1) Qué es un analizador de protocolos?

Un analizador de protocolos (también llamado sniffers) es una herramienta que sirve para desarrollar y depurar protocolos y aplicaciones de red. Permite al ordenador capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado, es decir que se emplea para observar los mensajes que intercambian dos entidades en comunicación a través de una red. Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP...) y muestra al usuario la información decodificada. Gracias a estos analizadores, se puede ver la relación que hay entre diferentes protocolos, para así, comprender mejor su funcionamiento. Son una herramienta de ayuda para los administradores de redes.

2) Comparar 2 analizadores: Wireshark y TCPDUMP.

**Wireshark** es un analizador de protocolos de red, con interfaz gráfico, que nos permitirá capturar las tramas que entran y salen de nuestro ordenador para luego "diseccionarlas" y estudiar el contenido de los mismas. Wireshark, emplea la misma librería de captura de paquetes (libpcap) que otros sniffers conocidos, como tcpdump, aunque es capaz de leer muchos otros tipos de formato de captura. Además es un software de libre distribución que puede correr en distintas plataformas (Windows, Linux/Unix, y Mac). Pero, probablemente, lo más destacable sea su interfaz gráfica y la potente capacidad de filtrado que presenta.

**TCPDUMP:** Es una herramienta de consola de comandos. La librería de captura de tcpdump es la misma que emplea Wireshark, y la sintaxis de filtrado es muy similar. Existe una adaptación de tcpdump para los sistemas Microsoft Windows que se llama WinDump y que hace uso de la biblioteca Winpcap.