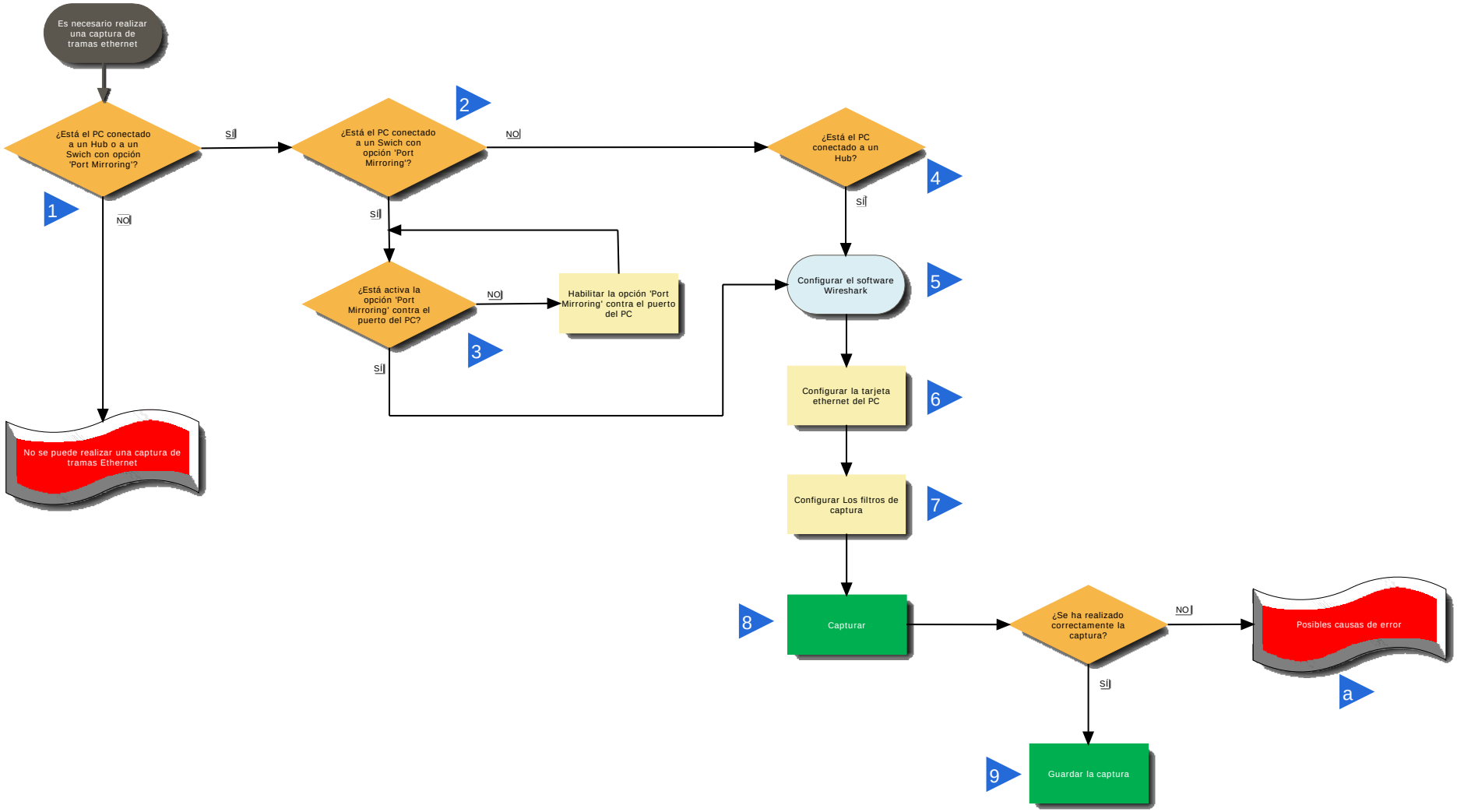
# Guía de diagnóstico

Software WIRESHARK para la captura de tramas Ethernet


Centro de Competencia Técnica

Schneider Electric



# 1. ¿Qué es Wireshark?



**WireShark es un software 'espía', capaz de capturar paquetes / tramas de comunicación que circulen por una red Ethernet de forma que puedan mostrarse de la forma más detallada posible para poder ser analizados.**

## Características importantes del software WireShark

- **Es un paquete de software Open Source (libre y gratuito): www.WireShark.org**
- **Captura y visualización de paquetes de información en tiempo real.**
- **Paros de captura por diferentes tipos de disparos (por tiempo, por cantidad de paquetes recibidos,...).**
- **Guardado / importación / exportación de archivos de capturas.**
- **Filtrado de paquetes.**
- **Estadísticas de red.**

- **Con WireShark no se pueden enviar ni manipular paquetes de información, solamente capturarlos y mostrarlos.**

Volver al diagrama de flujo

# 2. ¿Qué es WinPcap/AirPcap?



**WinPcap es un driver que necesitamos tener instalado conjuntamente con WireShark; es el complemento que permite a WireShark realizar las capturas de paquetes de información.**

**AirPcap es la versión del driver para interfaces Wireless.**

## Características importantes de WinPcap/AirPcap

- **Es un paquete de software que se obtiene y se instala por separado de Ethereal/WireShark; también es Open Source (libre y gratuito): www.WireShark.org / http://www.winpcap.org**
- **Es conveniente instalar el driver WinPcap/AirPcap antes que el software Ethereal/WireShark (la instalación de Ethereal/WireShark detecta si la versión del driver WinPcap/AirPcap es correcta)**

