

Universidad Autónoma de Aguascalientes.

Centro de Ciencias Básicas.



“Manual de Usuario del Analizador de paquetes”

**Materia:** Redes de Computadoras I

**Profesor:** Javier Santiago Cortez López

**Integrantes del equipo:**

ID 349107 Emilio Ortiz Romo

ID 281466 Ricardo Almada Diaz

ID 349964 Ilse Jacqueline Martínez Espinosa

ID 349397 Uriel Rodríguez Guadarrama

# Introducción

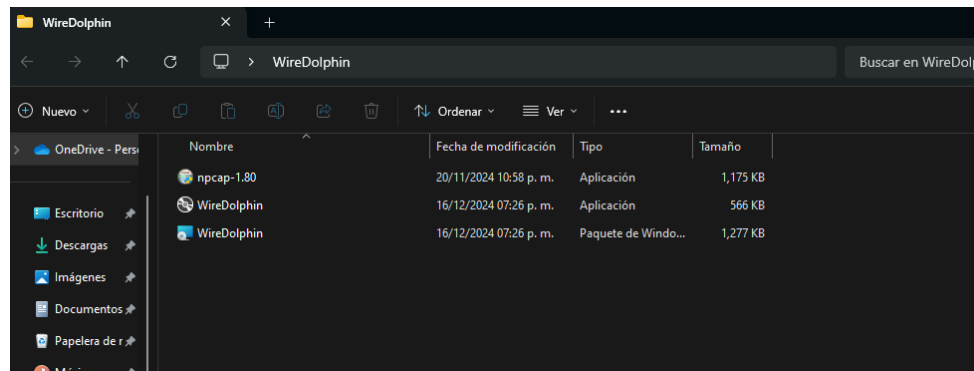
Por medio de este documento se presenta y brinda información sobre la aplicación creada para la captura y análisis de paquetes por medio de NPCAP (librería que se encarga del procesamiento de este tipo de datos), este mismo programa será brindado en la misma carpeta del presente documento, esto a fin de brindar al usuario herramientas para obtener información del tráfico de red, de la cual su dispositivo sea parte. Con este objetivo solicitamos al usuario lea la información presente en las siguientes páginas para el correcto funcionamiento de la aplicación.

## Requisitos Previos

Es necesario que el usuario tenga pleno conocimiento de sus adaptadores de red que estén actualmente en funcionamiento, la aplicación brinda una lista de los identificados por el programa, sin embargo, es necesario el usuario seleccione alguno que actualmente este activo y recibiendo paquetes, para poder analizar los mismos.

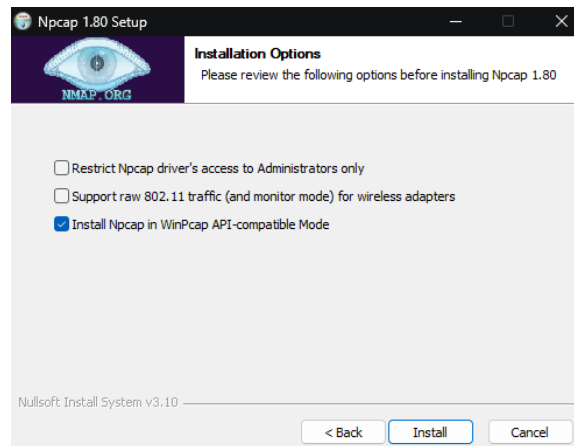
## Instalación

La instalación consta con una carpeta con dos aplicaciones y un paquete de Windows

