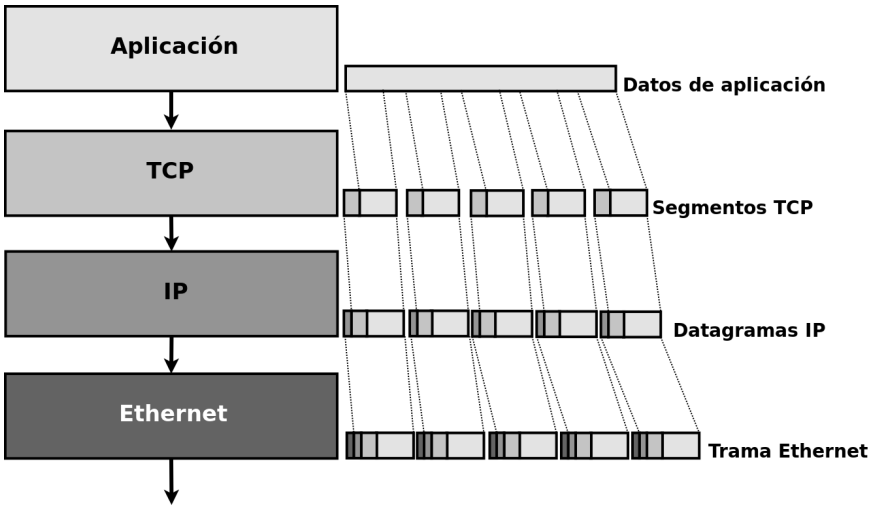
Redes 1
Introducción a Wireshark para el análisis de tramas

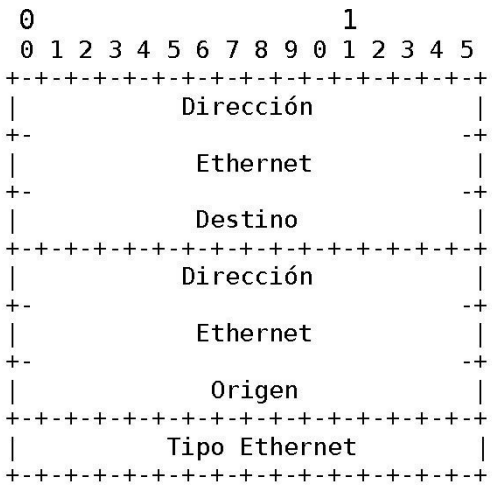
Pila de protocolos TCP / IP

La pila de protocolos TCP / IP es una arquitectura en capas, en las que los datos que envía una capa se encapsulan dentro de las unidades de transmisión de la capa inferior. Como ejemplo concreto de protocolos: Mensaje (Datos de aplicación), Segmento, Datagrama y Trama:



Cada protocolo tiene su propia cabecera con información necesaria para realizar la comunicación. A continuación se incluyen los esquemas de las correspondientes a Ethernet, IP y TCP. En las figuras, debe tenerse en cuenta que los bytes mostrados se transmiten consecutivamente, empezando de izquierda a derecha y de arriba a abajo, siendo esta la representación elegida para facilitar el conteo.

