Objetivos de aprendizaje

- Poder explicar el propósito de un analizador de protocolos (Wireshark).

- Poder realizar capturas básicas de la unidad de datos del protocolo (PDU) mediante el uso de Wireshark.

Información básica

Wireshark es un analizador de protocolos de software o una aplicación "husmeador de paquetes" que se utiliza para el diagnóstico de fallas de red, verificación, desarrollo de protocolo y software y educación. Antes de junio de 2006, Wireshark se conocía como Ethereal.

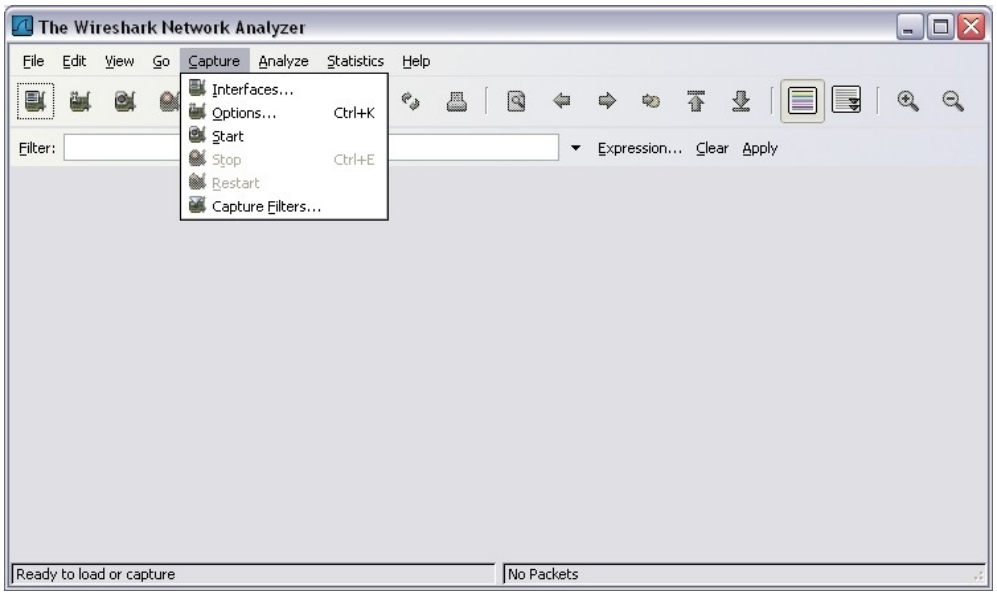
Un husmeador de paquetes (también conocido como un analizador de red o analizador de protocolos) es un software informático que puede interceptar y registrar tráfico de datos pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el husmeador "captura" cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo a la RFC correcta u otras especificaciones.

Para obtener más información y para descargar el programa visite: http://www.Wireshark.org

Escenario

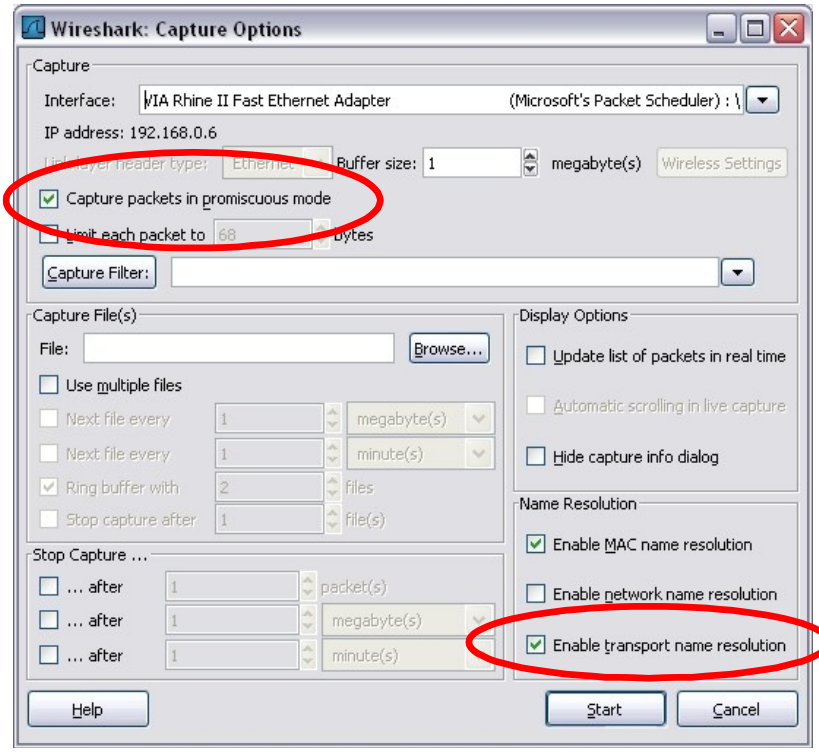
Para capturar las PDU, la computadora donde está instalado Wireshark debe tener una conexión activa a la red y Wireshark debe estar activo antes de que se pueda capturar cualquier dato.

