Universidad de Buenos Aires
Facultad de Ingeniería

Seguridad en Redes
TP – Análisis de Protocolos con Wireshark

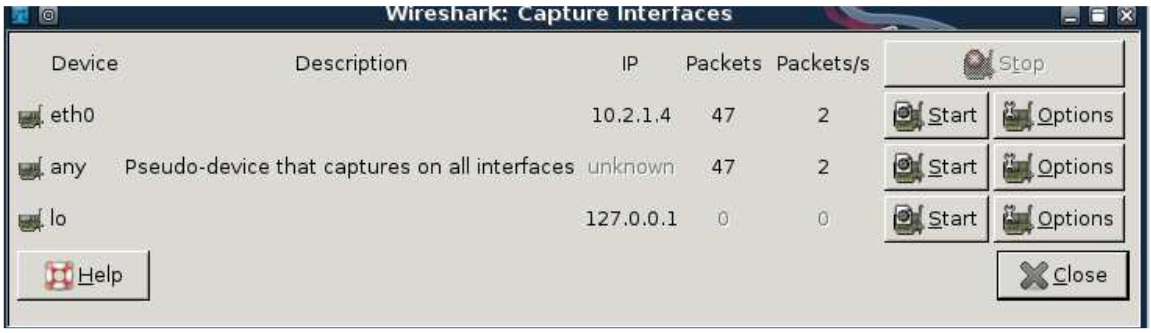
1. Objetivo

El objetivo de este trabajo práctico es proporcionar los elementos básicos de Wireshark para que el alumno pueda trabajar realizando análisis de protocolos en los trabajos prácticos posteriores de la materia.

Wireshark

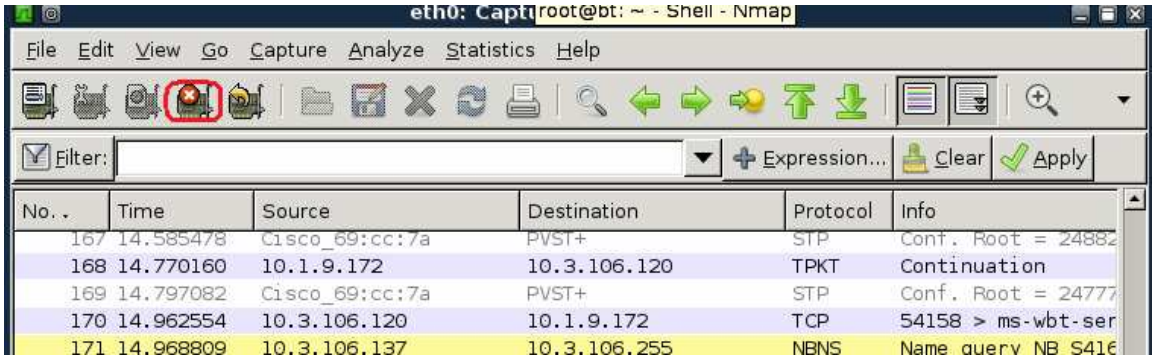
El *Wireshark* es un *sniffer*, es decir, un programa que al ejecutarse va copiando todos los frames que llegan a este host. Se encuentra incluido en la mayoría de las distribuciones de Linux, y también puede descargarse gratuitamente de www.wireshark.org
Este software nos resultará útil para la práctica de laboratorio, donde deberemos analizar protocolos de aplicación.
Para ilustrar su uso, realizaremos un ejemplo con el protocolo de aplicación POP.

Mediante el menú `Capture` – `Interfaces` podemos comenzar a "escuchar" la red y buscar la información que nos interesa. El programa presentará la siguiente pantalla:

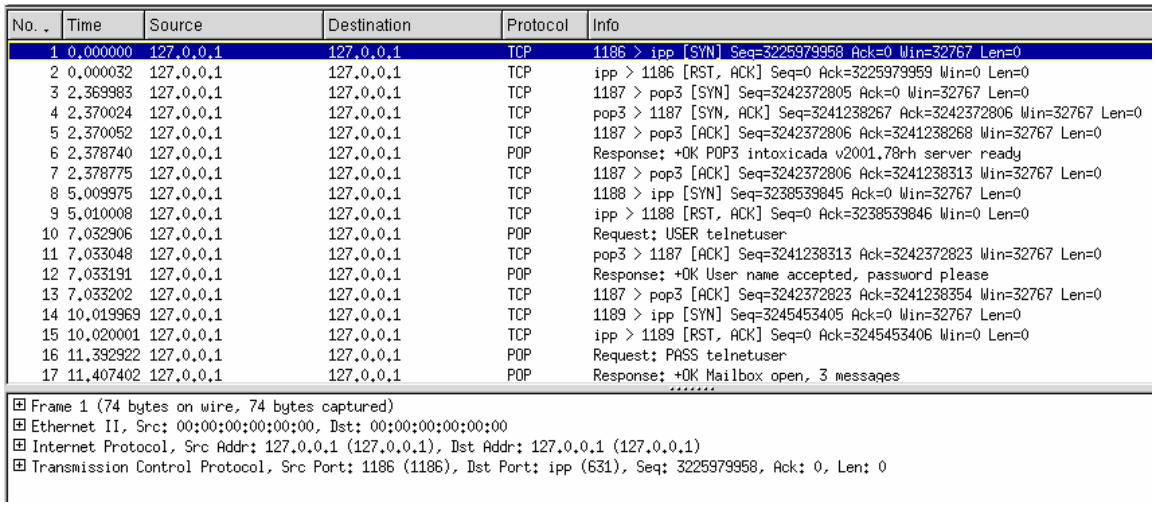


Acá debemos seleccionar la interfaz sobre la que queremos trabajar (Ej: `eth0`) y presionar Start para comenzar.

Ahora se deberán iniciar las acciones correspondientes al protocolo que se quiere analizar. En este ejemplo nos conectamos al demonio POP que se encuentra corriendo en la misma máquina donde estamos, o sea, el *localhost* (127.0.0.1).
Al presionar el botón `Stop`,

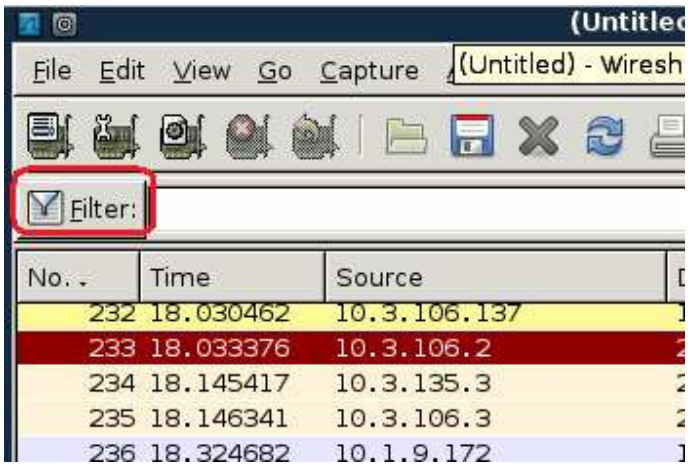


se obtiene la siguiente pantalla:

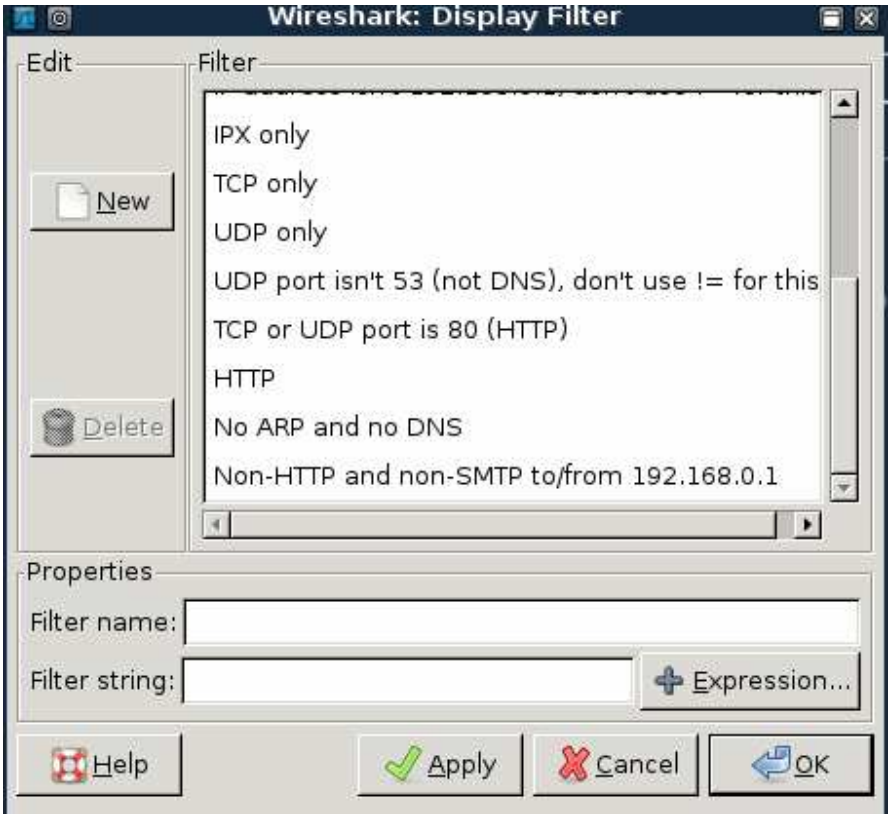


En cada línea de la parte superior podemos ver cada frame que Ethereal levanto de la interfase.
Las columnas son: número de paquete, un *timestamp*, dirección de origen, dirección de destino, protocolo, y un resumen de la información que contiene el frame.
En la parte central observamos que hay cuatro o cinco líneas por cada frame seleccionado en la parte superior. Cada una de estas líneas corresponde a los protocolos usados de las distintas capas del modelo TCP/IP.
En nuestro caso sólo nos interesa la línea inferior, que es la que corresponde a la capa de aplicación (inmediatamente debajo de “TCP”).
En la parte inferior se encuentra el *dump* del frame tanto en hexadecimal como en ASCII.

