REDES DE COMPUTADORES

FACULTAD DE INGENIERIA ELECTRONICA

UNIVERSIDAD PONTIFICIA BOLIVARIANA

Profesor: Jhon Jairo Padilla Aguilar, Ph.D.

PRACTICA DE LABORATORIO

# TITULO: MANEJO DE UN ANALIZADOR DE PROTOCOLOS DE RED

## OBJETIVOS:

Con esta práctica el estudiante estará en capacidad de:

- Manejar un programa de análisis de protocolos de red común
- Afianzar los conceptos de: Paquete, Tarjeta de Red, Dirección IP, Arquitectura de protocolos, Arquitectura TCP/IP
- Realizar análisis de tráfico en una red para determinar: los protocolos empleados en la red, la cantidad de tráfico generada por cada protocolo, las direcciones de origen y destino de los paquetes, etc.

## REQUISITOS

Conocer los conceptos de Paquete, Arquitectura de protocolos TCP/IP, direcciones IP.

## MARCO TEORICO

WireShark es un programa gratuito, para Windows de Microsoft, que permite analizar los protocolos de los paquetes que pasan por una tarjeta de red de los tipos utilizados comúnmente hoy en día, tales como Tarjetas Ethernet, Wi-Fi, etc.

Este programa permite hacer análisis tales como la jerarquía de protocolos de los paquetes analizados y gráficos del tráfico capturado total o del tráfico por cada tipo de protocolo.

WireShark toma los paquetes de datos que pasan por la tarjeta de red (estos paquetes tienen el formato del protocolo de Acceso al Medio) y luego analiza cada una de las cabeceras de los diferentes protocolos que van encapsulados en cada paquete. Las herramientas de análisis del programa permiten observar la jerarquía de los protocolos que han sido utilizados en los paquetes muestreados; además, se pueden realizar gráficas del número de bits que han sido transmitidos utilizando cada uno de los protocolos en la medida que transcurre el tiempo. A continuación se describirá el procedimiento necesario para realizar una toma de muestras de paquetes y cómo utilizar las herramientas de análisis que tiene el programa WireShark.

PROCEDIMIENTO

1. Primero debe instalarse el paquete WireShark , para lo que debe ejecutarse el programa instalador. La instalación se realizará automáticamente.
2. Abrir el programa Wireshark haciendo doble-click sobre el ícono del programa en Windows.
3. El programa desplegará una ventana típica de las aplicaciones en Windows (ver la figura 1), con unos menús en la parte de arriba y algunos botones que permiten dar algunas órdenes más directamente. Los datos capturados se mostrarán en tres áreas destinadas a este propósito. El área superior muestra información de cada uno de los paquetes capturados, tal como la dirección IP origen, dirección IP destino, el protocolo que lo envía, el tiempo en que se capturó (tomando como cero el inicio de la captura) y una breve descripción de la función que cumple el paquete.