Para empezar con la captura de datos es necesario ir al menú **Capture** y seleccionar **Options**.
El cuadro de diálogo **Options** provee una serie de configuraciones y filtros que determinan el tipo y la cantidad de tráfico de datos que se captura.



Primero, es necesario asegurarse de que Wireshark está configurado para monitorear la interfaz correcta. Desde la lista desplegable **Interface**, seleccione el adaptador de red que se utiliza. Generalmente, para una computadora, será el adaptador Ethernet conectado.

Luego se pueden configurar otras opciones.



Modo promiscuo.

Si esta característica NO está verificada, sólo se capturarán las PDU destinadas a esta computadora. Si esta característica está verificada, se capturarán todas las PDU destinadas a esta computadora Y todas aquellas detectadas por la NIC de la computadora en el mismo segmento de red (es decir, aquellas que "pasan por" la NIC pero que no están destinadas para la computadora).
Nota: La captura de las otras PDU depende del dispositivo intermediario que conecta las computadoras del dispositivo final en esta red. Si utiliza diferentes dispositivos intermediarios (hubs, switches, routers).

Resolución del nombre de red

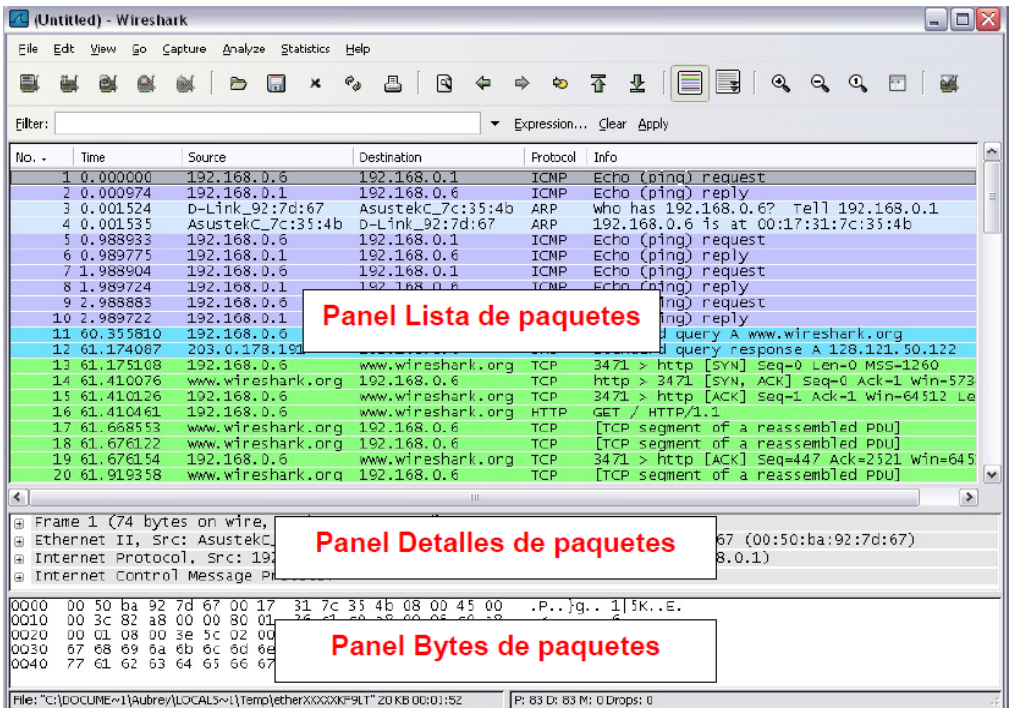
Esta opción le permite controlar si Wireshark traduce a nombres las direcciones de red encontradas en las PDU. A pesar de que esta es una característica útil, el proceso de resolución del nombre puede agregar más PDU a sus datos capturados, que podrían distorsionar el análisis.

Botón **Start** para comenzar el proceso de captura de datos y una casilla de mensajes muestra el progreso de este proceso.

Mientras se capturan las PDU, los tipos y números se indican en la casilla de mensajes.

Si hace clic en el botón **Stop**, el proceso de captura termina y se muestra la pantalla principal.

La ventana de visualización principal de Wireshark tiene tres paneles.



El panel de **Lista de PDU** (o Paquete) ubicado en la parte superior del diagrama muestra un resumen de cada paquete capturado. Si hace clic en los paquetes de este panel, controla lo que se muestra en los otros dos paneles.

El panel de **detalles de PDU** (o Paquete) ubicado en el medio del diagrama, muestra más detalladamente el paquete seleccionado en el panel de Lista del paquete.

El panel de **bytes de PDU** (o paquete) ubicado en la parte inferior del diagrama, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado en el panel de Lista del paquete y resalta el campo seleccionado en el panel de Detalles del paquete.

Cada línea en la Lista del paquete corresponde a una PDU o paquete de los datos capturados.
Si seleccionó una línea en este panel, se mostrarán más detalles en los paneles “Detalles del paquete” y “Bytes del paquete”.

El panel Detalles del paquete muestra al paquete actual (seleccionado en el panel “Lista de paquetes”) de manera más detallada. Este panel muestra los protocolos y los campos de protocolo de los paquetes seleccionados. Los protocolos y los campos del paquete se muestran con un árbol que se puede expandir.

El panel Bytes del paquete muestra los datos del paquete actual (seleccionado en el panel “Lista de paquetes”) en lo que se conoce como estilo “hexdump”. En esta práctica de laboratorio no se examinará en detalle este panel. Sin embargo, cuando se requiere un análisis más profundo, esta información que se muestra es útil para examinar los valores binarios y el contenido de las PDU.

Tarea 1: Captura de paquetes mediante el uso del comando ping

Paso 1: Después de asegurarse de que la topología y configuración de laboratorio estándar son correctas, inicie Wireshark en un equipo del laboratorio.

Desde la línea de comando del equipo, haga ping en la dirección IP de de una dirección perteneciente a su red.

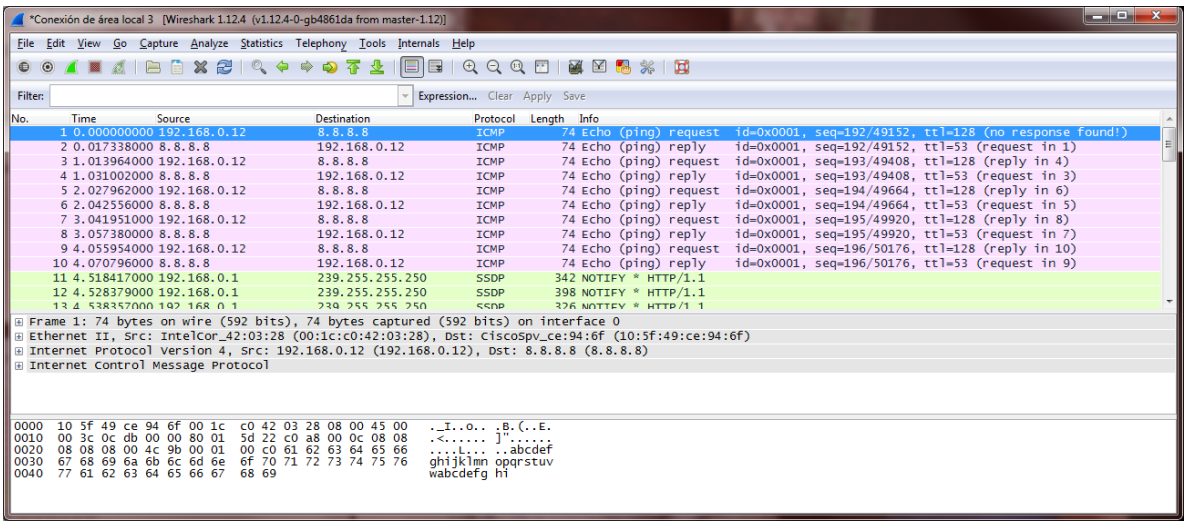
C:\>ping 8.8.8.8 -t

Configure las opciones de captura como se describió anteriormente, en la descripción general e inicie el proceso de captura.

Después de recibir las respuestas exitosas al ping en la ventana de línea de comandos, detenga la captura del paquete.

Paso 2: Examine el panel Lista de paquetes.

El panel Lista de paquetes en Wireshark debe verse ahora parecido a la imagen que se muestra a continuación:



Observe los paquetes de la lista de arriba. Nos interesan los números de paquete 1 y 2

Paso 3: Responda las siguientes preguntas en base a la captura de paquetes realizada con Wireshark:

¿Qué protocolo se utiliza el comando ping? _____
¿Cuál es el nombre completo del protocolo? _____
¿Cuáles son los nombres, información de los dos mensajes ping? _____

_____

Localice las dos direccione físicas de “Origen” y “Destino” - MAC. ¿Por qué hay dos tipos?

_____

¿Cuál es la versión del protocolo ip utilizada, en que parte o capa se puede obtener esta información?

_____

¿Cuáles es el protocolo que se encuentra en la capa de Ethernet, indique el valor del campo type (nombre del protocolo, su valor)?

Complete la siguiente tabla con la información que se solicita (recorra las diferentes capas que le presenta la aplicación)

Dirección IP origen:	
Dirección IP destino:	
Dirección MAC origen:	
Dirección MAC destino:	
Fabricante MAC origen:	
Fabricante MAC destino:	
Tipo:	
Data:	
Versión del protocolo	
Tipo de comunicación (únicast – multicast)	