Ignacio Vásquez Oscar

Forense. Tarea 1:

PCAP:

Es una interfaz de una aplicación para captura de paquetes. La implementación de pcap en Unix se conoce como libpcap, en windonws es WinPcap.

PCAPNG:

Formato de captura de paquetes que contiene un "volcado" de paquetes de datos capturados a través de una red; guardado en el formato de archivo PCAP Next Generation, un formato estándar para almacenar datos capturados.

RAW:

Un formato de imagen, es una copia bit a bit de los datos del disco o volumen almacenado

EWF (Expert Witness Disk Image Format):

Los archivos EWF son un tipo de imagen de disco, es decir, 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 (RAM) de una computadora.

AFF (Advanced Forencis Format):

Formato extensible para el almacenamiento de imágenes de disco con o sin compresión, junto con metadatos relacionados que pueden almacenarse dentro de imágenes de disco o por separado.

RAW	EWF	AFF
Tamaño igual al original	Limita el tamaño	Tamaño igual al original
No permite comprimir la información.	Permite comprimir información	No permite comprimir la información
No guarda metadatos	Guarda metadatos, pueden ser externos.	Guarda metadatos de forma arbitraria.