Redes y TCP/IP

Contenido

[Wireshark Lab: Primeros pasos 2](#_Toc19473127)

[Introducción 2](#_Toc19473128)

[Ejecutando Wireshark 3](#_Toc19473129)

[Un test rápido 4](#_Toc19473130)

[Práctica HTTP 6](#_Toc19473131)

## Wireshark Lab: Primeros pasos

## Introducción

La comprensión de los protocolos de red a menudo se puede profundizar en gran medida al "ver protocolos en acción" y al "jugar con los protocolos": observar la secuencia de mensajes intercambiados entre dos entidades de protocolo, profundizar en los detalles de la operación del protocolo y hacer que los protocolos realizar ciertas acciones y luego observar estas acciones y sus consecuencias. Esto se puede hacer en escenarios simulados o en un entorno de red "real" como Internet.

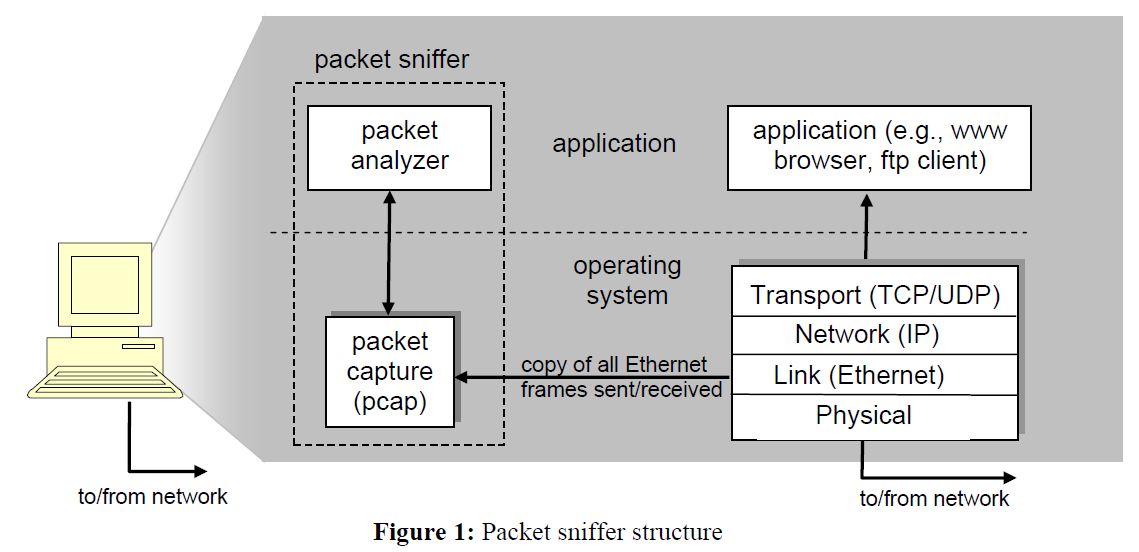
Mediante la herramienta Wireshark ejecutarás varias aplicaciones de red en diferentes escenarios usando tu propia computadora. Observarás los protocolos de red en su computadora "en acción", interactuando e intercambiando mensajes con entidades de protocolo que se ejecutan en otras partes de Internet. Un manual completo de Wirehark lo podemos consultar aquí:

<https://www.wireshark.org/docs/wsug_html_chunked/>

Wireshark funciona en computadoras que utilizan Ethernet, LAN inalámbricas 802.11 y muchas otras tecnologías de capa de enlace.

En este primer laboratorio de Wireshark, te familiarizarás con Wireshark y harás algunas capturas y observaciones de paquetes simples.

La herramienta básica para observar los mensajes intercambiados entre entidades de protocolo en ejecución se denomina **sniffer de paquetes**. Como su nombre lo indica, un rastreador de paquetes captura ("esniga") los mensajes enviados / recibidos desde / por su computadora; normalmente también almacenará y / o mostrará el contenido de los diversos campos de protocolo en estos mensajes capturados. Un sniffer de paquetes en sí es pasivo. Observa los mensajes enviados y recibidos por las aplicaciones y protocolos que se ejecutan en su computadora, pero nunca envía paquetes en sí. Del mismo modo, los paquetes recibidos nunca se dirigen explícitamente al sniffer de paquetes. En cambio, un sniffer de paquetes recibe una *copia*de los paquetes que se envían / ​​reciben desde / por la aplicación y los protocolos que se ejecutan en su máquina.



