Universidad de Alcalá

Departamento de Automática

ARQUITECTURA DE REDES
Laboratorio

Práctica 3:
"Analizadores de protocolos. Manual de Wireshark"

Grado en Ingeniería Informática
Curso 2021/22

Introducción

Los analizadores de protocolos de red ("*sniffers*"), visualizan el tráfico de paquetes que circulan por las redes de computadores, permitiendo analizar el comportamiento de las mismas, detectando errores, congestión, etc.

Su funcionamiento consiste en **capturar** una copia de estos paquetes para un realizar un análisis posterior, el cual se presenta textual o gráficamente, dependiendo de las capacidades de la herramienta en cuestión.

Normalmente realizamos varios tipos de análisis siendo los fundamentales el estructural y el estadístico. Con el análisis estructural observamos la composición y detalles de los paquetes capturados como contenido de cabeceras, nombre protocolo, datos del cuerpo del mensaje, etc. Con el análisis estadístico obtenemos estimados de tráfico: cantidad de paquete por tipo y tiempo. Por ejemplo, un administrador de red puede estudiar qué partes de la red están más saturadas y cuáles protocolos y máquinas están generando más tráfico, y de ese modo podrá sugerir las acciones correctivas necesarias.

Adicionalmente, muchos analizadores son capaces de seguir una "conversación" con lo que facilitan la resolución de problemas y la depuración del software de red durante su desarrollo.

Wireshark: descripción general

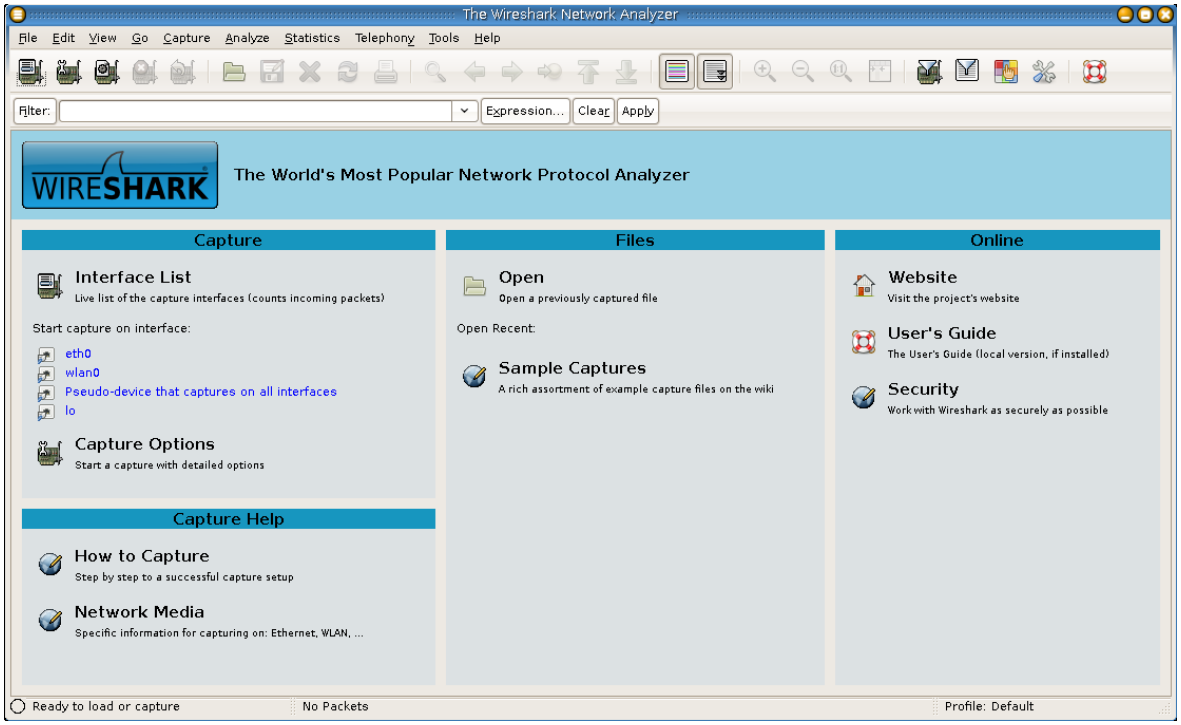
El analizador Wireshark, es uno de los más populares analizadores que existen. Se trata de una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. Se trata de un producto gratuito cuyas características más relevantes son:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Hasta el año 2006 el programa se distribuía bajo la denominación de *Ethereal*.

