ETHEREAL es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. En el argo IT se denominan analizadores de protocolos de red, analizadores de paquetes, *packet sniffer* o *sniffer*. Ethereal permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Ethereal.

A partir del año 2006 Ethereal es conocido como **WireShark**[1] y hoy en día está categorizado como uno de los TOP 10 como *sniffer* junto a Nessus y Snort ocupando el segundo lugar entre estos.

Algunas de las características de WireShark son las siguientes:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Es importante tener presente que WireShark no es un IDS (*Instrusion Detection System*) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red. Si embargo, permite a los profesionales de IT analizar y solventar comportamientos anómalos en el tráfico de la red.

[1] A partir de esta nota nos referiremos a Ethereal como WireShark.

Instalación de WireShark

El instalador y los archivos binarios de Ethereal pueden ser descargados en http://www.ethereal.com/download.html y sus últimas versiones como se menciono anteriormente en http://www.wireshark.org/download.html. Adicional a esto en http://wiki.ethereal.com y http://wiki.wireshark.org podrás obtener una amplia cantidad de información relacionada con la aplicación, listas de correo tanto para usuarios finales como desarrolladores.

WireShark soporta múltiples plataforma entre ellas UNIX, LINUX y Windows, a continuación se describe la instalación para cada uno de estos sistemas operativos.

Instalación UNIX

Para iniciar la instalación debemos contar con las siguientes utilidades instaladas:

- GTK+, GIMP Tool Kit y Glib (puede obtener en el siguiente site: www.gtk.org)
- libpcap (puede obtener en el siguiente site: www.tcpdump.org)

Si es el caso de obtener los archivos fuentes los siguientes pasos describen el proceso para descomprimir los archivos y generar el ejecutable:

1. Según la distribución de UNIX, se aplica el comando correspondiente para descomprimir el archivo obtenido.

   - En versiones de UNIX con GNU tar

     ```
     tar zxvf wireshark-1.0.0-tar.gz
     ```

   - En caso contrario se deberá ejecutar los siguientes comandos

     ```
     gzip –d wireshark-1.0.0-tar.gz
     tar xvf wireshark-1.0.0-tar
     ```

2. Cambiar al directorio raíz de WireShark.

   ```
   cd <ruta_directorio_wireshark>
   ```

3. Configuración de los archivos fuentes con el objetivo de asegurar su buen funcionamiento en la versión de UNIX correspondiente.

```
./configure
```

4. Para generar el archivo ejecutable se debe aplicar el siguiente comando.

```
make
```

5. Finalmente para culminar la instalación de la aplicación se ejecuta el comando:

```
make install
```

Otros métodos son aplicados para la instalación según las distribuciones de UNIX todos estos disponibles en el siguiente link http://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallUnixInstallBins.html, particularmente para el caso de DEBIAN se aplica el siguiente comando para hacer uso de la interfaz gráfica para APT:

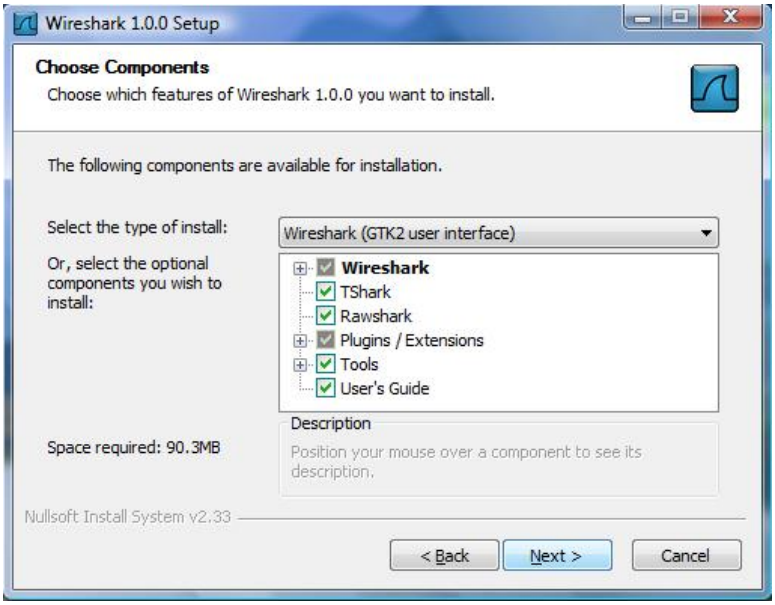
```
aptitude install wireshark
```

Instalación Windows

1. Una vez que se obtiene el instalador desde http://www.wireshark.org/download.html se ejecuta el archivo wireshark-setup-1.0.0.exe (en este caso la versión es 1.0.0) para iniciar la instalación. Es importante mencionar que las librerías necesarias como WinPcap están incluidas en el instalador.