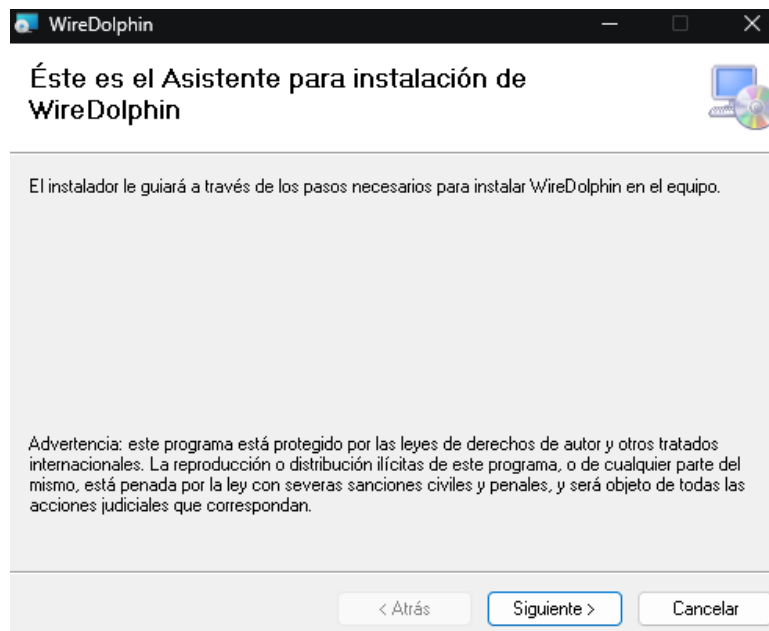


La aplicación npcap es un instalador de este mismo y es necesario para que la aplicación pueda ser usada adecuadamente, es decir, sin esta la aplicación no funciona.

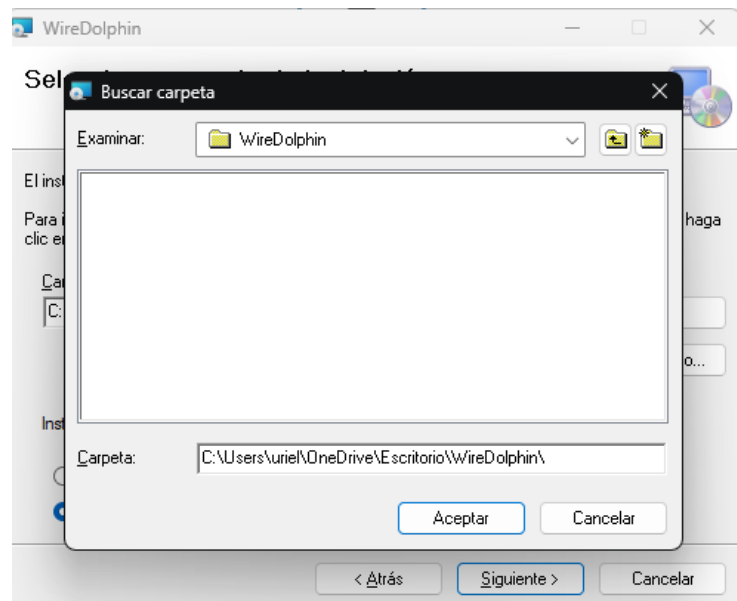
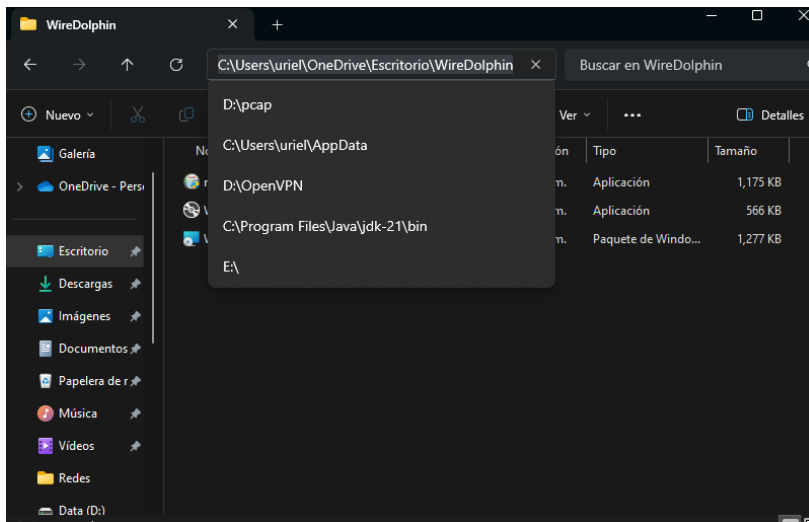
Es importante que al realizar la instalación del npcap instalarlo en WinPcap



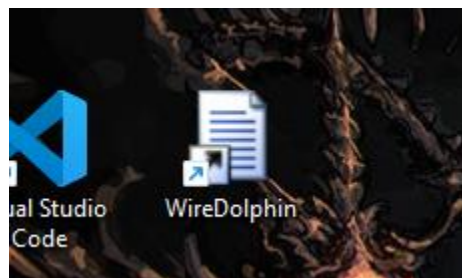
Una vez ya instalado el npcap ya podemos pasar a la instalación de la aplicación, podemos usar cualquiera de los dos instaladores restantes que aparecen en la carpeta, lo importante es que los dos deben de estar en esta misma.