Primera Captura

Al arrancar, es necesario seleccionar la tarjeta de red de nuestra máquina sobre la que deseamos hacer capturas Esta será ***eth0*** normalmente, así que seleccionaremos "*Capture*" sobre esta interfaz de red.



La captura de paquetes comenzará y se mostrará una ventana en la que poco a poco irán apareciendo diferentes estadísticas sobre los paquetes que progresivamente se van capturando hasta que se pulse "*detener*". Seguramente registraremos tráfico de tipo difusión (*broadcast*) y poco a poco veremos que se registra alguna actividad.

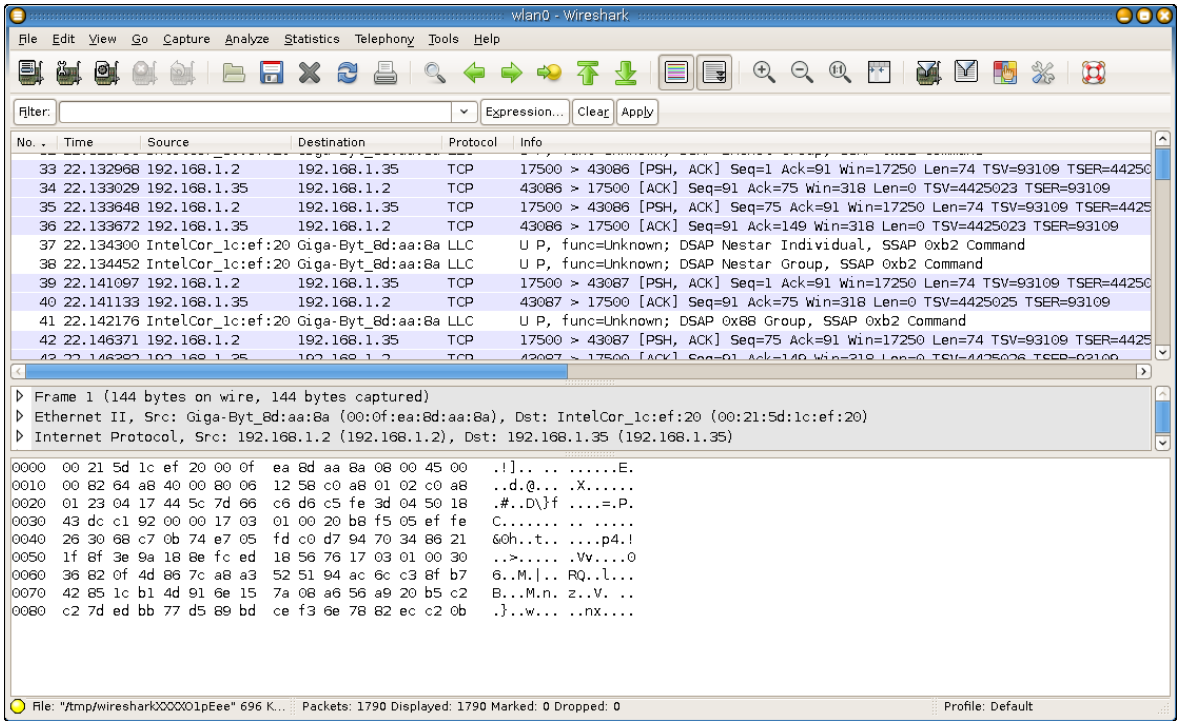
Para crear tráfico de red, es conveniente hacer alguna acción como arrancar un navegador (*Firefox* o *Mozilla* en Linux), o dar un comando al sistema operativo que genere actividad (`ping www.uah.es`), conectarse a otra máquina o todas estas acciones simultáneamente.

Ventana principal

Una vez tengamos algunos paquetes capturados, observemos qué sucede al detener el proceso de captura:
Los paquetes capturados se muestran en la ventana principal de Wireshark. Esta se compone a su vez de tres ventanas.

1. La ventana superior es la lista de los paquetes capturados. Incluye hora, fuente, destino, protocolo y una descripción breve de cada uno. Según el paquete que esté seleccionado en cada momento, se controla la información que aparece la ventana intermedia.

2. La ventana intermedia muestra en detalle el paquete seleccionado en la primera ventana. Incluye el nombre de los protocolos empleados en los distintos niveles de la arquitectura y los valores correspondientes a los campos de cada uno de los protocolos en listas desplegables.
3. La ventana inferior muestra el valor los datos del paquete en hexadecimal y ASCII. Al seleccionar alguno de los campos en la ventana intermedia, se destaca el rango de valores correspondientes a dicho campo en el paquete.