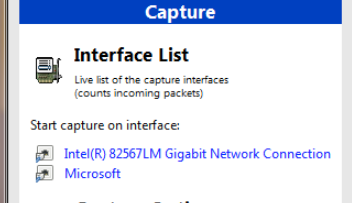
La **biblioteca de captura de paquetes**recibe una copia de cada marco de capa de enlace que envía o recibe su computadora. Recuerde que los mensajes intercambiados por protocolos de capa superior como HTTP, FTP, TCP, UDP, DNS o IP se encapsulan en frames de capa de enlace que se transmiten a través de medios físicos. medios como un cable Ethernet.

En la Figura 1, el medio físico supuesto es un Ethernet, por lo que todos los protocolos de la capa superior finalmente se encapsulan dentro de un frame Ethernet. La captura de todos los frames de la capa de enlace le brinda todos los mensajes enviados / recibidos de / por todos los protocolos y aplicaciones que se ejecutan en su computadora.

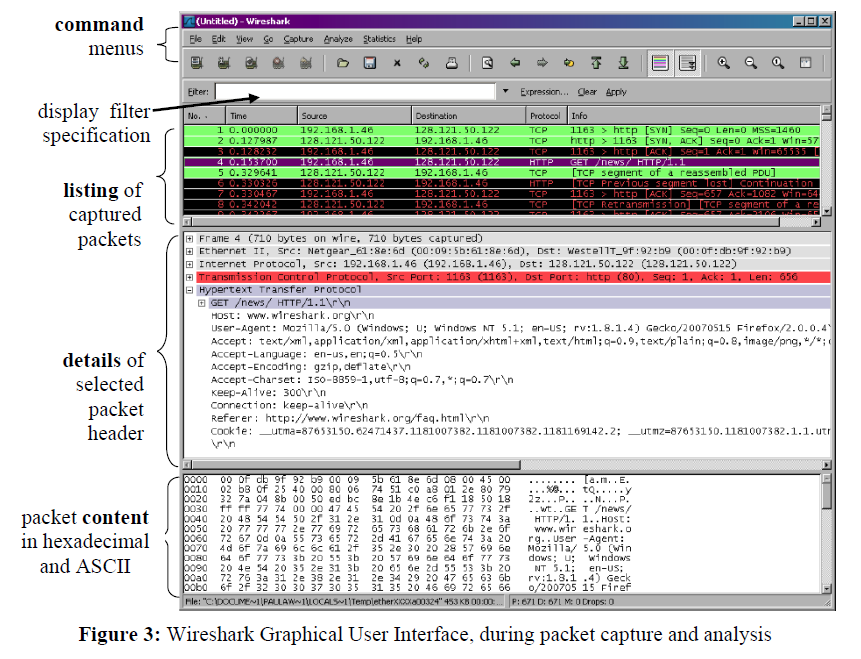
El segundo componente de un sniffer de paquetes es el **analizador de paquetes**, que muestra el contenido de todos los campos dentro de un mensaje de protocolo. Para hacerlo, el analizador de paquetes debe "comprender" la estructura de todos los mensajes intercambiados por los protocolos.

## Ejecutando Wireshark

La primera consideración importante es que dispondremos de una "Lista de interfaces". Esta es la lista de interfaces de red en su computadora. Una vez que elija una interfaz, Wireshark capturará todos los paquetes en esa interfaz. En el ejemplo siguiente, hay una interfaz Ethernet (conexión de red Gigabit) y una interfaz inalámbrica ("Microsoft").