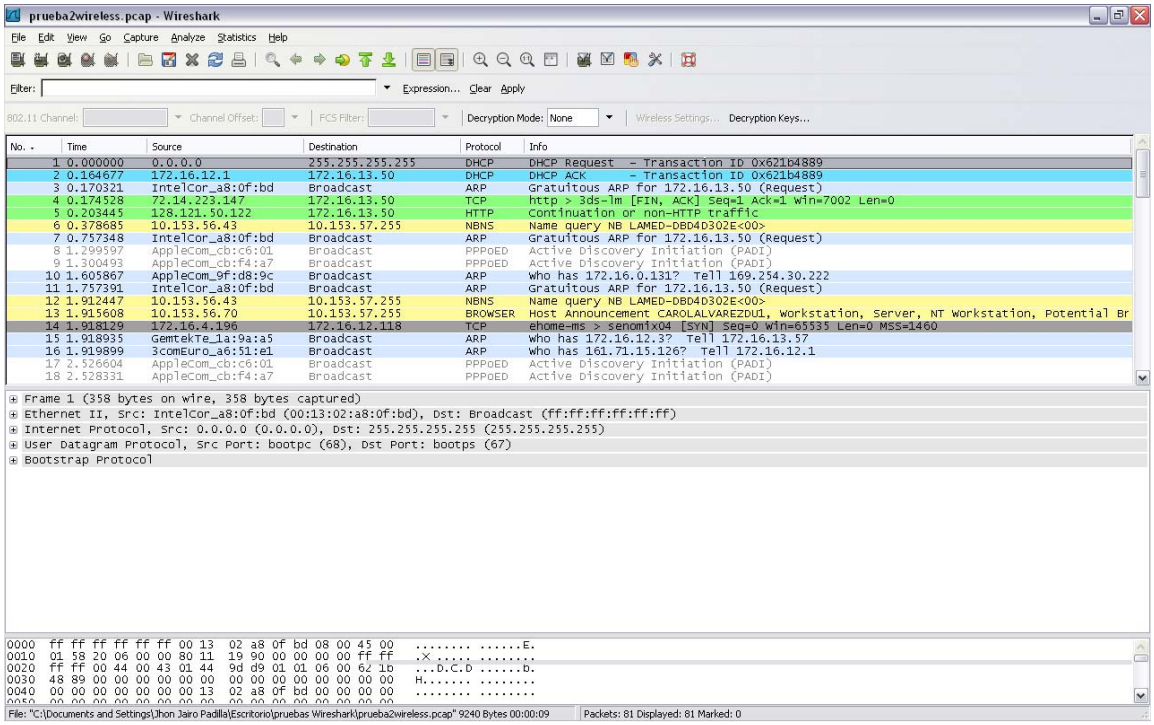


Figura 1. Ventana principal del programa WireShark

4. Establecimiento de Condiciones iniciales:
    a. Antes de Iniciar una captura, debe establecerse cuál es la interfaz física (tarjeta de red) que se utilizará para tomar las muestras de tráfico. Esto se hace mediante el menú “Capture” en la opción “Interfaces”. Al hacer click en esta opción, se desplegará una ventana como la de la figura 2, en donde se encuentran todas las interfaces físicas disponibles en el computador utilizado. En esta ventana deberá

escogerse la tarjeta de red Ethernet si el computador está conectado a una red LAN tipo Ethernet, o una tarjeta de red inalámbrica tipo Wi-Fi, si la conexión a analizar fuese la de una red inalámbrica de este tipo.

