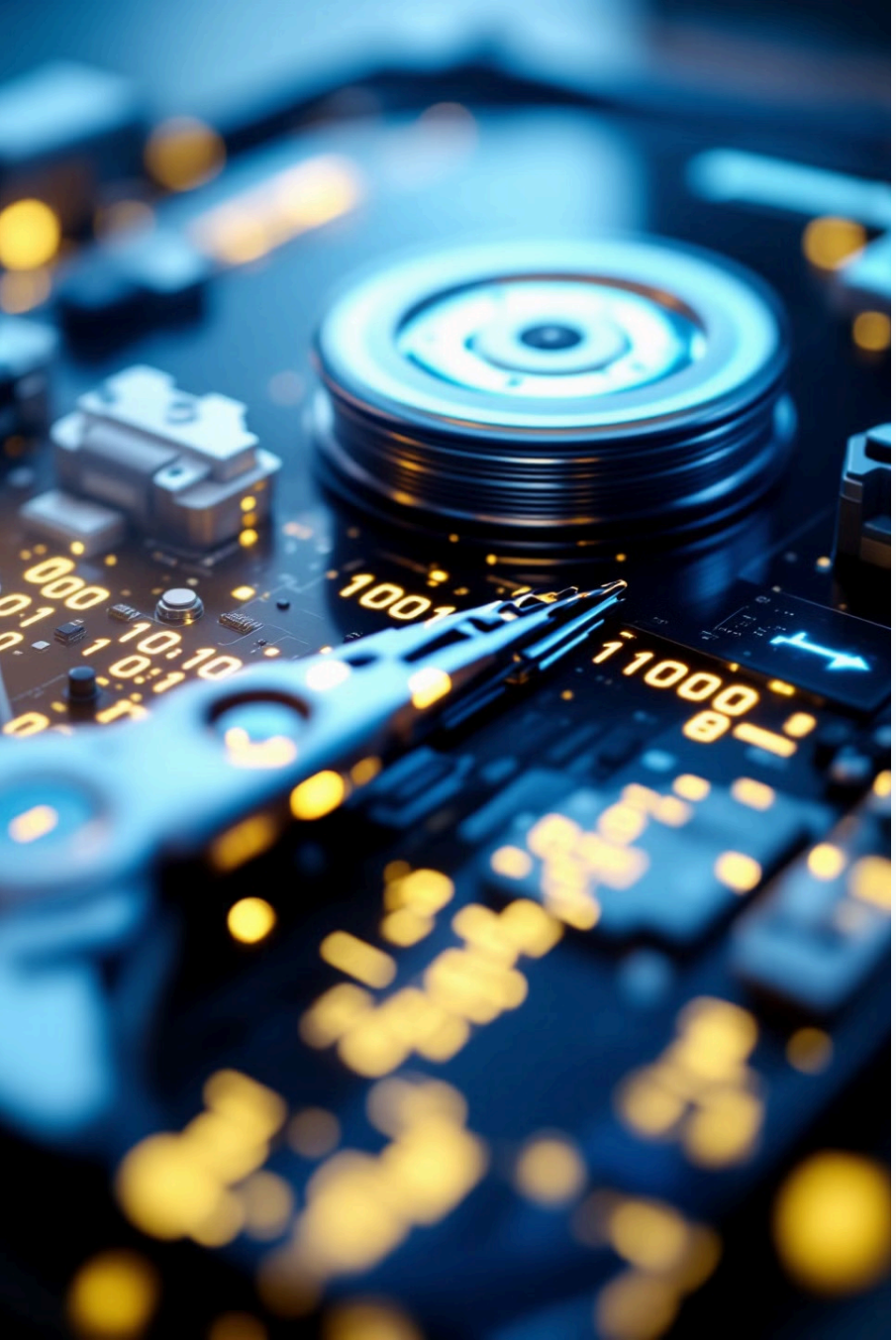
Formatos de Imagen Forense en Autopsy

Exploraremos los principales formatos de imagen utilizados en análisis forense digital, su relación con Autopsy y las ventajas y desventajas de cada uno.



RAW: El Formato Básico

Copia bit a bit

RAW (.raw, .dd, .img) es una copia exacta del contenido del disco.

Compatibilidad universal

Es compatible con la mayoría de herramientas forenses, incluido Autopsy.

Sin compresión

Ocupa mucho espacio debido a la falta de compresión.

EWF: El Estándar de EnCase

Formato EnCase

EWF (.E01, .E02) es un formato propietario ampliamente adoptado en forense digital.

Metadatos incluidos

Contiene hashes, información temporal y comentarios del investigador.

Compresión eficiente

Ahorra espacio comprimiendo los datos sin perder información.

