

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE SISTEMAS

TELEMÁTICA III – JUAN C. CASTILLO E.

Práctica No. 1: Uso de Wireshark para ver las 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 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 analizador de red o analizador de protocolo 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.

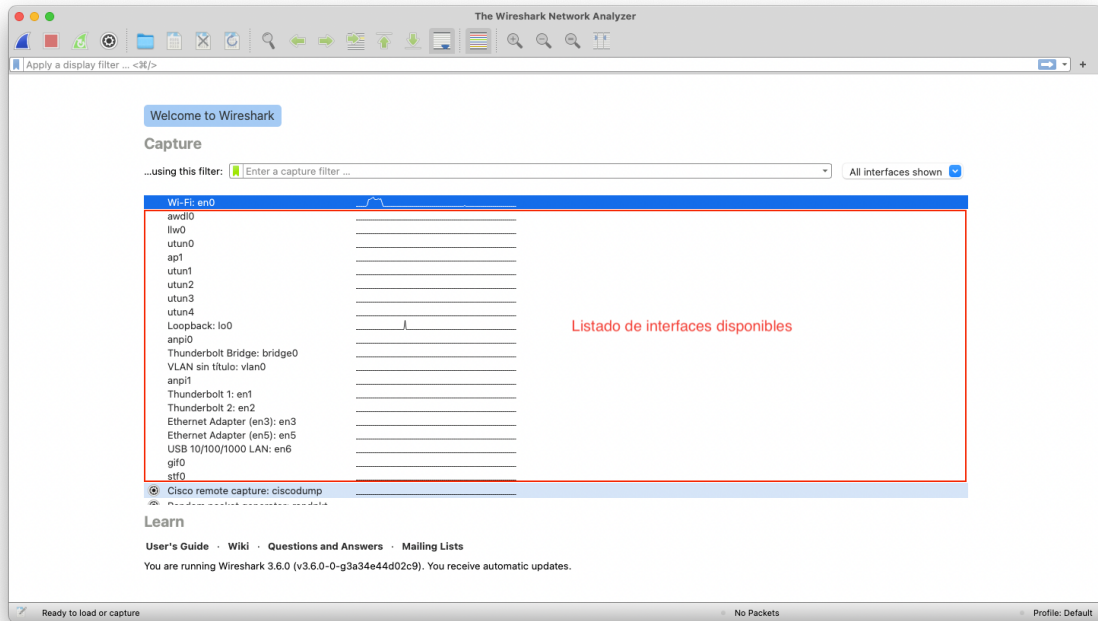
Wireshark está programado para reconocer la estructura de los diferentes protocolos de red. Esto le permite mostrar la encapsulación y los campos individuales de una PDU e interpretar su significado.


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.

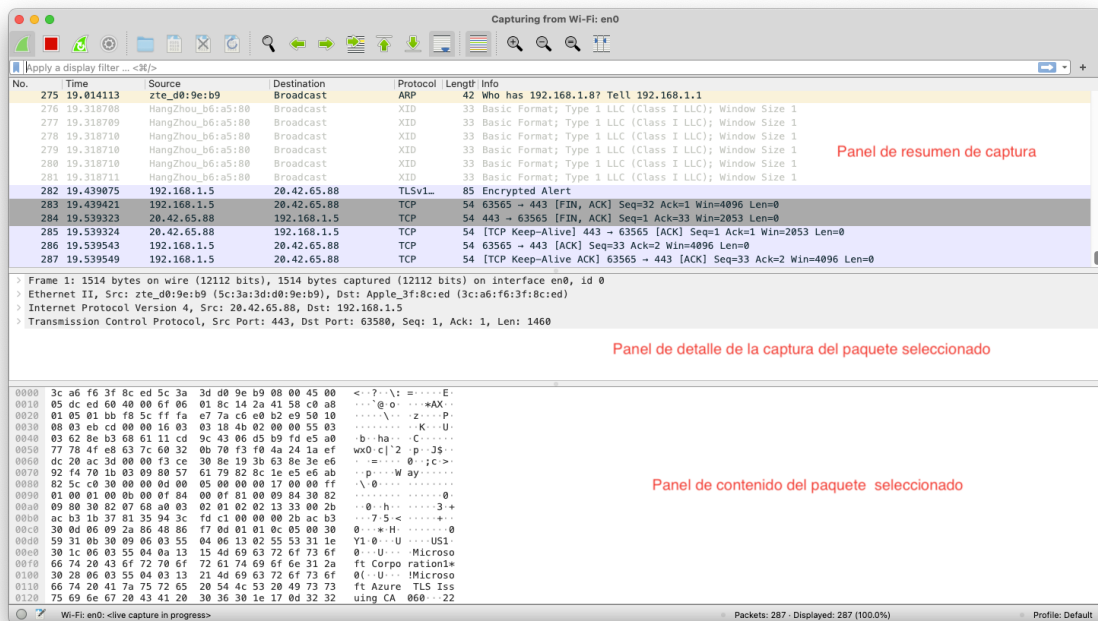
Para obtener más información y para descargar el programa visite: <http://www.Wireshark.org>

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 iniciar la captura de tráfico, se debe seleccionar la interfaz de red por la cual se realizará la captura. Seleccione la interfaz “Ethernet” y a continuación haga clic en el ícono de aleta de tiburón . Wireshark iniciará la captura de todo el tráfico entrante y saliente por la interfaz de red seleccionada y podrá observar algo similar a lo que se muestra a continuación



El panel de resumen de captura se muestra el listado de PDU (o Paquete) 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 detalle de la captura del paquete seleccionado muestra más detalladamente el paquete seleccionado en el panel de resumen de captura.

El panel de contenido del paquete seleccionado, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado y resalta el campo seleccionado en el panel de Detalles. Cada línea en la Lista del paquete corresponde a una PDU o paquete de los datos capturados. 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.

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.

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 a la dirección IP 192.68.185.68. 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 y responda las siguientes preguntas:

¿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? ¿Por qué?

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

Tarea 2: Captura de FTP (File Transfer Protocol) PDU

Paso 1: Inicie la captura de paquetes y abra una consola de línea de comandos (cmd).

Ingresa el comando ftp 192.68.185.68

```
C:\>ftp 192.68.185.68
```

Cuando se establezca la conexión, ingrese la siguiente información:

Username: telematica

Password: sinclave

En este momento ha ingresado al sistema de transferencia de archivos del laboratorio y deberá quedar ubicado en un prompt como el siguiente:

```
ftp>
```

Ingresa el comando

```
ftp> get saludo.txt
```

Con el comando anterior, descargará desde el servidor el archivo `saludo.txt` a su computador. Termine la sesión en el servidor escribiendo el comando:

```
ftp> bye
```

Detenga la captura en Wireshark

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?

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 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.