Tal como se encuentra, la captura realizada presenta la información que no nos es de utilidad en este momento:
FILTRO: Si sólo nos interesa ver la información correspondiente al protocolo POP, podemos aplicar un filtro de información. Al presionar el botón `Filter`, que se encuentra en la esquina superior izquierda.



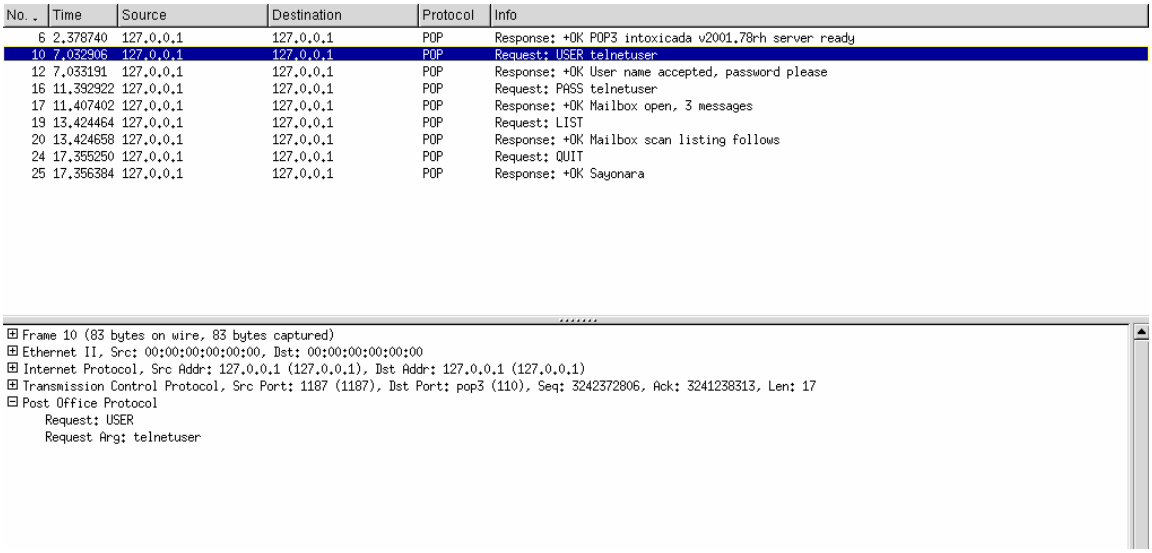
se abre la siguiente ventana:



Acá podemos escribir filtros complejos, usando expresiones lógicas e información de los protocolo/s que queramos analizar.

Sin embargo, nosotros sólo necesitamos filtrar el protocolo POP. Para esto alcanza con completar la caja de texto que está al lado del botón `Filter` en la pantalla principal con la expresión “pop”

(sin las comillas y con minúscula) y presionar el botón `Apply`. Así obtendremos la siguiente información:



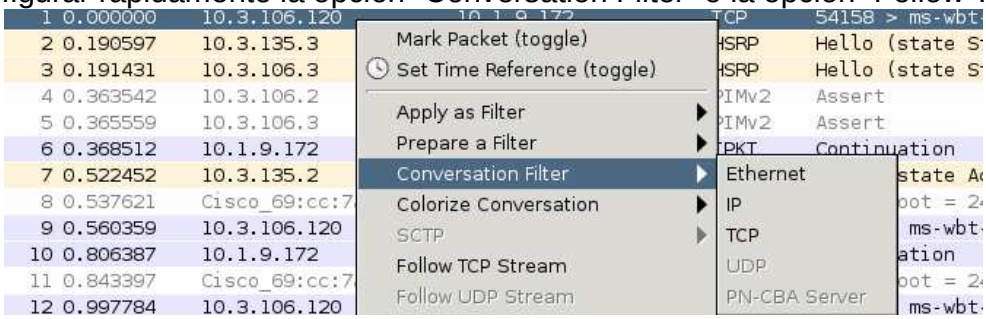
Expandiendo la quinta línea, como se muestra en la figura, podemos ver la información correspondiente al protocolo que queremos analizar.

CONSEJOS:

Tal vez necesite filtrar paquetes por dirección IP de origen y destino además de por protocolo.

Si se quiere hacer el seguimiento de una conexión

Se puede configurar rápidamente la opción “Conversation Filter” o la opción “Follow TCP Stream



Filtros por MAC eth.addr == 00:78:AC:...