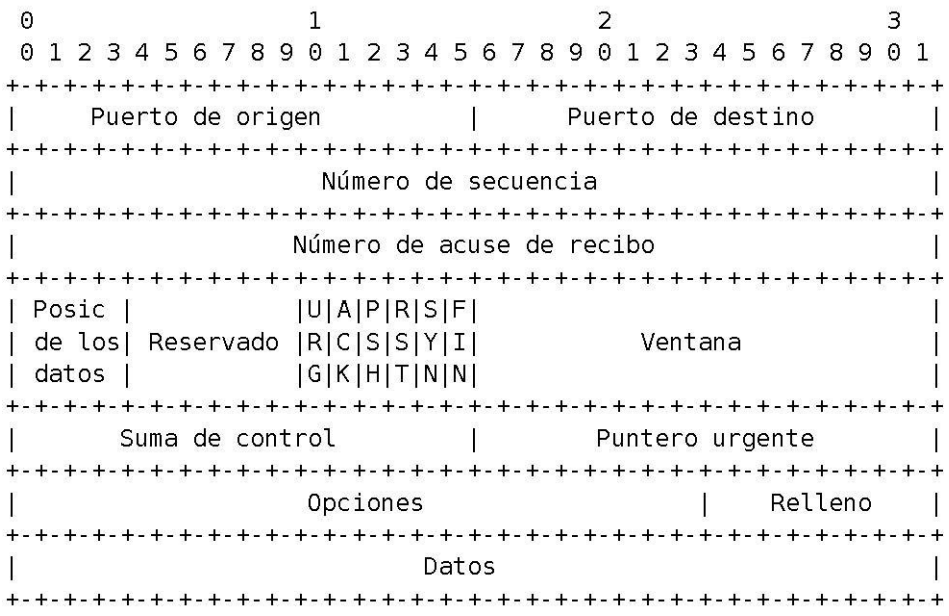
Ethernet



IP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Versión
IHL
Tipo Servicio
Longitud Total
Identificación
Flags
Posición
Tiempo de Vida
Protocolo
Suma de Control de Cabecera
Dirección de Origen
Dirección de Destino
Opciones
Relleno

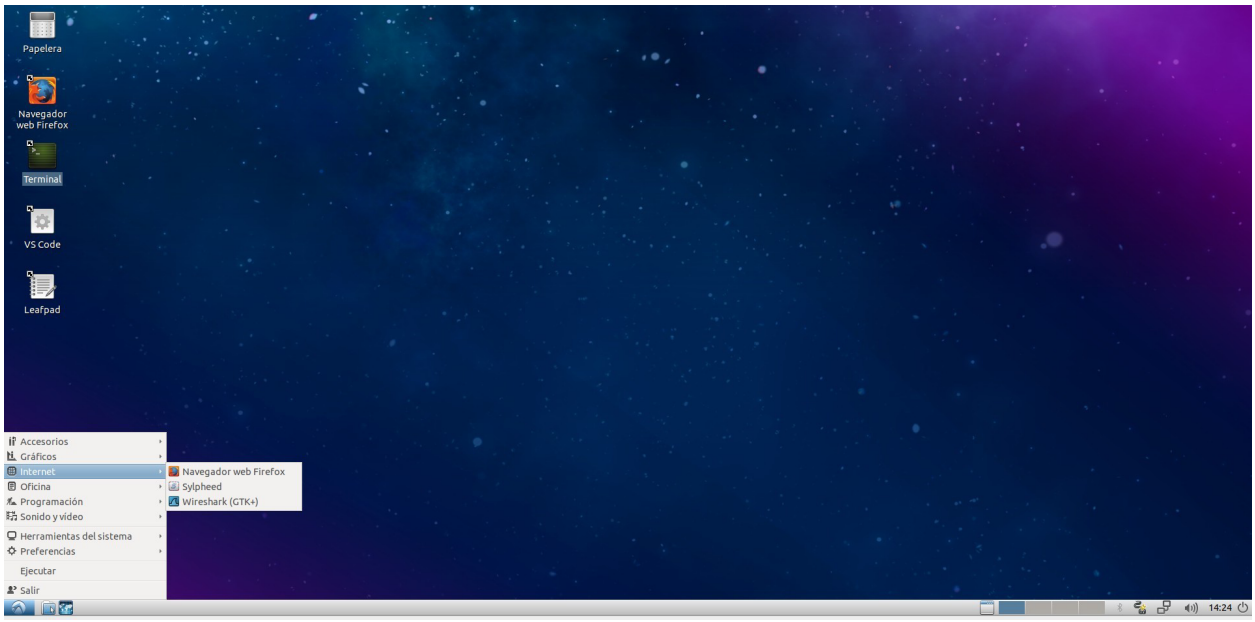
TCP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Puerto de origen
Puerto de destino
Número de secuencia
Número de acuse de recibo
Posic de los datos
Reservado
U A P R S F
R C S S Y I
G K H T N N
Ventana
Suma de control
Puntero urgente
Opciones
Relleno
Datos

Ejecución (e introducción) de Wireshark

Wireshark es una potente herramienta de software libre que permite capturar el tráfico que entra o sale por cualquiera de los enlaces de red de un equipo. Wireshark (conocido antiguamente como Ethereal) dispone de un entorno gráfico que usaremos para capturar, filtrar y analizar el tráfico de red en cada una de las prácticas de la asignatura.

