- RAW – El formato de imagen RAW es una copia bit-a-bit de un disco o volumen guardado en múltiples archivos. No hay metadatos guardados en estas imágenes. Muchas herramientas crean un archivo de texto separado que contiene los detalles de la imagen incluido el hardware/software utilizado y los valores hash.

  Las imágenes Raw son también llamadas imágenes dd debido a que el formato proviene originalmente de la herramienta dd.

- EWF – Expert Witness Disk Image Format. Es un tipo de imagen de disco que contiene la estructura completa de un dispositivo de almacenamiento, volumen, o RAM. Consiste en una o más secciones, cada una con su propio header y sección de datos, usualmente en la forma de Adler-32 checksum. Comprime una imagen en chunks de 32kb que son almacenados en tablas con índices para mejorar el acceso aleatorio. Puede tomar dos formas, imagen forense o archivo de evidencia lógica.

- AAF – Advanced Forensics Format. Es un formato abierto para el almacenamiento de las imágenes forenses. Su mérito es ofrecer un formato de imagen de disco que no está atado a propiedad de software.

  Este formato de imagen ya no es utilizado comúnmente.

- Pcap – Packet Capture. Es la grabación sistemática de paquetes de datos en diferentes dispositivos. Pcap pueden ser utilizados para identificar archivos temporalmente eliminados que fueron transferidos durante un evento de transferencia de archivos como FTP, TFTP o HTTP, y donde la evidencia de la existencia del archivo ya no existe en el sistema objetivo o fuente. Adicionalmente puede ser utilizados en análisis de malware.

- Pcapng – Formato nuevo de los archivos pcap, que incluye definir mútiples interfaces, mejora de los timestamp, comentarios embebidos, metadatos adicionales, formato extendido.