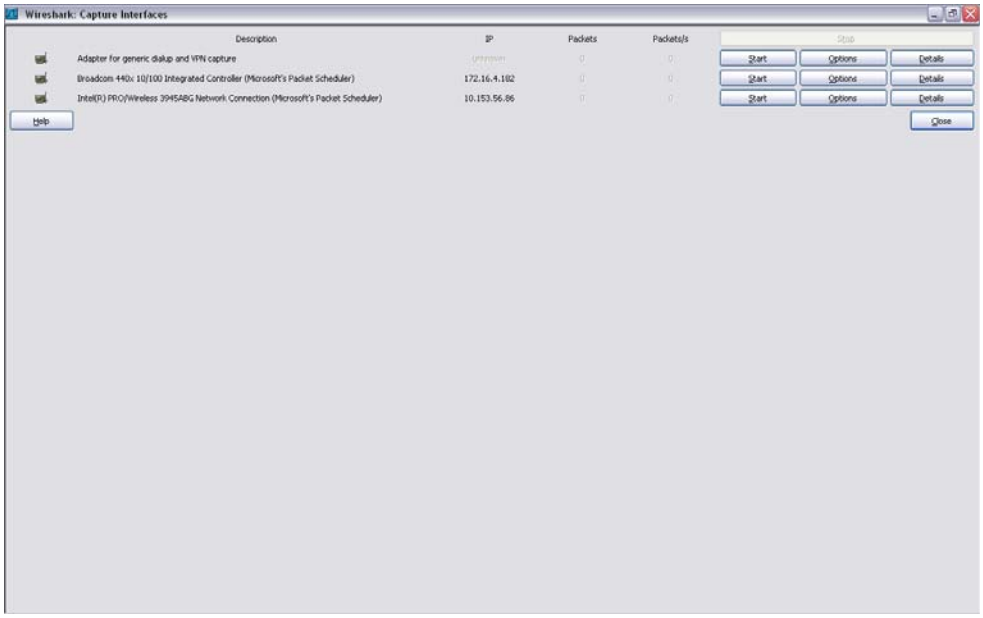



Figura 2. Ventana de la opción "Interfaces" de WireShark.

b. Para establecer las condiciones de la captura, deberán establecerse las condiciones de la misma haciendo click en el botón "Options" de la Interfaz de red deseada. Al hacer esto, aparecerá una ventana como la de la figura 3 (se escogió la tarjeta de red Ethernet).

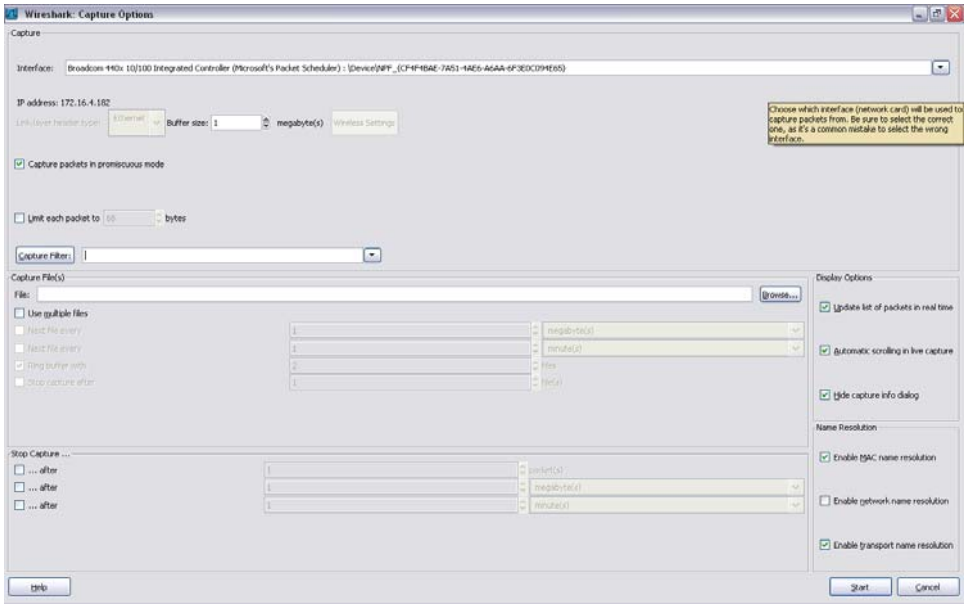



Figura 3. Ventana "Options" de una tarjeta de red Ethernet

c. En la ventana “Options” aparecerán entre otras opciones: el nombre de la tarjeta de red a utilizar, su dirección IP asignada, el tamaño del buffer de almacenamiento en Megabytes y una opción para capturar datos en modo promíscuo. El modo promíscuo es una opción que permite que se capturen paquetes que pertenezcan a comunicaciones de otros computadores diferentes al utilizado para la captura. El modo “No promiscuo” sería lo totalmente opuesto, es decir, sólo permite capturar los paquetes que salen o entran desde/hacia el computador que realiza la captura. Es importante aclarar que cuando se utiliza una tarjeta de red inalámbrica tipo Wi-Fi, sólo se permite la captura en el modo “No Promiscuo”, por lo que no se realizarán capturas con esta interfaz si se utiliza el modo Promiscuo.

5. Inicio de la operación de Captura:

   Una vez se establezcan las condiciones iniciales, se podrá dar inicio a la operación de captura simplemente haciendo click en el botón “Start” de la ventana “Options”. Es importante aclarar que no es indispensable ir a la ventana “Options” para dar inicio a la captura. Si las condiciones de la tarjeta están correctas desde un principio, podría hacerse click en el botón “Start” en la ventana “Interfaces” de la figura 2.