Si hace clic en una de estas interfaces para iniciar la captura de paquetes (es decir, para que Wireshark comience a capturar todos los paquetes que se envían a / desde esa interfaz), se mostrará una pantalla como la siguiente, que muestra información sobre los paquetes que se están capturando. Una vez que comience la captura de paquetes, puede detenerla utilizando el menú desplegable Capturar y seleccionando Detener.



## Un test rápido

Mientras Wireshark se está ejecutando, ingrese la URL:

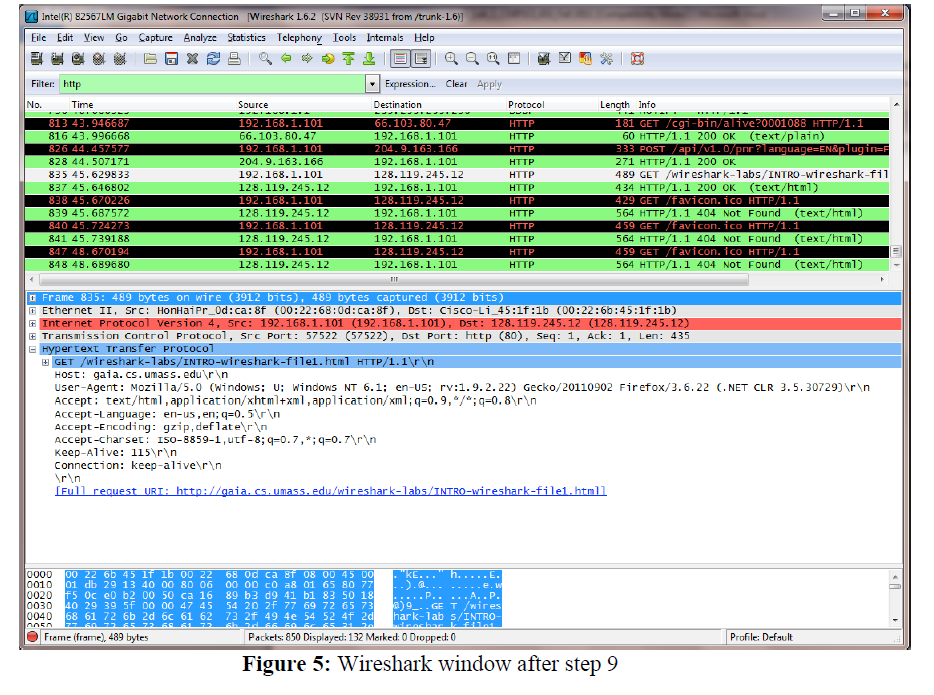
[http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html](https://translate.google.com/translate?hl=es&prev=_t&sl=auto&tl=es&u=http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html)

Después de que su navegador haya mostrado la página INTRO-wireshark-file1.html (es una simple línea de felicitaciones), detenga la captura de paquetes de Wireshark seleccionando detener en la ventana de captura de Wireshark. La ventana principal de Wireshark ahora debería ser similar a la Figura anterior. ¡Ahora tiene datos de paquetes en vivo que contienen todos los mensajes de protocolo intercambiados entre su computadora y otras entidades de red! El intercambio de mensajes HTTP con el servidor web gaia.cs.umass.edu debería aparecer en algún lugar de la lista de paquetes capturados. Pero también se mostrarán muchos otros tipos de paquetes. Aunque la única acción que tomó fue descargar una página web, evidentemente había muchos otros protocolos ejecutándose en su computadora que el usuario no veía.

Escriba "http" (sin las comillas y en minúsculas: todos los nombres de protocolo están en minúsculas en Wireshark) en la ventana de especificación del filtro de visualización en la parte superior de la ventana principal de Wireshark. Luego seleccione Aplicar (a la derecha de donde ingresó “http”). Esto hará que solo se muestre un mensaje HTTP en la ventana de listado de paquetes.