   Se muestra la siguiente pantalla del asistente:

2. Presionando el botón Next > se despliega la especificación de la licencia y al presionar el botón I Agree se despliega la siguiente ventana para seleccionar los componentes que se desean instalar.



Para esta instalación se seleccionarán los siguientes:

- Wireshark, GUI del analizador de protocolos.
- TShark, línea de comando del analizador de protocolos. Plugins/Extensions, especificar plugins y extensiones para TShark y Wireshark en este punto deberá seleccionar todos los ítems listados.
- Tool, ofrece herramientas adicionales aplicar a los archivos que contienen los paquetes para su análisis seleccionar todas las ofrecidas durante la instalación.

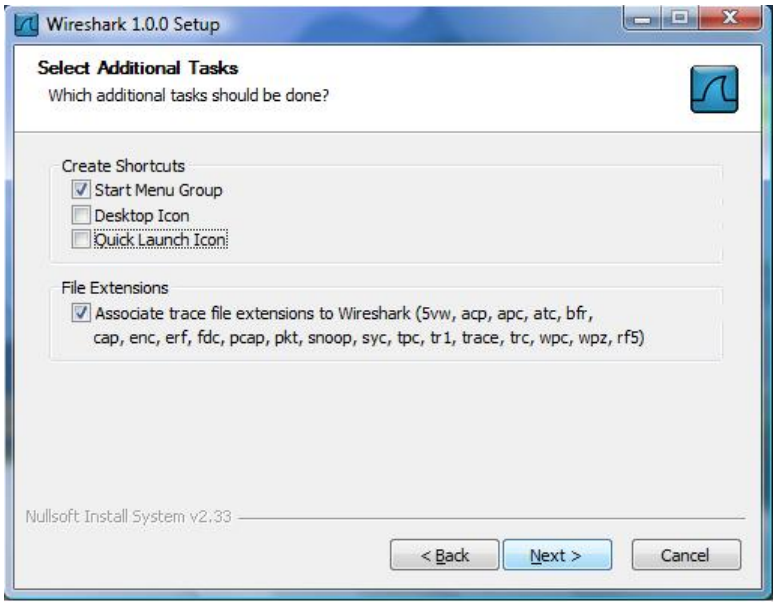
Editcap, para manipular los archivos.

Text2Pcap, convierte un archivo ASCII en formato libpcap.

Mergecap, permite obtener un archivo desde la combinación de 2 o más archivos de paquetes capturados.

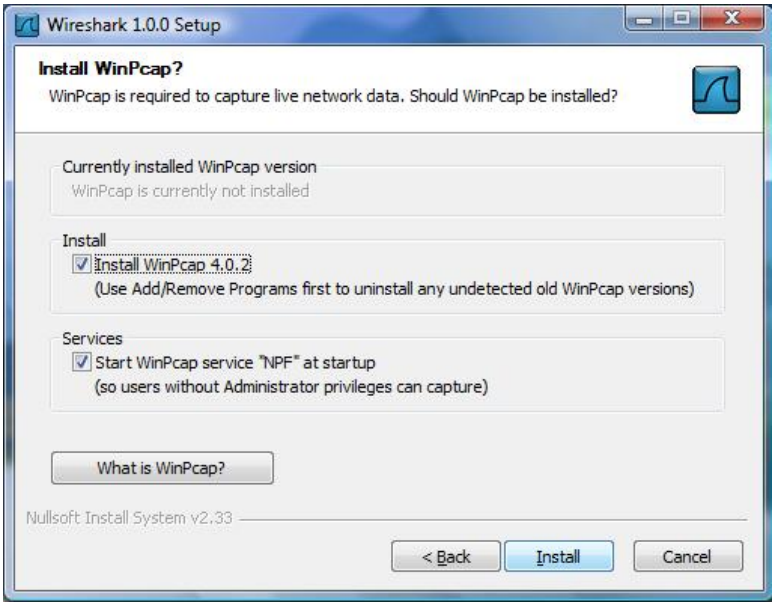
Capinfos, es un programa que proporciona información de los paquetes capturados.

3. La siguiente pantalla permite seleccionar si se desea crear un acceso directo a la aplicación en el escritorio, crear un menú de inicio y visualizar el icono en la barra de tareas. Adicionalmente se tiene la posibilidad de permitir, que los archivos generados por otros analizadores de tráfico puedan ser visualizados con Wireshark (opción que debemos seleccionar).