Si queremos ejecutar Wireshark para abrir una traza ya almacenada en nuestro ordenador, lo podremos encontrar en el menú de aplicaciones, en Internet:

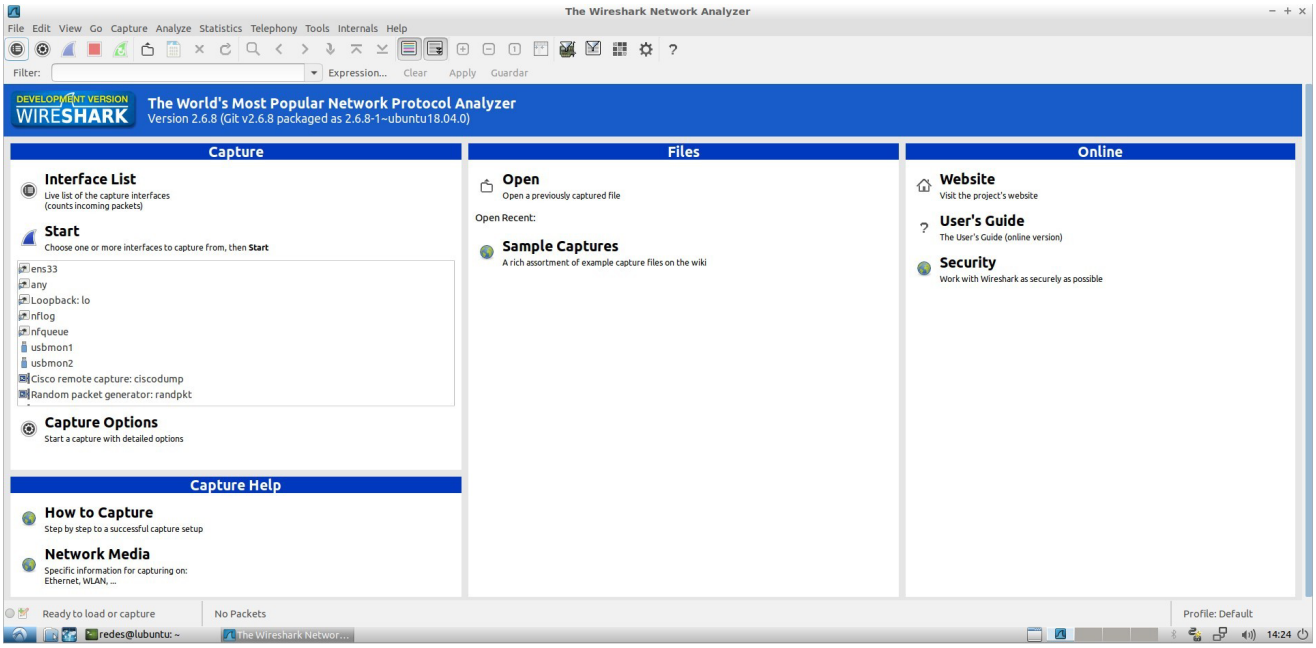


Por el contrario, si lo que queremos es realizar una captura en vivo, debemos lanzarlo con permisos de root utilizando el comando

```
$ sudo wireshark-gtk
```

en la terminal:

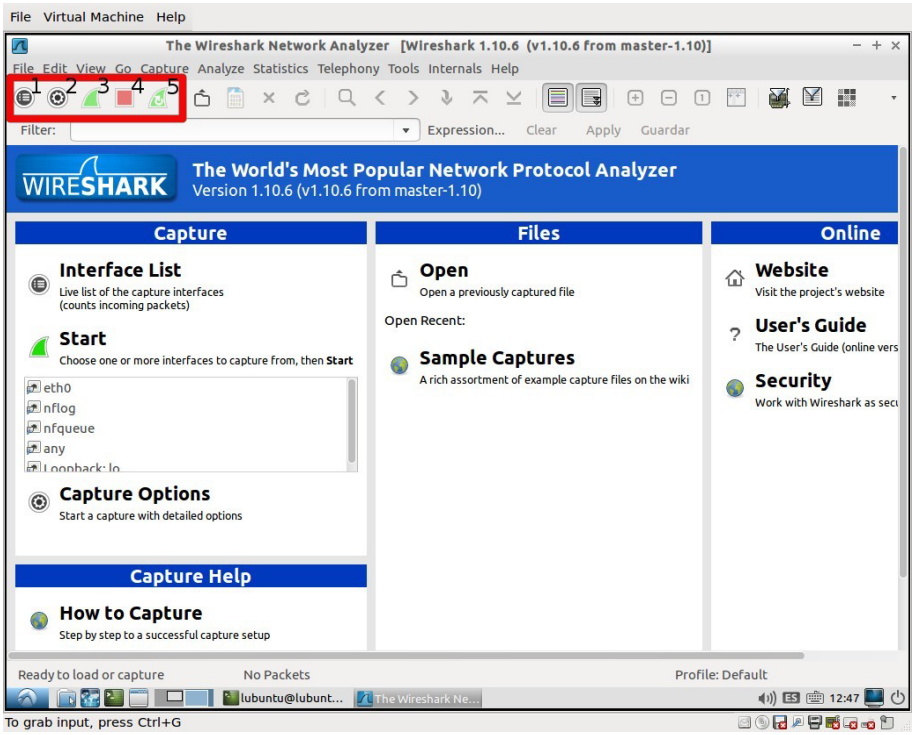
Si todo va bien, **Wireshark se mostrará en nuestro escritorio**:



