

Wireshark

Módulo profesional: Planificación y Administración de Redes

Ciclo Formativo: C.F.G.S. Administración de Sistemas Informáticos en Red

Curso: 1º

Profesor: Anabel Serradilla Fernández

¿Qué es?

Wireshark, antes denominado Ethereal, es un “packet sniffer”, un capturador de paquetes que capta todo:

- Si la red es cableada coge todo lo que llega o sale por tu cable
- Si es WiFi captura todo

En general, las herramientas analizadoras de tráfico pueden resultar de gran utilidad para detectar, analizar y correlacionar tráfico identificando las amenazas de red para, tras su estudio, limitar su impacto.

Los paquetes de datos pueden verse en tiempo real o pueden guardarse en archivos para analizarlos sin conexión.

Es una herramienta muy útil. ¡No utilizarla para cometer delitos!

¿Qué podemos ver con Wireshark?

Algunas de las cosas que podemos ver con esta herramienta:

- Ver qué está pasando cuando algo en la red no funciona como debería y ya has probado todo lo demás
- Detectar intrusos y comportamientos no deseables en la red
- Detectar ataques


Para instalarla:

- Windows: lo descargas de la web oficial y se instala con un asistente
- Linux (Debian) con los comandos: `sudo apt-get update`
`sudo apt-get install Wireshark`

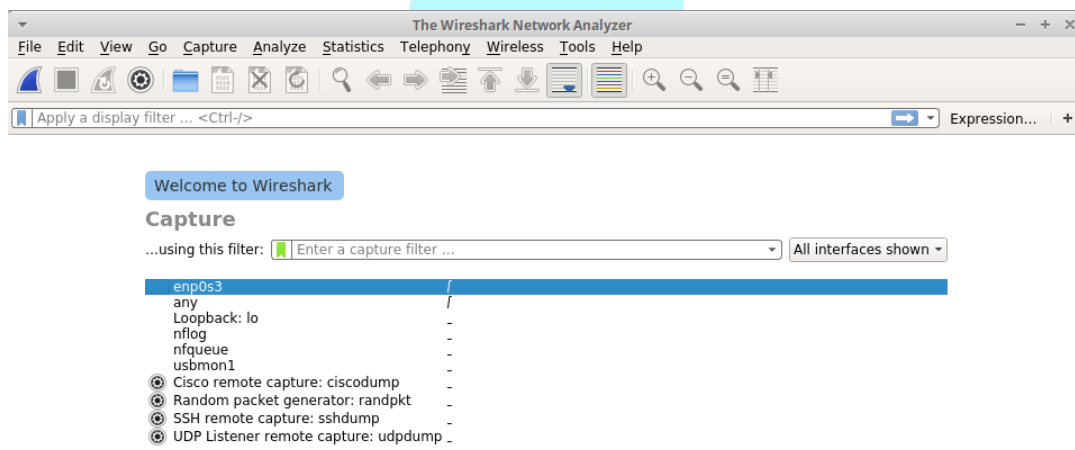
¿Cómo se usa?

En los equipos de clase ya está instalada. Para ejecutarla el comando es:

`sudo /usr/bin/wireshark`

En un momento concreto Wireshark puede estar capturando tráfico o detenido. El botón de capturar difiere ligeramente de unas versiones a otras, pero está en la parte superior izquierda. 

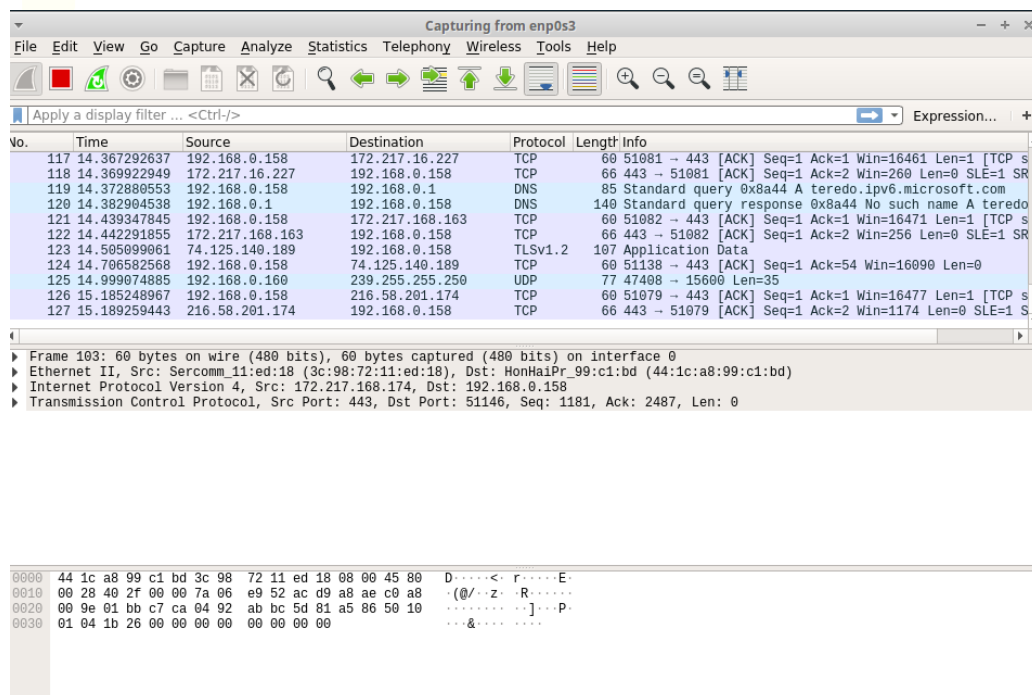
Para empezar a trabajar con esta aplicación el primer paso es elegir la interfaz adecuada en la que se quieren capturar los paquetes.



Por defecto Wireshark se ejecuta en “modo promiscuo”, lo que significa que captura cualquier paquete que sea visible en esa interfaz, independientemente de si está destinado a ella o no.

La pantalla principal se divide en tres ventanas horizontales:

- La ventana superior lista los paquetes capturados.
- La ventana intermedia muestra en detalle el paquete seleccionado en la primera ventana.
- La ventana inferior muestra el valor de los datos del paquete en HEX y ASCII.



Ventana superior

Ventana intermedia

Ventana inferior

Lista de paquetes

Cada paquete tiene su propia línea con la siguiente información:

Hora (Time): marca de tiempo en la que se capturó el paquete. El formato por defecto de esta marca temporal muestra la cantidad de segundos transcurridos desde que se comenzó la captura. Se puede modificar en Ver/Formato de visualización de hora.

Fuente (Source): dónde se originó el paquete.

Destino (Destination): dirección a la que se envía el paquete.

Protocolo (Protocol): el nombre del protocolo del paquete, como por ejemplo TCP.

Longitud (Length): la longitud del paquete en bytes.

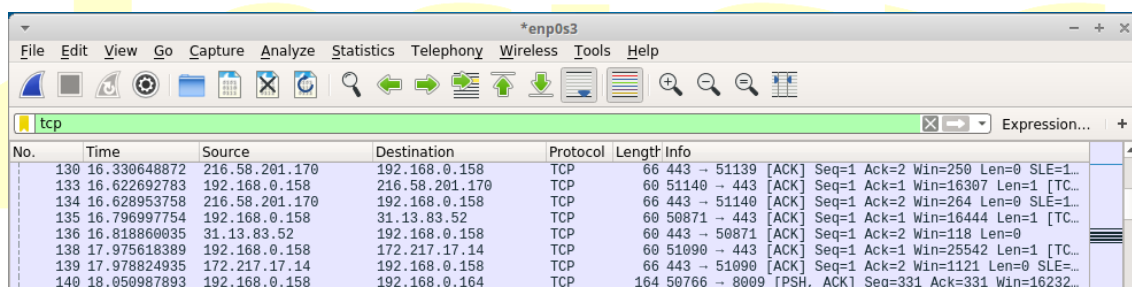
Información (Info): se muestran aquí detalles adicionales sobre el paquete. El contenido de esta columna varía mucho dependiendo del contenido del paquete.

Mientras la captura, se pueden aplicar filtros para mostrar en pantalla la información que necesitamos. Independientemente de los filtros seleccionados Wireshark siempre captura todo, aunque solo muestre lo que se seleccione con los distintos filtros.

Filtros

Algunos de los filtros más importantes son:

- ARP: Muestra el tráfico de tipo ARP. Útil para aprender cómo funciona y detectar ataques de tipo envenenamiento ARP, flooding, etc.
- DNS: Muestra el tráfico de tipo DNS (servidor de nombres). Útil para ver a qué servidores se quiere acceder, detectar problemas de conexión, etc.
- ICMP: Muestra tráfico de tipo ICMP, como “ping”
- ip.addr==a.b.c.d: Muestra todos los paquetes que vienen o van de o a la IP a.b.c.d (¡OJO!, muestra el tráfico si llega al cable o interfaz seleccionado)
- ip.src==a.b.c.d: Muestra el tráfico que sale de la IP a.b.c.d
- ip.dst==a.b.c.d: Muestra el tráfico que va a la IP a.b.c.d
- FTP: Muestra el tráfico de tipo FTP (File transfer protocol). Útil para detectar problemas de conexión con este protocolo.
- HTTP: Muestra el tráfico HTTP (tráfico Web)
- SSH, TELNET, POP3, IMAP, ...



No.	Time	Source	Destination	Protocol	Length	Info
130	16.330648872	216.58.201.170	192.168.0.158	TCP	66	443 → 51139 [ACK] Seq=1 Ack=2 Win=250 Len=0 SLE=1...
133	16.622692783	192.168.0.158	216.58.201.170	TCP	60	51140 → 443 [ACK] Seq=1 Ack=1 Win=16307 Len=1 [TC...
134	16.628953758	216.58.201.170	192.168.0.158	TCP	66	443 → 51140 [ACK] Seq=1 Ack=2 Win=264 Len=0 SLE=1...
135	16.796997754	192.168.0.158	31.13.83.52	TCP	60	50871 → 443 [ACK] Seq=1 Ack=1 Win=16444 Len=1 [TC...
136	16.818860035	31.13.83.52	192.168.0.158	TCP	60	443 → 50871 [ACK] Seq=1 Ack=2 Win=118 Len=0
138	17.975618389	192.168.0.158	172.217.17.14	TCP	60	51090 → 443 [ACK] Seq=1 Ack=1 Win=25542 Len=1 [TC...
139	17.978824935	172.217.17.14	192.168.0.158	TCP	66	443 → 51090 [ACK] Seq=1 Ack=2 Win=1121 Len=0 SLE=...
140	18.050987893	192.168.0.158	192.168.0.164	TCP	164	50766 → 8009 [PSH, ACK] Seq=331 Ack=331 Win=16232...

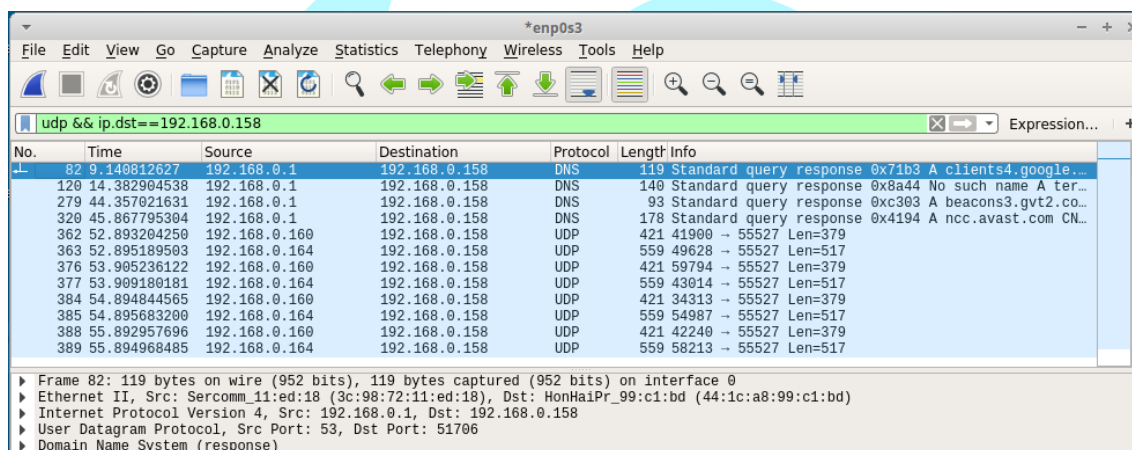
Se pueden configurar dos tipos de filtro:

- Filtros de pantalla o visualización: son los que se aplican sobre una captura para que se muestren aquellos que coincidan con el filtro indicado.
- Filtros de captura: se configuran con antelación a la captura para que Wireshark solo capture los paquetes que coincidan con el filtro indicado.

Wireshark proporciona filtros predefinidos, tanto de uno como de otro tipo.

Se pueden combinar filtros con las siguientes operaciones:

- FILTRO1 && FILTRO2: Se muestran los paquetes que cumplen a la vez los dos filtros
- FILTRO1 || FILTRO2: Se muestran los paquetes que cumplen cualquiera de los dos filtros (uno, el otro o los dos)
- Combinaciones, por ejemplo: (FILTRO1 && FILTRO2) || FILTRO3



Una vez que se han capturado los paquetes se podrá ver la información que contiene en la ventana intermedia. Esta información depende del tipo de paquete que sea, aunque en la mayor parte de los casos el aspecto que presenta es similar al de la imagen:

