**Instituto Tecnológico de Culiacán**



## “AR – Tarea 6”

Instituto tecnológico de Culiacán

Materia: Administración de redes

Maestro: Lic. Carlos Sandoval Castellanos

Alumno: Güémez Sánchez Diego Arturo

Bertha Quetzaly Marquez Caro

Fecha: 08 de Diciembre del 2017.

**Introducción**

El objetivo de este trabajo de investigación es el de instalar y operar un analizador de protocolos, por medio de pantallas documentar la instalación y operación, determinaremos funcionalidades, analizaremos paquetes e información que circule por la red por medio de la captura de tramas e identificación de protocolos.

Se tiene el objetivo de abrir diferentes sitios web y habilitar servicios web tales como messenger, whatsup, google, correo, youtube, bases de datos, etc

En caso de que el software nos lo permita, se documentaran dashboard o gráficos de desempeño.

Para el desarrollo del trabajo de investigación elegimos Wireshark como el analizador de protocolos a documentar. Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca. [1]

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark. [1]

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. [1]

**Antecedentes**

A finales de 1997, Gerald combs necesitaba una herramienta para la localización de problemas de red y quería conocer más información sobre la creación de redes por lo que empezó a Escribir Ethereal como una forma de resolver ambos problemas.

Ethereal fue lanzado inicialmente, después de varias pausas en el desarrollo, en julio 1998 como la version 0.2.0, luego en octubre de 1998, Guy Harris de networ Appliance estaba buscando algo mejor que tcpview por lo que comenzó la aplicación de parches y ayudo a la codificación de Ethereal.

En 2006 el proyecto se mudo de casa y volvió a surgir con otro nombre: Wireshark. Ya para el 2008 después de 10 años de desarrollo Wireshark llego a su versión 1.0 este fue el primer lanzamiento que se considero completo, con las características mínimas implementadas. Su lanzamiento coincidió con la primera Wireshark Developer Conference usuario llamado Sharkfest. [2]

****

**Imagen 1: Logo de WireShark.**

**¿Qué es WireShark?**

Se trata de un potente sniffer de red de software libre heredero de Ethereal que nos permite capturar y monitorizar todos los paquetes de red que pasan por nuestro equipo con el solo hecho de poner nuestra tarjeta de red a escuchar en modo promiscuo, es decir, diciéndole a nuestra tarjeta que capture todo el tráfico que pase por ella.

A diferencia de TCPDump nos ofrece una amigable interfaz gráfica con muchas opciones para filtrar y buscar la información. [3]

**¿Para qué nos sirve?**

Tener la información detallada que nos facilita este programa nos permite poder analizar el tráfico que pasa por nuestra red y así poder solucionar o incluso prevenir los posibles problemas que puedan surgir.

También se puede emplear para el aprendizaje de los diferentes protocolos de red, ya que nos permite observar de forma detalla las cabeceras de los protocolos que hemos estudiado teóricamente y con ello ayudarnos a comprender la utilidad y la función de cada uno de sus campos.

Otra posibilidad, es utilizarlo de modo delictivo con la intención de robar información de terceros, por ejemplo, para intentar conectarse a una red Wi-Fi protegida con WEP. [3]

**Proceso de instalación**

En Windows y OS X podemos utilizar la siguiente liga para ir directo a la página de WireShark y efectuar la descarga: <http://www.wireshark.org/download.html>