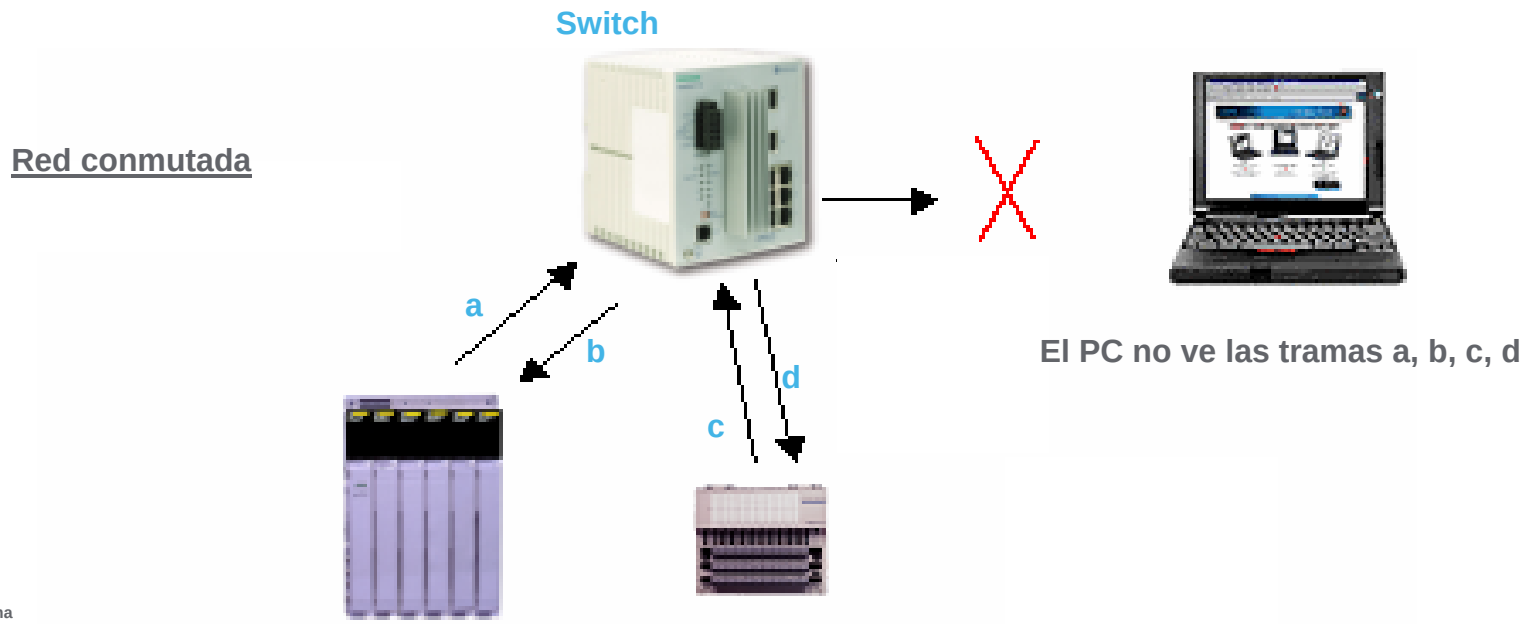
Volver al diagrama de flujo

# 3a. Métodos de captura de tramas en redes Ethernet



- En una red ethernet, el PC desde el cual se ejecuta el software Wireshark sólo puede 'ver' y, por tanto, capturar capturar las tramas recibidas por su tarjeta de red.

- En una red ethernet conmutada (es decir, que los elementos de interconexión entre equipos son switches) esto puede ser un problema ya que las tramas que se pretenden capturar no son direccionadas al puerto del switch al que se conecta el PC y, por tanto, no son vistas por la tarjeta de red de dicho PC.



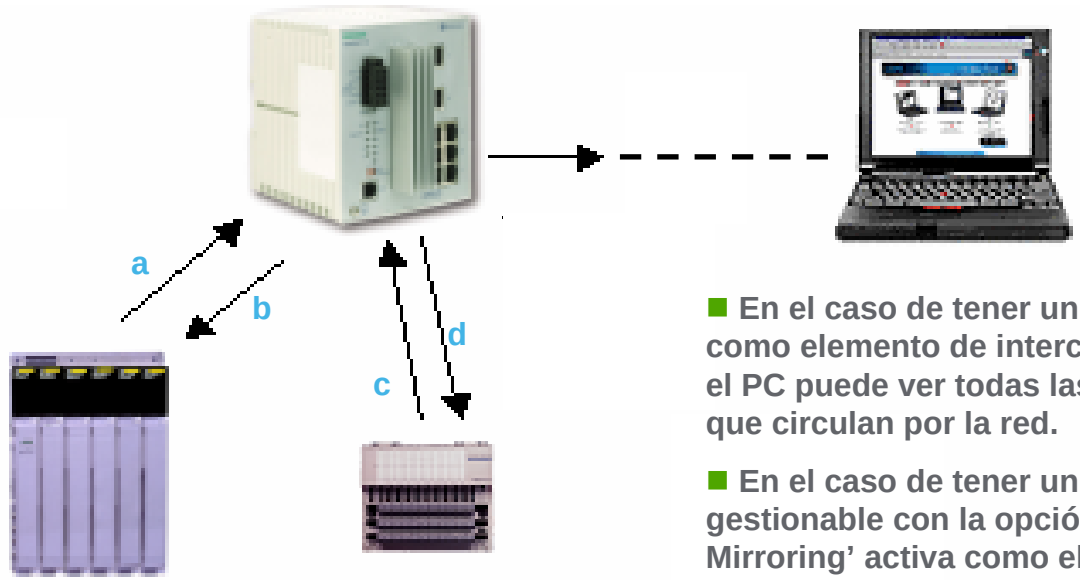

Volver al diagrama de flujo

# 3b. Métodos de captura de tramas en redes Ethernet



- **Para conseguir que las tramas que circulan por la red puedan ser 'vistas' por la tarjeta ethernet del PC y, por tanto capturadas por el software Wireshark, el elemento de interconexión de dispositivos al cual ha de estar conectado el PC ha de ser bien un Hub, bien un Switch gestionable que disponga de servicio 'Port Mirroring' o similar.**

**Hub o Switch con opción 'Port Mirroring' activa**

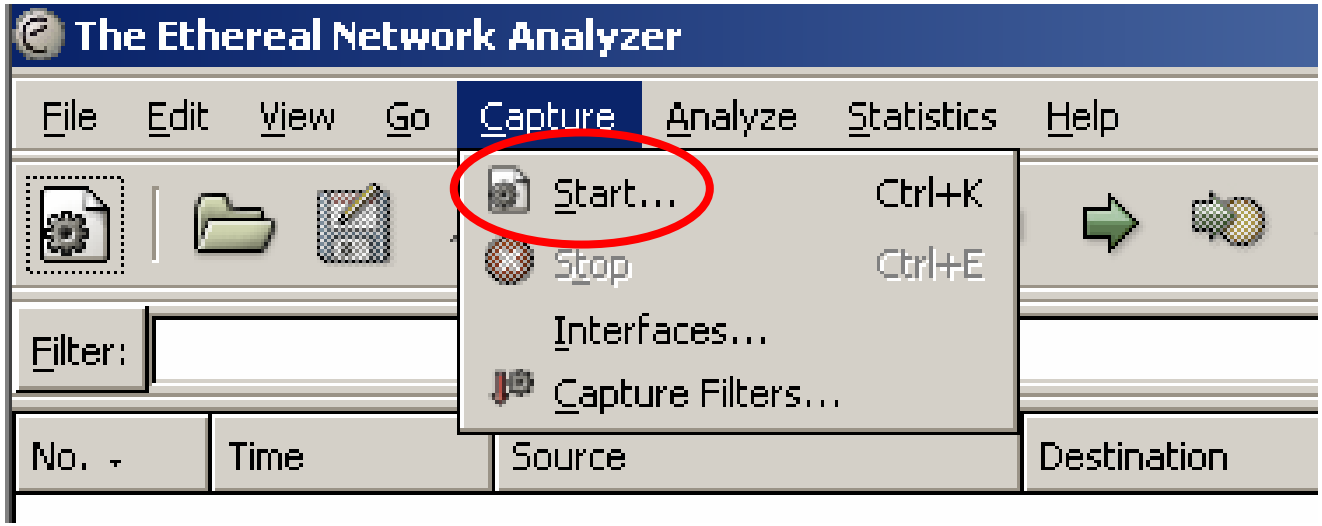


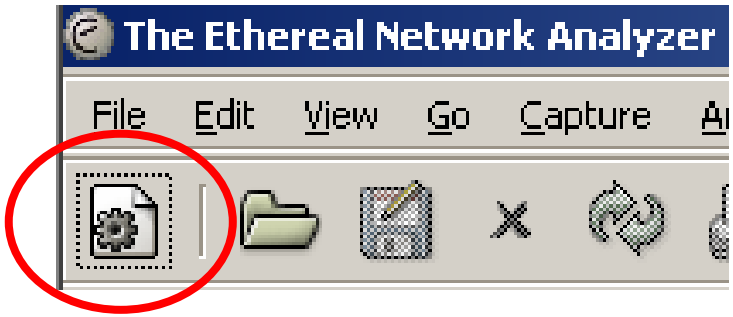

- **En el caso de tener un Hub como elemento de interconexión, el PC puede ver todas las tramas que circulan por la red.**
- **En el caso de tener un Swich gestionable con la opción 'Port Mirroring' activa como elemento de interconexión, el PC puede ver las tramas correspondientes a un dispositivo (a y b o bien c y d)**

Volver al diagrama de flujo

# 4. Cómo iniciar una captura






Volver al diagrama de flujo

# 5a. Opciones de captura



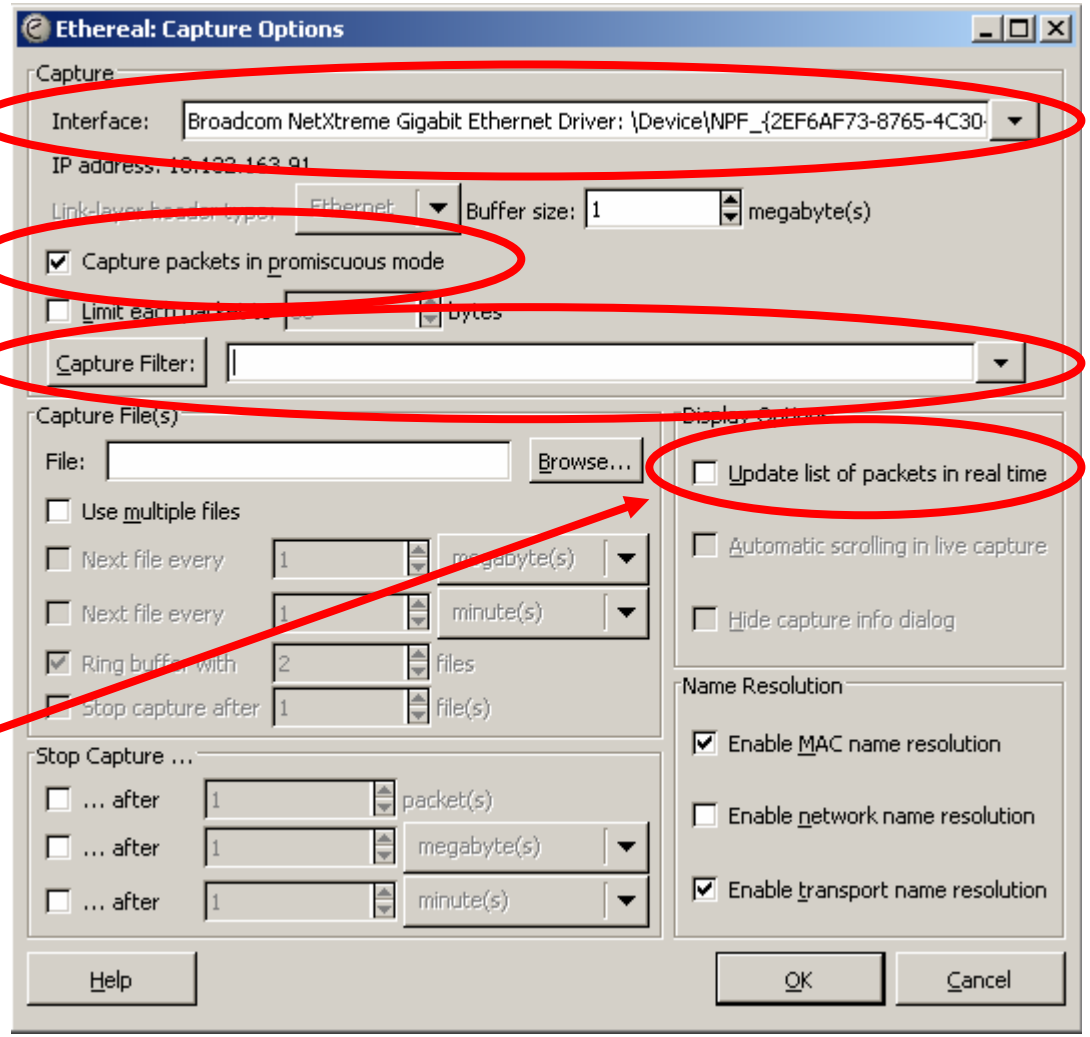
**Las más importantes/usuales son:**

**Interface de captura**

**Captura en modo promiscuo**

**Filtros de captura**

**Refresco de visualización en tiempo real**




Volver al diagrama de flujo

# 5b. Opciones de captura



- **Interface de captura: enlace físico (puerto) desde el que se realizará la captura.**
- **Captura en modo promiscuo: si no está seleccionado, sólo se capturarán los paquetes cuyo origen o destino sea el PC de captura; seleccionando ésta opción, se podrá capturar cualquier paquete que circule por la red a la que el PC está conectado.**
- **Filtros de captura: especificación de las opciones de filtrado previas a la captura.**
- **Refresco de visualización en tiempo real: habilitación de la posibilidad de visualizar los paquetes de información según se van capturando.**

## Observaciones.

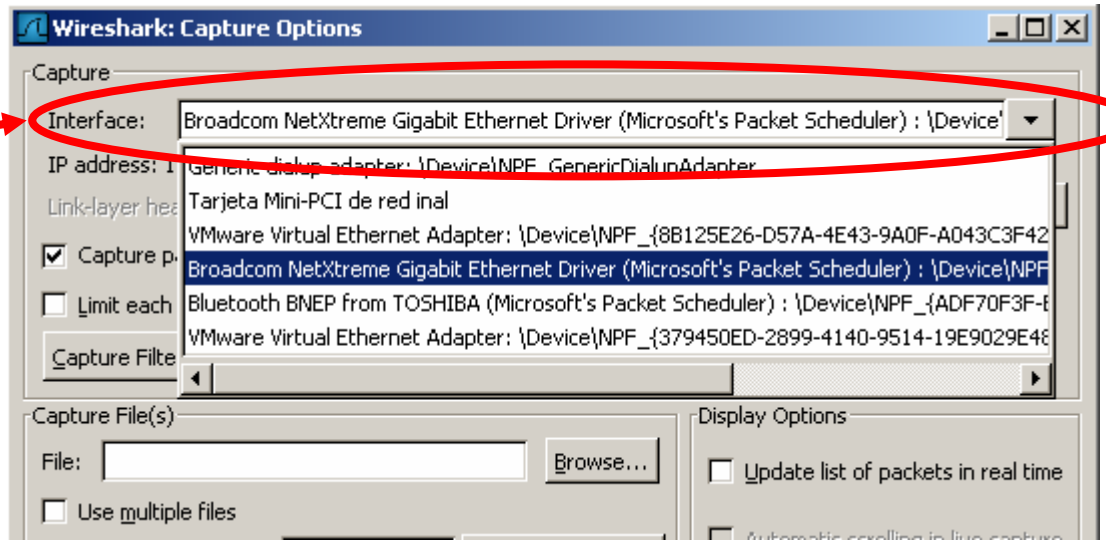
- **La opción de captura en modo promiscuo mediante un interface Wireless sólo está disponible para las versiones de software bajo sistema operativo Linux (nota de la versión 0.10.13).**
- **Configurar una visualización con refresco en tiempo real puede ocasionar una pérdida de tramas de información.**
- **Configurar un filtro de captura puede ocasionar una pérdida de tramas de información por lo que es aconsejable NO configurarlo de inicio, realizar una captura completa y aplicar el filtro al final, una vez la captura haya finalizado.**

Volver al diagrama de flujo

# 5c. Opciones de captura



Interface de captura




**Puede darse el caso que un PC disponga de varias opciones o tarjetas de ethernet (puerto ethernet RJ45, conexión wireless, conexiones virtuales,…).**

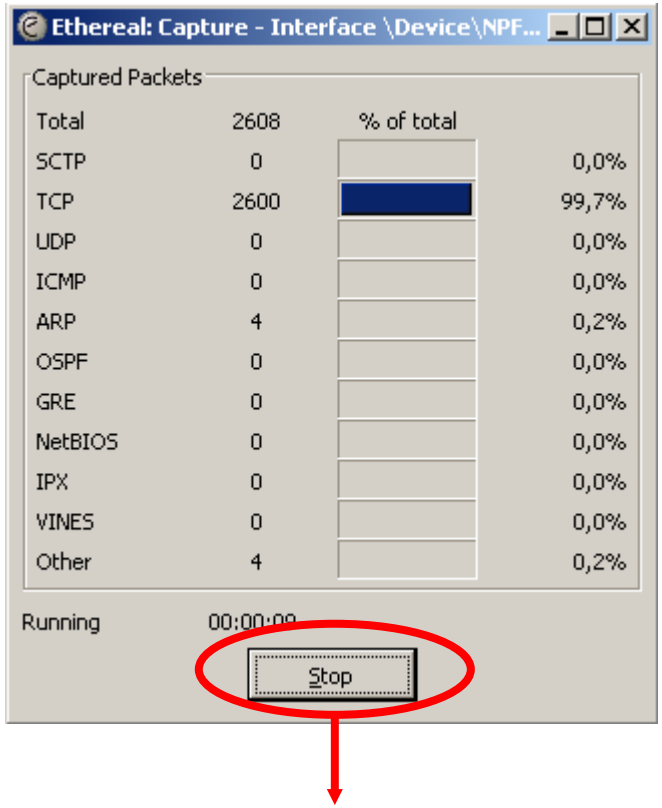
**El software Wireshark necesita que se le indique cuál de todas éstas opciones es por la que ha de realizar la captura de tramas.**

Volver al diagrama de flujo

# 6. Detalle de la captura / estadísticas



**Una vez iniciada la captura tenemos la visión de 2 ventanas; la primera es la de Estadísticas de captura: tenemos la información de cuántos paquetes en total se están capturando, cuántos por cada protocolo (SCTP, TCP, ...) y el tiempo total de captura.**