   Una vez que se inicia la captura de los paquetes, irá apareciendo la información de los paquetes capturados en la ventana principal del WireShark (Figura 1). Cuando se desee terminar la captura se puede dar click en la opción “Stop” del menú “Capture”. Este es un tipo de finalización de captura que se realiza cuando el usuario lo desee. Es importante aclarar que las capturas de información ocupan gran cantidad de espacio en disco duro, por lo que no es deseable dejar demasiado tiempo funcionando la operación de captura. Otra forma de detener la operación de captura es programar el tiempo que tardará la captura en la ventana “Options”.

6. Almacenamiento de los datos:

   Antes de iniciar cualquier operación de análisis, es importante almacenar los datos de la captura. El almacenamiento se hace en forma de archivos en un formato especial del WireShark. Para almacenar los datos, deberá hacerse click en el menú “File” en la opción “Save” o en la opción “Save As”. Para este ejemplo, haga click en la opción “Save As” y aparecerá una ventana como la de la figura 4.

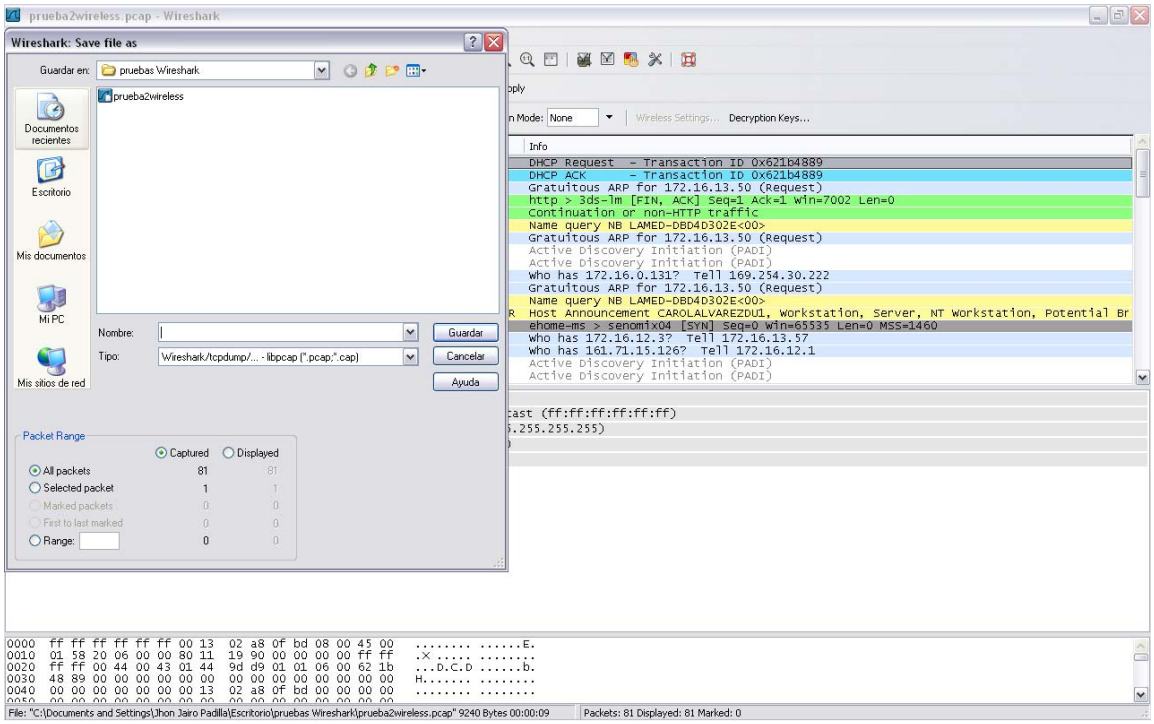
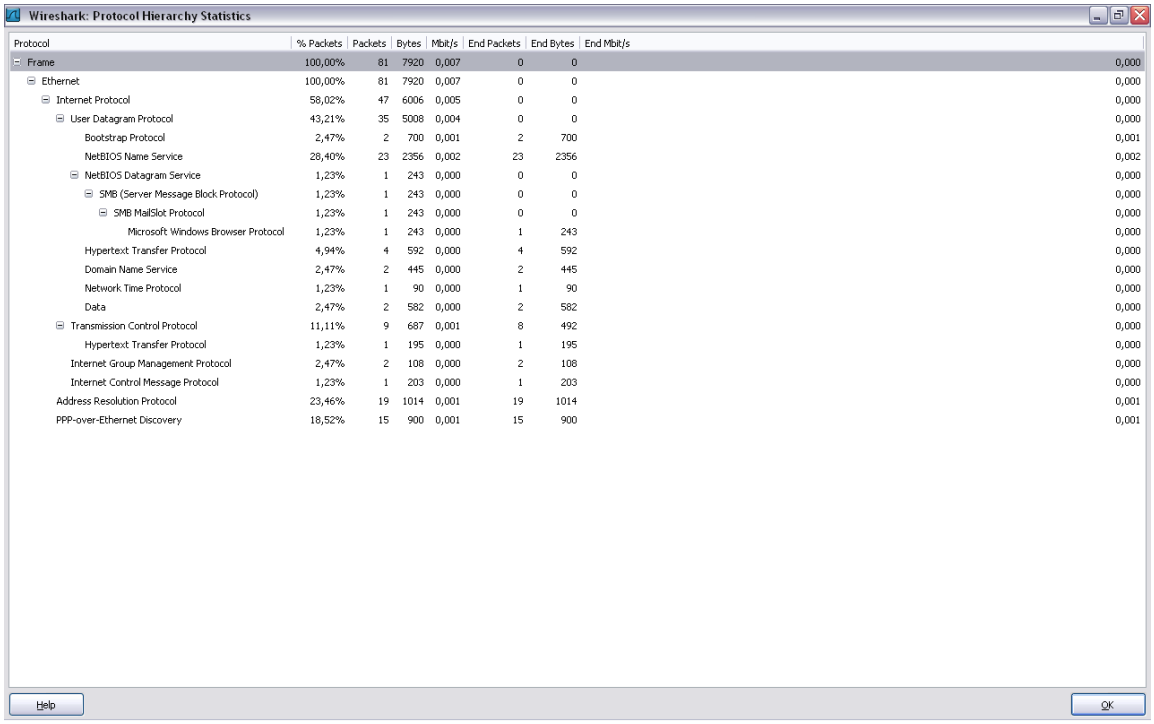


Figura 4. Ventana de la opción “Save As” del WireShark.

Escoja la carpeta donde se ubicará el archivo y el nombre del archivo, por ejemplo “Prueba1”. Utilice el formato de archivo por defecto que tiene el WireShark. Finalmente de la opción “Guardar”. Observe que en esta ventana también se tiene la opción de almacenar todos los paquetes s sólo los que hayan sido seleccionados, o también se puede dar un rango de paquetes según su orden de captura.

7. Análisis de los paquetes:
    a. Un primer análisis puede realizarse sencillamente observando la ventana principal del WireShark (ver figura 1). En la parte superior aparecen los datos principales de cada paquete: El número de orden en que se capturó, el tiempo en que se capturó a partir del inicio de la captura, la dirección IP fuente, la dirección IP destino, el tipo de protocolo que transporta (según la información de la capa más alta que contenga) y una breve descripción de la función de este paquete. En la parte intermedia de la ventana principal, aparecen todos los protocolos que utilizan este paquete para enviar su información. Finalmente, en la parte más baja de la ventana principal aparece la información útil que transporta el paquete. Esta información útil es mostrada en forma de caracteres ASCII, por lo que, dependiendo de la aplicación, si esta transporta texto claro, se podrá ver la información claramente, mientras que si transporta otro tipo de información (vídeo, voz, imágenes, texto encriptado) ésta ya no podrá ser legible.

b. Un segundo tipo de análisis utiliza la descripción en forma de árbol que muestra todos los protocolos utilizados en todos los paquetes muestreados. Para observar esta herramienta de análisis, haga click en el menú “Statistics” y en la opción “Protocol Hierarchy”. Aparecerá una ventana que se observa en la figura 5.




| Protocol | % Packets | Packets | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|---|---|---|---|---|---|---|---|
| Frame | 100,00% | 81 | 7920 | 0,007 | 0 | 0 | 0,000 |
| Ethernet | 100,00% | 81 | 7920 | 0,007 | 0 | 0 | 0,000 |
| Internet Protocol | 58,02% | 47 | 6006 | 0,005 | 0 | 0 | 0,000 |
| User Datagram Protocol | 43,21% | 35 | 5008 | 0,004 | 0 | 0 | 0,000 |
| Bootstrap Protocol | 2,47% | 2 | 700 | 0,001 | 2 | 700 | 0,001 |
| NetBIOS Name Service | 28,40% | 23 | 2356 | 0,002 | 23 | 2356 | 0,002 |
| NetBIOS Datagram Service | 1,23% | 1 | 243 | 0,000 | 0 | 0 | 0,000 |
| SMB (Server Message Block Protocol) | 1,23% | 1 | 243 | 0,000 | 0 | 0 | 0,000 |
| SMB MailSlot Protocol | 1,23% | 1 | 243 | 0,000 | 0 | 0 | 0,000 |
| Microsoft Windows Browser Protocol | 1,23% | 1 | 243 | 0,000 | 1 | 243 | 0,000 |
| Hypertext Transfer Protocol | 4,94% | 4 | 592 | 0,000 | 4 | 592 | 0,000 |
| Domain Name Service | 2,47% | 2 | 445 | 0,000 | 2 | 445 | 0,000 |
| Network Time Protocol | 1,23% | 1 | 90 | 0,000 | 1 | 90 | 0,000 |
| Data | 2,47% | 2 | 582 | 0,000 | 2 | 582 | 0,000 |
| Transmission Control Protocol | 11,11% | 9 | 687 | 0,001 | 8 | 492 | 0,000 |
| Hypertext Transfer Protocol | 1,23% | 1 | 195 | 0,000 | 1 | 195 | 0,000 |
| Internet Group Management Protocol | 2,47% | 2 | 108 | 0,000 | 2 | 108 | 0,000 |
| Internet Control Message Protocol | 1,23% | 1 | 203 | 0,000 | 1 | 203 | 0,000 |
| Address Resolution Protocol | 23,46% | 19 | 1014 | 0,001 | 19 | 1014 | 0,001 |
| PPP-over-Ethernet Discovery | 18,52% | 15 | 900 | 0,001 | 15 | 900 | 0,001 |

Figura 5. Herramienta de análisis de la Jerarquía de Protocolos en la muestra total de paquetes.

Puede observarse que en el árbol de protocolos, se inicia la raíz con el protocolo Ethernet. De este nace una rama con el protocolo IP y luego se abren dos ramas con los protocolos de transporte TCP y UDP. De estos protocolos se desprenden los protocolos de las aplicaciones. Finalmente, hay dos protocolos cuyas ramas no nacen del protocolo IP, estos son ARP y Descubrimiento PPP sobre Ethernet.

Para cada protocolo se especifica el porcentaje de paquetes que lo transportan, el número de paquetes, el número de bytes y la velocidad en Mbps, entre otros datos.

c. Una tercera herramienta muy útil para análisis del tráfico son las gráficas del tráfico de paquetes en función del tiempo. Para utilizar esta herramienta, haga click en el menú “Statistics” y luego haga click en la opción “I/O Graphs”. Aparecerá una ventana como la de la figura 6.

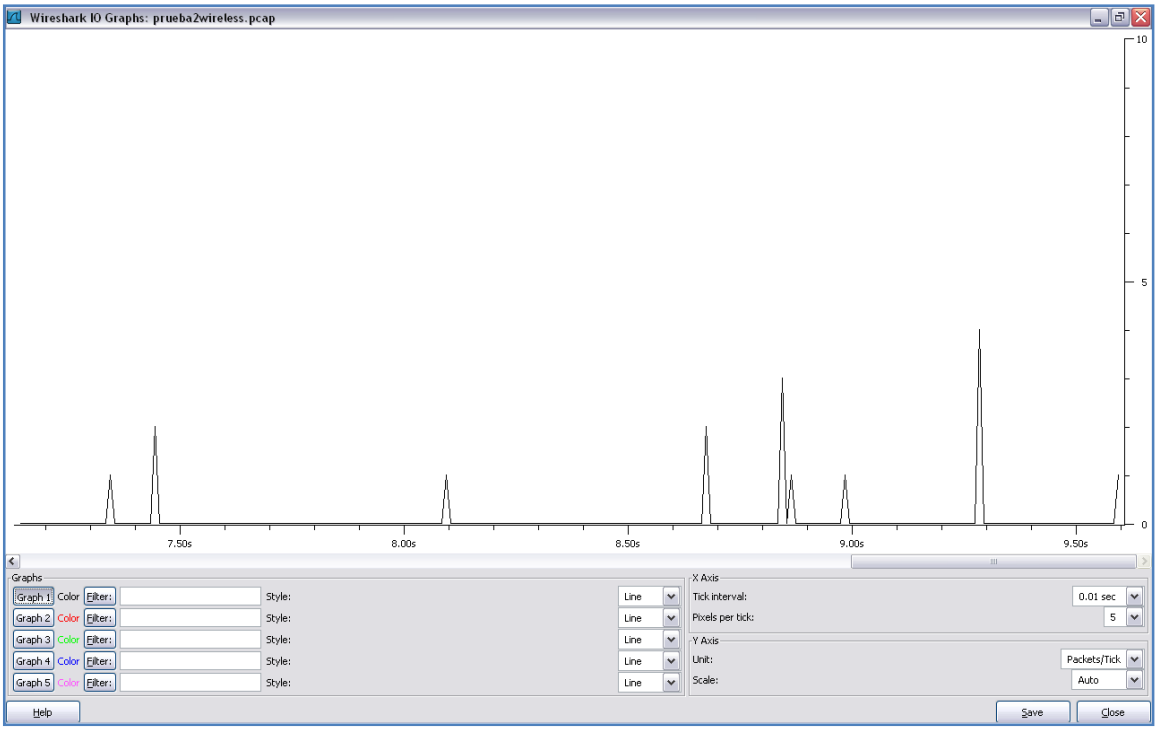


Figura 6. Herramienta para graficar la variación del tráfico en el tiempo.

En la ventana inicial de la herramienta aparecerá una gráfica que muestra la variación del tráfico total durante el tiempo que duró el muestreo. Esta gráfica aparece en Negro. En la parte inferior derecha se observan los parámetros de la gráfica, tales como la escala ("Tick Interval"), el número de píxeles por marca, las unidades del Eje Y (puede ser en paquetes/marca, bytes/marca o bits/marca) y la escala del eje Y, que inicialmente se asigna automáticamente.

Esta gráfica puede complementarse agregando gráficos del comportamiento de algún protocolo en especial que se desee analizar. Esto puede lograrse escribiendo por ejemplo en la línea de la gráfica 2, en su casilla Filtro ("Filter"), el nombre del protocolo a graficar (p.ej. teclee "udp"). Luego se hace click en el botón "Graph 2" y aparecerá en color rojo la variación del tráfico, tal como se observa en la figura 7. En realidad, la forma del gráfico por defecto es como líneas. Sin embargo, para ver las dos gráficas es necesario cambiar una de ellas a "impulsos" en lugar de líneas (ya que la línea negra del tráfico total no deja ver las otras líneas algunas veces). En la figura 7, el tráfico total se observa como impulsos negros, mientras que el tráfico UDP se observa en forma de líneas rojas.