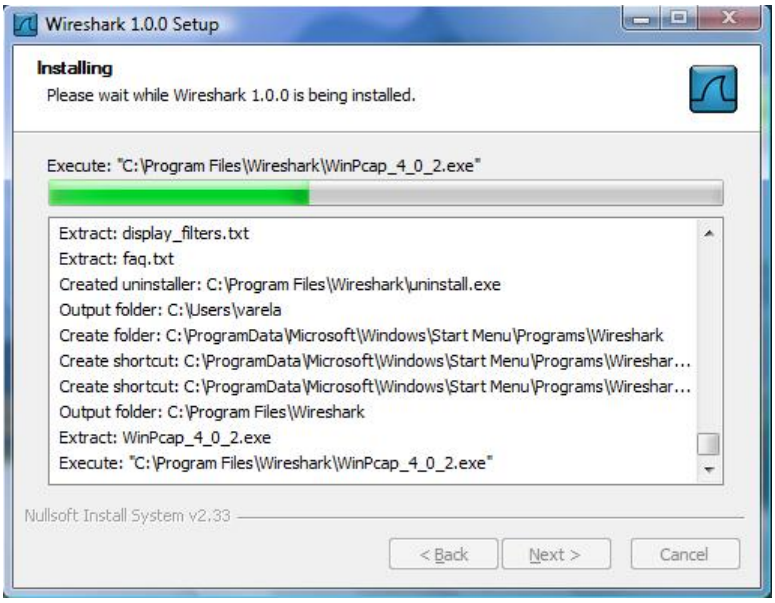


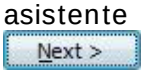
4. A continuación se deberá seleccionar el directorio donde se instalará la aplicación, en este punto se acepta el indicado por defecto en el instalador.

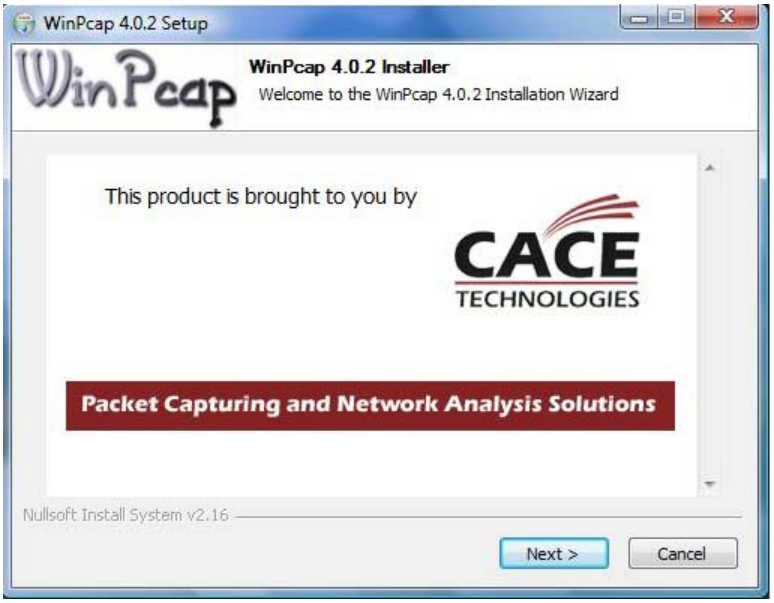
   El instalador de WireShark contiene una versión de WinPcap se verifica si se debe actualizar versión en el PC donde se está realizado la instalación y ofrece la opción de agregar un servicio para que usuarios que no tiene privilegios de administrador pueda capturar paquetes. En este punto se seleccionan ambos ítems.

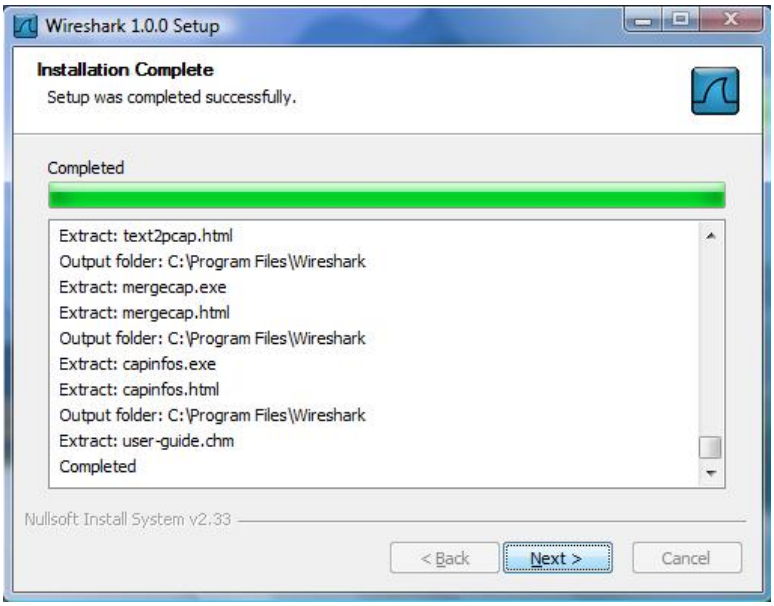


Se presiona el botón  para iniciar el proceso de instalación.



