

# Tarea 1

Pérez Martínez Josué Saúl

22 de Septiembre 2020

## 1. Formato de imágenes forenses

Las imágenes forenses son una técnica de recopilación típica información contenida en dispositivos físicos de almacenamiento, sin alterar su contenido, independientemente del sistema operativo que utilicen. Se puede crear con software o con dispositivos de hardware especializados.

RAW	EWFF (Formato de imagen de disco de testigo experto)	AAF Especificación de objeto de formato de autoría avanzada
Es una copia de bit a bit de los datos del disco o volumen almacenado en uno o varios archivos	Imagen que contiene la estructura y datos de un dispositivo de almacenamiento, un volumen de disco o la memoria RAM	Formato de archivo basado en objetos que envuelve metadatos junto con video, audio y otros flujos de bits
No hay metadatos almacenados en los archivos de imagen.	Constan de una o más secciones, cada una con su propia cabecera	Los metadatos AAF se almacenan en Mobs (objetos de metadatos) que son equivalentes a los paquetes en formato MXF.
La principal ventaja del formato de imagen RAW es el hecho de que los archivos solo contienen datos de origen sin modificar	Se utiliza generalmente para capturar y 'congelar' el contenido y la estructura de los dispositivos de almacenamiento, por ejemplo, discos duros, disquetes, unidades de cinta, discos ópticos o unidades flash USB. Puede copiar sector por sector de la fuente, replicando así la estructura y el contenido del dispositivo de almacenamiento	AAF tiene como objetivo eliminar los cuellos de botella de los proyectos entre plataformas que a menudo se producen cuando los archivos se intercambian entre aplicaciones.
Carece de cualquier forma de compresión, lo que hace que las imágenes sean tan grandes como la unidad de origen.	Incluyen metadatos incrustados sobre su creación, datos de fijez y otros elementos que proporcionan elementos para una cadena de custodia	Los Mobs tienen uno o más 0 MobSlots que representan el paso del tiempo

El formato PCAP se ha definido para capturar el tráfico de la red. Un archivo PCAP solo contiene tramas Ethernet. Se usa ampliamente para la captura de paquetes en la industria de la seguridad y la red.

El formato de archivo de captura PCAP Next Generation (PCAPng) es una mejora refrescante que agrega extensibilidad, portabilidad y la capacidad de combinar y agregar datos a un rastreo de cables.