

Práctica de laboratorio 2.6.2: Uso de Wireshark™ para visualizar unidades de datos del protocolo

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.
- Poder realizar un análisis básico de la PDU en un tráfico de datos de red simple.
- Experimentar con las características y opciones de Wireshark, como captura de PDU y visualización de filtrado.

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.

Wireshark está programado para reconocer la estructura de los diferentes protocolos de red. Esto le permite mostrar la encapsulación y los campos individuales de una PDU e interpretar su significado.

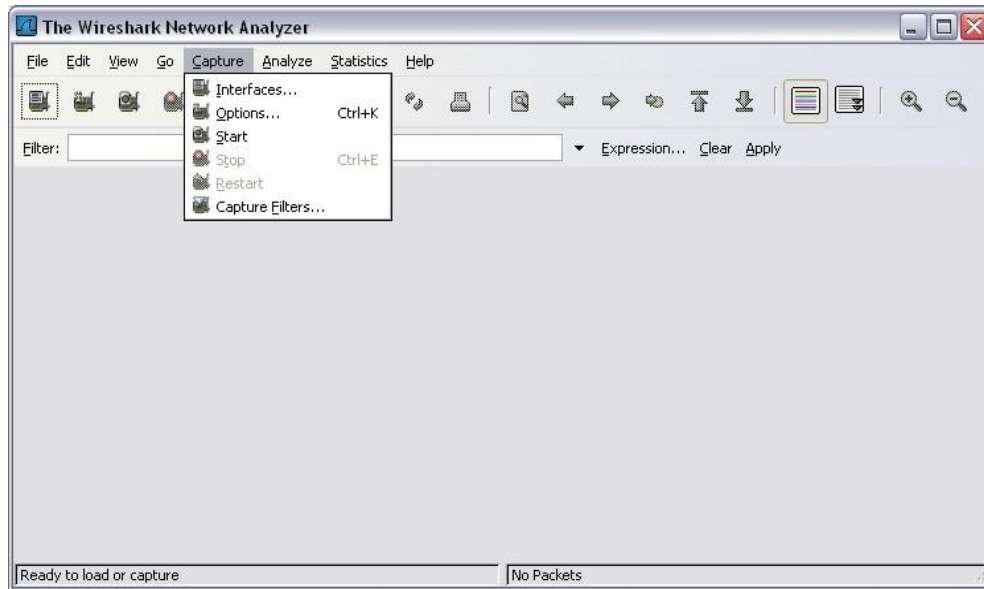
Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar en la mayoría de las prácticas de laboratorio en los cursos CCNA para el análisis de datos y el diagnóstico de fallas.

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

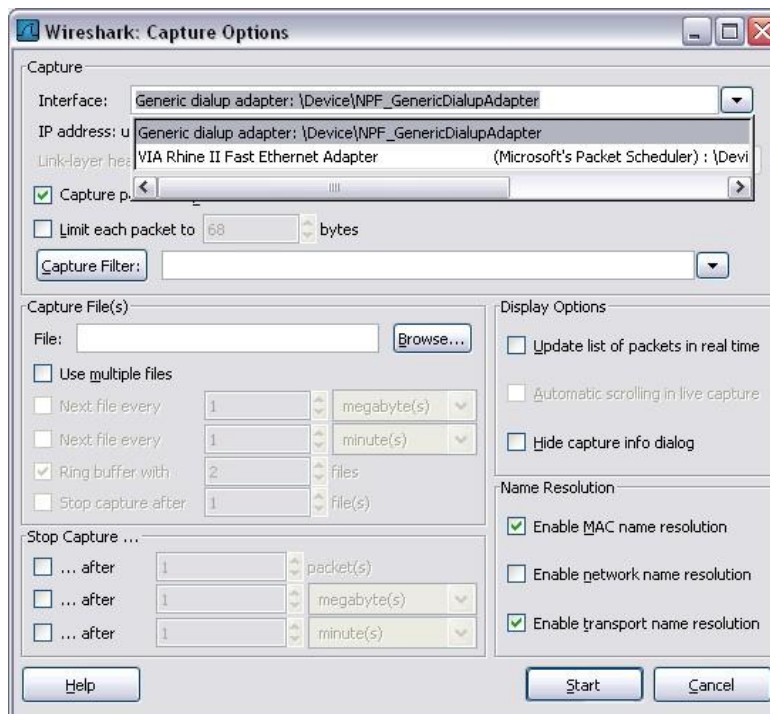
Escenario

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.