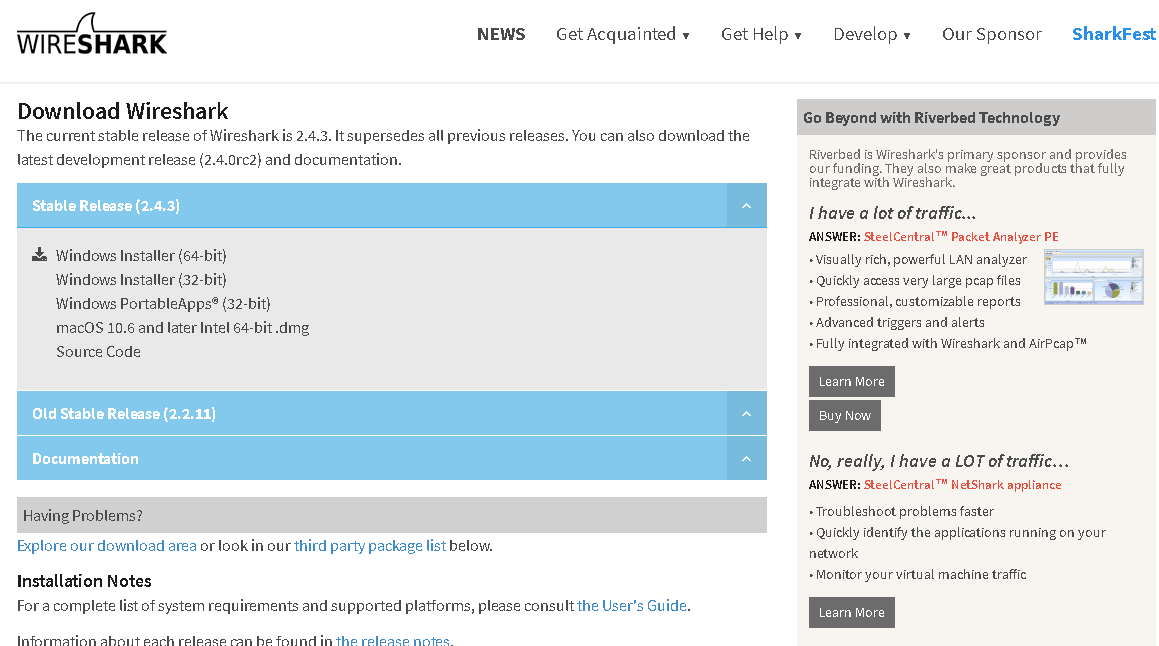


Imagen 2: Pagina principal de WireShark.

Una vez obtenido el instalador, se ejecuta el archivo wireshark-setup-1.0.0.exe para iniciar la instalación.

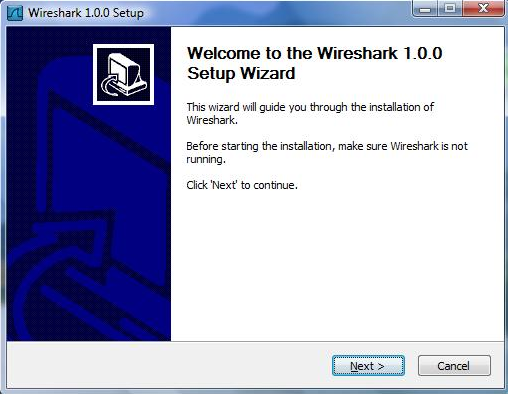


Imagen 3: Pantalla del asistente.

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

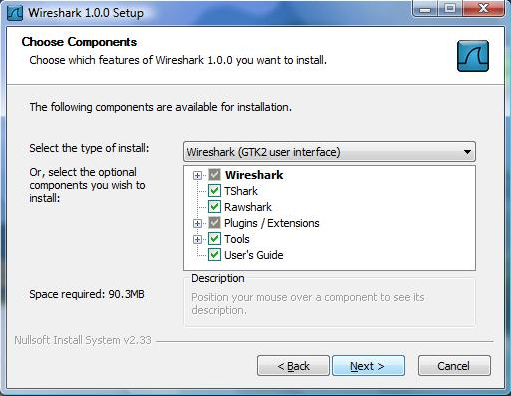


Imagen 4: Ventana de selección de componentes.

Seleccionaremos los siguientes componentes de la ventana: Wireshark, TShark, Tool, Editcap, Mergecap y capinfos.

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, seleccionaremos esa opción.

