comunicaciones, intercambio de datos de aplicaciones, del sistema operativo, publicidad no deseada, etc. e incluso **malware**).

Por ello, a la hora de realizar un experimento propuesto en las prácticas de la asignatura, es fundamental acotar el tiempo de captura para que los paquetes capturados sean en su mayor parte los asociados al experimento. Esto no será posible muchas veces y será necesario llevar a cabo una acción adicional: **el filtrado de paquetes**.

2.2 Filtrado de paquetes

Cuando se realiza una captura de información en una red de comunicaciones, existirá gran cantidad de información que no precisemos para el análisis del estado de funcionamiento de la red. Un filtro hace referencia a un conjunto de reglas que deben cumplir los paquetes capturados para poder ser **visualizados**. Las reglas pueden estar dadas en base a las direcciones origen y/o destino del paquete, tipo de protocolo o *pattern matching* (que hace referencia a que el contenido de un byte o grupo de bytes dentro de un paquete coincida con unos valores especificados), etc.

Los filtros de visualización se definen en el cuadro que aparece debajo de la barra de iconos de menús de Wireshark.

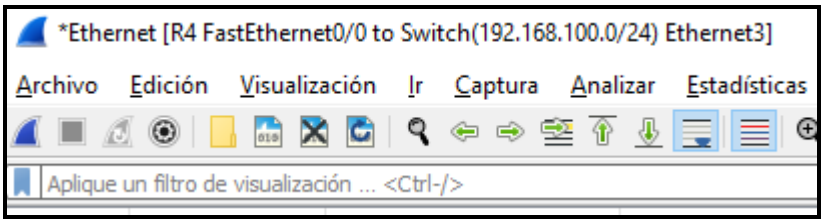

Figura 8. Introducción de filtros de visualización en Wireshark.

La definición de un filtro consiste en una expresión que indica las condiciones que debe verificar un paquete. Estas condiciones están relacionadas con las características de los protocolos presentes en el paquete. El formato de estas expresiones sigue el estándar del software **tcpdump** (un monitor de red de libre distribución en modo texto disponible para varios sistemas operativos), aunque Wireshark nos proporciona una herramienta muy útil para definirlos sin conocer la sintaxis de tcpdump.

Para abrir el asistente de creación de filtros de visualización, debe pulsarse con el botón derecho sobre el cuadro de filtros de visualización y seleccionar '**Display Filter Expression**'.

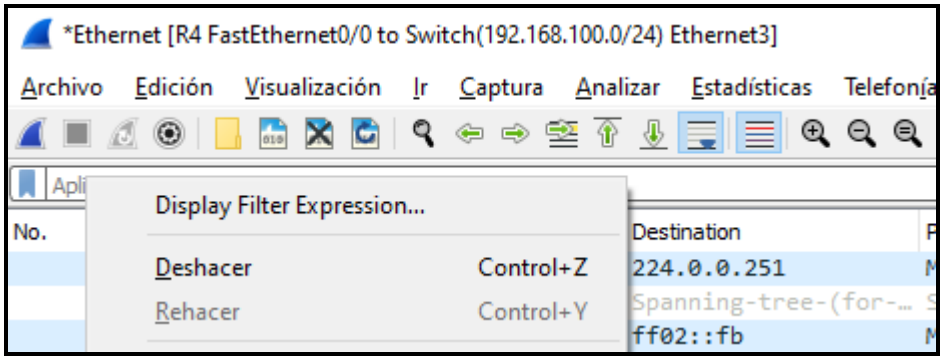

Figura 9. Acceso al asistente de filtros de visualización en Wireshark.

Una vez abierto el asistente de filtros de visualización, podemos asociar a las características de cada protocolo una relación del tipo ==, >, <, >=, <=, !=, contiene o existe, con un valor determinado. Por ejemplo, si queremos capturar todos los paquetes cuya dirección MAC Ethernet de origen es 00:02:10:3F:45:F4, seleccionamos el protocolo Ethernet y dentro de éste el campo eth.src. A continuación se indica qué relación se va a emplear, que en nuestro caso será ==. Y al indicarla podremos especificar un valor de comparación, que será 00:02:10:3F:45:F4.