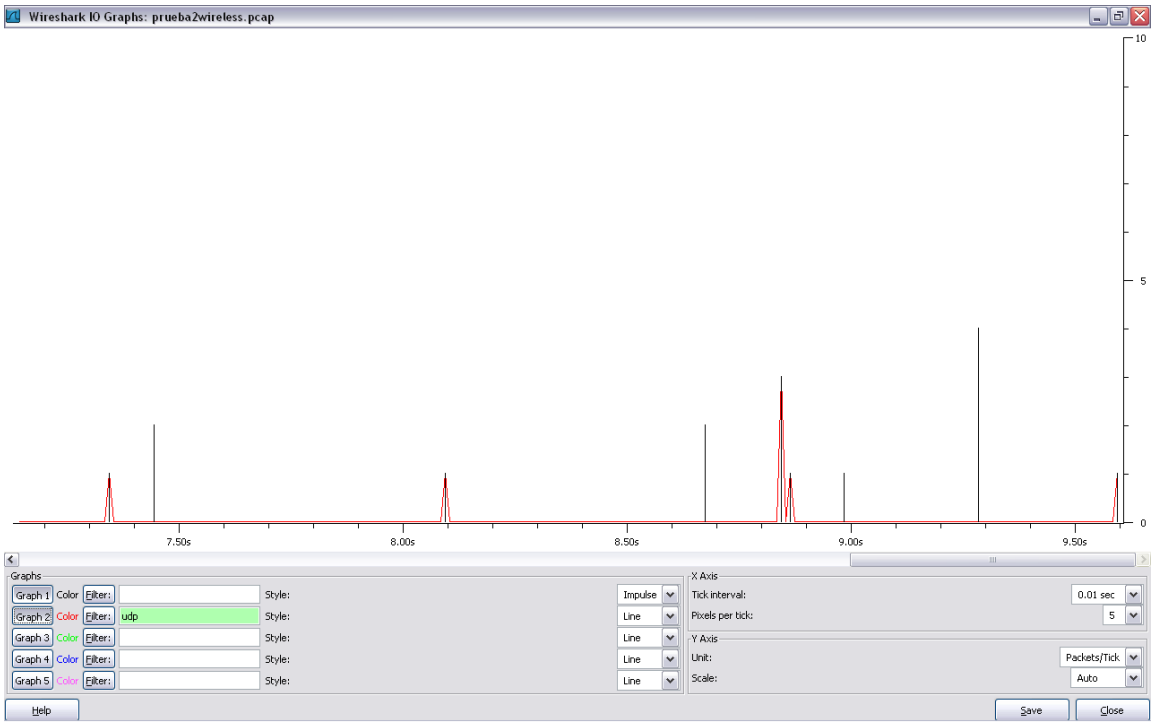



Figura 7. Gráfica del tráfico del protocolo UDP.

Los gráficos obtenidos pueden grabarse en archivos de tipo png, bmp, etc. Esto se logra haciendo click en el botón "Save". Entonces aparecerá una ventana solicitando el nombre del archivo y el tipo de formato que tendrá.

EVALUACION

Realice una toma de muestras de la tarjeta de red Ethernet del computador. Puede ser por un tiempo de 10 a 30 segundos. Analice los protocolos que intervienen en las comunicaciones establecidas. Describa qué hace cada protocolo (si no lo conoce, investigue en casa). Haga un estudio del porcentaje de paquetes de cada protocolo (puede usar diagramas de pastel). También describa qué direcciones son utilizadas en los paquetes (Hay alguna razón para que se usen mucho ciertas direcciones de origen ó destino?). Genere las gráficas del comportamiento del tráfico de los protocolos Ethernet, IP, TCP y UDP. Explique por qué hay más tráfico de algunos protocolos que de otros.

Todos estos aspectos deben ser consignados en el informe de la práctica.