Al seleccionar siguiente nos pedirá la ruta de descarga, es importante poner esta ruta en la misma carpeta en la que se encuentran los tres instaladores. Como en mi caso yo tengo la carpeta en la ruta que se muestra en la imagen a continuación la instalación la hago en la misma ruta/carpeta.



Una vez seleccionada la carpeta se procederá la instalación, cuando finalice tendremos todo lo necesario para ejecutar la aplicación que automáticamente tendrá una ruta para abrirla en el escritorio.

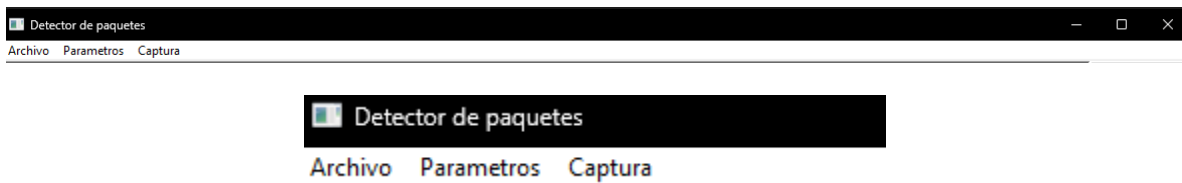


Al dar doble click se ejecutará la aplicación y si toda la instalación se hizo correctamente no presentara ningún problema en su ejecución.

# Funciones básicas

## Menú de Usuario.

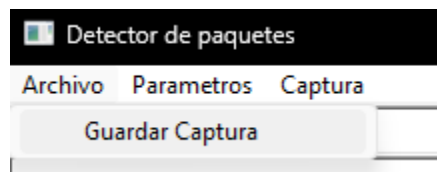
Es el apartado principal con el cual se hará interacción del usuario, representado por una barra de menú ubicada en el borde superior, por medio de esta barra se darán indicaciones para que el programa realice las tareas que necesite el usuario, así como definir parámetros, o guardar datos en un archivo CSV.



Este se define por 3 apartados los cuales cuentan con un objetivo diferente entre si, cada uno de ellos permite crear e implementar los datos o herramientas que el usuario necesite.

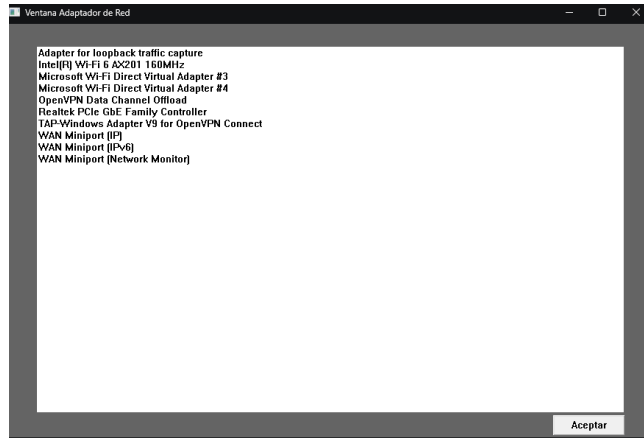
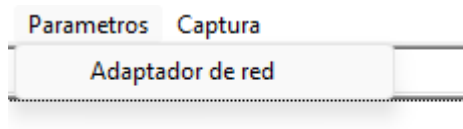
### Archivo – Guardar Captura:

En este apartado al abrirlo se desplazará un botón secundario para el almacenamiento de los datos de captura que se hayan generado anteriormente, por medio del cual se mostrará una interfaz que permita manipular el nombre ya que esto lo que hace es sobrescribir los datos de la captura actual con otra pasada.