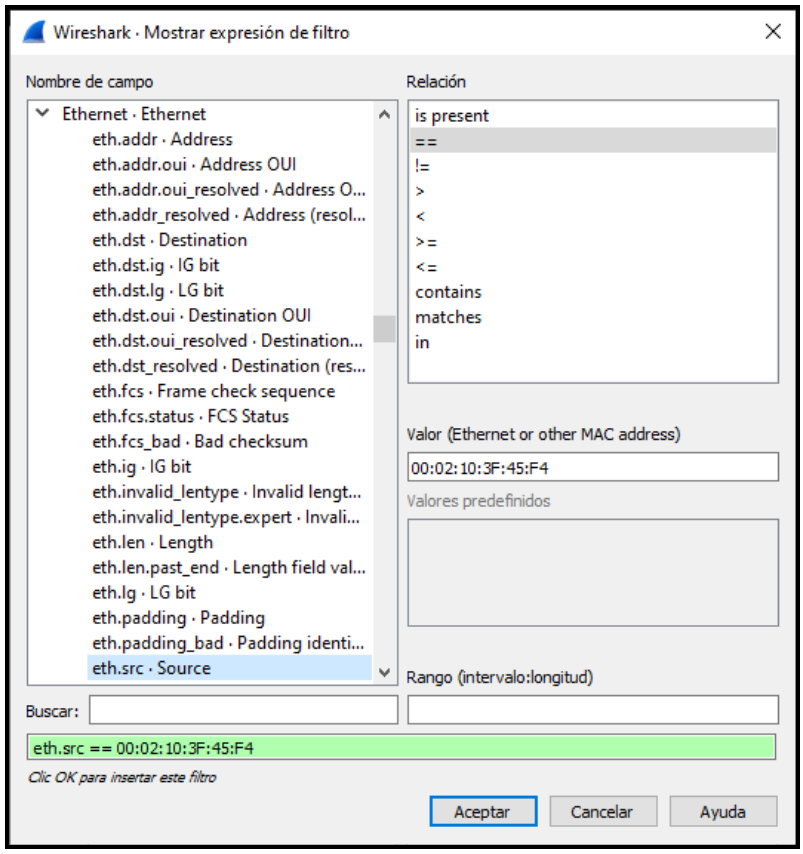

Figura 11. Asistente de filtros de visualización en Wireshark.

Pulsando en **Aceptar'** aparecerá la expresión **eth.src == 00:02:10:3F:45:F4** en el cuadro de filtros de visualización de Wireshark. A continuación, pulsando en la '**Flecha Blanca/Azul**' al final del cuadro de filtros, éste se aplicará sobre los paquetes capturados. Así, en la ventana principal de Wireshark aparecerán sólo los paquetes que verifican el filtro. Para no filtrar y visualizar de nuevo todos los paquetes capturados pulsar el botón **'Aspa Gris'** que hay junto al botón de la 'Flecha Blanca/Azul'.

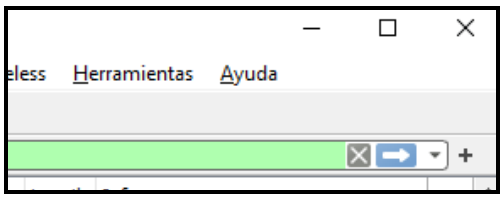

Figura 11. Botones para aplicar/eliminar un filtro de visualización en Wireshark.

Un filtro puede constar de más de una expresión relacionándolas con los operadores **and**, **or** y **not**. Si queremos filtrar los paquetes que envía o recibe el PC con dirección MAC 00:02:10:3F:45:F4, tendríamos que indicar en el filtro la expresión **eth.src == 00:02:10:3F:45:F4 or eth.dst == 00:02:10:3F:45:F4**.

Algunos ejemplos de la sintaxis de filtrado en **Wireshark** son los siguientes:

Tráfico de Difusión o 'broadcast'

En el cuadro de filtros indicar **eth.dst == FF:FF:FF:FF:FF:FF**

Filtro por dirección IP en general

En el cuadro de filtros indicar: **ip.addr == 193.145.233.8**

Filtro por dirección IP destino

En el cuadro de filtros indicar: **ip.dst == 193.145.233.8**

Filtro por dirección IP origen

En el cuadro de filtros indicar: **ip.src == 193.145.233.8**

Filtro por dirección IP destino y origen

En el cuadro de filtros indicar: **ip.dst == 193.145.233.8 and ip.src == 172.20.43.203**

Filtro por tamaño de paquete

En el cuadro de filtros indicar: **ip.len < 100** (paquetes IP con tamaño inferior a 100 bytes). Los operadores válidos son: ==, !=, >, <, >=, <=. Es decir, igual que, distinto de, mayor que, menor que, mayor o igual y menor o igual. También puede usarse la notación hexadecimal 0x, como por ejemplo 0x64 para el valor decimal 100.

Filtrado de todos los paquetes IP con el campo TTL mayor o igual a 64

En el cuadro de filtros indicar**: ip.ttl >= 0x40** o **ip.ttl >= 64** .

Filtrado de todos los paquetes IP que contengan el texto aula24

En el cuadro de filtros indicar: **ip contains "aula24"**.

Para una mayor comprensión acerca de la sintaxis de filtrado, se recomienda el acceso a la web oficial del software Wireshark http://www.wireshark.org/.

3. DOCUMENTACIÓN COMPLEMENTARIA

- **https://www.wireshark.org**/. Pagina Web Oficial Wireshark