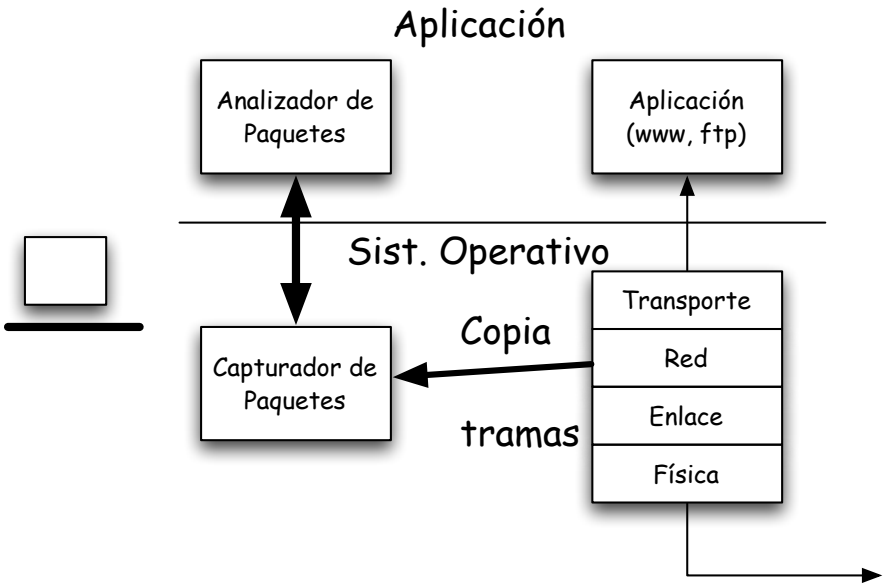
Practica #1 : Sniffing de paquetes.

Andrés Arcia-Moret

Un sniffer de paquetes sirve para observar el trafico que circula por una red y así poder comprender los protocolos que intervienen en una trozo de la comunicación. El sniffer es capaz de mostrar los campos de los paquetes que se obtienen de forma pasiva (después de ser capturados). El sniffer de paquetes no genera paquetes, simplemente obtiene una copia de la cual se puede extraer la información.

