RAW

RAW quiere decir “crudo” en inglés. Por lo tanto, se trata de un formato con el cual conservamos la foto cruda, sin procesar, como si no la hubiésemos tomado aún.

Cuando disparamos una foto en el formato habitual JPG la cámara graba la imagen en la tarjeta de memoria de manera definitiva y no admite cambios posteriormente. En cambio, si disparamos la foto en formato RAW estamos “conservando” la escena dentro de la tarjeta de memoria y así mantenemos la posibilidad de terminar de tomar la foto posteriormente, en nuestro ordenador.

Un fichero RAW es un archivo que contiene la información lumínica que recibe cada uno de los píxeles del sensor y una serie de metadatos proporcionados por la configuración de la cámara en el momento de la toma. Equivale a la imagen latente que contenía la película sensible en fotografía analógica antes de obtener el negativo.

EWF

Los archivos EWF son un tipo de imagen de disco, es decir, archivos que contienen el contenido y la estructura de un dispositivo de almacenamiento de datos completo, un volumen de disco o la memoria física de una computadora (RAM). Los archivos EWF constan de una o más secciones, cada una con su propio encabezado y datos de fijeza de nivel de sección.

AFF

El formato Advanced Forensics Format (AFF) es un formato muy recomendable para el análisis forense. Además de permitir la incrustación de metadatos, ofrece dos poderosos medios de compresión y posibilidad de cifrar. Por un lazo, zlib, que es rápido y efectivo. Adicionalmente soporta re-compresión con LZMA, que aunque es lento, produce reducciones de tamaño drásticas.

PCAP

El .pcap extensión de archivo se asocia principalmente con Wireshark; .pcap son archivos de datos creados mediante el programa y que contiene el paquete de datos de una red. Estos archivos se utilizan principalmente en el análisis de las características de la red de una fecha determinada. Estos archivos también contribuyen a controlar con éxito el tráfico de una determinada red, ya que están siendo monitoreados por el programa. Los datos y los resultados del análisis de redes se guardan con el .pcap extensión de archivo que es porqué se llaman .pcap archivos.

PCAPNG

Un archivo PCAPNG contiene paquetes de datos capturados a través de una red. El archivo se guarda en el formato PCAP Next Generation (PCAPNG). Los paquetes de datos almacenados en el archivo PCAPNG son utilizados por las aplicaciones del analizador de protocolo de red, como Wireshark, para monitorear y administrar los datos de la red. Los paquetes de datos en el archivo PCAPNG capturan varios tipos de información en varios bloques y guardan los paquetes de datos en un formato estructurado. La información guardada en varios bloques, como el bloque de encabezado de sección, el bloque de descripción de la interfaz, el bloque de paquetes mejorado, el bloque de resolución de nombres, etc., se puede utilizar para reconstruir los datos capturados.

| RAW | EWF | AFF |
|---|---|---|
| No guarda el MD5 o sha1 | Guarda Md5 y sha1 | Guarda Md5 y sha1 |
| No comprime | Compresión con zlib | Compresión con zlib |
| Software libre | Usado en ENcase | AccessDAtas FKT y ASR |