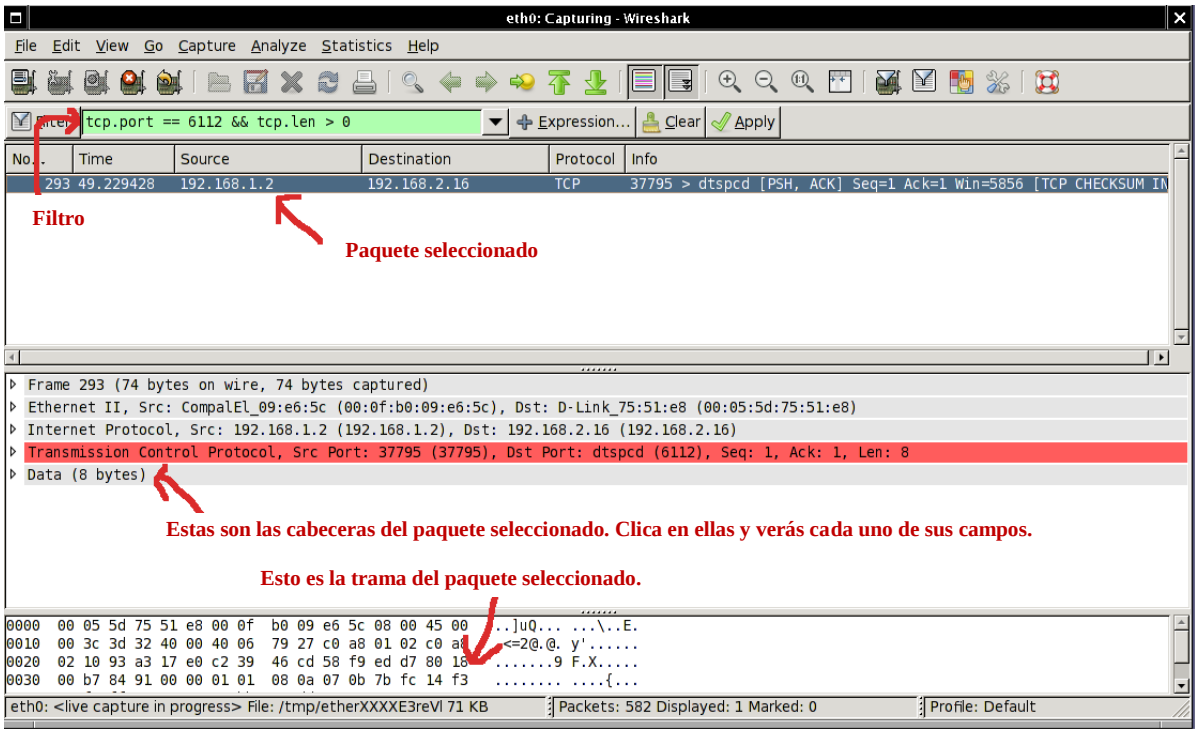
PRÁCTICA 5: Análisis de tráfico FTP y HTTP con WIRESHARK

Introducción

Wireshark es una aplicación de diagnóstico y análisis de tráfico. Captura todo el tráfico que transita por la tarjeta de red y lo vuelca en pantalla o en un archivo. Desde éste se pueden realizar multitud de operaciones como edición, filtrado, estadísticas, etc. Wireshark divide la ventana en tres paneles: en el primero se muestra la lista de paquetes capturados con una breve descripción, en el segundo aparece el paquete seleccionado estructurando sus contenidos en forma de árbol, y en el último la trama de bits asociada.

Wireshark identifica cada una de las cabeceras anidadas dentro de la trama (capa enlace, capa de red, transporte…). De cada una se pueden visualizar sus campos mediante una jerarquía en forma de árbol. Para conocer los valores iremos pulsando en cada nudo desplegando así sus contenidos. Al mismo tiempo en la ventana inferior aparecerá seleccionado el fragmento de la trama que estamos interpretando. Cuando algún campo está constituido por banderas, igualmente podemos desglosar el contenido bit a bit, apareciendo una referencia de su significado al lado.

Una de las herramientas más útiles es el uso de filtros, ubicados bajo el menú "Analizar". Mediante éstos podemos seleccionar una determinada sesión dentro del tráfico, o los paquetes de un determinado tipo. De esta forma podemos restringir la búsqueda de problemas a los paquetes implicados.



REALIZACIÓN

Para la realización de la práctica será necesario que instaléis la aplicación **wireshark** y la ejecutéis al tiempo que otras que irán siendo precisas. Los pasos a realizar son:

1- Activar Wireshark en modo captura.

