Hernández Vásquez Edgar

Análisis Forense.

RAW

Es básicamente una copia bit a bit de los datos RAW (en crudo) del disco o del volumen almacenado en uno o varios archivos.
No hay metadatos almacenados en los archivos de imagen. La mayoría de las herramientas crean un archivo de texto separado que contiene todos los detalles relacionados con el archivo de imagen, incluido el hardware/software utilizado.

EWF

Expert Witness Format. Son un tipo de imagen de disco, son archivos que contienen el contenido y la estructura de un dispositivo de almacenamiento de datos completo, un volumen de disco o (en algunos casos) la memoria física de una computadora (RAM).

AFF

Significa Advanced Forensics Format o Formato Forense Avanzado y es un formato abierto para el almacenamiento de imágenes forenses. Su objetivo es ofrecer un formato de imagen de disco que no esté vinculado a software propietario.

PCAP

Es el registro sistemático de los paquetes que fluyen a través de un dispositivo o dispositivos de captura, y es un representante del tráfico y los patrones de la red durante un tiempo determinado.

PCAPNg

Es el formato de archivo de volcado de próxima generación de PCAP, es un intento de superar las limitaciones del formato libpcap ampliamente utilizado (pero limitado).

Tabla comparativa RAW, EWF y AFF.

RAW	EWF	AFF
Software libre como dd lo pueden generar	Usado por EnCase	Usado por AccessData's FTK y ASR Data's SMART
No guarda automáticamente el MD5 o SHA1	Guarda automáticamente el MD5 y SHA1	Guarda automáticamente el MD5 y el SHA1
Extensión .RAW o .001	Extensión .E01 o .EX01	Extensión .AFF .AFD o .AFM
No compresión	Compresión con Zlib	Compresión con Zlib
Aún en uso	Aún en uso	En desuso

Fuentes.

FORENSICS 101: WHAT IS A FORENSIC IMAGE?. https://www.raedts.biz/forensics/forensics-101-forensic-image/

EXPERT WITNESS DISK IMAGE FORMAT (EWF) FAMILY. https://www.loc.gov/preservation/digital/formats/fdd/fdd000406.shtml

FORENSICS SOURCES PART 1: PACKET CAPTURE (PCAP). https://www.keirstenbrager.tech/pcap1/

PCAPNG. https://wiki.wireshark.org/Development/PcapNg