Busque el mensaje HTTP GET que se envió desde su computadora al servidor HTTP gaia.cs.umass.edu. (Busque un mensaje HTTP GET en la parte "listado de paquetes capturados" de la ventana de Wireshark que muestra "GET" seguido de la URL gaia.cs.umass.edu que ingresó. Cuando selecciona HTTP El mensaje GET, la trama Ethernet, el datagrama IP, el segmento TCP y la información del encabezado del mensaje HTTP se mostrarán en la ventana del encabezado del paquete (Recuerde que el mensaje HTTP GET que se envía al servidor web gaia.cs.umass.edu está contenido dentro de un segmento TCP, que está contenido (encapsulado) en un datagrama IP, que está encapsulado en una trama Ethernet).

Su pantalla Wireshark ahora debería verse aproximadamente como se muestra en la siguiente figura:



## Práctica HTTP

1. Inicie su navegador web.

2. Inicie Wireshark, pero aún no comience la captura de paquetes. Ingrese “http” (solo las letras, no las comillas) en la ventana de especificación del filtro de visualización, para que solo los mensajes HTTP capturados se muestren más adelante en la ventana de listado de paquetes. (Aquí solo nos interesa el protocolo HTTP, y no queremos ver el desorden de todos los paquetes capturados).

3. Espere un poco más de un minuto (veremos por qué en breve) y luego comience la captura de paquetes de Wireshark.

4. Ingrese lo siguiente en su navegador:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

Su navegador debe mostrar el muy simple archivo HTML de una línea.

5. Detenga la captura de paquetes de Wireshark.

Si no puede ejecutar Wireshark en una conexión de red en vivo, puede descargar un rastreo de paquetes en:

<http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

Preguntas:

1. ¿Su navegador ejecuta HTTP versión 1.0 o 1.1? ¿Qué versión de HTTP está ejecutando el servidor?

**HTTP/1.1**

2. ¿Qué idiomas (si los hay) indica su navegador que puede aceptar en el servidor?

**es-ES**

3. ¿Cuál es la dirección IP de su computadora? ¿Del servidor gaia.cs.umass.edu?ç

**192.168.1.66**

**128.119.245.12**

4. ¿Cuál es el código de estado devuelto desde el servidor a su navegador?

**304 (not modified)**

5. ¿Cuándo se modificó por última vez el archivo HTML que está recuperando en el servidor?

**Thu, 17 Jul 2025 07:36:05 GMT**

6. ¿Cuántos bytes de contenido se devuelven a su navegador?

**293**

7. Al inspeccionar los datos sin procesar en la ventana de contenido del paquete, ¿ve encabezados dentro de los datos que no se muestran en la ventana de listado de paquetes? Si es así, nombre uno.

**User agent (Mozilla)   
Server host: Apache en CentOS**

Siga ahora los siguiente pasos:

• Inicie su navegador web y asegúrese de que la memoria caché de su navegador esté limpia.

• Inicie Wireshark

• Ingrese la siguiente URL en su navegador

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

Su navegador debe mostrar un archivo HTML de cinco líneas muy simple.

• Ingrese rápidamente la misma URL en su navegador nuevamente (o simplemente seleccione el botón Actualizar en su navegador)

• Detenga la captura de paquetes de Wireshark e ingrese “http” en la ventana de especificación del filtro de visualización, de modo que solo los mensajes HTTP capturados se muestren más adelante en la ventana de listado de paquetes.

Responda las siguientes preguntas:

8. Inspeccione el contenido de la primera solicitud HTTP GET de su navegador al servidor. ¿Ves una línea que indique algo similar a una comprobación de modificación en el HTTP GET?

**NO, ya que es la primera visita (caché limpia)**

9. Inspeccione el contenido de la respuesta del servidor. ¿El servidor devolvió explícitamente el contenido del archivo?

**Si**

10. Ahora inspeccione el contenido de la segunda solicitud HTTP GET de su navegador al servidor. ¿Ves una línea de comprobación de modificación en el HTTP GET? Si es así, ¿qué información sigue al encabezado?

**IF-MODIFIED (FECHA DE PRIMERA VISITA DESDE)**

11. ¿Cuál es el código y la frase de estado HTTP devueltos por el servidor en respuesta a este segundo HTTP GET?

**304 (no modificado)**

¿El servidor devolvió explícitamente el contenido del archivo?

**No**