Selección y configuración del Interfaz de captura de Tráfico

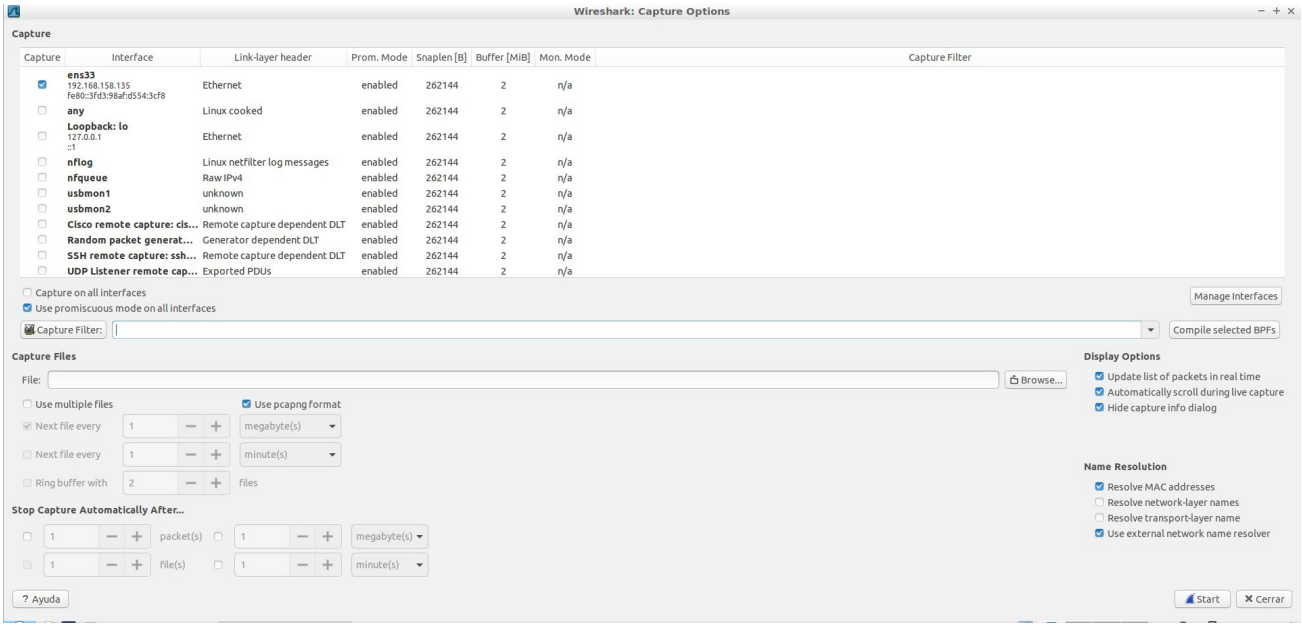
Una vez arrancado Wireshark, y si vamos a realizar una captura en vivo, será necesario seleccionar un interfaz de red (puede haber varios) y configurar la forma de capturar el tráfico por dicho interfaz.

Para ello, utilizaremos los iconos de la barra superior que hay a la izquierda (anotados del 1 al 5):



El icono 1 nos ofrece un panel donde aparecen todas los interfaces de red disponibles en el sistema y un grupo de botones para activar rápidamente la captura de tráfico por cualesquiera de ellos:

Al pulsar sobre el icono 2, Wireshark nos presenta la que es, sin duda, la ventana más importante de configuración para la captura de tráfico:



En esta ventana, lo primero que habrá que hacer el seleccionar el interfaz por el que vamos a realizar la captura de tráfico entrante y saliente (campo '**Interface**').