5. Como se mencionó anteriormente el instalador de WireShark para Windows permite hacer la instalación de las librerías, plugins, servicios, etc. Particularmente para el caso de WinPcap se interrumpe la instalación en el punto que muestra la pantalla arriba e inicia el asistente para la instalación de WinPcap. Se debe seleccionar  hasta finalizar la instalación.





La siguiente pantalla indica que la instalación ha finalizado exitosamente.

Para la actualización de WireShark se debe realizar el proceso descrito anteriormente. Se descarga la nueva versión y se ejecuta el instalador, una buena manera de estar actualizados en el mundo de Wireshark es a través de las lista de correo ofrecidas.

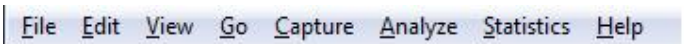
Interfaz de Usuario

A continuación se muestra y detalla la interfaz de usuario y como se aplican las principales funciones de WireShark (Capturar, Desplegar y Filtrar paquetes).

Existen dos maneras de iniciar la aplicación una es desde la línea de comando (*shell*) y otra desde el entorno gráfico. Cuando se inicia desde la línea de comando se tiene la posibilidad de especificar opciones adicionales que depende de las funciones que se quieran aprovechar.

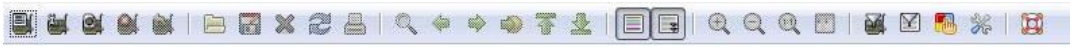
La interfaz principal de WireShark cuenta con varias secciones:

- El Menú principal es utilizado para iniciar las acciones y/o funciones de la aplicación.



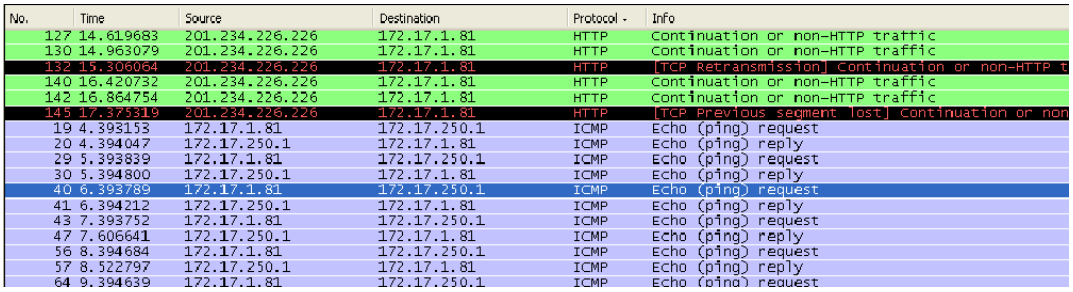
File, similar a otras aplicaciones GUI este contiene los ítems para manipular archivos y para cerrar la aplicación Wireshark.
Edit, este menú contiene ítems aplicar funciones a los paquetes, por ejemplo, buscar un paquetes especifico, aplicar una marca al paquete y configurar la interfaz de usuario.
View, permite configurar el despliegue de la data capturada.
Go, contiene ítems que permiten el desplazamiento entre los paquetes.
Capture, para iniciar y detener la captura de paquetes.
Analyze, contiene ítems que permite manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.
Statistics, contiene ítems que permiten definir u obtener las estadísticas de la data capturada.
Help, menú de ayuda.

- Barra de herramientas principal, permite el acceso rápido a las funciones más utilizadas.

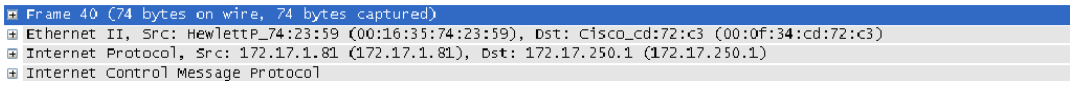


- Barra de herramientas para filtros, aquí se especifica el filtro que se desea aplicar a los paquetes que están siendo capturados.

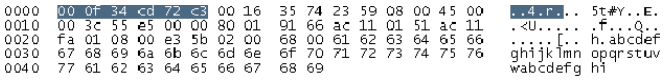
- Panel de paquetes capturados, en este panel se despliega la lista de paquetes capturados. Al hacer clic sobre algunos de estos se despliega cierta información en los otros paneles.



- Panel para detalles del paquete, aquí se despliega información detallada del paquete seleccionado en el panel de paquetes.



- Panel de paquetes capturados en bytes, despliega en bytes la información contenida en el campo seleccionado desde el panel de detalles del paquete seleccionado en el panel de paquetes.



- La barra de estado, muestra información acerca del estado actual del programa y de la data capturada.