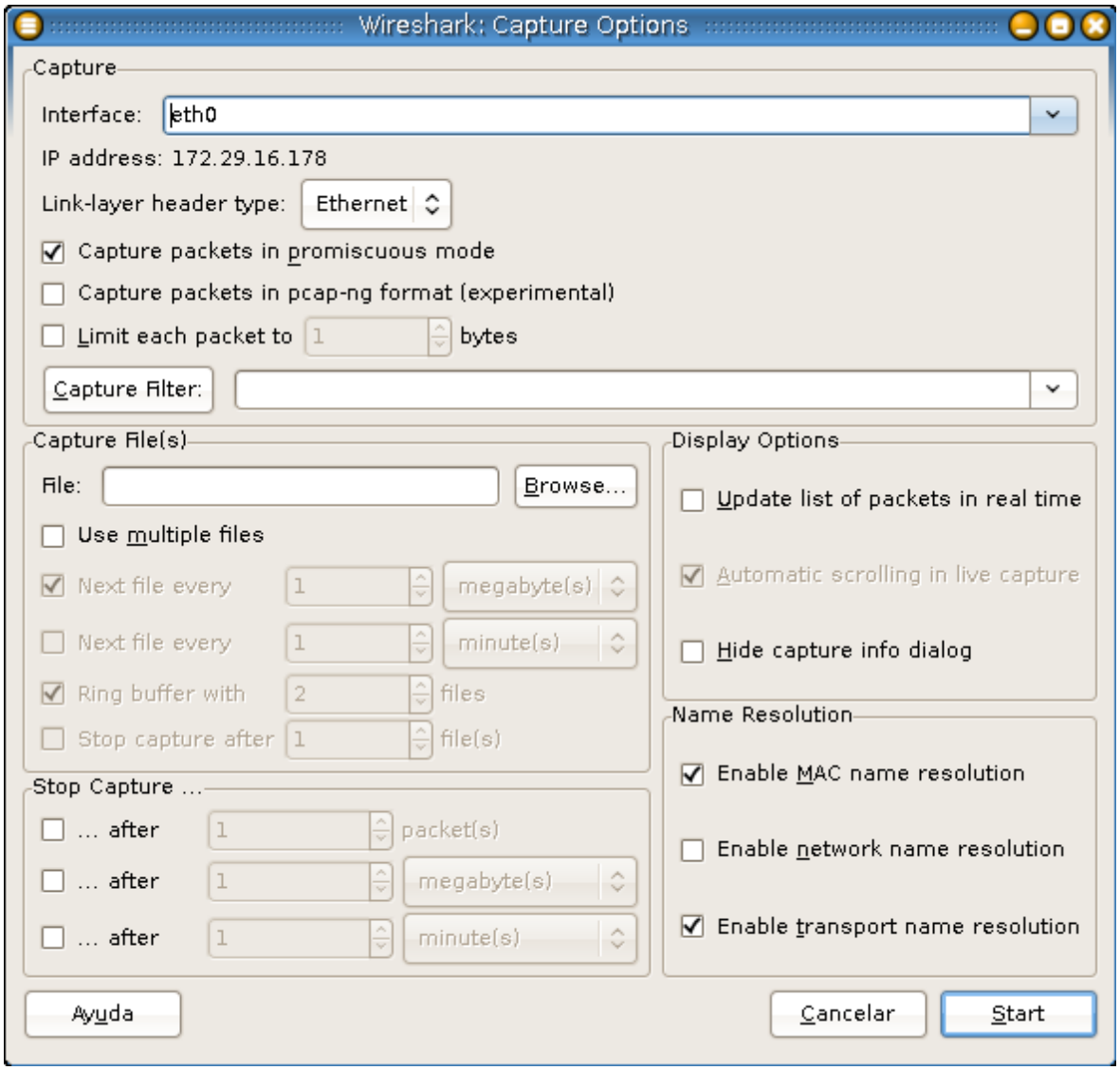


Además en la ventana principal de Wireshark tenemos:

- **Barra Principal:** con acceso a opciones de captura,, archivado e impresión, movimiento y búsqueda de paquetes en la lista, zoom, aspecto de visualización, filtrado y edición de preferencias. En esta barra se encuentra "iconizadas" muchas de las opciones de los menús de la parte superior de la GUI de la aplicación.
- **Barra de Filtro:** muestra y permite especificar en el filtro aplicado a los paquetes para visualización aunque también navega a la ventana de definición de filtros de captura y visualización.
- **Barra de status**: Al pié de las ventanas a la izquierda vemos el nombre del fichero temporal donde se ha guardado la captura. A la derecha hay información sobre los paquetes:
    - P: número de paquetes capturados
    - D: número de paquetes que se muestran (superan el filtro)
    - M: número de paquetes marcados

Nuevas capturas: opciones

Controlamos la captura con los primeros iconos de la barra principal. También hallamos estas opciones en el menú *Capture*. Podemos establecer opciones de captura, iniciar una nueva captura, parar o reiniciar una captura en marcha.