Normalmente encontraremos estos interfaces (uno o varios de ellos):

- **lo**: El interfaz 'lo' es el 'loopback'. Cuando un proceso de la máquina se comunica por red con otro proceso de la misma máquina, se utiliza el 'loopback' para que el tráfico no salga de la máquina (es un truco 'software' para evitar un consumo innecesario de recursos de red).
- **ensX**: Típicamente estos interfaces representan las tarjetas de red Ethernet, con las que se trabaja habitualmente en las redes locales. La X representa un número para distinguir unas de otras.
- **wlanX**: Interfaz de comunicación inalámbrica.

Por defecto, Wireshark opera en modo promiscuo, es decir, se captura todo el tráfico que entra y sale por el interfaz seleccionado, esté o no esté dirigido desde/hacia la dirección física que tiene el interfaz. En la realidad, activar o desactivar el modo promiscuo no influye mucho en la captura del tráfico que vayamos a obtener (los conmutadores ya eliminan ese tráfico que no vaya dirigido a la dirección del interfaz de red).

Existen numerosas opciones de visualización del trafico que se captura entre las que cabe resaltar:

- **'Update list of packets in real time'**: Mientras una captura está en vuelo, casi todos los botones de Wireshark están desactivados (hasta que se pare o termine la captura). Esta opción permite actualizar la ventana principal con los paquetes que se van filtrando, de modo que se puede observar en tiempo real cómo evoluciona el filtrado. En caso de no activar esta opción, hasta que no detengamos la captura, Wireshark no mostrará el tráfico capturado. **Se recomienda activarla**.
- **'Name Resolution'**: Para cada paquete capturado por Wireshark, existen

direcciones de red que pueden ser mostradas numéricamente o mediante un nombre. Para poder mostrar el nombre Wireshark debe 'resolver' (convertir) el número en un identificador (en el caso de la MAC es el fabricante, y en el caso de direcciones IP es el dominio). Mientras el alumno no esté familiarizado con la herramienta, **se recomienda desactivar las opciones de resolución de nombres**.

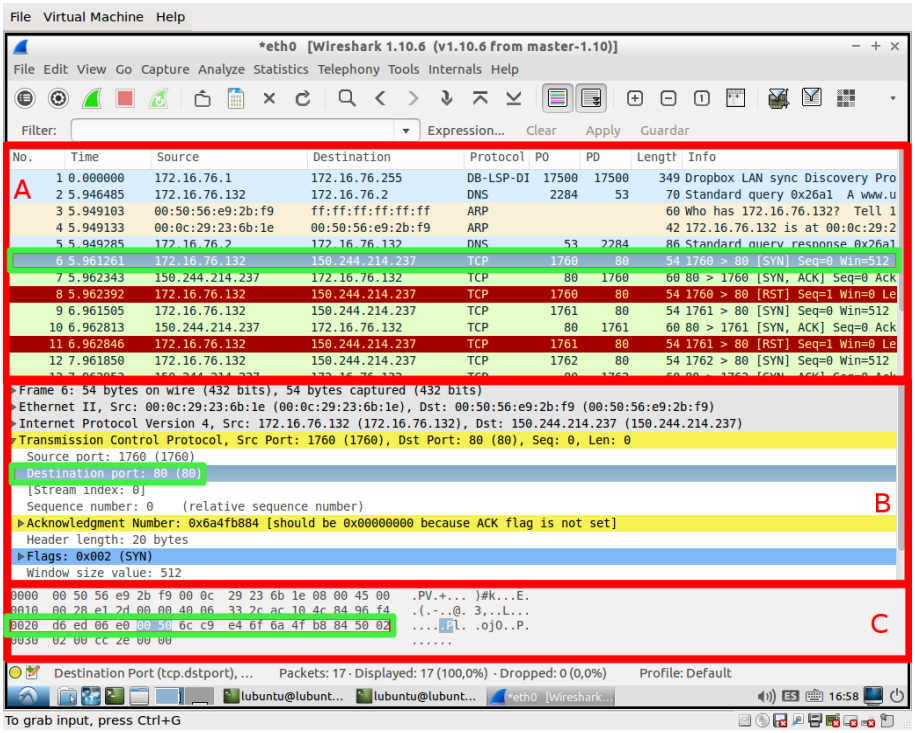
- **'Capture Filter'**: Este campo nos permitirá **filtrar el tráfico que será capturado**. Normalmente la cantidad de paquetes que entran y salen del equipo es una cantidad elevada, por lo que supone mucho trabajo al técnico de red interpretar toda la información. Lo ideal es "filtrar" el tráfico que realmente queremos analizar; de hecho, a lo largo de las prácticas implementaremos esta funcionalidad "a mano" con un fin pedagógico evitando su empleo. Estos filtros **no deben ser confundidos con los filtros de visualización**, que serán explicados más adelante dada su gran utilidad a la hora de validar los resultados de las prácticas y debuggear las aplicaciones implementadas.

