WIRESHARK

Wireshark es una herramienta de análisis de protocolos de red de código abierto que permite capturar y examinar el tráfico de red en detalle. En este documento, se explicará cómo funciona la aplicación y cómo se puede utilizar para analizar el tráfico de red.

Descarga e instalación de Wireshark

1. Para empezar a utilizar Wireshark, lo primero que se debe hacer es descargar e instalar la aplicación en el equipo. Wireshark está disponible para Windows, Mac OS X y Linux, y se puede descargar de forma gratuita desde la página web oficial.

Una vez descargado, se debe instalar la aplicación en el equipo y ejecutarla para empezar a capturar y analizar el tráfico de red.

Captura de paquetes de red

1. Una vez que se ha iniciado Wireshark, se puede empezar a capturar el tráfico de red en el equipo. Para hacer esto, se debe seleccionar la interfaz de red que se desea capturar en la lista de interfaces disponibles en la ventana principal de Wireshark.

Una vez seleccionada la interfaz, se puede iniciar la captura de paquetes haciendo clic en el botón "Start" o presionando la tecla F5. Wireshark comenzará a capturar todos los paquetes de red que pasen por la interfaz seleccionada.

Análisis de paquetes de red

1. Una vez que se han capturado los paquetes de red, se pueden analizar en detalle utilizando las diversas herramientas de análisis de Wireshark.

La ventana principal de Wireshark muestra una lista de todos los paquetes capturados, junto con información detallada sobre cada paquete, como el tiempo de captura, la dirección IP de origen y destino, el protocolo utilizado y el contenido del paquete.

Al hacer clic en un paquete en la lista, se puede ver una vista detallada del contenido del paquete en la ventana de detalles de paquete de Wireshark. Esta vista muestra información detallada sobre cada campo del paquete, incluyendo el encabezado y los datos del cuerpo.

Wireshark también proporciona una variedad de herramientas de análisis avanzado, como filtros de paquete, estadísticas de red y gráficos de flujo, que permiten analizar y visualizar el tráfico de red en detalle.

Filtros de paquete

1. Los filtros de paquete de Wireshark permiten filtrar y analizar los paquetes de red en función de ciertos criterios, como la dirección IP de origen y destino, el protocolo utilizado, el puerto de origen y destino y el contenido del paquete.

Para aplicar un filtro de paquete, se puede ingresar el filtro deseado en la barra de filtro en la parte superior de la ventana principal de Wireshark y presionar la tecla Enter. Wireshark filtrará automáticamente la lista de paquetes para mostrar solo los paquetes que cumplen con los criterios especificados.

Estadísticas de red

1. Wireshark también proporciona estadísticas detalladas sobre el tráfico de red capturado, incluyendo información sobre los protocolos utilizados, los hosts y puertos más activos, la duración de la captura y la tasa de transferencia de datos.

Para ver las estadísticas de red, se debe seleccionar la opción "Statistics" en la barra de herramientas de Wireshark y seleccionar el tipo de estadística deseada en el menú desplegable.

1. Gráficos

Wireshark también proporciona herramientas de gráficos que permiten visualizar el tráfico de red en diferentes formatos, como gráficos de flujo, gráficos de barras y gráficos de pastel.

Los gráficos de flujo muestran el tráfico de red entre dos hosts específicos en forma de diagrama de flujo, lo que permite identificar patrones y tendencias en el tráfico de red.

Los gráficos de barras y pastel muestran información estadística sobre el tráfico de red, como la cantidad de paquetes de cada protocolo, la cantidad de bytes transmitidos por host y la tasa de transferencia de datos en tiempo real.

Uso avanzado de Wireshark

1. Además de las funciones básicas de captura y análisis de paquetes, Wireshark también proporciona una serie de características avanzadas para usuarios más experimentados.

Estas características incluyen la capacidad de crear perfiles personalizados de captura, integración con otros programas de análisis de red, y la capacidad de utilizar Wireshark para probar y depurar aplicaciones de red.