U.N.A.M. – C.E.R.T.

Forense

Alumno: Luis Fernando Resendiz Cruz

RAW.

Este tipo de formato es el mas usado en los sistemas Linux. Se puede obtener mediante el comando dd y lo que realiza es el copiado bit a bit de un dispositivo.

EWF (Expert **W**itness **F**ile**).**

Es un archivo de imagen de disco el cual contiene los datos y la estructura de un dispositivo de almacenamiento, un volumen de disco he incluso una memoria volátil.

AAF (Advanced **F**orensics **F**ormat**).**

Es un formato que es open source y extensible, es capaz de almacenar información como imágenes de discos, archivos exportados entre otros.

PCAP (Packet **CAP**ture**).**

Es un formato utilizado para realizar el volcado de los paquetes capturado en un archivo. Estos archivos son el resultado de la catura de paquetes de las capas 2 a la 7 del modelo OSI por medio de una API.

PCAPNG (Packet **CAP**ture **N**ext **G**eneration**).**

En esencia es lo mismo que el pcap, es un formato utilizado para realizar el volcado de paquetes capturados en un archivo, pero tiene la ventaja que es capaz de almacenar más información que pcap como puede ser precisión de timestamp, información de la interfaz que captura, estadísticas de captura, tipos de capas de enlaces mixtos, información de resolución de nombres, comentarios de usuario, etc.

	RAW	**EWF**	AFF
Ventajas.	-Rápida transferencia de datos. -Evita errores de lectura en el dispositivo de origen. - Es compatible con la mayoría de las herramientas de forense.	-La imagen puede ser comprimida lo cual ahorra espacio. - La imagen puede ser también dividida, se verifica la integridad de cada segmento.	-Es compatible con varias herramientas de forense. -Guarda los metadatos de la información evitando posibles errores. - Es comprimible y se puede segmentar en distintos tamaños.
Desventajas.	-Requiere de un espacio igual que el original. -No recopila los sectores defectuosos.	-No todas las herramientas aceptan este formato. - Tiene una limitación con los el tamaño de los segmentos. La segmentación típica es de 650 MB o 2GB.	-El tamaño de página de compresión predeterminado de AFF de 16 MB puede imponer una sobrecarga al acceder a NTFS Master File Tables - El acceso de una imagen en este formato suele ser mas tardado.