Tabla comparativa de los formatos de imágenes forenses

RAW (dd image)	**EWF Expert Witness Disk Image Format**	**AAF Advanced Forensic Format**
No almacenan metadatos	Tipo de imagen conformada tanto por la estructura como el contenido de algún volumen o un conjunto de volúmenes	Es un formato open source para trabajar imágenes forenses.
Consiste en copiar bit a bit todos los sectores del equipo a revisar en un solo archivo	En algunos casos, puede contener información sobre la memoria RAM	Es extensivo: se pueden agregar nuevas funcionalidades, sobre todo de compatibilidad
Son ampliamente usadas debido a que pueden ser cargadas por prácticamente cualquier herramienta forense actual	Obtiene información importante como el datetime de creación, última modificación, último acceso, permisos, etc	Su principal ventaja es que las imágenes que genera están comprimidas por lo que no es muy costoso a nivel de espacio en disco
Este tipo de imágenes, no están comprimidas, por lo que suelen ser muy pesadas a nivel de espacio	Podemos encontrar a las E01, E02, etc, que son el tipo de imágenes más usadas para el análisis forense	Trabaja en dos capas: Data-Storage: se encarga de almacenar la información del volúmen y Disk-Representation, la cual se encarga de asociar metadatos con los diferentes segmentos del disco

Pcap vs pcapng

Pcap: Acrónimo de packet capture. Es una interfaz usada por muchas aplicaciones como Wireshark, tcpdump, snort y WinCap entre otras, para capturar los paquetes que sean mandados desde una o más interfaces de red. Suelen contener packets a nivel de capa 2 y 3 del modelo OSI.

Pcapng: Acrónimo de packet capture next generation. Presenta mejoras interesantes al ampliamente usado pcap, como la de capturar paquetes de manera simultánea en múltiples interfaces de red, un mejor y más preciso manejo de timestamps, comentarios embebidos dentro de la captura de paquetes, inclusión de metadatos a la hora de realizar las capturas y la principal ventaja, es el formato extensible que nos brinda.

Referencias

- https://www.coursehero.com/file/p4p1pbc/What-is-AAF-data-storage-format-List-some-advantages-and-disadvantages-of-this/
- https://www.loc.gov/preservation/digital/formats/fdd/fdd000406.shtml
- https://www.raedts.biz/forensics/forensics-101-forensic-image/
- https://dash.harvard.edu/bitstream/handle/1/2829932/Malan_AdvancedForensic.pdf?sequence=4
- https://cloudshark.io/articles/5-reasons-to-move-to-pcapng/
- https://www.reviversoft.com/file-extensions/pcap
- https://wiki.wireshark.org/Development/PcapNg#:~:text=The%20PCAP%20Next%20Generation%20Dump,(but%20limited)%20libpcap%20format.