Wireshark

Gustavo Rivas y Luis Suárez

¿Qué es Wireshark?

Es un analizador de paquetes gratuito y open source.

Analizador de paquetes

Software que nos permite interceptar y registrar el tráfico que nos podemos encontrar en la red.

¿Para que sirve?

- Solucionar problemas en redes.
- Analizar redes.
- Desarrollo de software y protocolos.
- Educación.

Funcionalidades

- Licencia GPL.
- Disponible para Linux, Windows y Mac.
- Muy robusto.
- Reconstrucción de sesiones TCP.
- Compatible con más de 480 protocolos.
- Lee archivos de captura de más de 20 productos.
- Permite generar estadísticas.
- Tshark.
- Gran capacidad de filtrado.

Filtrado

- Filtros de captura.
- Filtros de visualización.

¿Qué no hace Wireshark?

- No detecta si hay alguien infiltrado en tu red.
- No manipula objetos de la red.
- No permite mandar paquetes.