1. Cercioraos de que el PC accede a Internet. La tarjeta de red debe tener IP, máscara, puerta de enlace y DNS configuradas. Esto puede ser automático (configuración por defecto con DHCP) o manual (recordad la práctica 4). Activad wireshark.
2. Dentro del menú `Captura`, seleccionad la tarjeta de red a monitorizar (cuidado, podéis tener varias, seleccionad la que tiene tráfico) y ejecutad `Iniciar`.

2- Realizar una consulta a la web de la uhu.

Se abre la web **www.uhu.es** en un navegador. Inmediatamente después, se detiene la captura. Una vez hecho esto buscad los paquetes relacionados con vuestra descarga. Para ello tened en cuenta lo siguiente:

-Reducid al máximo el tiempo de captura: Preparad el wireshark y el navegador, luego pulsad iniciar en uno, recargar página web en el otro y detener en el primero en tan sólo unos segundos. Así os será fácil encontrar los paquetes http.

-Poned en el filtro "**http"** y buscad al principio de la lista uno que indique "GET…"

-Sobre el paquete que indica "GET…", clicad con el botón derecho del ratón, `Analizar` → `Seguir` → `flujo TCP`. Cerrad la ventana emergente (la de renglones rojizos y azulados). Con esta opción se activa un filtro que oculta todo excepto los paquetes referentes a la conexión TCP a la que pertenece el elegido.

3- Rellenad el cuestionario (parte obligatoria 6 puntos)

Sobre **ese paquete que contiene el GET** responded a las siguientes preguntas:

1. ¿IP del sitio web (*destination address* en cabecera IP)?_____
2. ¿Puerto que utiliza el servidor web (*destination port* en TCP)?_____
3. Y en tu PC, ¿qué socket* es el que se utiliza? IP_____Puerto_____
4. ¿Cuál es la MAC origen y destino (ver cabecera Ethernet)?
   MACorig_____ MACdest_____
5. ¿A qué equipos corresponden? (indicad si esas MAC corresponden al servidor al que estáis conectados, al switch de vuestra casa…)
   Origen_____
   Destino_____
6. ¿Qué número identifica el protocolo usado en capa de transporte (en este caso TCP) dentro de la cabecera IP (esto es el SAP entre transporte y red)?_____
7. ¿Un servidor puede saber qué navegador estás usando (Ver cabecera http)?_____
8. ¿Cuántos paquetes TCP preceden al GET?___¿Tienen el bit SYN de TCP activo?___¿Y el ACK?_____

*socket = combinación **IP:Puerto** que utiliza una aplicación dada para comunicarse con otra a través de la red. Existe un socket local (el de la aplicación en el propio equipo, por ejemplo el navegador) y existe un socket remoto (el de la aplicación en el servidor). Es lo que se visualiza en cada línea con el comando netstat –an. En este caso debéis mirar *source address* en la cabecera IP y *source port* en la cabecera TCP.

4-Realizad descargas ftp (parte optativa).

Para iniciar una sesión ftp abrid una ventana de consola (cmd en Windows, xterminal en Linux). Escribid en la línea de comandos "ftp *IPdelServidorFTP*". A continuación os pedirá un login y password. En ftp existe la cuenta "anonymous" para usuarios externos, que carece de clave o cuya clave es también anonymous. Una vez aceptados el prompt cambia para informaros que habéis establecido la sesión. A partir de aquí tenéis a vuestra disposición una serie de comandos:

put archivo: coloca el archivo en el servidor.
get archivo: descarga el archivo sito en el servidor.
ls: proporciona una lista de los ficheros que hay en el directorio
?: muestra una lista de comandos.
!***comando***: ejecuta el comando como si estuviera en el cliente.
hash: muestra una serie de ! conforme realiza una transferencia.
binary: establece transferencia binaria
asc: establece transferencia ascii(traduce los caracteres de texto de este sistema a acii al transferir)

Además existen clientes FTP en el mercado con una funcionalidad ampliada y más amigable. Por otro lado los navegadores suelen ofrecer una interfaz cómoda usando el formato ftp://nombredelservidorftp.

5.-Responded a las siguientes preguntas (parte optativa, hasta 10):

Activa wireshark en modo captura y sin filtros activos, luego conectaos al servidor **ftp.rediris.es**. Usad "anonymous" en usuario. Listad los archivos disponibles con "ls" y descargad uno denominado "welcome.msg" usando *get*. Luego detened la captura.

1. (7)¿Qué 2 puertos utiliza ftp **en el servidor** (son 2 conexiones TCP)?_____
2. (8)¿Cómo se refleja la petición ("*get*") del archivo (ved capa FTP y buscad el comando que se envía)?_____
3. (9)¿Y la orden "*put*"? (Aunque falle, la petición de subir un archivo se lanza y se puede ver en wireshark)_____
4. (10)¿Qué banderas (flags) utiliza TCP para finalizar la conexión cuando ejecutáis "*quit"*?_____