La interfaz de usuario puede ser cambiada desde el menú principal en la opción de *Preferences* en el menú *Edit*, según sea las necesidades.

Panel de paquetes capturados

Cada línea corresponde a un paquete capturado al seleccionar una de estas, ciertos detalles son desplegados en el resto de los paneles (Detalles y bytes). Y las columnas muestran datos del paquete capturado, Wireshark dispone de una gran cantidad de detalles que pueden agregarse en estas columnas desde el menú *Edit->Preferences*, por defecto se tienen:

- No.: posición del paquete en la captura.
- *Time*: muestra el *Timestamp* del paquete. Su formato puede se modificado desde el menú *View->Time Display Format*.
- *Source*: dirección origen del paquete.
- *Destination*: dirección destino del paquete.
- *Protocol*: nombre del protocolo del paquete.
- Info: información adicional del contenido del paquete.

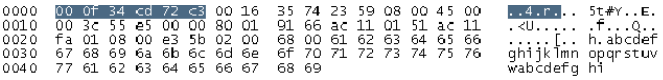
Panel para detalles de paquetes capturados

Contiene el protocolo y los campos correspondientes del paquete previamente seleccionado en el panel de paquetes capturados.

Seleccionando una de estas líneas con el botón secundario del Mouse se tiene opciones para ser aplicadas según las necesidades.

Panel de paquetes capturados en Bytes

En este panel se despliega el contenido del paquete en formato hexadecimal.



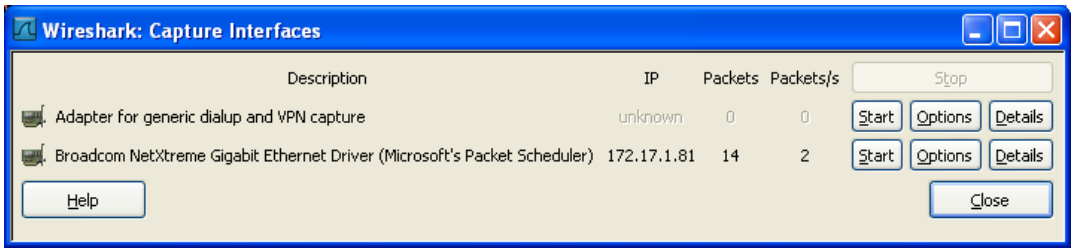
De izquierda a derecha se muestra el *offset* del paquete seguidamente se muestra la data del paquete y finalmente se muestra la información en caracteres ASCII si aplica o "." (Sin comillas) en caso contrario.

Captura de Paquetes

Una de las principales funciones de WireShark es capturar paquetes con la finalidad de que los administradores y/o ingenieros de redes puedan hacer uso de estos realizar el análisis necesario para tener una red segura y estable. Como requisito para el proceso de capturar datos es ser administrador y/o contar con estos privilegios y es necesario identificar exactamente la interfaz que se quiere analizar.

WireShark cuenta con cuatro maneras para iniciar la captura de los paquetes:

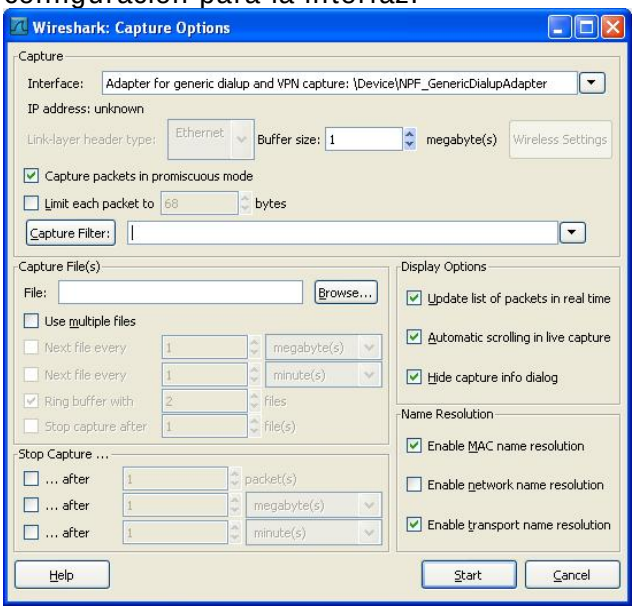
1. Haciendo doble clic en  se despliega una ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes.



Tres botones se visualizan por cada interfaz

- Start, para iniciar
- Options, para configurar
- Details, proporciona información adicional de la interfaz como su descripción, estadísticas, etc.

2. Otra opción es seleccionar con el Mouse el icono  en la barra de herramientas, se despliega la siguiente ventana donde se muestra opciones de configuración para la interfaz.