Las opciones de captura nos llevan a una ventana en que podemos establecer parámetros de captura: la ventana de diálogo "*Capture Options*". Las más relevantes son:

Marco de captura:

1. Selección de Interfaz
2. *Modo promiscuo*: en este modo el programa capturará cualquier paquete que sea visible a la tarjeta de red, independientemente de si está o no destinado a ella. Si no

seleccionamos el modo promiscuo, solo se capturarán paquetes que van destinados a, o que provienen de nuestra tarjeta de red.

3. *Buffer Size*: con el fin de limitar el uso de recursos, podemos indicar la cantidad máxima de bytes que vamos a guardar de cada paquete capturado.
4. *Filtro de captura*: podemos navegar a la definición de filtros de captura para desechar la captación de algunos mensajes (ver siguiente apartado).

Marco de Ficheros
Las opciones en este marco se refieren al uso de uno o varios ficheros concretos para la captura en lugar del temporal que usa el sistema, cómo ha de organizarse la secuencia para ficheros múltiples y si ha de pararse la captura en relación a éstos.

Marco de Opciones de Presentación:
Podemos optar por ver en tiempo real los paquetes que se van capturando y también podemos elegir que se realice un desplazamiento vertical automático de la pantalla *(scrolling)*.

Marco de condiciones de parada:
En este marco podemos seleccionar si deseamos parar la captura al alcanzar cierto número de paquetes, de cierto número de Megabytes (incompatible con el modo de captura multi-fichero) o de tiempo. Si no seleccionamos ninguna condición de parada, ésta será manual.

Filtros de Captura en Wireshark

Wireshark hace uso de *libpcap* para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (*and/or*) con la opción de ser negada por el operador *not:*

```
[not]Expresion[and|or[not]expresion ... ]
```

La siguiente expresión define un filtro para la captura de paquetes desde/hacia los host con dirección IP 172.17.250.1 y 172.17.1.81:

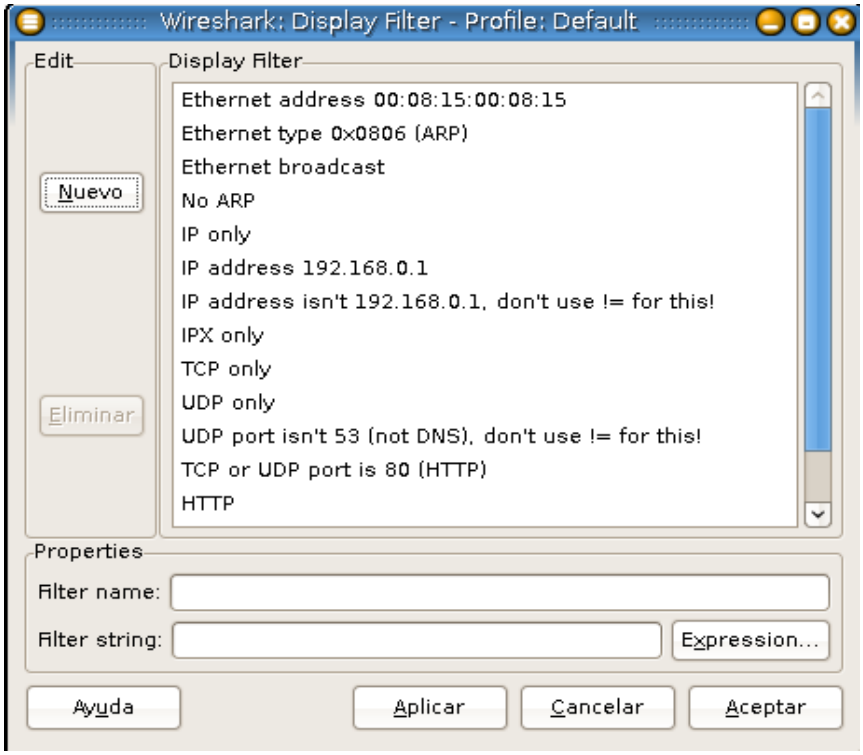
```
ip.addr==172.17.250.1 and ip.addr==172.17.1.81
```

En el sitio http://wiki.wireshark.org/CaptureFilters podrá obtener una serie de filtros que son usualmente aplicados por los administradores de red.