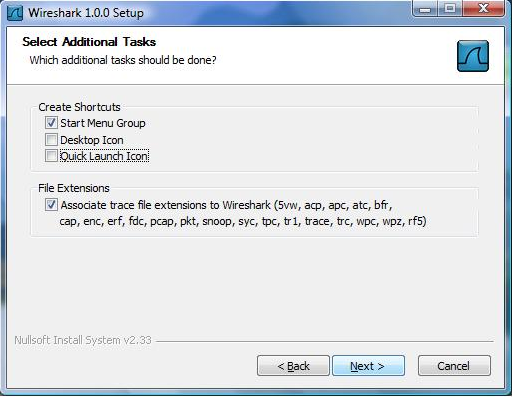


Imagen 5: Pantalla de selección de tareas adicionales.

seleccionaremos 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.

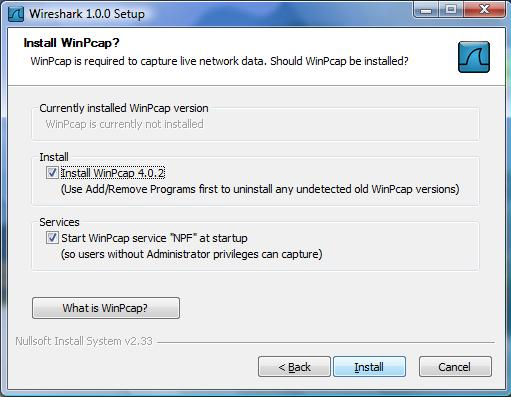


Imagen 6: Pantalla de instalación de WireShark.

Se presiona el botón  para iniciar el proceso de instalación.

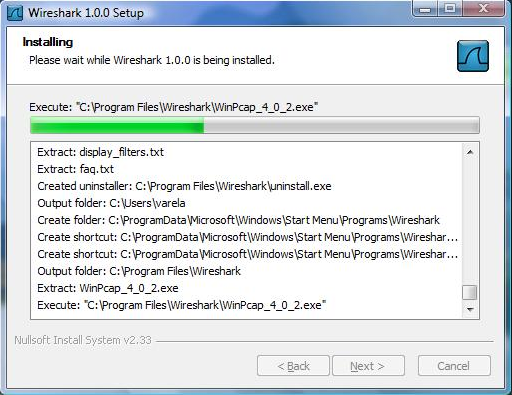


Imagen 7: Ventana de instalación.

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 e inicia el asistente para la instalación de WinPcap.

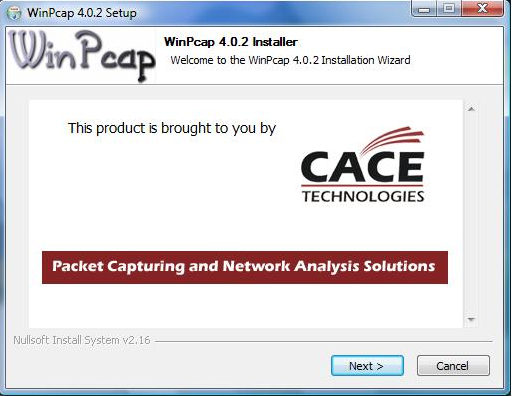


Imagen 8: Asistente para la instalación de WinPcap.

Se debe seleccionar  hasta finalizar la instalación.

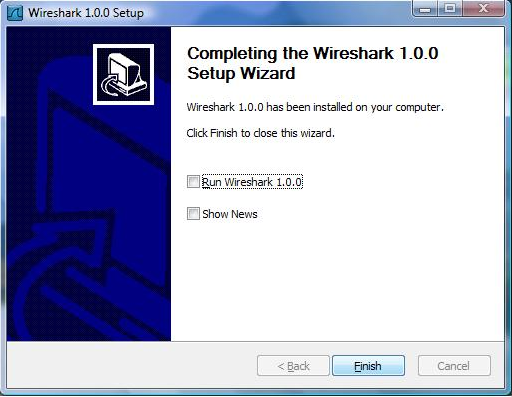


Imagen 9: Descarga finalizada con éxito.

**Operación y Funcionalidades**

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:



Imagen 10: Menú principal de acciones.



Imagen 11: Barra de herramientas principal.



Imagen 12: Barra de herramientas para filtros.

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 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

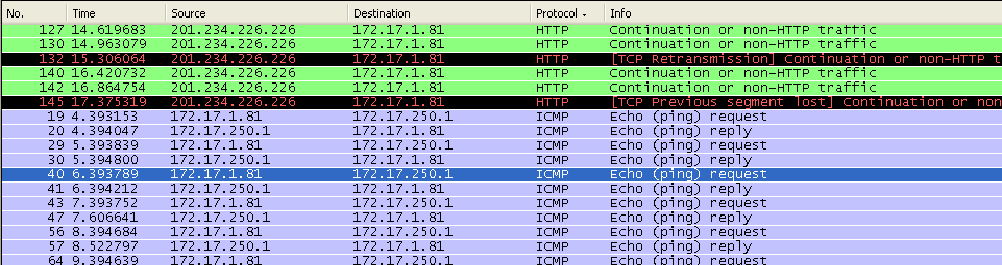


Imagen 13: Panel de paquetes capturados.

Panel para detalles de paquetes: 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.

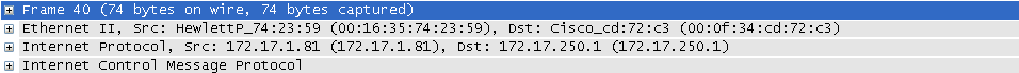


Imagen 14: Panel para detalles de paquetes.

Panel de paquetes capturados por 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.

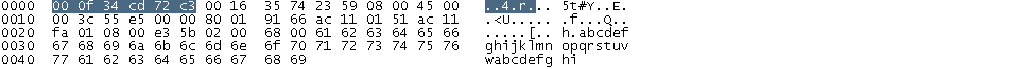


Imagen 15: Panel de paquetes capturados en Bytes.



Imagen 16: Barra de estado.

**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 y realizar el análisis necesario para tener una red segura y estable. un 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.

**Detener/Reiniciar la captura de paquetes:**

Para detener la captura de paquetes podemos Hacer uso del icono capture_stop_24 desde el menú Capture o desde la barra de herramientas.

Para reiniciar el proceso de captura de paquetes se debe seleccionar el icono capture_restart_24 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*.

**Expresiones de filtrado**

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

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.

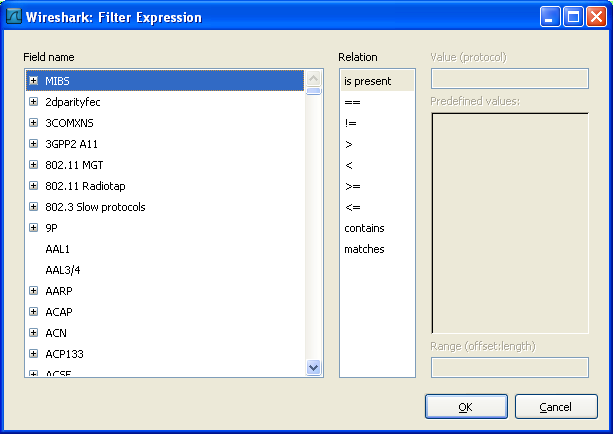


Imagen 17: Pantalla de filtrado de expresiones.

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.