3. Si es el caso donde se ha predefinido las opciones de la interfaz, haciendo clic en  se inicia la captura de paquetes inmediatamente.

4. Otra manera de iniciar la captura de paquetes es desde la línea de comandos ejecutando lo siguiente:

```
wireshark –i eth0 -k
```

   Donde eth0 corresponde a la interfaz por la cual se desea iniciar la captura de paquetes.

Detener / Reiniciar la captura de paquetes

Para detener la captura de paquetes podemos aplicar una de las siguientes opciones:

- Haciendo uso del icono  desde el menú *Capture* o desde la barra de herramientas.
- Haciendo uso de ctrl+E.
- La captura de paquetes puede ser detenida automáticamente, si una de las condiciones de parada definidas en las opciones de la interfaz se cumple, por ejemplo: si se excede cierta cantidad de paquetes.

Para reiniciar el proceso de captura de paquetes se debe seleccionar el icono  en la barra de herramientas o en desde el menú *Capture*.

Filtrado de paquetes

Wireshark hace uso de libpcap para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (*and*/*or*) con la opción de ser negada por el operador *not*.

```
[not] Expresión [ and|or [not] expresión…]
```

La siguiente expresión define un filtro para la captura de paquetes desde/hacia los host con dirección IP x.y.z.w y a.b.c.d

```
ip.addr==172.17.250.1 and ip.addr==172.17.1.81
```

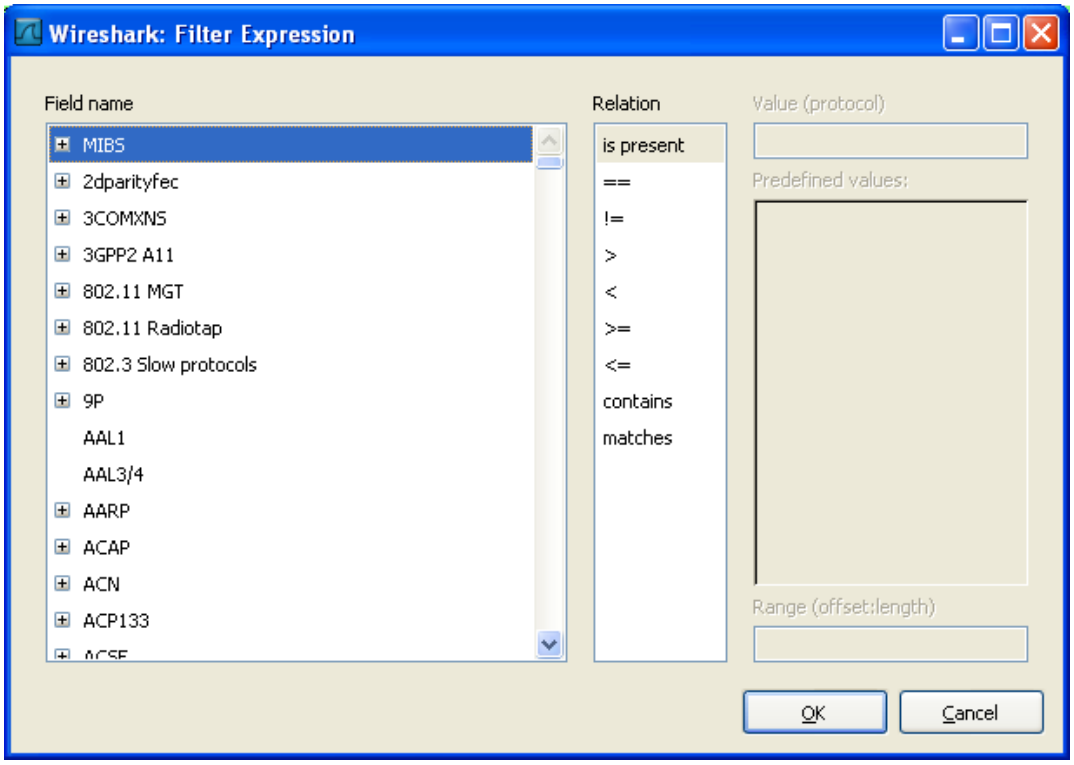
En el site http://wiki.wireshark.org/CaptureFilters podrá obtener una serie de filtros que son usualmente aplicados por los administradores de red.

Expresiones de filtrado

WireShark proporciona una poderosa herramienta para construir filtros más complejos. Permite comprar valores así como también combinar expresiones dentro de otra expresión.

