

Network Miner



Qué es Network Miner ?

NetworkMiner es una herramienta de análisis forense de redes (NFAT) para Windows. NetworkMiner puede ser utilizado como una herramienta pasiva de sniffer/captura de paquetes para detectar sistemas operativos, sesiones, nombres de host, puertos abiertos, etc. sin poner ningún tráfico en la red. NetworkMiner también puede analizar los archivos PCAP para el análisis fuera de línea y para regenerar/reensamblar los archivos transmitidos y los certificados de los archivos PCAP.

Analizando PCAPS con Network Miner

Hemos obtenido una captura de red que nos ha dado como resultado un archivo **.PCAP** que contiene todo el tráfico que estaba pasando por la red, podemos hacer uso de herramientas como Network Miner que nos ayudan a parsear la información del **.PCAP** de una manera rápida y sencilla.

Lo primero que haremos es abrir nuestra tool Network Miner y pasarle el archivo **.PCAP**.