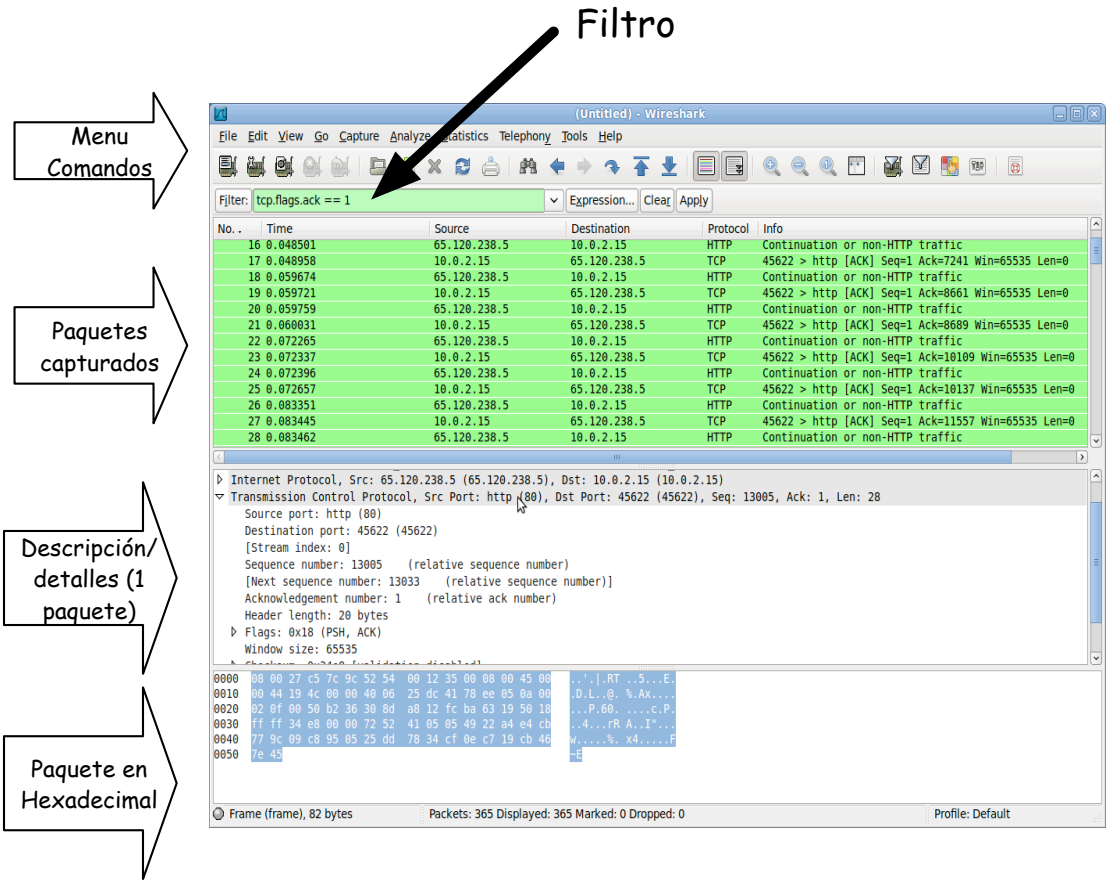


En la figura #1 se muestra la arquitectura del sniffer. Al arquitectura está compuesta principalmente por dos capas de funcionalidades importantes. La primera corresponde a la captura del paquete propiamente dicho. El sniffer es capaz de obtener una copia de la trama que será descompuesta posteriormente por el analizador de paquetes, quien mostrará la información contenida en la captura. El análisis hecho por el analizador de paquetes corresponde a la separación de los diferentes protocolos que se encuentran encapsulados dentro de la trama recien capturada. Así, se puede ver el paquete IP que contiene al paquete TCP, que a su vez transporta un mensaje HTTP; producto seguramente de una consulta a través de un navegador WEB. Recordemos que estos mensajes tienen a su vez un proposito específico dentro del proceso de recuperación de la información. Puede entonces haber una consulta del tipo GET para obtener una página de un servidor, un POST para enviar una planilla al servidor, etc.

Para obtener el wireshark podemos descargarlo de la página Web: http://www.wireshark.org. El software es completamente gratuito y puede ser descargado para distintas plataformas.

Andrés Arcia-Moret
Universidad de Los Andes, Mérida.

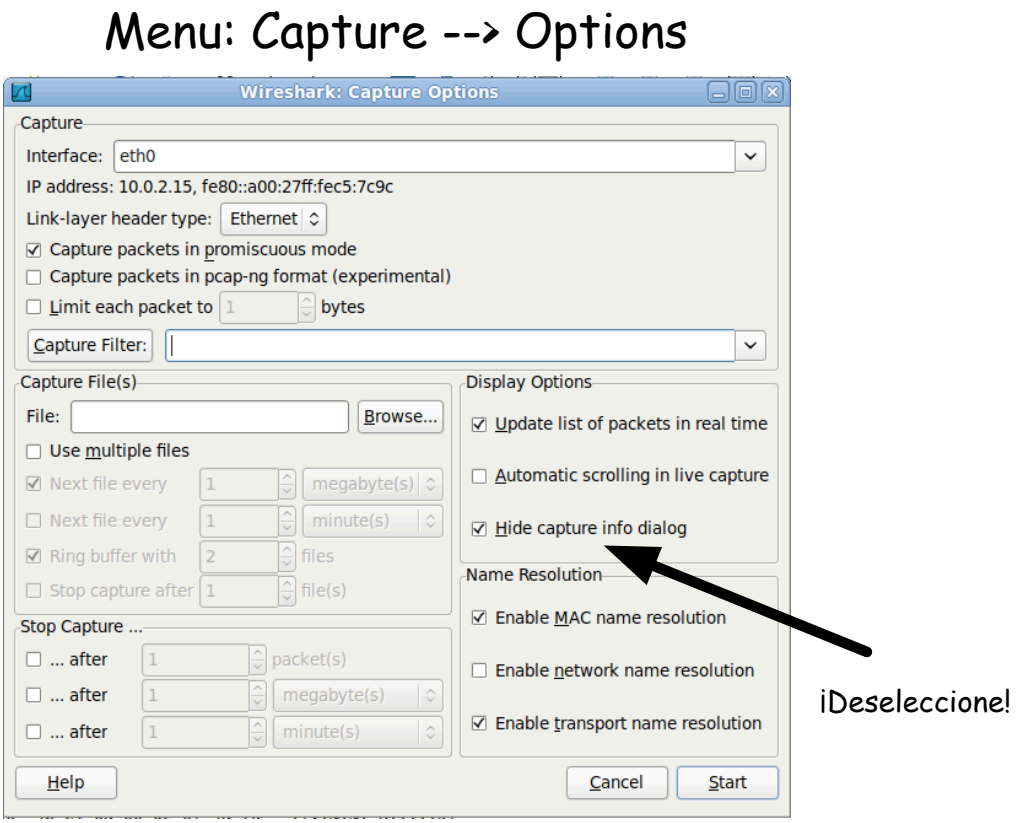
Ejecución del Wireshark:



En la figura anterior observamos la interfaz típica de Wireshark. Este resultado fue obtenido luego de haber hecho los siguientes pasos:

1. Iniciar un navegador web, en el cual se puede desplegar (posteriormente) la siguiente pantalla: http://webdelprofesor.ula.ve/ingenieria/amoret.
2. Iniciar el Wireshark en modo superusuario para poder tener acceso a la captura de paquetes de algunas de las interfaces de interés. Note que los privilegios de acceso son necesarios para la captura de paquetes. En este momento las ventanas de captura, descripción y valor hexadecimal de paquetes deben estar vacías.
3. Para hacer una captura, diríjase al menu “Capture” y luego “Options”, donde aparecerá como primera opción un listado de todas las interfaces disponibles. Recuerde deseleccionar la caja “Hide capture info dialog” para poder observar en tiempo real el conteo de los paquetes que están siendo retenidos.
4. Inicie la captura en la interfaz de salida a la Internet.
5. Habiendo cargado el navegador (paso 1) escriba la dirección web en la barra de navegación. Observe en el Wireshark como la cuenta de los

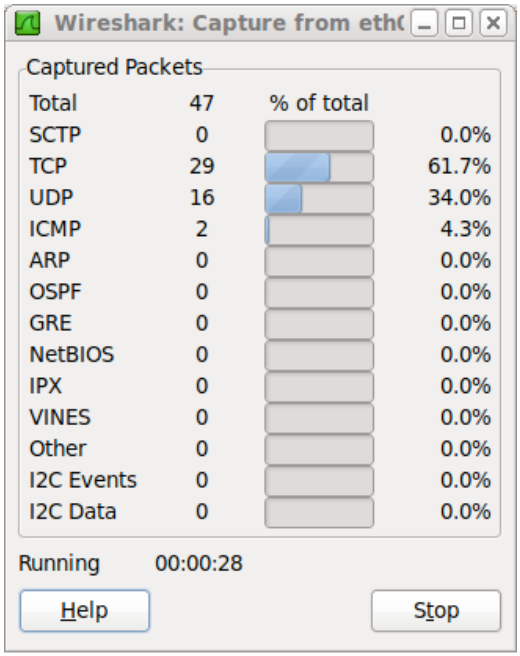
paquetes capturados incrementa. Luego de haber obtenido el resultado deseado en el navegador, detenga la captura en el Wireshark.



6. En la ventana de dialogo “Capture → Options” puede dejar la mayoría de los valores por omisión. Puede luego pulsar el boton “Start” para comenzar la captura.
7. Una vez que usted se dirija al navegador y coloque la dirección web (paso 1), la captura comenzará y se mostrará por pantalla la caja de dialogo que cuenta los paquetes que están siendo capturados.

Andrés Arcia-Moret
Universidad de Los Andes, Mérida.

Estadísticas de la Captura



8. Luego en el cuadro de diálogo podrá observar la captura de las tramas Ethernet (si es el caso) que contiene los encabezados IP, TCP y HTTP.
9. Recuerde detener la captura en cuanto el objeto Web que solicitó haya llegado completamente. Observe los diferentes protocolos que han sido observados en la captura.
10. Ahora podemos observar un poco las bondades del filtro de paquetes. Escriba en el espacio "Filter", el nombre del protocolo que desea observar: "http" y luego pulse "Apply", o "tcp" y luego pulse "Apply". ¿Con que filtro aparecen más paquetes? Ayudese de la opción "Statistics → Summary". ¿Cuantos paquetes HTTP aparecen? ¿Cuántos paquetes TCP **puros** aparecen?
11. Al haber seleccionado "http" como protocolo, debería aparecer como primera fila el un mensaje HTTP GET indicando la solicitud de la página al servidor WEB. Cuando observe el paquete HTTP GET podrá ver también que fue transportado por con un encabezado TCP, IP y probablemente Ethernet. Si usted maximiza el la ventana que contiene la información del paquete HTTP podrá ver los campos a detalle transportados hacia el servidor.
    a. Anote la versión del protocolo HTTP utilizado
    b. ¿Cómo se identifica la máquina que usted usa y que se está reportando al servidor?
12. Puede usted salir de Wireshark pues ha completado la práctica introductoria.

Ejercicios prácticos:

1. Cuando se hizo la primera captura (en modo promiscuo) se observan los paquetes de todas las máquinas que se encuentran en el laboratorio.

Añada una regla de filtrado para observar solamente los paquetes destinados a su máquina.

2. Luego de haber hecho la observación del punto 11, ¿Puede usted identificar el campo donde viaja el nombre de la página WEB?
3. Haga una lista de los diferentes protocolos que observó en la captura realizada. Obtenga también el significado de las siglas y a través de un diagrama, diga donde se ubica cada uno de estos protocolos.
4. ¿Cuanto tiempo transcurrió entre el primer mensaje HTTP GET que fue enviado y la respuesta HTTP/1.X 200 OK fue recibida? Puede ayudarse con los distintos formatos para mostrar el tiempo de captura de la traza. Vaya a "View" y luego "Time Display Format". ¿Cuántos objetos fueron solicitados y obtenidos dentro de su captura?
5. Marque las direcciones de Internet (o direcciones IP) que intervinieron en el proceso de captura, es decir, la de su computador y la de webdelprofesor.ula.ve.
6. Exporte el paquete seleccionado en formato postcript y observelo por pantalla.

Referencia: Wireshark, Getting Started. Version 2.0. J.F. Kurose, K.W. Ross. 2009.