Por otro lado, es importante comprobar que **no se utilice el formato pcap-ng** a la hora de guardar los ficheros de tráfico, ya que este formato no es compatible con algunos de los elementos que se utilizarán en las siguientes prácticas.

En la máquina virtual el interfaz de red principal, que deberemos utilizar para capturar el tráfico, será el **interfaz 'eth0'**. Una vez que el interfaz está configurado, simplemente habrá que activar la captura de tráfico pulsado en el botón '**Start**'. Cuando queramos detener la captura de tráfico,**habrá que pulsar en el icono 4**, en la barra de herramientas. Una vez detenida la captura, podremos analizar los paquetes capturados (y filtrados) en profundidad con toda la potencia que ofrece la herramienta.

Análisis del tráfico capturado

Una vez detenida la captura de tráfico, los paquetes aparecerán en filas en la ventana principal de Wireshark:



Tal y como se puede la ventana principal de Wireshark está dividida en tres partes. En la figura las hemos marcado en color rojo para familiarizarnos con ellas:

- **Parte A**: Es el listado de todos los paquetes capturados.
- **Parte B**: Decodificación que hace Wireshark del paquete que hayamos seleccionado (mediante un click) en la parte superior. Wireshark decodifica todos los campos (que conozca) del paquete seleccionado. Esta es la parte que más nos interesa a la hora de análizar el tráfico.
- **Parte C**: Volcado hexadecimal del paquete seleccionado en la parte superior. Si en la parte intermedia hacemos click en un determinado campo del paquete, en la parte inferior aparecerán resaltados los bytes que configuran dicho campo. Es importante tener siempre en cuenta que los bytes se muestran alineados en grupos de 16.

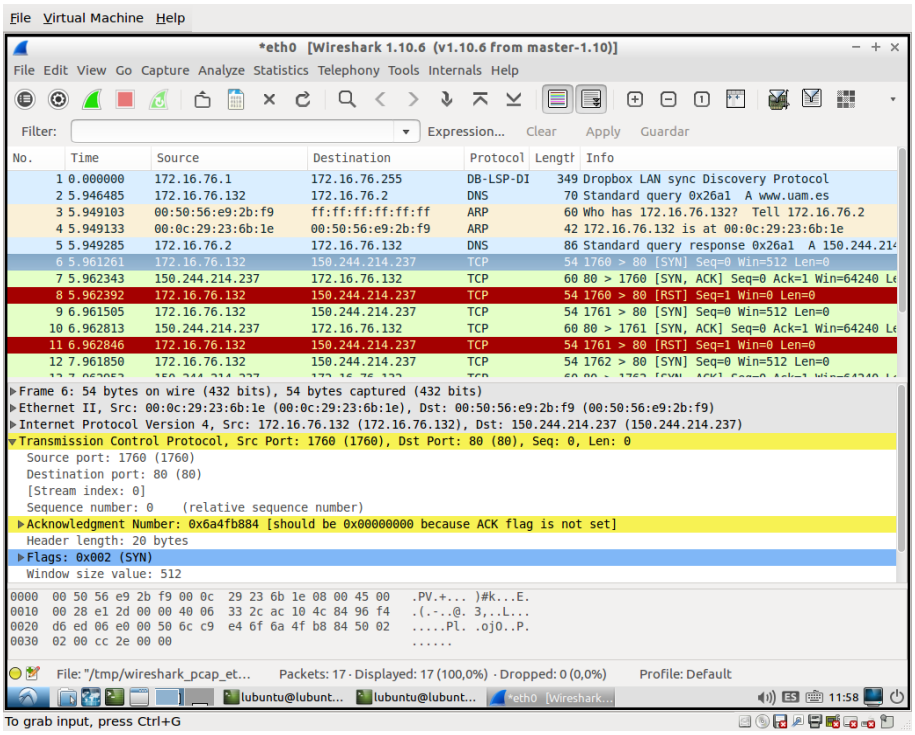
La parte intermedia tiene una jerarquía en árbol debido a la propia naturaleza de inclusión (encapsulación) de las cabeceras de unos protocolos dentro de otros. De este modo, cada línea de la parte intermedia representa un protocolo, pudiéndose expandir para mostrar los campos que incluye dicho protocolo; en la figura se ha expandido la línea correspondiente a TCP.

Como puede verse en el ejemplo, al seleccionar el paquete 6 (marcado con un recuadro verde en la Parte A), el campo 'Destination port' (marcado con un recuadro verde en la Parte B) está incluido en la cabecera de este protocolo, que está a su vez encapsulado en un paquete IP (con sus propios campos particulares). En este caso, en la parte inferior aparecen señalados los bytes 0050 (en la línea marcada en verde en la Parte C),

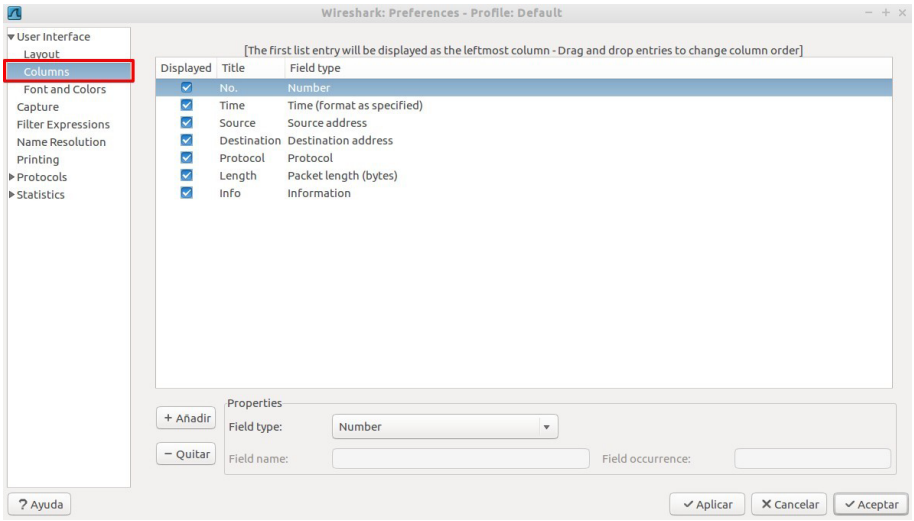
correspondiente al campo seleccionado.

Otra funcionalidad muy interesante de Wireshark es la inclusión de nuevas columnas. En nuestro caso, por ejemplo, se han añadido las columnas 'PO' y 'PD' que representan, respectivamente, los puertos origen y destino de los paquetes de red. Aunque todavía no se ha explicado el significado de estos campos, fundamentales para ciertos análisis, vamos a aprender cómo se puede configurar Wireshark para que aparezca este campo.

En primer lugar, partimos de la ventana sin estas columnas:

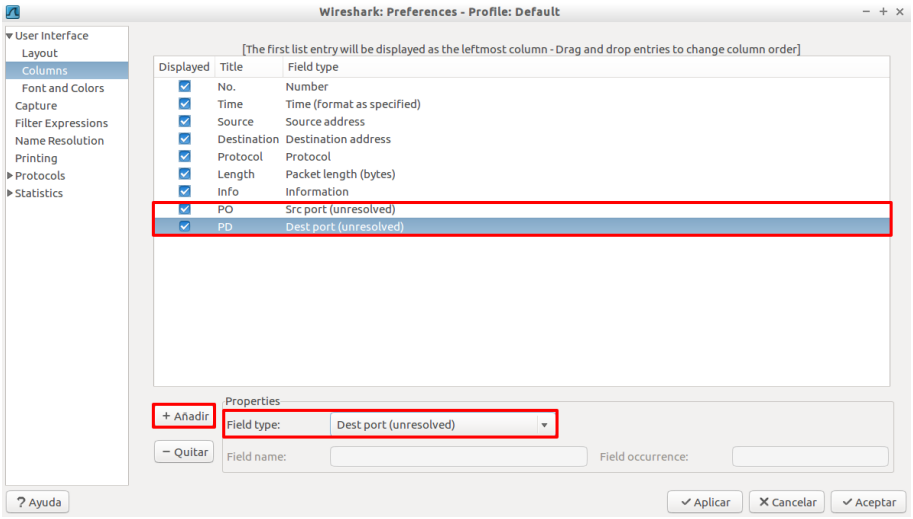


Vamos al menú 'Edit'->'Preferences'. Aparecerá la ventana de edición de preferencias, en la que podremos configurar distintos aspectos de Wireshark. Entramos en el apartado 'User Interface'->'Columns':



Observamos que aparece un listado de las distintas columnas existentes, indicando si son mostradas o no, el nombre de la columna, y el tipo de campo que muestran. Para incluir

nuestras nuevas columnas, pulsamos **'Añadir'**. Introducimos en **'Title'** el nombre deseado ('PO'), el tipo de campo (**'Src port (unresolved)'**). Hecho esto, añadimos otra columna de la misma forma, con el nombre ('PD') y el tipo de campo (**'Dst port (unresolved)'**) adecuados:



Podemos cambiar el orden de las columnas para que se ajusten a nuestras necesidades simplemente arrastrando la fila a la posición adecuada, teniendo en cuenta que el orden en el que se muestran es de izquierda a derecha, comenzando por la superior.

Ejercicios de captura de tráfico

1. Durante la realización de las prácticas, será muy común disponer de una consola donde ejecutaremos comandos que mandan y reciben tramas por un interfaz de red. En paralelo tendremos en ejecución a Wireshark, que estará capturando el tráfico que nos interese. Este ejercicio muestra un ejemplo típico a realizar en prácticas posteriores:

1. Abra una consola o *shell*, y déjela abierta en espera de ejecutar algún comando.
2. Ejecute Wireshark y seleccione y configure el interfaz por el que se capturará el tráfico (habitualmente será **eth0**) Acuérdese de seleccionar las opciones de visualización que más le convenga.
3. Inicie la captura de tráfico pulsando en el botón 'Start'.
4. Vuelva a la consola y ejecute el siguiente comando (tecléelo y pulse <enter>):

   ```
   $ sudo hping3 -S -p 80 www.uam.es
   ```

5. Detenga la captura de tráfico mediante el botón 'Stop'.
6. Analice el tráfico capturado (aunque no lo entienda en detalle)
7. Guarde la traza en un fichero **(Importante: no utilizar el formato pcap-ng)**.
8. Cierre Wireshark, y vuelva a abrirlo.
9. Abra el fichero almacenado y compruebe que se almacenó correctamente.
10. Utilizando las columnas que se han añadido durante el tutorial, ordene con respecto al campo 'PO' en sentido descendente y contabilice el número de paquetes en el que este campo tiene valor 53.

Describa el proceso realizado y discuta los problemas que haya encontrado durante la realización del ejercicio.

2. Tras haber leído las documentación online facilitada, empiece a capturar tráfico. Abra un navegador y genere tráfico a partir de la visualización de páginas web. Pare la captura, y añada un filtro en el interfaz de modo que solo se visualicen paquetes que sean de tipo IP y que tengan un tamaño de paquete mayor a 1000 Bytes.

1. Copie el filtro realizado.
2. ¿Cómo almacenaría en una captura solo los paquetes mostrados?
3. Compare el tamaño del primer paquete IP, y el campo 'length' del protolo IP del mismo. Repita para los primeros 5 paquetes, ¿qué relación encuentra?

3. Añada una columna llamada *interarrival* que muestre el tiempo entre paquetes consecutivos. Explique brevemente qué menús y opciones ha seleccionado.

4. Modifique la forma en que Wireshark muestra la información en la columna 'Time' de cada paquete. En concreto muestre los tiempos en formato para humanos, y en tiempo Unix con resolución en segundos. Explique brevemente los pasos realizados.

5. Inicie una captura en Wireshark pero aplicando **filtros de captura**, en concreto solo queremos capturar tráfico UDP. Mientras captura tráfico, genere durante algunos instantes

tráfico a partir de la visualización de páginas web, y ejecute al mismo tiempo en una consola el comando

```
$ sudo hping3 -S -p 80 www.uam.es.
```

Compruebe que solo se capturan paquetes UDP, y describa brevemente los pasos realizados.