Tarea 1 - Formatos RAW, EWF, AAF, PCAP y PCAPNG.

Liberos Sánchez José Angel

22 de septiembre de 2020

1 Formatos

- **RAW**: Contiene sólo los datos del disco fuente, no contiene ningún header o metadato en el archivo imagen, pero algunas utilidades pueden incluir un archivo separado con los metadatos. La extensión más populares para estos archivos es DD, IMG o RAW. estos archivos son un archivo sin comprimir de una copia sector por sector de bits almacenados.

- **EWF**: EWF/E01, este tipo de archivos contiene un header y footer con el contenido de los metadatos de la imagen, esto incluye cosas como el tipo de versión de software con el que fue creada la imagen, el sistema operativo del disco, timestamp y los hashes. Por default estos archivos están comprimidos a nivel de bloque, de está manera el bloque es leído y el CRC es calculado. El CRC (Cyclical Redundancy Check) provee un método para verificar la integridad de la información de los bloques, es similar a un hash.

- **AFF**: Advanced Forensics Format, es un formato que te permite almacenar cualquier tipo de información forense, a diferencia de otros fromactos, este formato permite almacenar información en un menor uso de espacio en disco, permite almacenar imagenes de un disco de manera comprimida o sin compresión, de igual manera nos permite almacenar los metadatos de manera separada o en la misma imagen del disco, entre otras.

- **PCAP**: Packat Capture, es un registro de los paquetes que son enviados de un dispositivo a otro a través de una red o conexión, este tipo de archivos nos permiten identificar si algún archivo ha sido eliminado, modificado o enviado a través de alguna conexión o interacción por HTTP, FTP, etc., de igual manera se pueden usar para analizar malware.

- **PCAPNG**: Es una mejora del formato PCAP que agrega cosas como portabilidad y la capacidad de combinar y agregar datos en un rastreo, entre otras.

2 Tabla Comparativa

Formato	Compresión	Datos	Metadatos
RAW	Es un archivo no comprimido para mantener la integridad de la información.	Copia los datos sector por sector de un dispositivo.	No se tiene los metadatos en un footer o header, algunas herramientas te permiten obtenerlos en un archivo separado.
EWF	Almacena la información de manera comprimida	Los datos son almacenados en bloques.	Contiene un header y un footer con los metadatos del archivo.
AFF	Puede almacenarse la información de manera comprimida o sin comprimir.	Permite almacenar cualquier tipo de datos forenses en un espacio reducido.	Permite almacenar los metadatos de manera separada o dentro del mismo archivo.