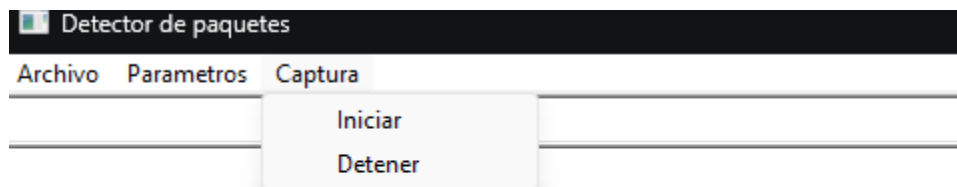
### Parámetros – Adaptador de red:

En esta sección se busca que el usuario seleccione la interfaz de red con la cual quiera realiza la captura de paquetes, en caso de seleccionar una red el mismo programa te lo indicara.



### Captura – Inicio/Detener:

En esta sección se cuenta con dos botones los cuales como su mismo nombre indica son para comenzar la captura y detenerla, es importante aclarar que, al empezar una captura sin haber seleccionado un dispositivo de red, se enviara un mensaje recordatorio de que se tiene que seleccionar, ya que sin el dispositivo escogido no se puede realizar la captura, de igual manera el botón de detener no funciona hasta que se inicie una captura.



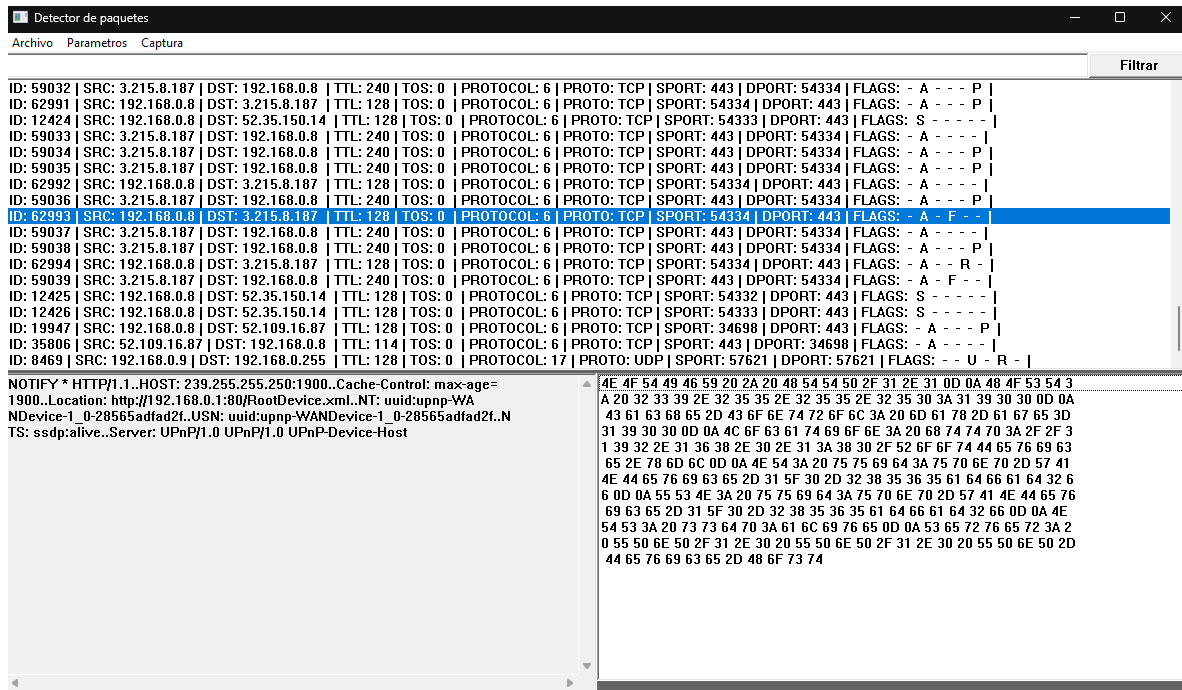
## Apartado de Filtros

Esta sección se encuentra en la parte de debajo del menú de usuario en donde se le puede escribir una filtración dada por el usuario para la captura de paquetes, es importante aclarar que al escribir el filtro deseado es necesario darle a filtrar y enseguida iniciar de nuevo la captura de paquetes ya que esta se detiene al ingresar un filtro/filtro nuevo.