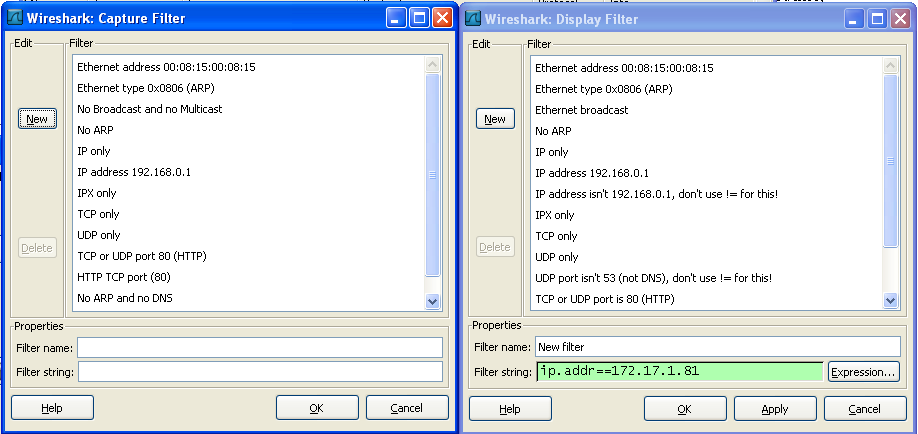


Imagen 18: Pantallas de captura de filtros nuevos.

Para definir un filtro se debe presionar el botón  se indica el nombre del filtro y la expresión y presionar  para salvar los cambios.

**Manipulación de paquetes capturados**

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.

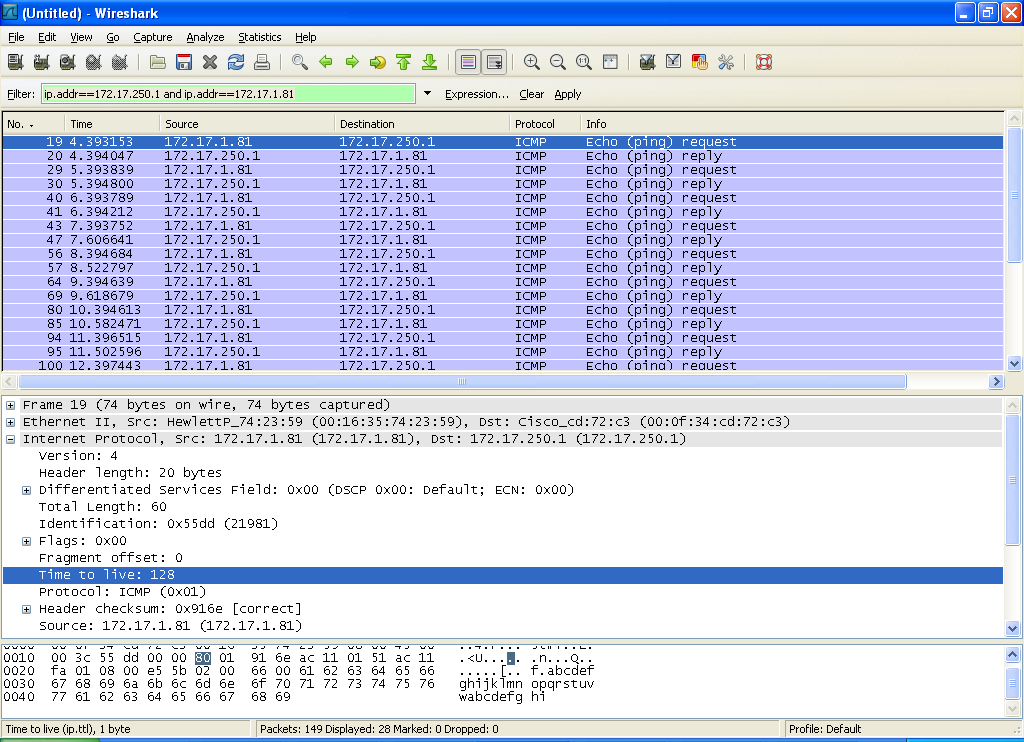


Imagen 19: panel de detalles de paquetes.

**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.



Imagen 20: Pantalla de búsqueda de paquetes.

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.

**Marcado de paquetes**

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

**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.

**Conclusión**

Bibliografia:

[1] https://es.wikipedia.org/wiki/Wireshark

[2 ] https://prezi.com/rlg-ha4f9udn/wireshark/

[3] https://www.seas.es/blog/informatica/wireshark-un-gran-analizador-de-protocolos/