Cuando se inicia Wireshark, se muestra la siguiente pantalla.

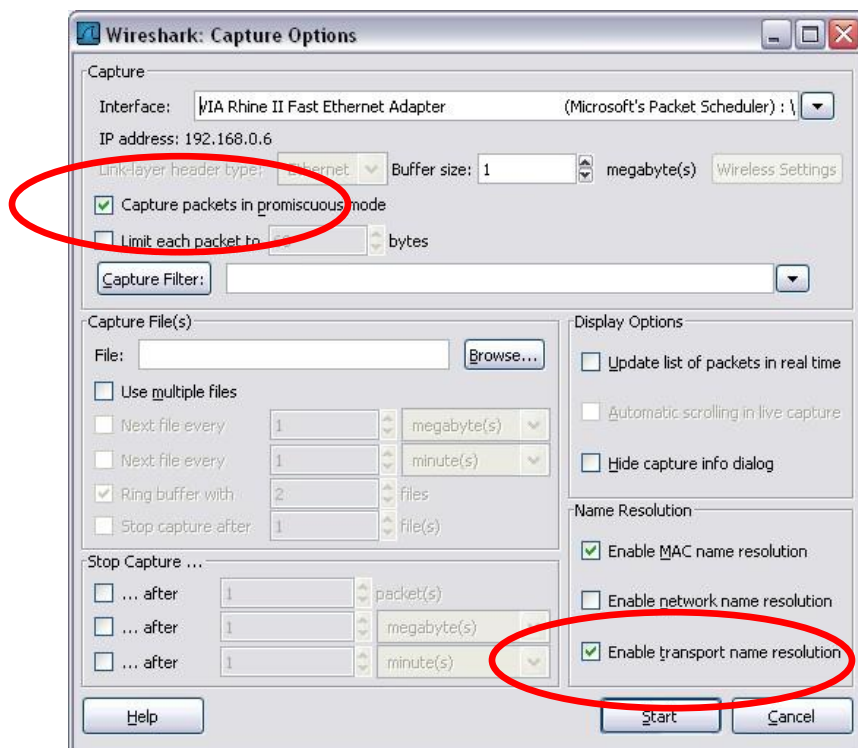


Para empezar con la captura de datos es necesario ir al menú **Captura** y seleccionar **Opciones**. El cuadro de diálogo **Opciones** provee una serie de configuraciones y filtros que determinan el tipo y la cantidad de tráfico de datos que se captura.



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

Luego se pueden configurar otras opciones. Entre las que están disponibles en **Opciones de captura**, merecen examinarse las siguientes dos opciones resaltadas.



Configurar Wireshark para capturar paquetes en un 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).

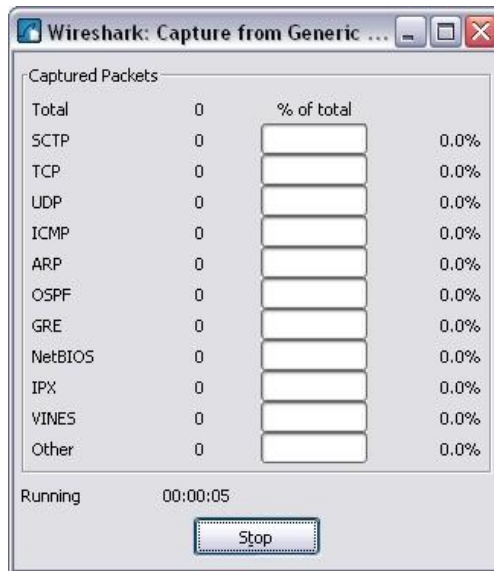
Nota: La captura de las otras PDU depende del dispositivo intermediario que conecta las computadoras del dispositivo final en esta red. Si utiliza diferentes dispositivos intermediarios (hubs, switches, routers) durante estos cursos, experimentará los diferentes resultados de Wireshark.

