Práctica #1: Probemos wireshark

¡La mejor forma de aprender sobre cualquier pieza nueva de software es probarla! Asumiremos que su computadora está conectada a Internet a través de una interfaz Ethernet con cable. De hecho, yo recomiendo que haga este primer laboratorio en una computadora que tenga una conexión Ethernet por cable, en lugar de solo una conexión inalámbrica. Haz lo siguiente:

1. Inicie su navegador web favorito, que mostrará su página de inicio seleccionada.
2. Inicie el software Wireshark. Inicialmente verá una ventana similar a esa se muestra en la Figura 2. Wireshark aún no ha comenzado a capturar paquetes.
3. Para comenzar la captura de paquetes, seleccione el menú desplegable Captura y seleccione Interfaces. Esto hará que se muestre la ventana "Wireshark: Capture Interfaces".
4. Verá una lista de las interfaces de su computadora, así como un recuento de los paquetes que se han observado en esa interfaz hasta el momento. Haz click en Inicio para la interfaz en la que desea comenzar la captura de paquetes (para este caso, escoge tu principal conexión de red). Ahora Wireshark comenzará la captura de paquetes: ¡Wireshark ahora está capturando todos los paquetes que se envían / reciben desde / hacia su computadora!
5. Una vez que comience la captura de paquetes, aparecerá una ventana similar a la que se muestra en la Figura 3. Esta ventana muestra los paquetes que se están capturando. Al seleccionar el menú desplegable Capturar y seleccionar Detener, puede detener la captura de paquetes. Pero no detenga la captura de paquetes todavía. Capturemos algunos paquetes interesantes primero. Para hacerlo, necesitaremos generar tráfico de red que sea interesante de mirar. Hazlo usando tu navegador web, que usará el protocolo HTTP que estudiaremos en detalle en clase para descargar contenido de un sitio web.
6. Mientras Wireshark se está ejecutando, entra en: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html y que esa página se muestre en su navegador. Para mostrar esta página, su el navegador se pondrá en contacto con el servidor HTTP en gaia.cs.umass.edu e intercambiará HTTP mensajes con el servidor para descargar esta página. Las tramas Ethernet que contienen estos mensajes HTTP (así como todas las demás tramas que pasen por su adaptador Ethernet) serán capturadas por Wireshark.
7. Después de que su navegador haya mostrado la página INTRO-wireshark-file1.html (es una simple línea de felicitaciones), detén la captura de paquetes de Wireshark seleccionando **parar** en la ventana de captura de Wireshark. La ventana principal de Wireshark debería ahora similar a la Figura 3. Ahora estás viendo datos de paquetes en vivo que contienen todo el protocolo mensajes intercambiados entre su computadora y otras entidades de red! Toma los que parece estar compartiendo mensajes HTTP con el servidor web gaia.cs.umass.edu en algún lugar de la lista de paquetes capturados. Pero habrá muchos otros tipos de los paquetes que se muestran también se verán los diferentes tipos de protocolos que se muestran en la columna de Protocolo. Aunque la única acción que tomó fue descargar una página web, evidentemente había muchos otros protocolos ejecutándose en su computadora que el usuario no puede ver. En cada práctica aprenderemos mucho más sobre estos protocolos a medida que avanzamos en las clases. Por ahora, solo debes tener en cuenta que a menudo sucede mucho más que de lo que ves en tu computadora.
8. Escriba "http" (sin las comillas, y en minúsculas, todos los nombres de protocolos 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 causará que solo se muestre el mensaje HTTP en el listado de paquetes ventana.

9. Escriba "http" (sin las comillas, y en minúsculas, todos los nombres de protocolos 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 causará que solo se muestre el mensaje HTTP en el listado de paquetes ventana.
10. Estamos listos con esta primera práctica