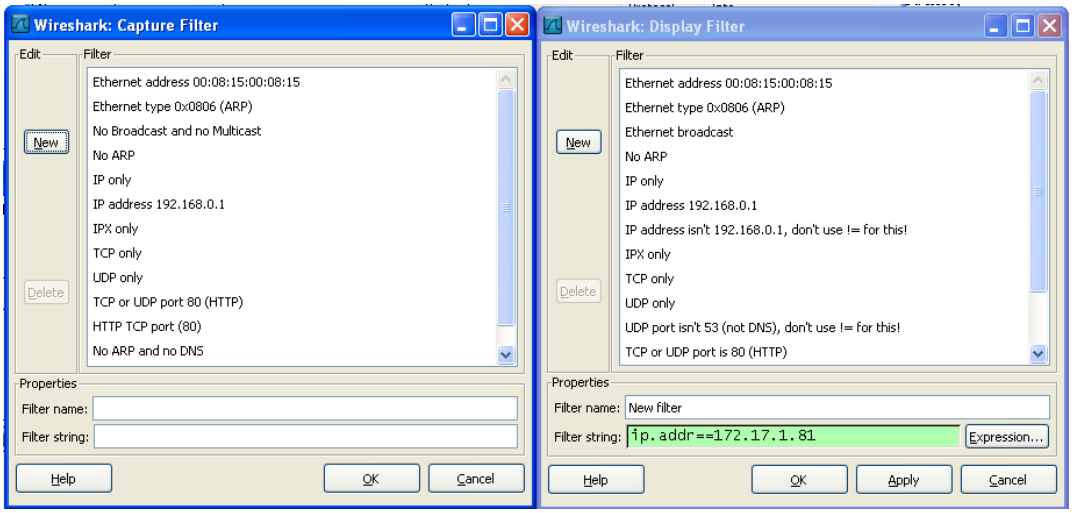
En el site http://wiki.wireshark.org/DisplayFilters podrá obtener una serie de expresiones que son usualmente aplicados por los administradores de red.

Cuando es bien conocido el campo por el cual se requiere hacer el filtrado es recomendable hacer uso de *Filter Expresion* desde la barra de herramientas para filtros presionando *Expresion…* facilitando la construcción de la expresión o fórmula seleccionando el campo (*field name*), el operador (Relation) y el valor contra el cual se quiere comparar.

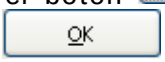


Es muy común que ciertos filtros y/o expresiones requieran ser utilizado en un futuro, para esto Wireshark permite definir los filtros y/o expresiones y guardarlas.

Para guardar o abrir un filtro existente (previamente creado y guardado) se debe seleccionar *Display Filter* en el menú *Analize* o *Capture Filter* que se encuentra en el menú *Capture.*



Para definir un filtro se debe presionar el botón 

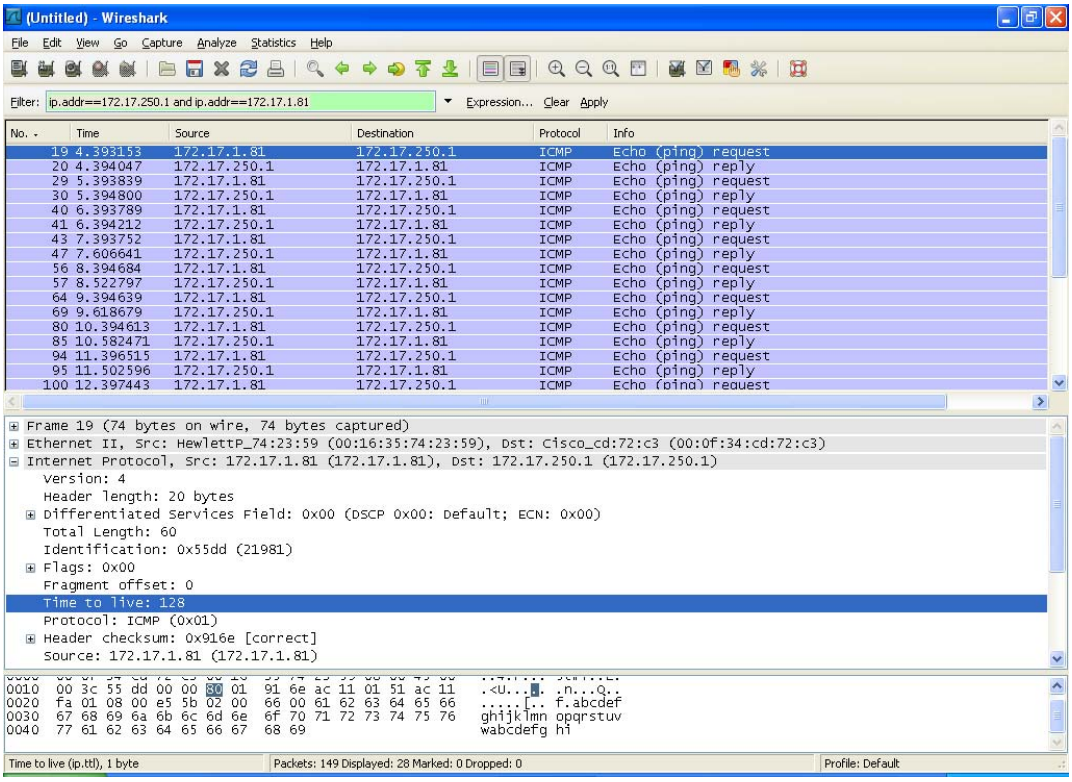
se indica el nombre del filtro y la expresión y presionar 

para salvar los cambios.

Manipulando las paquetes capturados (análisis)

Una vez que se tienen capturados los paquetes estos son listados en el panel de paquetes capturados, al seleccionar uno de estos se despliega el contenido del paquete en el resto de los paneles que son panel de detalles de paquetes y panel en bytes.

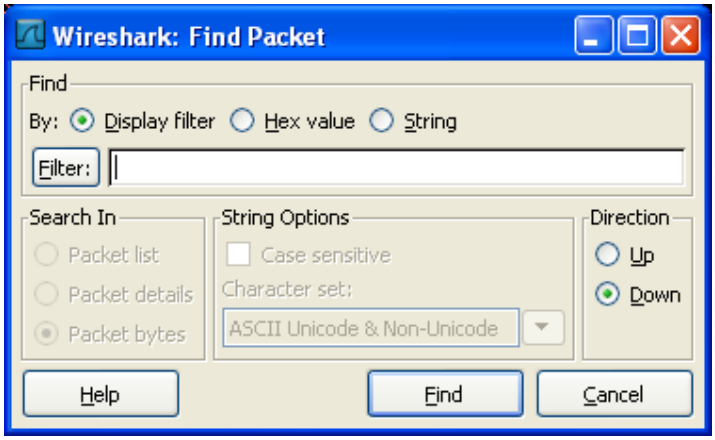
Expandiendo cualquiera parte del árbol presentado en el panel de detalle del paquete, se puede seleccionar un campo en particular cuyo contenido se muestra resaltado en negritas en el panel de bytes. En la siguiente imagen se identifica en campo TTL del la cabecera del IP.



Existe una manera de visualizar los paquetes mientras esta activo el proceso de captura esto se logra, seleccionando la opción *Update list packets in real time* desde menú *Edit->Preferentes->Capture*. Adicionalmente, Wireshark permite visualizar el contenido de un paquete seleccionado en el panel de paquetes capturados en una ventana individualmente seleccionando la opción Show Packet in new Windows en menú principal *View*. Esto permite comparar con más facilidad dos o más paquetes.

Función de búsqueda de paquetes

Cuando iniciamos la captura de paquetes por lo general se obtiene una gran cantidad de paquetes que cumple con los filtros y/o expresiones definidas, Wireshark permite realizar búsqueda(s) de paquete(s) que tienen cierta característica. Para esto se debe seleccionar la opción *Find Packet* en el menú *Edit* se despliega la siguiente ventana.



Se rellena el campo *Filter* con el criterio de búsqueda que se desea y el resto de los campos seguidamente se presiona el botón de búsqueda.

Otra opción es realizar la búsqueda del paquete anterior y próximo al que esta seleccionado en el panel de paquetes esto se aplica desde el menú de *Edit* las opciones *Find Next* y *Find Previous*.

Marcado de paquetes

Por lo general el análisis de tráfico es bastante complejo ya que son muchos los paquetes que se obtienen el la captura, WireShark permite marcar los paquetes para que sean identificados con más facilidad esta marca es aplicar colores a los paquetes en el panel correspondiente.

Existen tres funciones para aplicar el marcado de paquetes:

1. Mark packets (toggle) para marcar el paquete.
2. Mark all packets, aplica la marca a todos los paquetes.
3. Unmark all packets, elimina la marca para todos los paquetes.

Visualizando estadísticas

WireShark proporciona un rango amplio de estadísticas de red que son accedidas desde el menú *Statistics* que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo. Podemos distinguir entre cada una de las anteriores:

Estadísticas Generales

- Summary, la cantidad de paquetes capturados.
- Protocol Hierarchy, presenta las estadísticas para cada protocolo de forma jerárquica.
- Conversations, un caso particular es el tráfico entre una IP origen y una IP destino.
- Endpoints, muestra las estadísticas de los paquetes hacia y desde una dirección IP.
- IO Graphs, muestra las estadísticas en grafos.

Estadísticas específicas de los protocolos

- Service Response Time entre la solicitud (*request*) y la entrega *(response*) de algún protocolo existente.
- Entre otras.

Es importante tener presente que los números arrojados por estas estadísticas solo tendrán sentido si se tiene un conocimiento previo el protocolo de lo contrario serán un poco compleja de comprender.

Glosario

www.wireshark.com