Como se muestra en la imagen esta sección cuenta con los paquetes que se están capturando del dispositivo de red en tiempo real, esta sección desglosa los paquetes en nueve secciones ID, SRC, DST, TTL, No.Protocolo, Protocolo, SPORT, DPORT y Flags del paquete, cabe aclarar que se puede seleccionar cada paquete para verlo desglosado en las pantallas de abajo sin antes haber clickeado alguna de estas dos pantallas encontradas en la parte de abajo.

# Sub-ventanas Información de paquetes.

En estas ventanas podemos encontrar la información que contiene el paquete seleccionado por el usuario, es importante aclarar el hecho de que es necesario que cada vez que es seleccionado el paquete escogido para ser desglosado, clicar alguna de estas dos ventanas ya que sin esto no será actualizado el contenido del paquete, es decir “selección-paquete” -> clic en una ventana de abajo -> “selección-paquete” ->clic en una ventana de abajo.



Las dos ventanas se dividen de la siguiente manera.

## Información Hexadecimal:

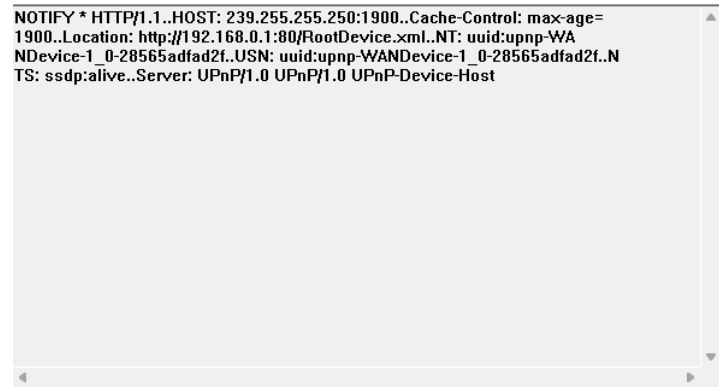
Aqui se obtuvieron los datos extraibles del paquete, los cuales estan en hexadecimal.

```
4E 4F 54 49 46 59 20 2A 20 48 54 54 50 2F 31 2E 31 0D 0A 48 4F 53 54 3
A 20 32 33 39 2E 32 35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D 0A
43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20 6D 61 78 2D 61 67 65 3D
31 39 30 30 0D 0A 4C 6F 63 61 74 69 6F 6E 3A 20 68 74 74 70 3A 2F 2F 3
1 39 32 2E 31 36 38 2E 30 2E 31 3A 38 30 2F 52 6F 6F 74 44 65 76 69 63
65 2E 78 6D 6C 0D 0A 4E 54 3A 20 75 75 69 64 3A 75 70 6E 70 2D 57 41
4E 44 65 76 69 63 65 2D 31 5F 30 2D 32 38 35 36 35 61 64 66 61 64 32 6
6 0D 0A 55 53 4E 3A 20 75 75 69 64 3A 75 70 6E 70 2D 57 41 4E 44 65 76
69 63 65 2D 31 5F 30 2D 32 38 35 36 35 61 64 66 61 64 32 66 0D 0A 4E
54 53 3A 20 73 73 64 70 3A 61 6C 69 76 65 0D 0A 53 65 72 76 65 72 3A 2
0 55 50 6E 50 2F 31 2E 30 20 55 50 6E 50 2F 31 2E 30 20 55 50 6E 50 2D
44 65 76 69 63 65 2D 48 6F 73 74
```



## Información Decodificada:

Es la traducción de los paquetes del hexadecimal.



```
NOTIFY * HTTP/1.1..HOST: 239.255.255.250:1900..Cache-Control: max-age=
1900..Location: http://192.168.0.1:80/RootDevice.xml..NT: uuid:upnp-WA
NDevice-1_0-28565adf2f..USN: uuid:upnp-WANDevice-1_0-28565adf2f..N
TS: ssdp:alive..Server: UPnP/1.0 UPnP/1.0 UPnP-Device-Host
```

## Código del Programa: