



ALUMNO JAVIER ISAC LÓPEZ HERNÁNDEZ

PROFESOR: ISMAEL JIMENEZ SÁNCHEZ

INGENIERÍA EN SISTEMAS COMPUTACIONALES

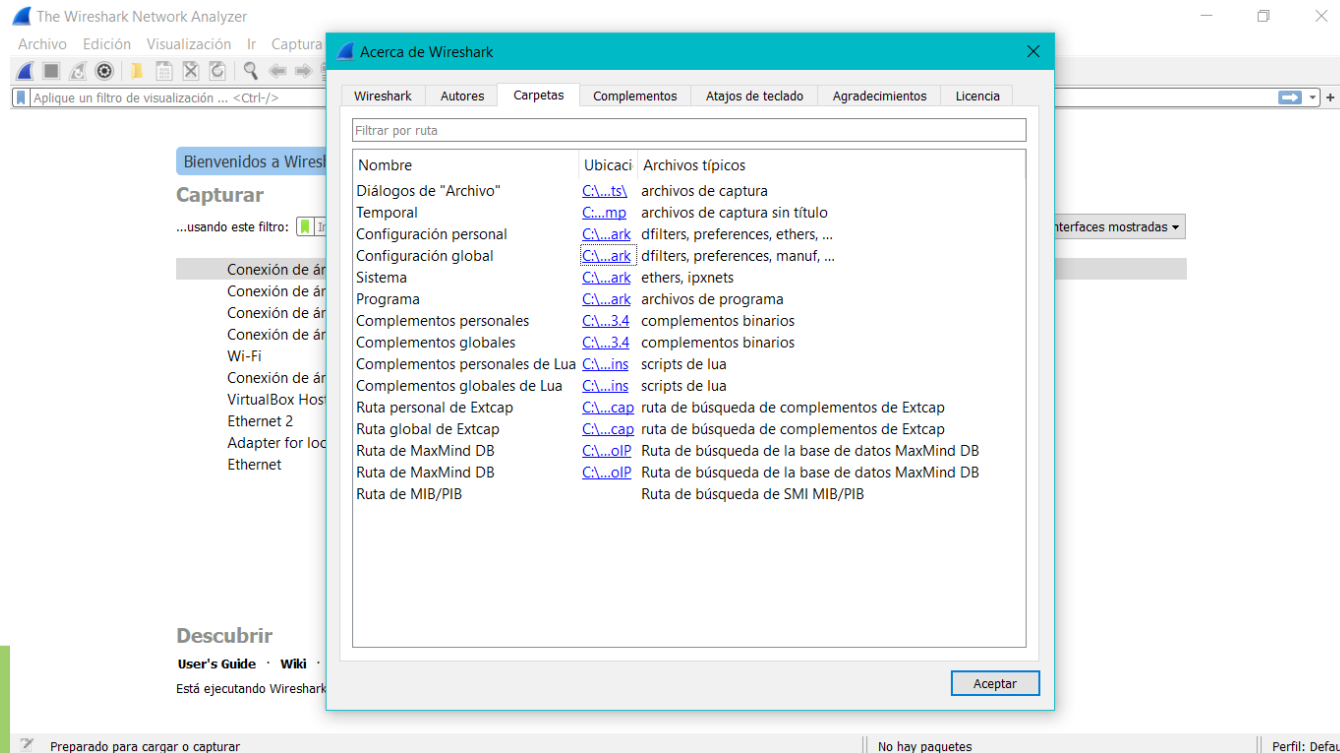
FUNDAMENTOS DE TELECOMUNICACIONES

CAPITULO 5: DEFINIR PREFERENCIAS GLOBALES Y PERSONALES



Preferencias globales y personales

En Wireshark existen las configuraciones globales y personales. Para poder ver la ubicación de las carpetas de la configuración global y personal nos dirigimos en la ventana de acerca de Wireshark, ahí podremos ver los directorios.



Preferencias globales y personales

Puede compartir estos archivos con otros simplemente enviándoles el archivo.

La nueva configuración estará disponible después el receptor coloca los archivos en su carpeta de configuración personal y reinicia Wireshark. Hay que tener cuidado de compartir archivos de configuración personal, como el archivo de preferencias, que contiene información sobre la estructura del directorio y el archivo reciente que contiene el directorio más reciente que visitó.



Se puede crear un perfil de configuraciones

Puede crear un perfil que utilice sus propios archivos de configuración. Por ejemplo se puede crear un perfil WLAN que incluya filtros, colores y columnas que lo ayuden a analizar Tráfico WLAN.



Algunas preferencias globales

- Entradas de lista máxima "Abrir recientes" (aumente este número a 30)
- Diseño del panel (coloque los paneles Detalles del paquete y Bytes del paquete uno al lado del otro)
- Captura | Actualizar la lista de paquetes en tiempo real (desactivar para reducir la sobrecarga)
- Configuración de resolución de nombres (habilite la resolución de nombres de red con precaución)
- Expresiones de filtro (agregue botones de filtro de pantalla clave al área de filtro de pantalla)
- Varias configuraciones de protocolo (deshabilitar la validación de suma de comprobación de IP para la descarga de tareas)



Cuando se actualiza Wireshark

se le solicita que desinstale la versión anterior. Durante el proceso de desinstalación puede elegir los componentes que desea guardar.

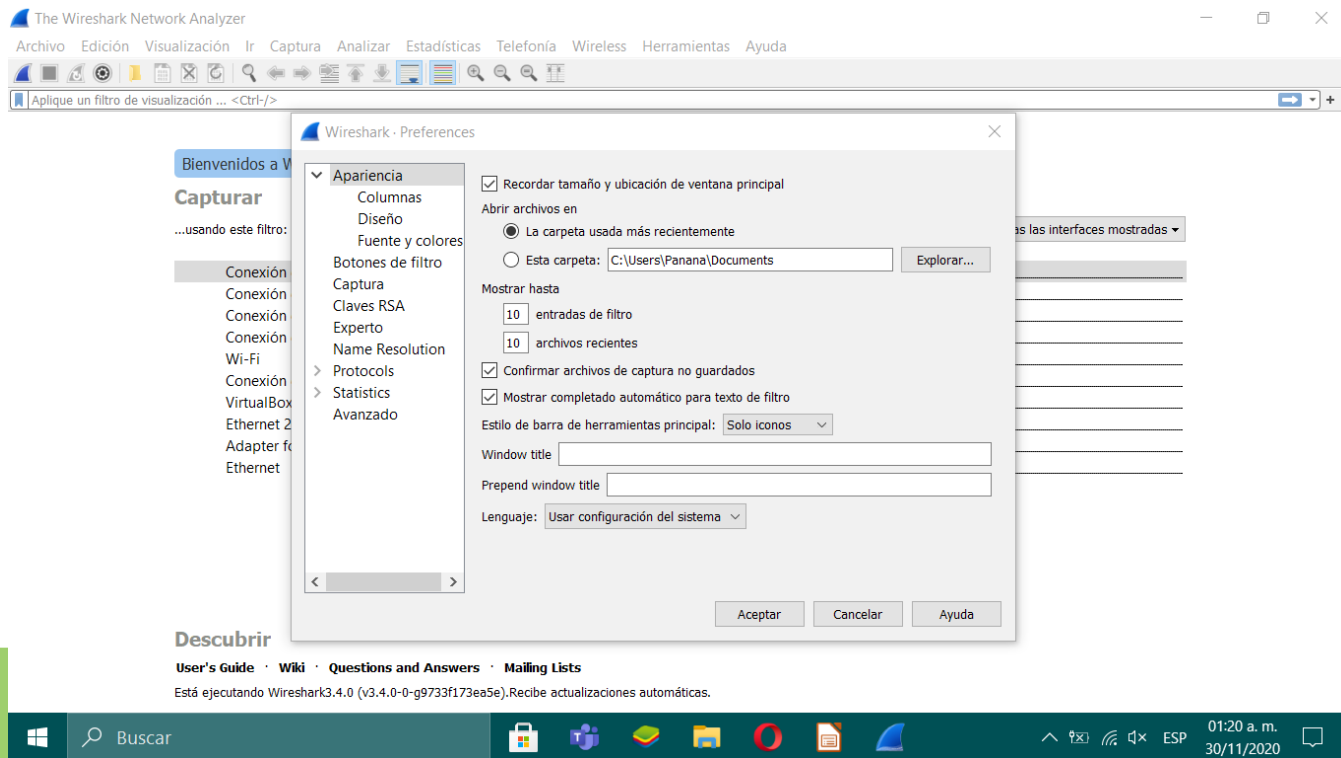
De forma predeterminada, Wireshark mantiene su configuración personal durante el proceso de actualización, pero anula la configuración global.

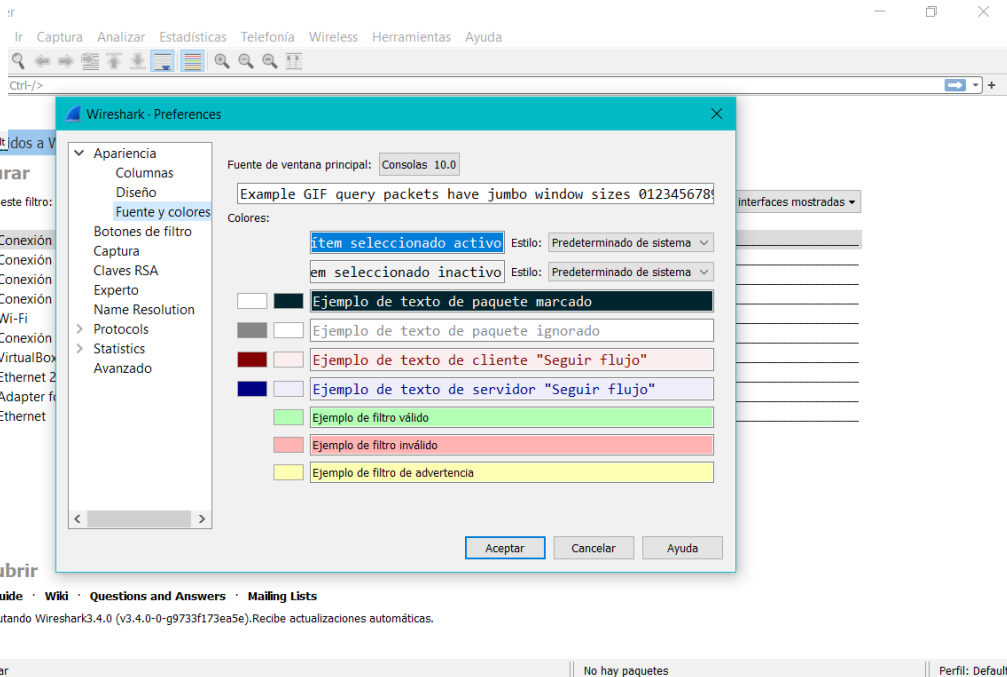
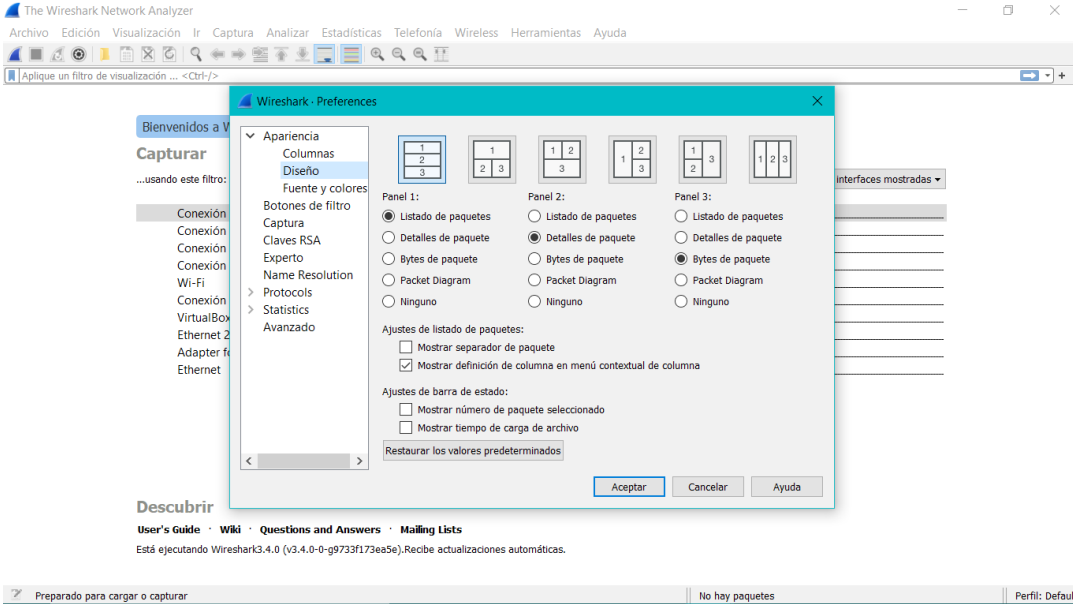
Después de instalar Wireshark, considere hacer una copia del archivo de preferencias original en caso de que necesite restaurarlo en algún momento en el futuro sin pasar por una reinstalación.



Personalizar la configuración de interfaz de usuario.

Seleccione Editar | Preferencias o haga clic en el icono de Preferencias en la barra de herramientas principal. La configuración de la interfaz de usuario El área contiene cinco secciones, la sección principal de la interfaz de usuario, diseño, columnas, fuentes y colores





Entrada máxima de lista

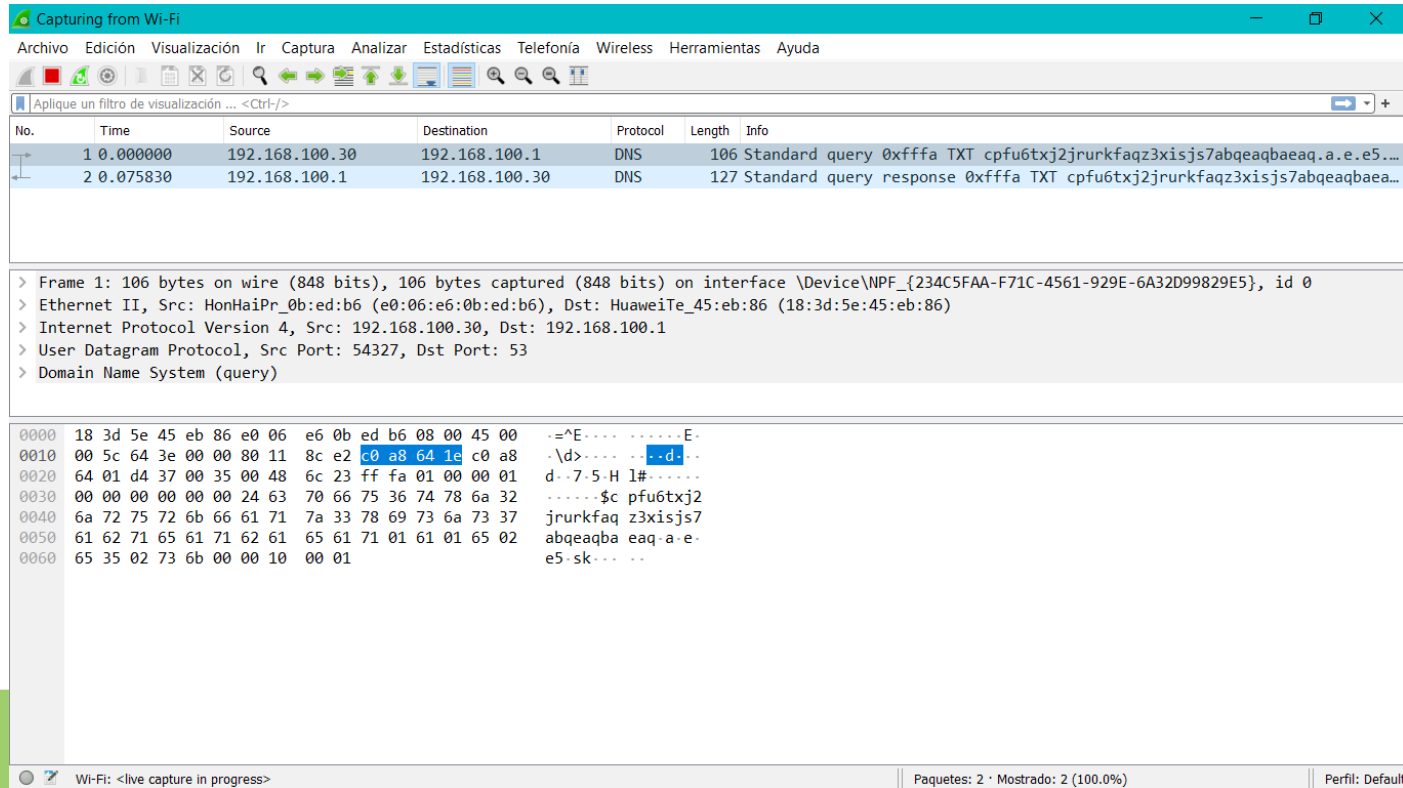
"Pantalla de filtro" controla el número de filtros de pantalla creados recientemente que deberían aparecer al hacer clic en la flecha desplegable junto a la pantalla.

"Abrir reciente" controla la cantidad de archivos de seguimiento abiertos recientemente que Wireshark aparece cuando selecciona Archivo | Recientemente abierto.



Panel de configuraciones

La configuración predeterminada del panel de Wireshark muestra tres paneles apilados, incluido el panel Lista de paquetes, el Panel de detalles y panel de bytes de paquetes.



The screenshot displays the Wireshark network protocol analyzer interface, titled "Capturing from Wi-Fi". The menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The toolbar contains various icons for file operations, capture control, and analysis.

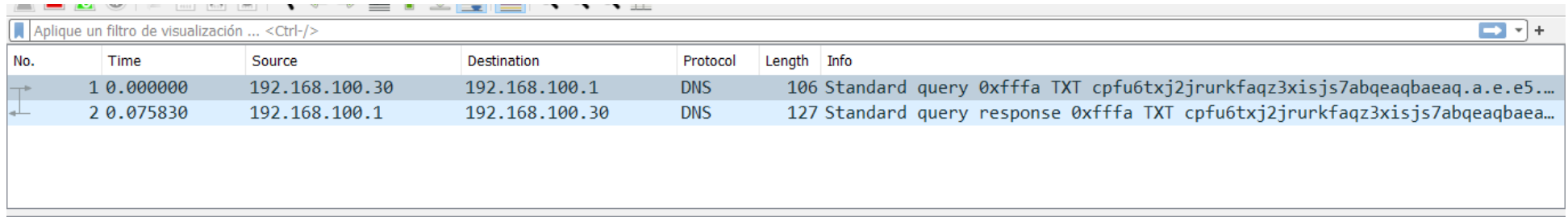
The main display area is divided into three stacked panels:

- Lista de paquetes (Packet List):** Shows a table of captured packets. The first packet is a DNS Standard query from 192.168.100.30 to 192.168.100.1. The second packet is a DNS Standard query response from 192.168.100.1 to 192.168.100.30.
- Panel de detalles (Packet Details):** Displays the hierarchical structure of the selected packet (Frame 1). It shows Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).
- Panel de bytes de paquetes (Packet Bytes):** Shows the raw bytes of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates "Wi-Fi: <live capture in progress>", "Paquetes: 2 · Mostrado: 2 (100.0%)", and "Perfil: Default".

Columnas

- Número de paquete (este valor nunca cambia para cada paquete)
- Hora: Configuración basada en Ver | Configuración del formato de visualización de la hora
- Fuente: dirección de origen de la capa más alta identificada (hardware / red)
- Destino: dirección de destino de la capa más alta identificada (hardware / red)
- Protocolo: protocolo de capa más alto identificado
- Longitud: longitud del marco [58]
- Información: detalles específicos del protocolo para cada paquete



A screenshot of a network packet capture tool interface. At the top, there is a search bar with the text "Aplice un filtro de visualización ... <Ctrl-/>". Below this is a table with columns: No., Time, Source, Destination, Protocol, Length, and Info. The table contains two rows of data. The first row shows a packet number 1, time 0.000000, source 192.168.100.30, destination 192.168.100.1, protocol DNS, length 106, and info "Standard query 0xffffa TXT cpfu6txj2jrurkfaqz3xisjs7abqeaqbaeq.a.e.e5....". The second row shows a packet number 2, time 0.075830, source 192.168.100.1, destination 192.168.100.30, protocol DNS, length 127, and info "Standard query response 0xffffa TXT cpfu6txj2jrurkfaqz3xisjs7abqeaqbaeq....".

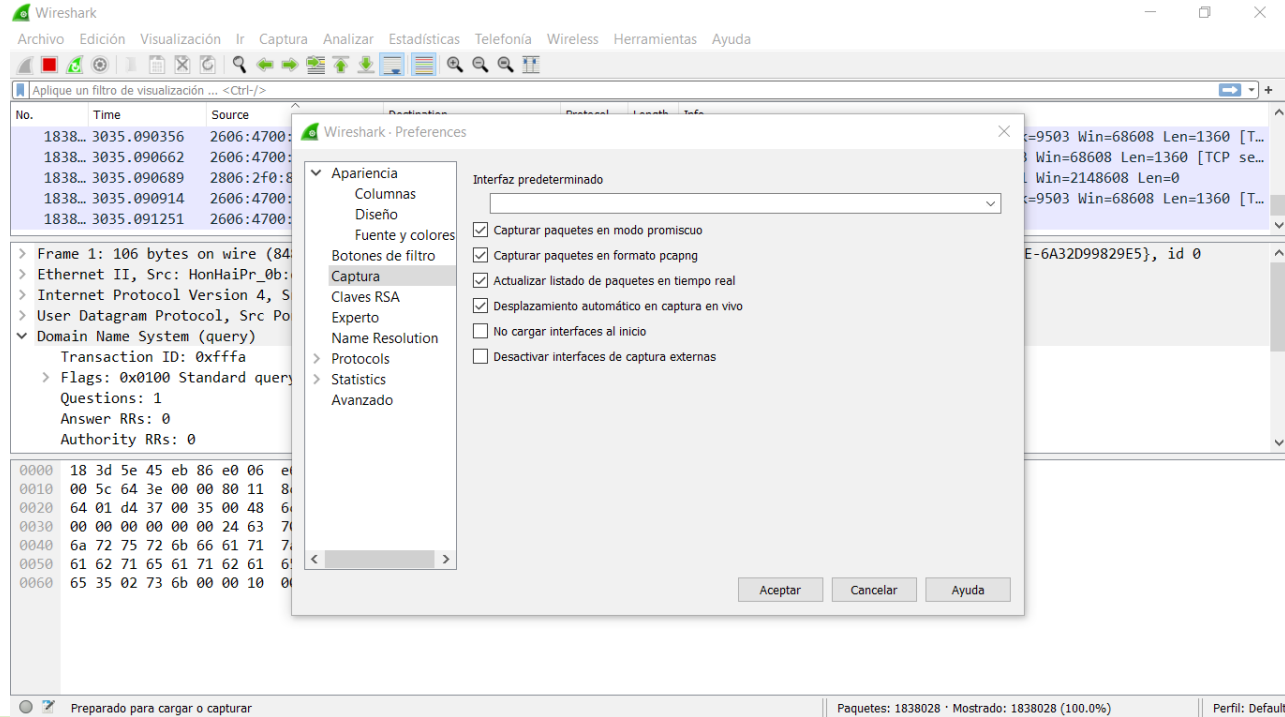
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 1 | 0.000000 | 192.168.100.30 | 192.168.100.1 | DNS | 106 | Standard query 0xffffa TXT cpfu6txj2jrurkfaqz3xisjs7abqeaqbaeq.a.e.e5.... |
| 2 | 0.075830 | 192.168.100.1 | 192.168.100.30 | DNS | 127 | Standard query response 0xffffa TXT cpfu6txj2jrurkfaqz3xisjs7abqeaqbaeq.... |

Seleccione Editar | Preferencias | Columnas y seleccione Agregar para elegir una de las columnas predefinidas para agregar a la Lista de paquetes



Preferencias de captura

Las preferencias de captura se utilizan para seleccionar una interfaz predeterminada para la captura y aplicar alguna configuración a esa interfaz.



Ver el trafico en tiempo real.

Esta característica le permite para comenzar a analizar de inmediato, mientras captura. Esta característica puede afectar negativamente a Wireshark rendimiento en una red ocupada.

Esta característica puede afectar negativamente a Wireshark rendimiento en una red ocupada.



Desplazarse automáticamente durante la captura.

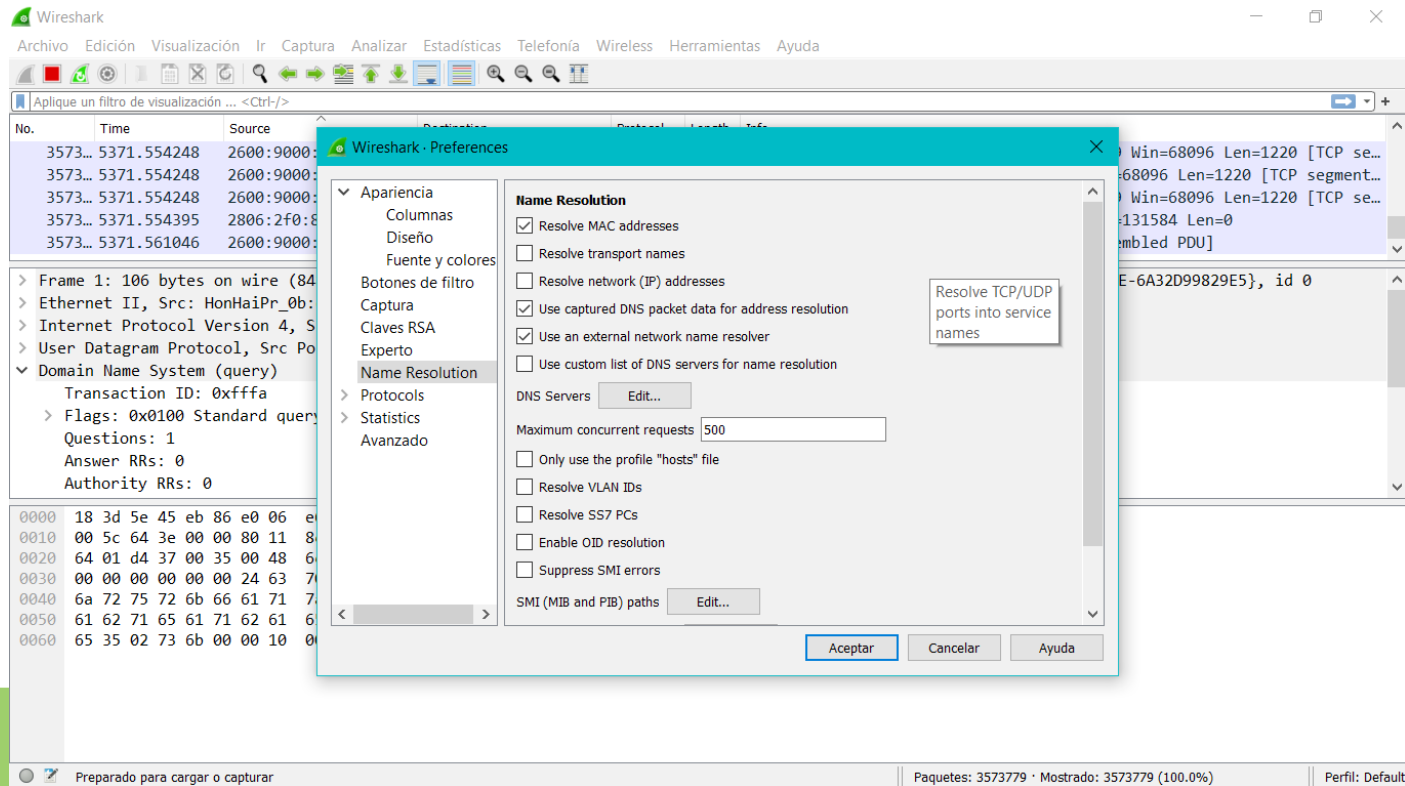
En una red muy ocupada, probablemente no podrá seguir el ritmo de los paquetes a medida que se desplazan rápidamente en la pantalla. Esta función puede resultar útil si ha aplicado un filtro de captura que limita la cantidad de paquetes capturado.

Esta función también puede afectar negativamente al rendimiento de Wireshark en una red ocupada.



Resolución de nombres

Wireshark ofrece muchas opciones para la resolución de nombres. Las opciones más utilizadas son el nombre MAC resolución, resolución de nombres de transporte y resolución de nombres de red.



Resolver información SNMP.

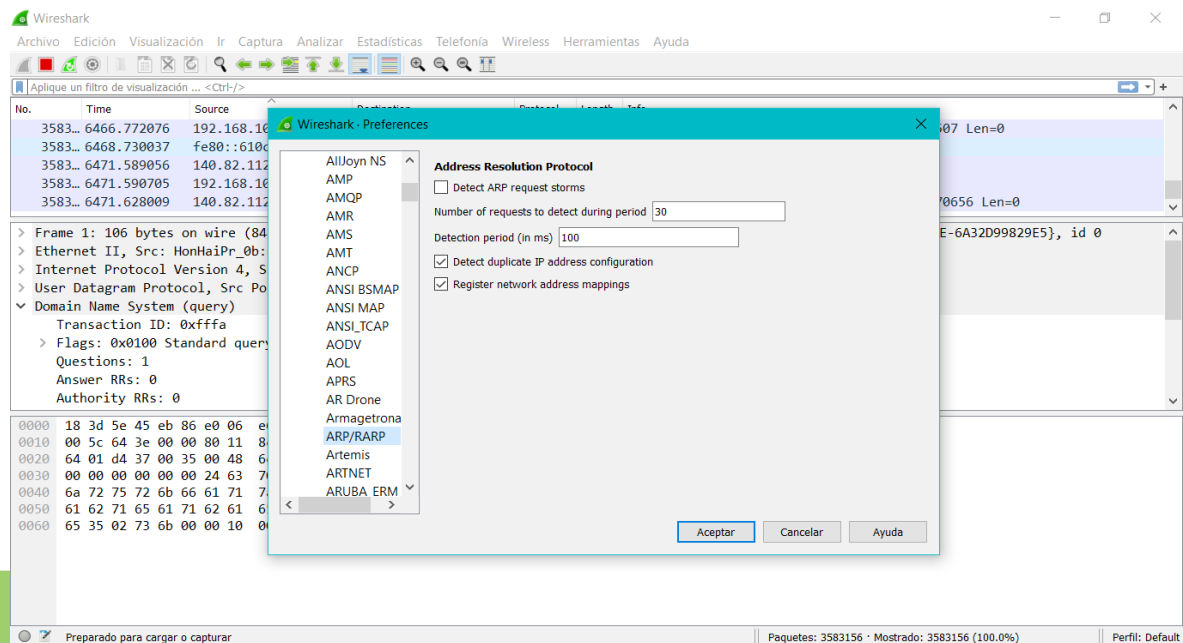
En la configuración de Resolución de nombres, habilite la resolución OID. Los archivos SNMP MIB (Management Information Base) se utiliza para resolver números ASN1 (Notación de sintaxis abstracta 1) en nombres de objetos en comunicaciones SNMP. Los Los módulos MIB están contenidos en el directorio \snmp\mibs en el directorio de archivos de programa Wireshark.



Detecte direcciones IP duplicadas y tormentas ARP.

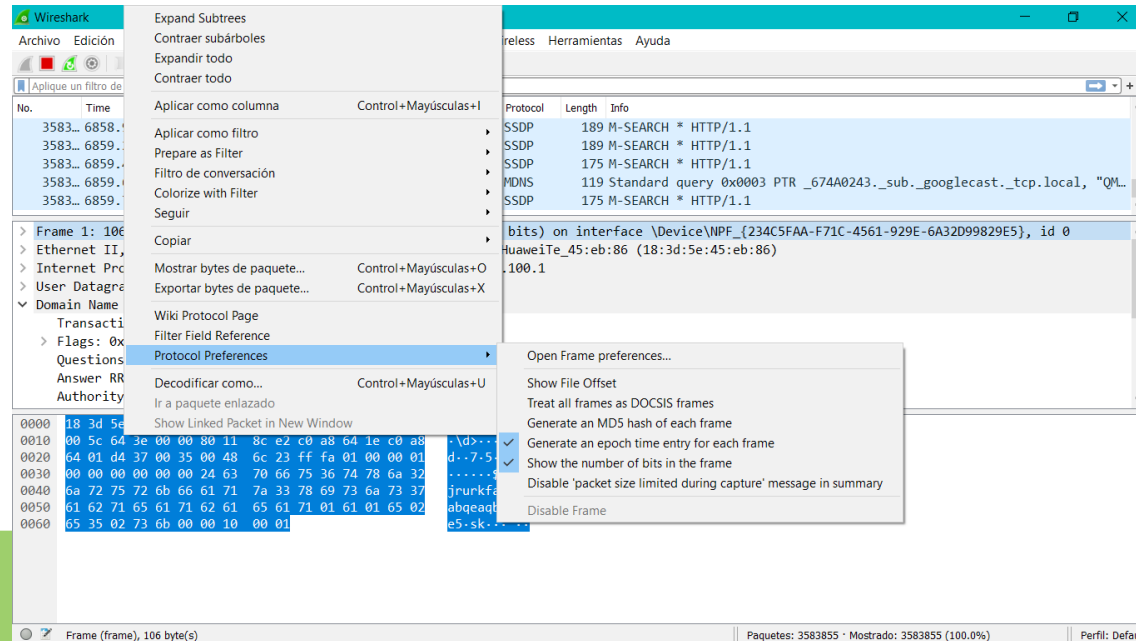
La detección de direcciones IP duplicadas está activada de forma predeterminada. Para habilitar la detección de tormentas ARP, debe definir el número de Paquetes ARP para detectar durante un período de detección específico.

Wireshark busca 30 paquetes ARP que ocurren dentro de los 100 ms antes de desencadenar un evento.



Configure los ajustes del protocolo de manera rápida.

Si se desea cambiar rápidamente la configuración del protocolo mientras examina un paquete, haga clic derecho en una sección de protocolo en el panel Detalles del paquete (por ejemplo, Ethernet, IP, TCP y HTTP). Se selecciona Preferencias de protocolo y entonces ya podemos configurar.



Gracias :)