Configurar Wireshark para la resolución del nombre de red

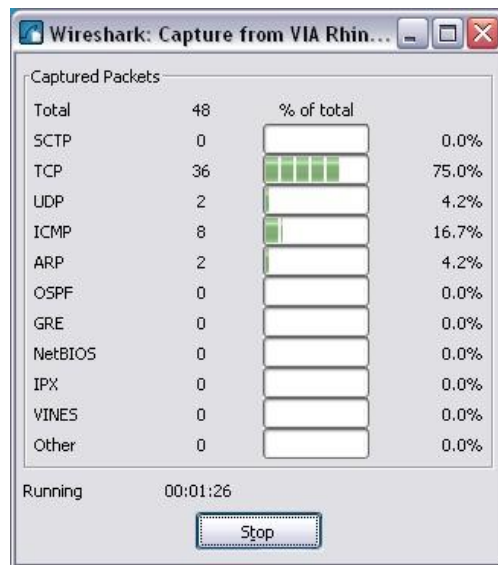
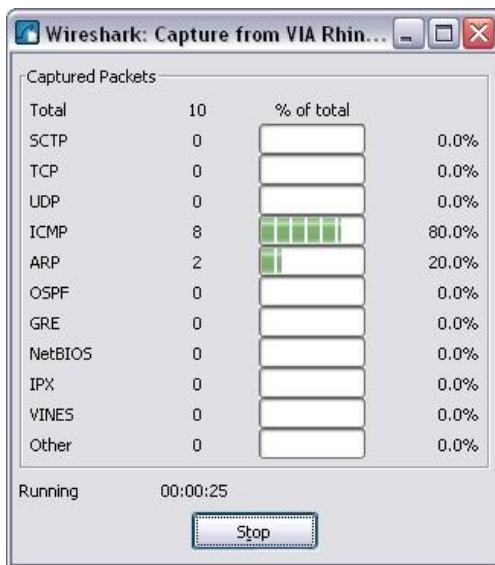
Esta opción le permite controlar si Wireshark traduce a nombres las direcciones de red encontradas en las PDU. A pesar de que esta es una característica útil, el proceso de resolución del nombre puede agregar más PDU a sus datos capturados, que podrían distorsionar el análisis.

También hay otras configuraciones de proceso y filtrado de captura disponibles.

Haga clic en el botón **Iniciar** para comenzar el proceso de captura de datos y una casilla de mensajes muestra el progreso de este proceso.



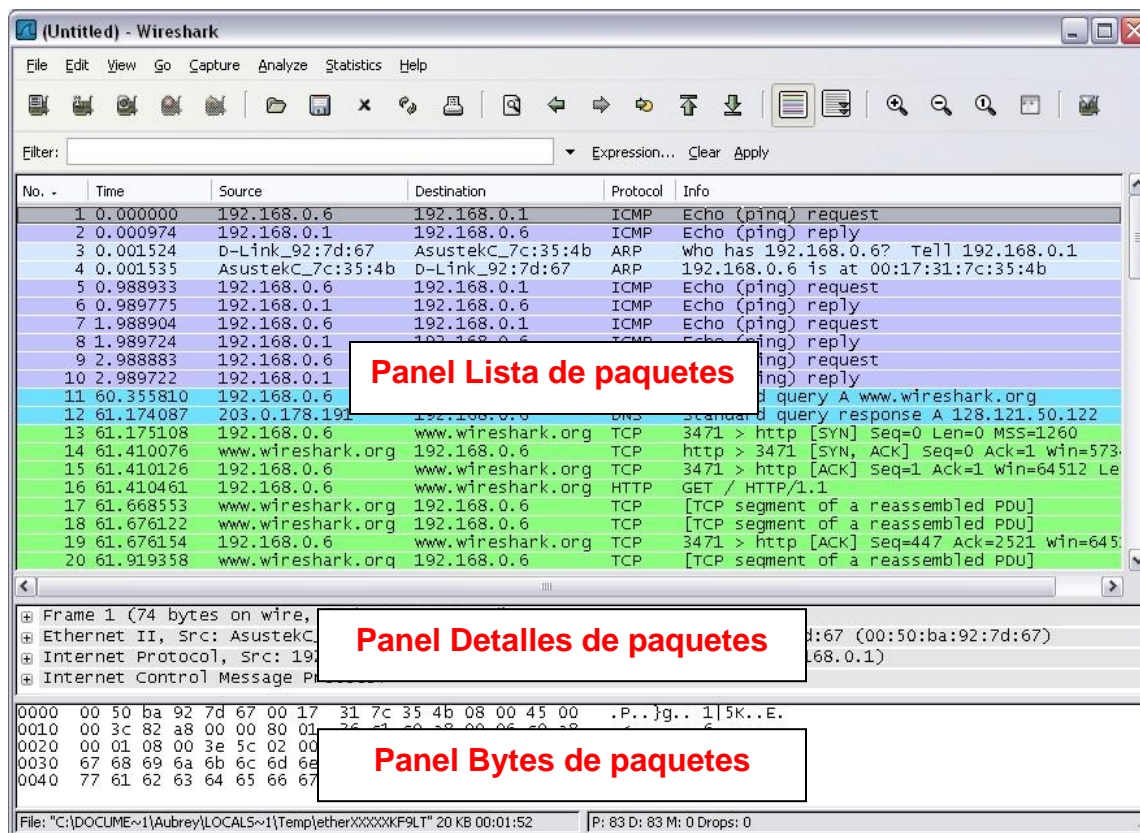
Mientras se capturan las PDU, los tipos y números se indican en la casilla de mensajes.



Los ejemplos de arriba muestran la captura de un proceso ping y luego el acceso a una página Web.

Si hace clic en el botón **Detener**, 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 ejemplo de arriba muestra las PDU capturadas cuando se utilizó la utilidad ping y cuando se accedió a <http://www.Wireshark.org>. Se seleccionó el paquete número 1 en este panel.

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 y colapsar.

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.

La información capturada para las PDU de datos se puede guardar en un archivo. Ese archivo se puede abrir en Wireshark para un futuro análisis sin la necesidad de volver a capturar el mismo tráfico de datos. La información que se muestra cuando se abre un archivo de captura es la misma de la captura original.

Cuando se cierra una pantalla de captura de datos o se sale de Wireshark se le pide que guarde las PDU capturadas.



Si hace clic en **Continuar sin guardar** se cierra el archivo o se sale de Wireshark sin guardar los datos capturados que se muestran.

Tarea 1: Captura de PDU mediante ping

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

Configure las opciones de captura como se describe arriba en la descripción general e inicie el proceso de captura.

Desde la línea de comando del equipo, haga ping en la dirección IP de otra red conectada y encienda el dispositivo final en la topología de laboratorio. En este caso, haga ping en Eagle Server utilizando el comando ping **192.168.254.254**.

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 éste:

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PagP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Observe los paquetes de la lista de arriba. Nos interesan los números de paquetes 6, 7, 8, 9, 11, 12, 14 y 15. Localice los paquetes equivalentes en la lista de paquetes de su equipo.

Si el usuario realizó el Paso 1 A de arriba, haga coincidir los mensajes que se muestran en la ventana de línea de comandos cuando el ping se ejecutó con los seis paquetes capturados por Wireshark.

Responda lo siguiente desde la lista de paquetes Wireshark:

¿Qué protocolo se utiliza por ping? _____

¿Cuál es el nombre completo del protocolo? _____

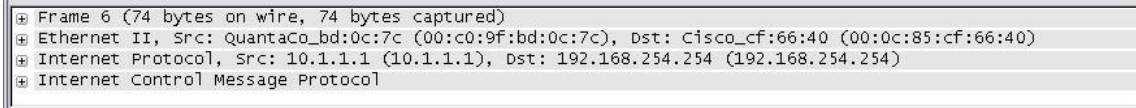
¿Cuáles son los nombres de los dos mensajes ping? _____

¿Las direcciones IP de origen y destino que se encuentran en la lista son las que esperaba? Sí / No

¿Por qué? _____

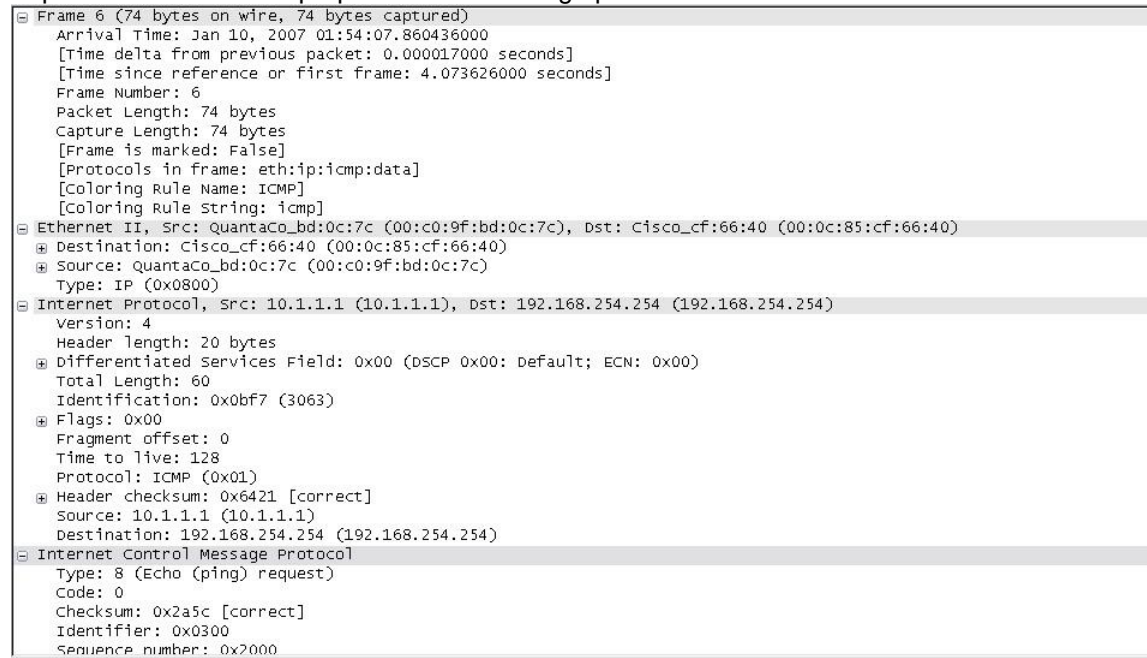
Paso 3: Seleccione (resalte) con el mouse el primer paquete de solicitud de eco en la lista.

El panel de Detalles del paquete mostrará ahora algo parecido a:



Haga clic en cada uno de los cuatro “+” para expandir la información.

El panel de Detalles del paquete será ahora algo parecido a:



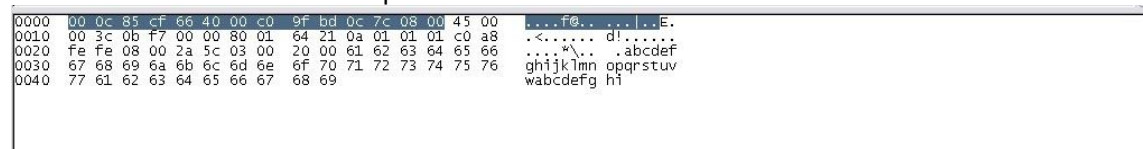
Como puede ver, los detalles de cada sección y protocolo se pueden expandir más. Tómese el tiempo para leer esta información. En esta etapa del curso, puede ser que no entienda completamente la información que se muestra, pero tome nota de la que sí reconozca.

Localice los dos tipos diferentes de “Origen” y “Destino”. ¿Por qué hay dos tipos?

¿Cuáles son los protocolos que están en la trama de Ethernet?

Si selecciona una línea en el panel de Detalles del paquete, toda o parte de la información en el panel de Bytes del paquete también quedará resaltada.

Por ejemplo, si la segunda línea (+ Ethernet II) está resaltada en el panel de detalles, el panel de Bytes resalta ahora los valores correspondientes.



Esto muestra los valores binarios particulares que representan la información de la PDU. En esta etapa del curso no es necesario entender esta información en detalle.

Paso 4: Vaya al menú Archivo y seleccione Cerrar.

Haga clic en **Continuar sin guardar** cuando se muestre esta casilla de mensaje.



Tarea 2: Captura de FTP PDU

Paso 1: Inicie la captura de paquetes.

Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción Iniciar en el menú **Captura** de Wireshark.

Ingrese **ftp 192.168.254.254** en la línea de comandos del equipo donde se ejecuta Wireshark.

Quando se establezca la conexión, ingrese **anónimo** como usuario, sin ninguna contraseña.

ID del usuario: **anónimo**

Password: <INTRO>

También se puede iniciar sesión con id de usuario **cisco** y contraseña **cisco**.

Una vez que inició sesión con éxito, ingrese `get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe` y presione la tecla ingresar <INTRO>. Con esa operación comenzará la descarga del archivo desde el servidor ftp. El resultado será similar a:

```
C:\Documents and Settings\ccnal>ftp eagle-server.example.com
Connected to eagle-server.example.com.
220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password:<ENTER>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.
```

Una vez que la descarga del archivo se haya completado, ingrese **quit**

```
ftp> quit
221 Goodbye.
C:\Documents and Settings\ccnal>
```

Una vez que los archivos se hayan descargado exitosamente, detenga la captura PDU en Wireshark.

Paso 2: Aumente el tamaño del panel de Lista de paquetes de Wireshark y desplácese por las PDU que se encuentren en la lista.

Localice y tome nota de las PDU asociadas con la descarga del archivo. Éstas serán las PDU del protocolo TCP de Capa 4 y del protocolo FTP de Capa 7.

Identifique los tres grupos de PDU asociados con la transferencia del archivo.

Si realizó el paso de arriba, haga coincidir los paquetes con los mensajes y las indicaciones en la ventana de línea de comandos FTP.

El primer grupo está asociado con la fase “conexión” y el inicio de sesión en el servidor. Haga una lista de ejemplos de mensajes intercambiados en esta fase.

Localice y haga una lista de ejemplos de mensajes intercambiados en la segunda fase, que es el pedido de descarga real y la transferencia de datos.

El tercer grupo de PDU está relacionado con el cierre de sesión y la “desconexión”. Haga una lista de ejemplos de mensajes intercambiados durante este proceso.

Localice los intercambios TCP recurrentes a través del proceso FTP. ¿Qué característica de TCP indica esto?

Paso 3: Examine los Detalles del paquete.

Seleccione (resalte) un paquete de la lista asociada con la primera fase del proceso FTP. Observe los detalles del paquete en el panel de Detalles.

¿Cuáles son los protocolos encapsulados en la trama?

Resalte los paquetes que contengan el nombre de usuario y contraseña. Examine la porción resaltada en el panel Byte del paquete.

¿Qué dice esto sobre la seguridad de este proceso de inicio de sesión FTP?

Resalte un paquete asociado con la segunda fase. Desde cualquier panel, localice el paquete que contenga el nombre del archivo.

El nombre del archivo es: _____

Resalte un paquete que contenga el contenido real del archivo. Observe el texto simple visible en el panel Byte.

Resalte y examine en los paneles Detalles y Byte; algunos de los paquetes intercambiados en la tercera fase de la descarga del archivo.

¿Qué características distinguen al contenido de estos paquetes?

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Tarea 3: Captura de HTTP PDU

Paso 1: Inicie la captura de paquetes.

Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción Iniciar en el menú Captura de Wireshark.

Nota: Si se continúa desde pasos anteriores de esta práctica de laboratorio, no es necesario configurar las opciones de captura.

Inicie un navegador Web en el equipo donde ejecuta Wireshark.

Ingrese el URL de Eagle Server ejemplo.com o ingrese la dirección IP-192.168.254.254. Una vez que la página Web se haya descargado por completo, detenga la captura del paquete Wireshark.

Paso 2: Aumente el tamaño del panel de Lista de paquetes de Wireshark y desplácese por las PDU que se encuentren en la lista.

Localice e identifique los paquetes TCP y HTTP asociados con la descarga de la página Web.

Observe el parecido entre este intercambio de mensajes y el intercambio FTP.

Paso 3: En el panel Lista de paquetes, resalte un paquete HTTP que tenga la notación “(text/html)” en la columna Información.

En el panel Detalles del paquete, haga clic en “+” al lado de “Datos de texto basado en línea: html”
¿Cuándo esta información expande lo que se muestra?

Examine la porción que resaltó en el panel Byte.
Esto muestra los datos HTML que contiene el paquete.

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Tarea 4: Reflexión

Considere lo que puede proveer Wireshark sobre la información de encapsulación referida a los datos de red capturados. Relacione esto a los modelos de la capa OSI y TCP/IP. Es importante que el usuario pueda reconocer y relacionar tanto los protocolos representados como la capa de protocolo y los tipos de encapsulación de los modelos con la información provista por Wireshark.

Tarea 5: Desafío

Analice cómo podría utilizar un analizador de protocolos como Wireshark para:

- (1) diagnosticar fallas de una página Web para descargar con éxito un navegador en un equipo e
- (2) identificar el tráfico de datos en una red requerida por los usuarios.

Tarea 6: Limpieza

A menos que el instructor le indique lo contrario, salga de Wireshark y apague el equipo correctamente.