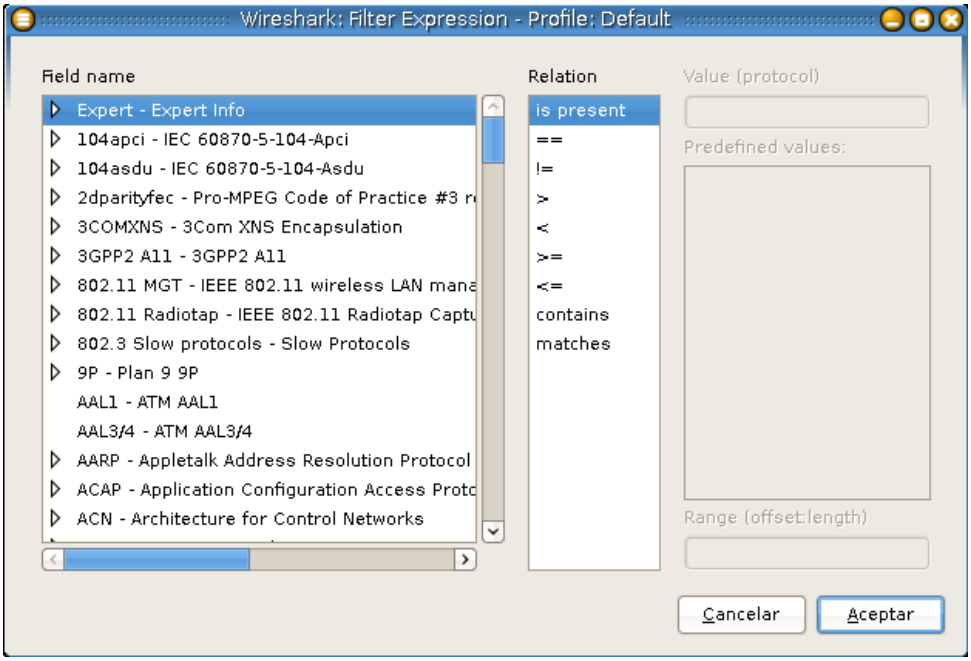
Al diálogo de filtros de captura podemos llegar desde la venta de opciones de captura o desde el menú de Capturas para establecer un filtro de captación de mensajes. Esto evitará la captación de algunos mensajes: antes solo los excluimos de la presentación en pantalla mediante el filtrado de presentación.

Si recorremos cada uno de los filtros predefinidos, veremos la expresión que los implemente en "*Filter String*". Esta lista puede aumentarse definiendo nuestras propias expresiones y asignando un nombre para ellas. Una expresión debe evaluarse a "true", se

define en minúsculas con una o más primitivas unidas con operadores lógicos. Una primitiva es un calificador seguido de un identificador.



La ventana *Filter Expressions* nos facilita la creación y modificación de filtros a nuestra voluntad.



Análisis de los paquetes capturados

Al seleccionar cualquiera de los paquetes capturados, se despliega el contenido del paquete en el resto de los paneles que son panel de detalles de paquetes y panel en bytes. Expandiendo cualquiera parte del árbol presentado en el panel de detalle del paquete, se puede seleccionar un campo en particular cuyo contenido se muestra resaltado en negritas en el panel de bytes.

Existe una manera de visualizar los paquetes mientras esta activo el proceso de captura esto se logra, seleccionando la opción *Update list packets in real time* desde menú *Edit->Preferentes->Capture*. Adicionalmente, Wireshark permite visualizar el contenido de un paquete seleccionado en el panel de paquetes capturados en una ventana individualmente seleccionando la opción *Show Packet in new Windows* en menú principal *View*. Esto permite comparar con más facilidad dos o más paquetes.

Cuando iniciamos la captura de paquetes por lo general se obtiene una gran cantidad de paquetes que cumple con los filtros y/o expresiones definidas, Wireshark permite realizar búsquedas sobre los paquetes capturados, seleccionando *Menú Edit>Find Packet*.

Wireshark permite marcar los paquetes para que sean identificados con más facilidad, a partir del menú contextual que se muestra al activar el botón derecho del ratón sobre el paquete en cuestión.

Wireshark proporciona un rango amplio de estadísticas de red que son accedidas desde el menú *Statistics* que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo.