**Práctica 1 (II): Wireshark – Protocolos de red**

**Descripción**

Mediante esta práctica se observarán los protocolos de red del equipo de trabajo mediante una herramienta de captura de paquetes, Wireshark.

**Objetivos**

Entender los fundamentos de la comunicación por redes.

Aprender el uso del **sniffer de paquetes** Wireshark (una herramienta para observar los mensajes intercambiados entre entidades de protocolos en ejecución).

**Información básica[[1]](#footnote-0)**

La herramienta básica para observar los mensajes intercambiados entre entidades de protocolos en ejecución es llamada un sniffer de paquetes. Como el nombre sugiere, un sniffer captura ("husmea") los mensajes enviados/recibidos desde/por el PC; también almacenará y/o visualizará los contenidos de los diversos campos del protocolo en estos mensajes capturados.

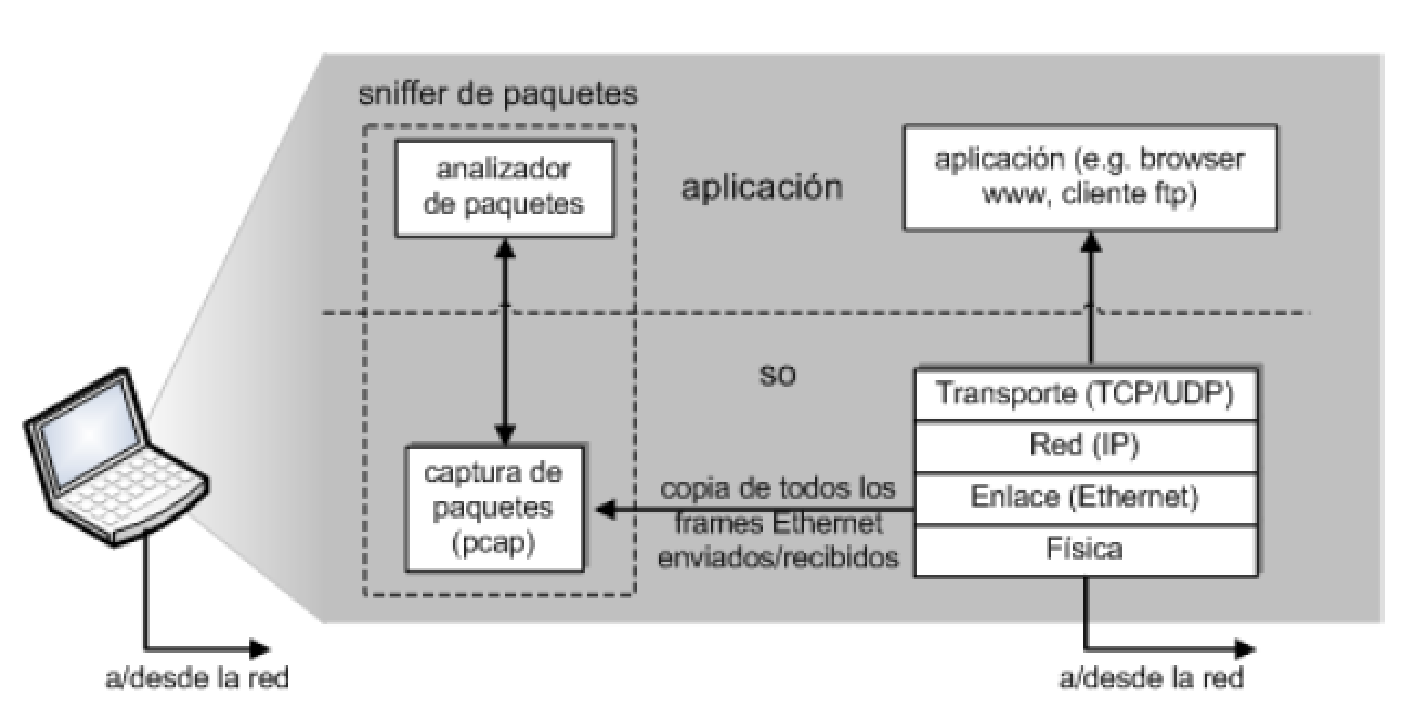
La figura 1 muestra la estructura de un sniffer de paquetes. A la derecha de la Figura 1 están los protocolos (en este caso, los protocolos de Internet) y las aplicaciones (tal como un navegador web ó un cliente ftp) que normalmente se ejecutan en el PC. El sniffer consta de dos partes. La **librería de captura de paquetes** recibe una copia de cada trama de la capa de enlace que es enviada desde ó recibida por la computadora. Recuerde que los mensajes intercambiados por los protocolos de las capas superiores tales como HTTP, FTP, TCP, UDP, DNS, o IP, son encapsulados en tramas de la capa de enlace, los cuales son transmitidos por medios físicos tal como un cable Ethernet. En la Figura 1, el medio físico supuesto es Ethernet, y así todos protocolos de las capas superiores van encapsulados en una trama Ethernet. Capturando todas las tramas de la capa de enlace se obtienen todos los mensajes enviados/recibidos desde/por todos los protocolos y aplicaciones que se ejecutan en el PC. 

Figura 1. Estructura del sniffer de paquetes

El segundo componente de un sniffer de paquetes es el **analizador de paquetes**, que muestra el contenido de todos los campos dentro de un mensaje del protocolo. Para hacerlo, el analizador de paquetes tiene que "comprender" la estructura de todos los mensajes intercambiados por los protocolos. Por ejemplo, supongamos que se está interesado en mostrar los diversos campos en los mensajes intercambiados por el protocolo HTTP en la Figura 1. El analizador de paquetes entiende el formato de la trama Ethernet, y así puede identificar el datagrama IP dentro de la trama. También entiende el formato del datagrama IP, así que puede extraer el segmento TCP dentro del datagrama IP. Finalmente, entiende la estructura del segmento TCP, así puede extraer el mensaje HTTP contenido en el segmento TCP. Finalmente, entiende el protocolo HTTP y así, por ejemplo, sabe que los primeros bytes de un mensaje HTTP contendrán el string "GET", "POST", Ó "HEAD".

Se usará el sniffer de paquetes Wireshark para las prácticas de laboratorio. Este es un producto gratuito y muy versátil, que no sólo permite capturar el tráfico de una red, sino también filtrarlo y analizarlo. Puede descargarse y obtener documentación desde http://www.wireshark.org. (Técnicamente hablando, Wireshark es un analizador de paquetes que usa una librería de captura de paquetes (libpcap ó WinPCap) que se instalará junto con Wireshark).

**Ejecutar Wireshark**

Cuando se inicia Wireshark, se observa la interfaz gráfica de usuario que se muestra en la Figura 2. Esta ventana da acceso rápido a algunos de los ítems, el más interesante la selección del interfaz de red sobre el que se va a realizar la captura de datos.

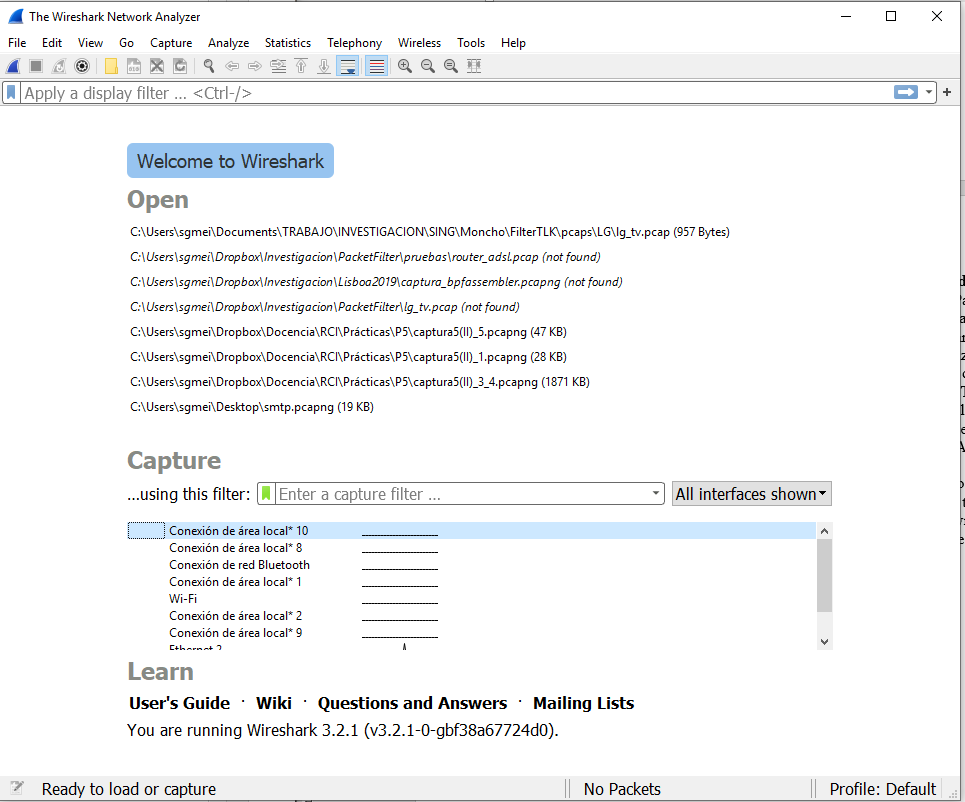


Figura 2. Interfaz gráfica de inicio de Wireshark

Una vez seleccionada la interfaz de captura de datos, se muestra la interfaz gráfica de la Figura 3.

|  |  |
| --- | --- |

Figura 3. Interfaz gráfica del usuario de Wireshark

La interfaz Wireshark tiene los siguientes componentes principales:

* El **menú de comandos**: es un menú estándar desplegable ubicado en la parte superior de la ventana. De interés para nosotros ahora es el menú File y Capture. El menú File permite guardar datos de paquetes capturados o abrir un archivo que contiene datos de paquetes previamente capturados, y salir de la aplicación Wireshark. El menú Capture permite comenzar a capturar paquetes.
* La **ventana lista de paquetes capturados**: muestra un resumen de 1 línea para cada paquete capturado, incluyendo el número de paquete (asignado por Wireshark; esto no es un número de paquete contenido en el encabezado de algún protocolo), el momento en que el paquete fue capturado, las direcciones fuente y de destino del paquete, el tipo de protocolo, e información específica del protocolo contenida en el paquete. El listado del paquete puede ser ordenado conforme a cualquiera de estas categorías con hacer clic sobre un nombre de columna. El campo *protocol type* lista el protocolo de más alto nivel que envió o recibió paquete, es decir, el protocolo que es origen o destino final para este paquete.
* La **ventana detalles del paquete seleccionado**: provee detalles acerca del paquete seleccionado (resaltado) en la ventana lista de paquetes capturados. (Para seleccionar un paquete en la ventana lista de paquetes capturados, coloque el cursor sobre el resumen de 1 línea del paquete en la ventana lista de paquetes capturados y haga clic con el botón izquierdo del mouse). Estos detalles incluyen información acerca de la trama Ethernet (suponiendo que el paquete fue enviado/recibido sobre una interfaz Ethernet) y del datagrama IP que contiene este paquete. La cantidad de detalle Ethernet y de la capa IP mostrada puede ser ampliada o minimizada con hacer clic en las cajitas +/- a la izquierda de la línea de la trama Ethernet o datagrama IP. Si interviene un protocolo de la capa de transporte, TCP o UDP, en el envío del paquete, también se muestran los detalles los mismos (y pueden ser ampliados o minimizados). Finalmente, se proporcionan detalles acerca del protocolo de más alto nivel que envió o recibió este paquete.
* La **ventana detalles del paquete seleccionado**: muestra todo el contenido de la trama capturada, tanto en formato ASCII como en hexadecimal.
* Hacia la parte superior de la interfaz gráfica de usuario de Wireshark, está la **barra de herramientas de filtros**, en la que se puede especificar un nombre de protocolo u otra información a fin de filtrar la información mostrada en la ventana lista de paquetes capturados (y por lo tanto en las ventanas detalles del paquete seleccionado y bytes del paquete seleccionado).

**Tareas**

1. Abre un navegador Web.
2. Abre Wireshark y selecciona la interfaz sobre la que vas a realizar la captura. (Puedes hacerlo directamente desde la sección, Figura 1, o seleccionar en el menú de comando **Capture-Options**).
3. Después de seleccionar la interfaz de red (doble clic desde display inicial o hacer clic en Start si has accedido desde el menú), comenzará la captura de paquetes (ahora todos los paquetes enviados/recibidos desde/por el PC están siendo capturados por Wireshark!)
4. Mientras se ejecuta Wireshark, accede desde tu navegador a la URL:

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

1. Para mostrar esta página, el navegador se conectará al servidor HTTP en gaia.cs.umass.edu e intercambiará mensajes HTTP con él para descargar esta página. Wireshark capturará las tramas que contienen esos mensajes HTTP.
2. Detén la captura. La ventana principal de Wireshark muestra todos los paquetes capturados desde que comenzó captura de paquetes. La ventana principal de Wireshark debe aparecer similar a la Figura 3. Ahora se tienen datos de paquetes vivos que contienen todos los mensajes de protocolos intercambiados entre el PC y otras ¡entidades de red! Los intercambios de mensajes HTTP con el servidor web gaia.cs.umass.edu deben de aparecer en alguna parte en la lista de paquetes capturados. Pero también se mostrarán muchos otros tipos de paquetes.

Aun cuando la única acción realizada fue descargar una página web, evidentemente hubo muchos otros protocolos ejecutados en el PC que no son vistos por el usuario y de los que se aprenderás a medida que avance la asignatura.

1. Vamos a usar un filtro para ver sólo los mensajes HTTP capturados. Teclea “http” en la barra de filtros y selecciona **Apply**.
2. Selecciona el primer paquete http mostrado en la ventana lista de paquetes capturados. Este debería ser el mensaje HTTP GET que fue enviada desde la computadora al servidor HTTP gaia.cs.umass.edu. Cuando se selecciona el mensaje HTTP GET, se mostrará la información de la trama Ethernet, del datagrama IP, del segmento TCP, y del encabezado del mensaje HTTP, en la ventana detalles del paquete seleccionado. Al hacer clic en el +/- a la izquierda de cada uno de los encabezados, se maximizan/minimizan los detalles de cada uno de ellos.
3. Guarda esta captura (prac1.2\_http.pcapng), la usarás en la siguiente práctica de laboratorio.

**Responde a las siguientes cuestiones:**

1. Escribe una lista con los diferentes protocolos que aparecen en la columna *Protocol* en la ventana lista de paquetes capturados no filtrada en el paso 6. Identifica la capa del modelo TCP/IP a la que pertenece cada uno.

Capa de red: ARP

Capa de transporte: STP, UDP, TLS, QUIC

Capa de aplicación: HTTP, SSDP

1. ¿Cuánto tiempo transcurrió desde que el mensaje HTTP GET fue enviado hasta que la respuesta HTTP OK fue recibida? (Por defecto, el valor de la columna Time en la ventana lista de paquetes capturados es la cantidad de tiempo, en segundos, desde el comienzo de la captura, se puede modificar el formato del campo Time en el menú **View-Time Display Format**).

Pasaron 0,120963 segundos.

1. Observa el mensaje HTTP GET ¿Cuál es la dirección IP del Servidor Web al que has accedido? ¿Cuál es la dirección IP de tu PC?

IP Servidor Web: 128.119.245.12

IP PC: 172.19.31.138

1. Accede a la url: https://www.cual-es-mi-ip.net/. Esta página devuelve la dirección IP con la que te conectas a Internet. ¿Cuál es? ¿Se corresponde con la IP de tu PC observada en la captura? Si la respuesta es negativa, intenta explicar por qué.

La IP que obtenemos con wireshark es la IP privada y la de la página web es la pública.

Deduje que es la IP privada porque encontré que estas tienen los siguientes rangos de valores:

· Class A: 10.0.0.0 — 10.255.255.255

· Class B: 172.16.0.0 — 172.31.255.255

· Class C: 192.168.0.0 — 192.168.255.255

La IP de wireshark se ajusta a la clase B y la de la página web a ninguna, por lo que debe ser la pública.

1. Adaptado de: Wireshark Labs v7.0 J.F. Kurose, K.W. Ross. [↑](#footnote-ref-0)