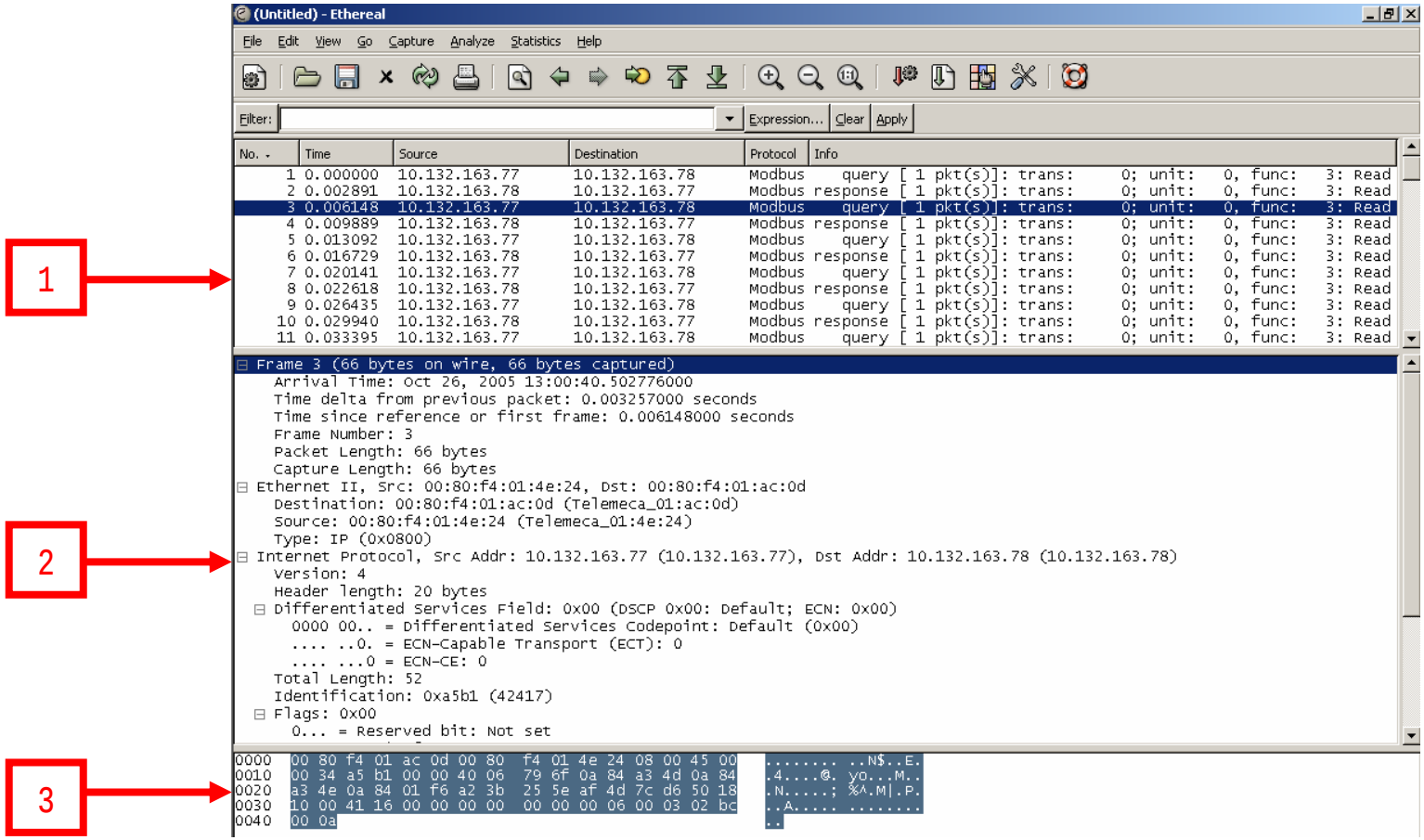

**Mediante la pestaña STOP detenemos la captura en curso**

Volver al diagrama de flujo

# 7a. Detalle de la captura / pantalla principal



**La segunda es la Pantalla principal: tenemos la siguiente información:**




Volver al diagrama de flujo

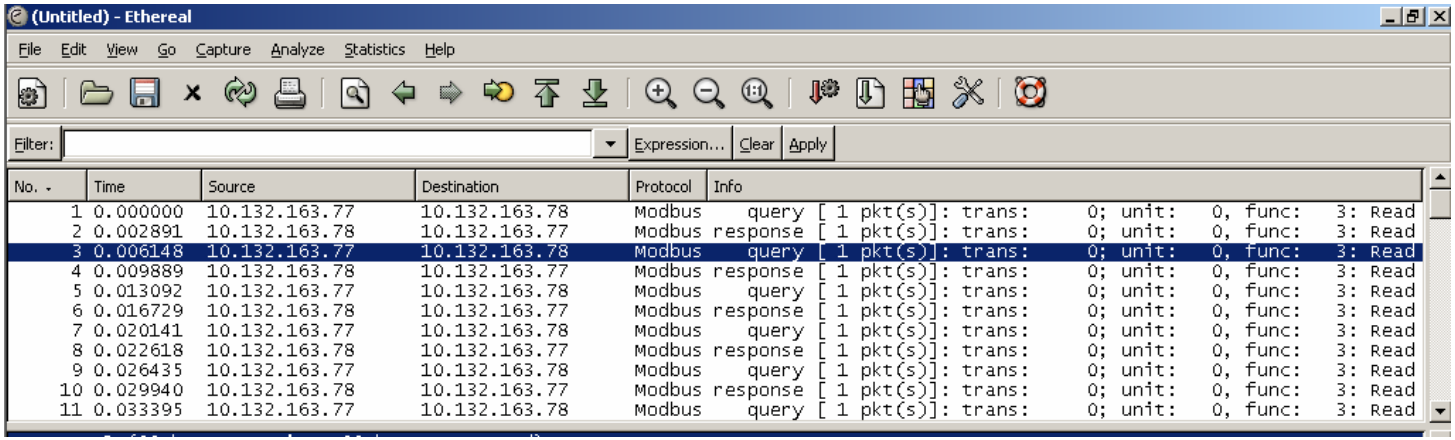
# 7b. Detalle de la captura / pantalla principal



1

**Ventana de lista de paquetes:**

- **Cada línea corresponde a un paquete de información configurado. De cada paquete encontramos la siguiente información (por columnas de izquierda a derecha):**
  - **Número de paquete dentro de ésta captura**
  - **Tiempo de retraso del paquete desde el inicio de la captura**
  - **Dirección de origen del paquete**
  - **Dirección de destino del paquete**
  - **Protocolo del paquete**
  - **Información adicional del paquete**




Volver al diagrama de flujo

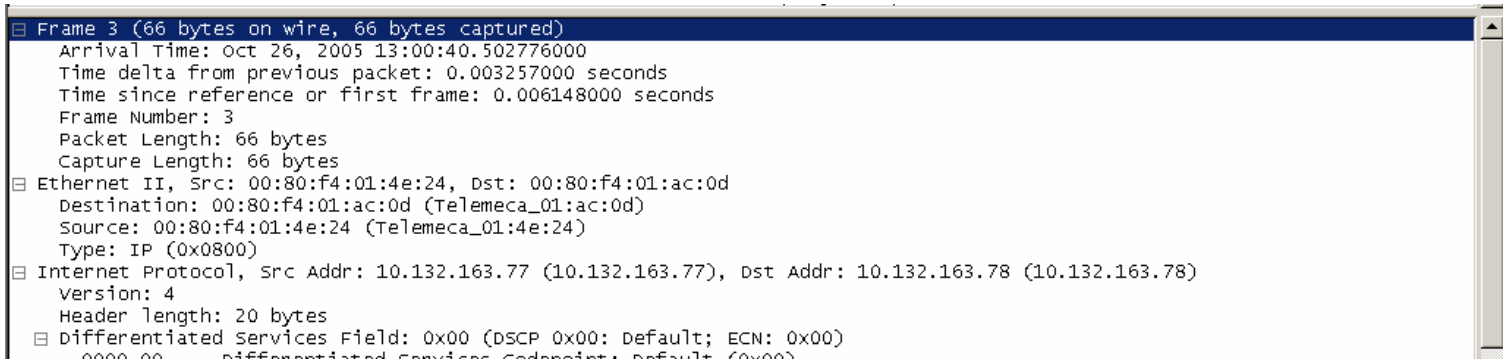
# 7c. Detalle de la captura / pantalla principal



2

**Ventana de detalle de paquetes (árbol de protocolo):**

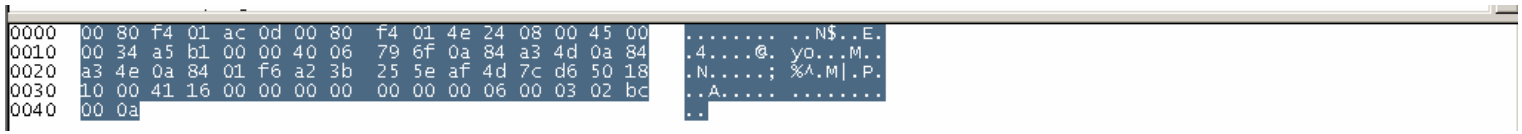
- **Se puede ver en detalle la información contenida en el paquete que está seleccionado en la ventana de lista de paquetes.**
- **Los campos que se detallan (algunos de ellos desplegables) dependen del protocolo del paquete a visualizar.**




3

**Ventana de detalle en Bytes de paquetes:**

- **Se puede ver en detalle la información contenida en el paquete que está seleccionado en la ventana de lista de paquetes en formato Byte y en formato ASCII.**
- **Además, de manera resaltada se especifica la parte de la información correspondiente al campo seleccionado en la ventana de detalle de paquetes.**



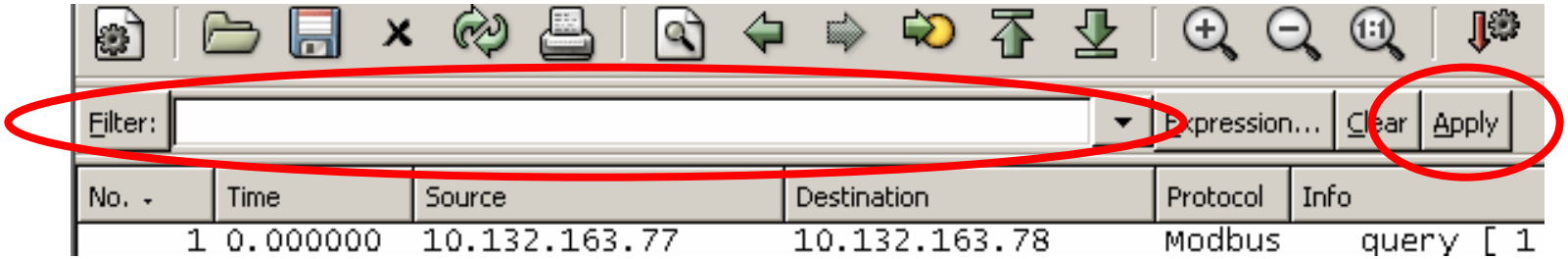

Volver al diagrama de flujo

# 8a. Filtros



**Debido a que podemos realizar capturas de información indiscriminada o poco selectiva en un principio, una vez finalizada ésta captura podemos filtrarla según los parámetros que necesitemos de forma que sólo veamos la información que nos sea relevante.**

**Para ello debemos aplicar el correspondiente filtro y, seguidamente presionar APLICAR (APPLY)**




**Hay múltiples criterios por los que filtrar la información capturada; los más comunes pueden ser:**

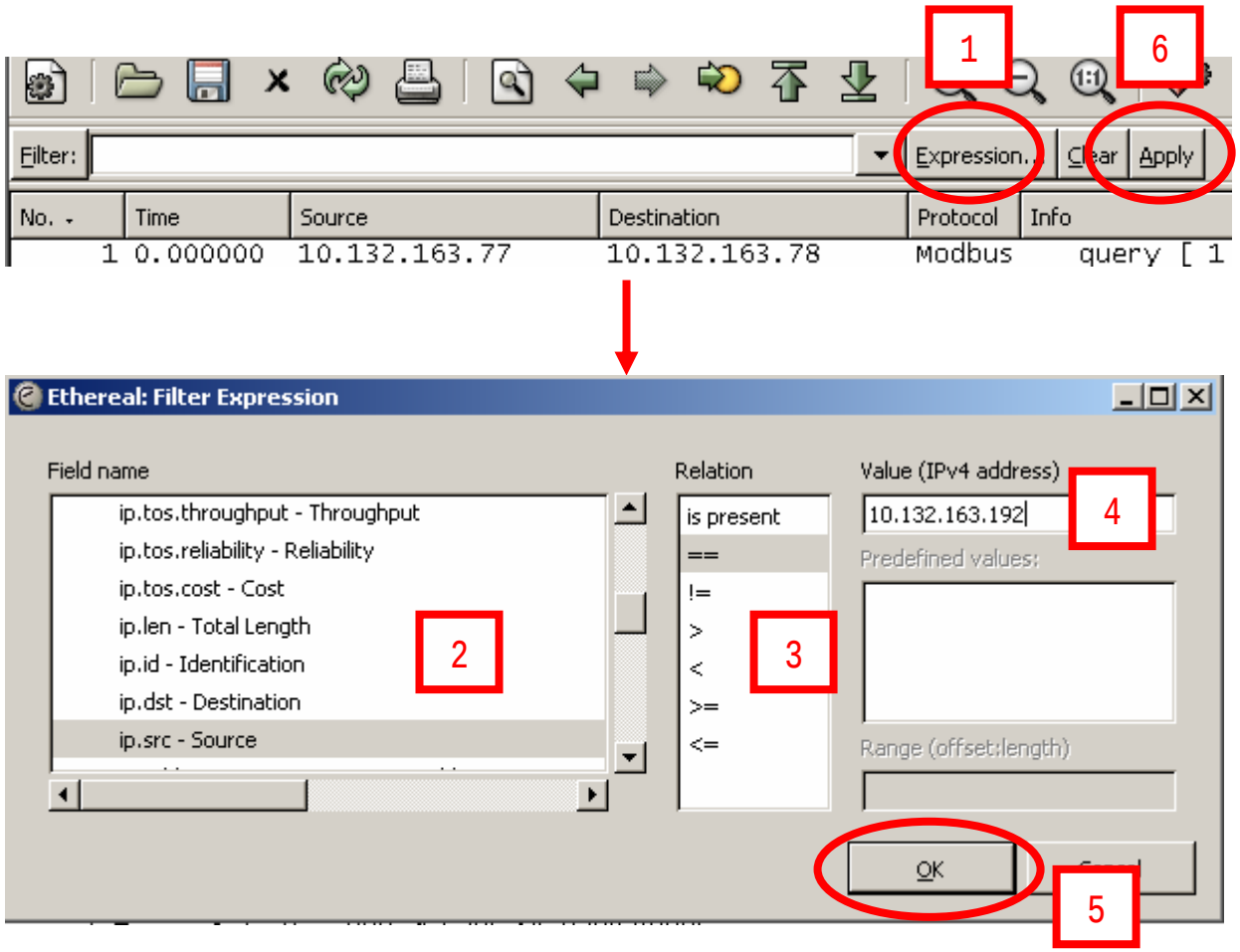
- **Por dirección IP (IP fuente / IP destino)**
- **Por dirección MAC (MAC fuente / MAC destino)**
- **Por protocolo de comunicación (TCP, TCP/ModBus, ARP, ...)**

Volver al diagrama de flujo

# 8b. Filtros: configuración



**¿Cómo configurar un filtro?**




Volver al diagrama de flujo

# 8c. Filtros: configuración



2

**Selección del protocolo y de los atributos por los que se quiere filtrar los paquetes de información.**

**Por ejemplo: IP . ADDR**

**Protocolo: IP** **Atributo: ADDR** → **Dirección IP**

3

**Selección de la relación de filtrado entre el protocolo/atributo seleccionado previamente y un valor determinado**

**Por ejemplo: IP . ADDR ==**

**Dirección IP igual a...**

4

**Valor de filtrado asociado al protocolo / atributo seleccionado.**

**Por ejemplo: IP . ADDR == 10.185.27.161**



**Dirección IP igual a 10.185.27.161**

Volver al diagrama de flujo

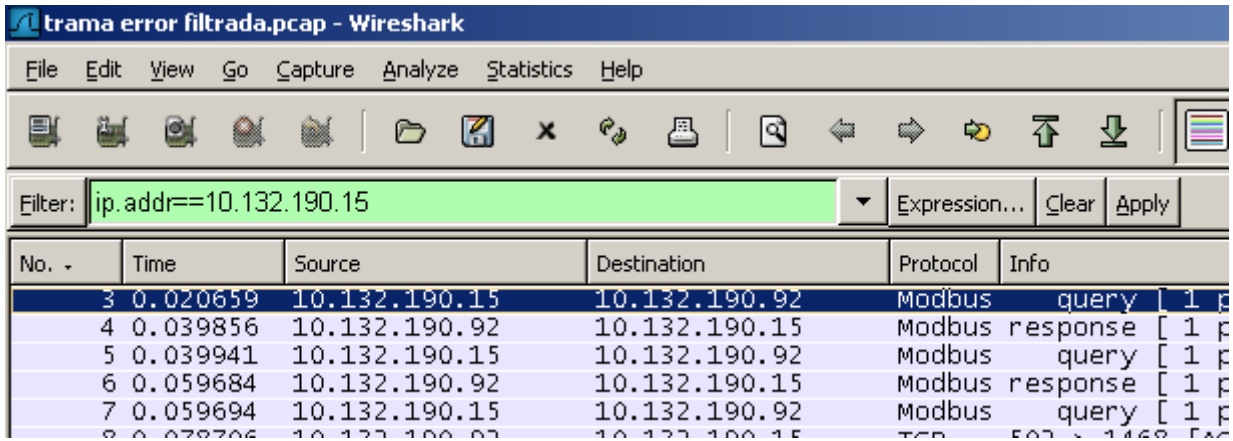
# 8d. Filtros: ejemplos



**Valor de filtrado asociado al protocolo / atributo seleccionado.**

**Por ejemplo: IP . ADDR == 10.185.27.161**

**Dirección IP igual a 10.185.27.161**




**En éste caso, estamos filtrando todas las tramas que tengan asociada la dirección IP 10.132.190.15, bien sea como dirección de origen, bien sea como dirección de destino del mensaje**

Volver al diagrama de flujo

# 8e. Filtros: ejemplos



**Algunos ejemplos de los filtros más comunes:**

- **arp → paquetes con protocolo ARP**

  **Ejemplo: arp**

- **ip.dst == <IP> → paquetes cuya dirección IP destino sea <IP>**

  **Ejemplo: ip.dst == 10.132.163.77**

- **ip.src == <IP> → paquetes cuya dirección IP origen sea <IP>**

  **Ejemplo: ip.src == 10.132.163.78**

- **ip.dst == <IP1> && ip. src == <IP2> → paquetes cuya IP origen sea <IP2> y cuya IP destino <IP1>**

  **Ejemplo: ip.dst == 10.132.163.77 && ip. src == 10.132.163.78**

Volver al diagrama de flujo

# 8f. Filtros: ejemplos



Network Protocol Analyzer

**Algunos ejemplos de los filtros más comunes:**

- **!(ip.addr == <IP>) → paquetes cuya IP no sea <IP>**

  **Ejemplo: !(ip.addr == 10.132.163.78)**

- **eth.addr > <MAC> → paquetes cuya dirección MAC sea superior a <MAC>**

  **Ejemplo: eth.addr > 00.00.54.4F.11.1A**

- **eth.src < <MAC> → paquetes cuya dirección MAC de origen sea inferior a <MAC>**

  **Ejemplo: eth.src < 00.00.54.4F.11.1A**

- **eth.dst == <MAC1> || eth.src == <MAC2> → paquetes cuya MAC origen sea <MAC2> o cuya MAC destino sea <MAC1>**

  **Ejemplo: eth.dst == < 00.00.54.4F.11.1A > || eth.src == < 00.00.80.AD.0F.29 >**

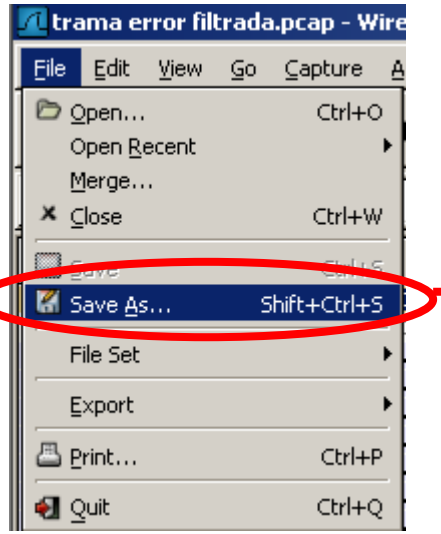
- **modbus_tcp.func.code is present <código MB> → paquetes que contengan el código ModBus <MB>**

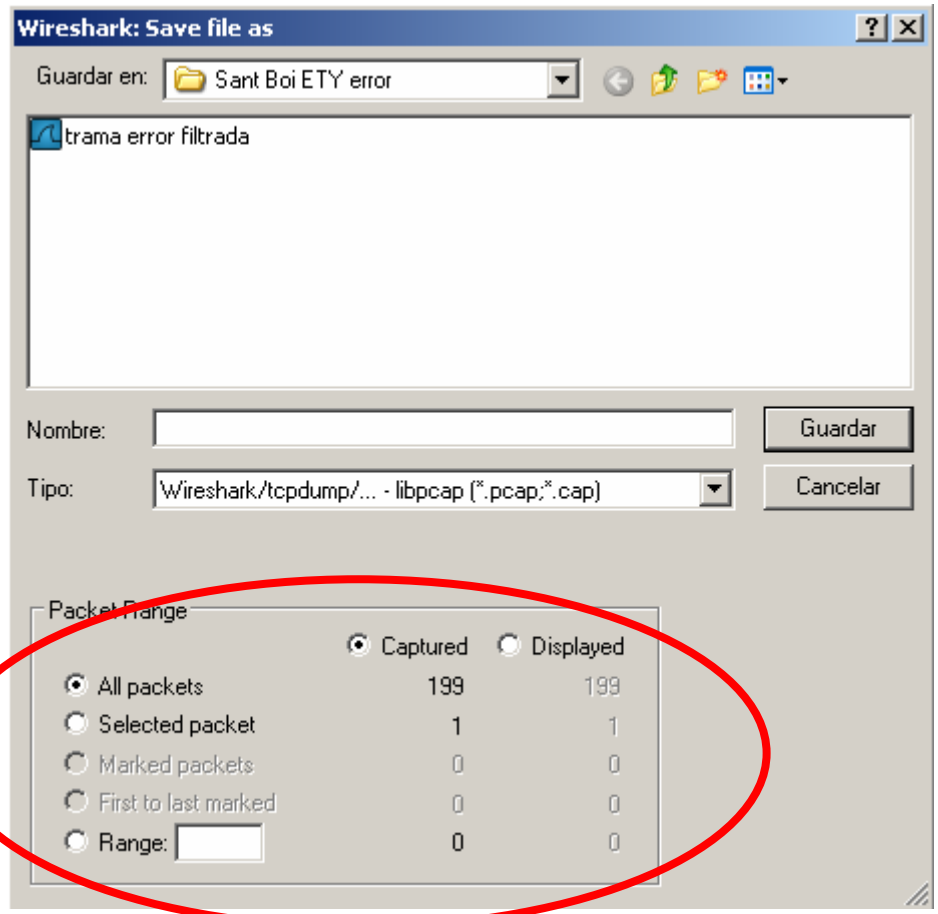
  **Ejemplo: modbus_tcp.func.code is present <03>**

Volver al diagrama de flujo

# 9. Guardado de la captura






**Seleccionar las opciones de captura:**

- **Sólo las tramas visualizadas (después de aplicar filtros)**
- **Todas las tramas capturadas**
- **Las tramas seleccionadas**

Volver al diagrama de flujo

# 10. Posibles errores en la captura



**Posibles causas por las que no se ha podido realizar o no se pueden visualizar correctamente la captura de tramas:**

- **No se pueden capturar tramas porque el elemento de interconexión de dispositivos al cual ha de estar conectado el PC no es un Hub o un Switch gestionable que disponga de servicio 'Port Mirroring' o similar activo en el puerto de conexión del PC.**
  - **Solución: conectar el PC a un Hub o a un Switch gestionable en el cual se ha de habilitar el servicio 'Port Mirroring'.**
  - **Ver diapositivas**

- **No se pueden capturar tramas porque en el software Wireshark no se ha seleccionado el interfaz ethernet del PC correctamente.**
  - **Seleccionar correctamente la tarjeta Ethernet del PC a través de la cual se pretende realizar la captura.**
  - **Ver diapositivas**

- **En el software Wireshark hay filtro activos que impiden visualizar las tramas capturadas.**
  - **Eliminar los filtros activos o modificarlos de manera que nos permita visualizar las tramas deseadas.**
  - **Ver diapositivas**

Volver al diagrama de flujo

# 11. Información y material



**Información y material necesarios en caso de tener que realizar el diagnóstico de una red ethernet con el software Wireshark y / o remontar el caso a un nivel técnico:**

## 1- Hardware

- Hub o Swich gestionable (con capacidad de Port Mirroring)
- Referencia equipo
- Versión  Hardware PV
- Versión Exec módulo Ethernet y CPU
- Versión Software programación

## 2- Entorno de aplicación

- Topología de la Red
- ¿Ha funcionado alguna vez?
- ¿Se ha realizado alguna modificación antes del error?
- Ocurrencia y frecuencia del error
- Se puede reproducir la avería

## 3- Entorno de instalación

- ¿La instalación de los cables es correcta?

## 4- Varios

- Cliente
- Criticidad / impacto avería
- Urgencia solución

## 5- Links

\\10.132.20.10\data$\AUT\Software_Herramientas\Utilidades AUT Imprescindibles\Utilidades Ethernet\Capturador de tramas Ethereal\wireshark-setup-0.99.3.exe

Wireshark: Go deep.

Volver al diagrama de flujo

# Anexo A: Port Mirroring

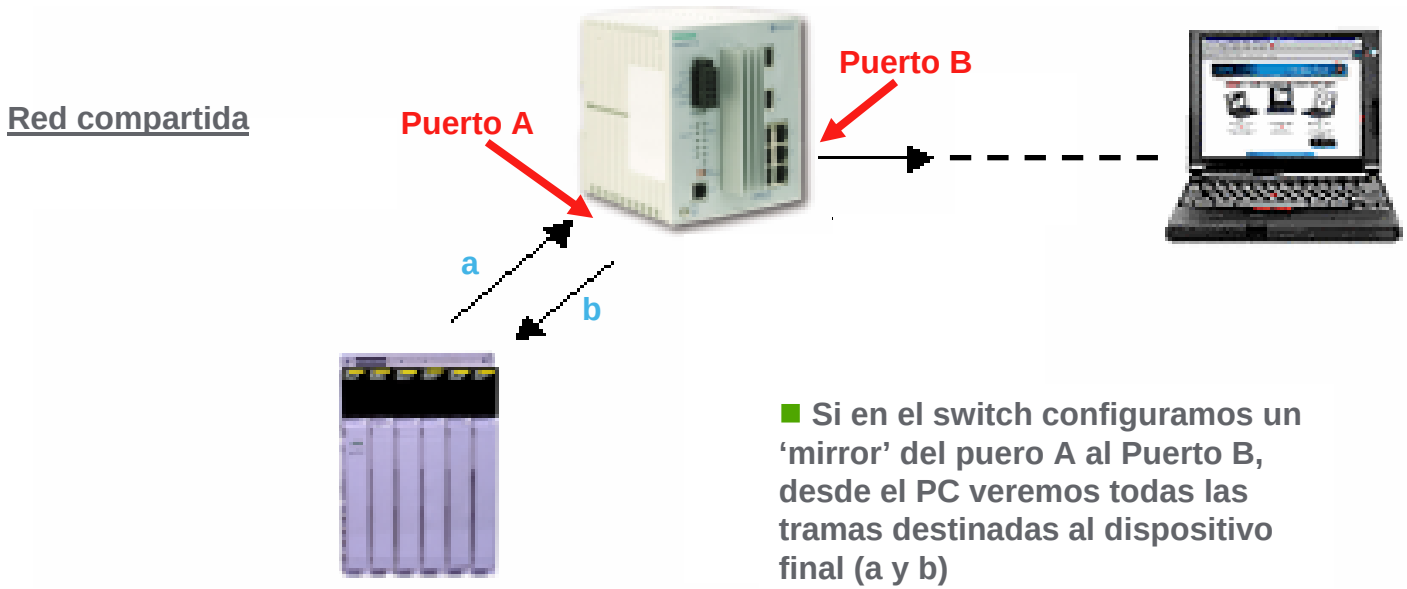


**El servicio 'Port Mirroring' está disponible para su configuración en gran parte de los switches gestionables del mercado.**

**Su función es la de reproducir (hacer un 'mirror') el tráfico de un puerto (puerto A) del swich a otro puerto (puerto B) del mismo switch.**

**De ésta manera en el primer puerto (puerto A) tendremos el dispositivo cuyas tramas de entrada o salida queremos capturar y en en segundo puerto (puerto B) tendremos el PC desde el que se realiza ésta captura.**

**Hub o Switch con opción 'Port Mirroring' activa**




- **Si en el switch configuramos un 'mirror' del puero A al Puerto B, desde el PC veremos todas las tramas destinadas al dispositivo final (a y b)**

Volver al diagrama de flujo

# *Make the most of your energy*

www.schneiderelectric.es