AFF: El Formato Abierto

Cifrado

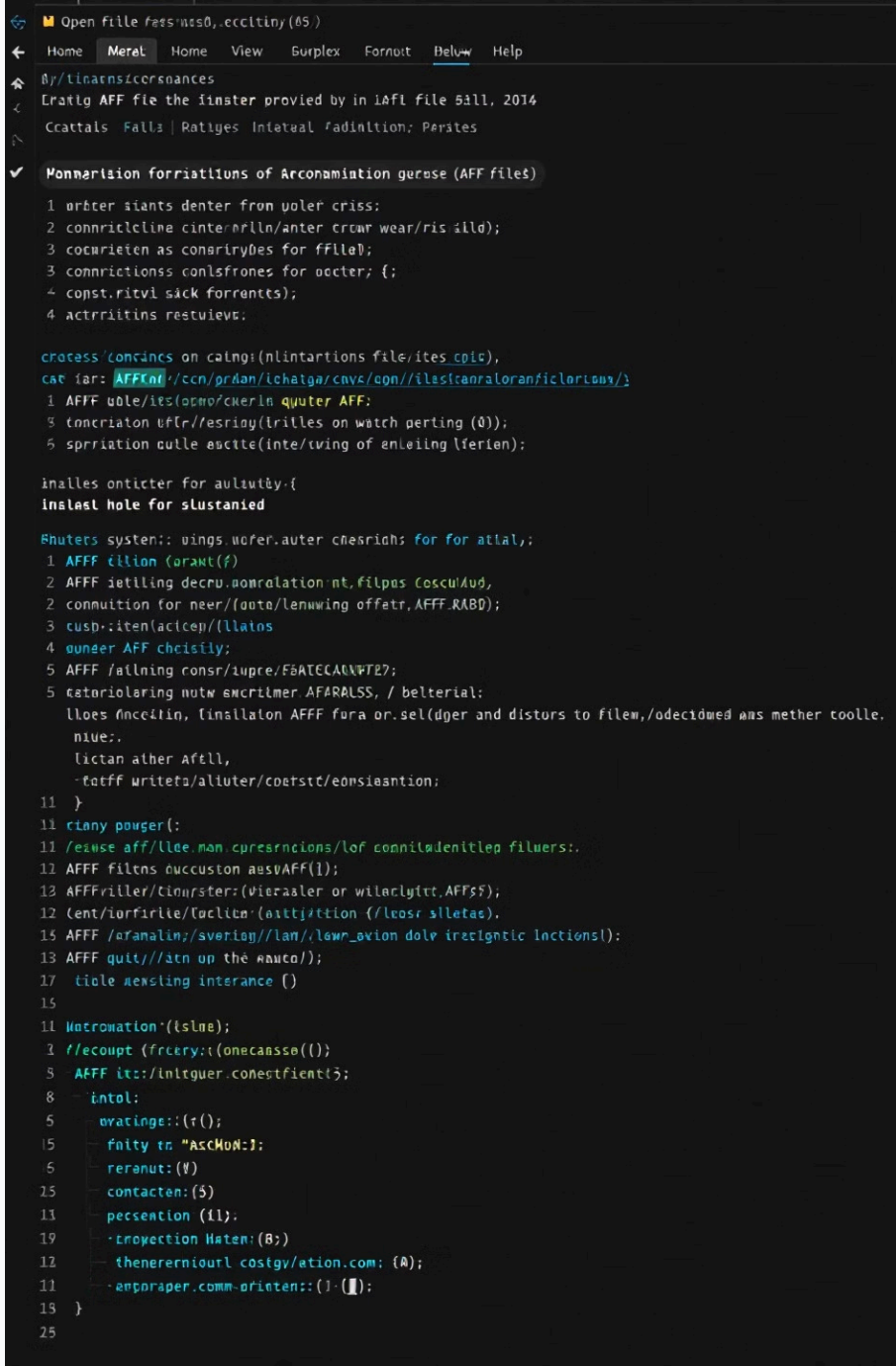
AFF (.aff, .afd) permite cifrar los datos para mayor seguridad.

Compresión

Ofrece compresión para reducir el tamaño de los archivos.

Estándar abierto

Diseñado como un formato abierto y bien documentado.



VHD/VHDX: Discos Virtuales

1

2

3

Creación

Se crean en entornos virtuales como Hyper-V o VirtualBox.

Análisis

Autopsy los trata como discos físicos para su análisis.

Aplicación

Útil para investigar máquinas virtuales comprometidas.

ISO: Imágenes Ópticas

Contenido óptico

ISO (.iso) contiene copias exactas de datos en CD/DVD.

Uso limitado

Menos común en análisis forense de discos duros.

Compatibilidad

Autopsy puede analizar su estructura y contenido.

TAR/ZIP: Archivos Comprimidos

1

Empaquetado

TAR/ZIP comprimen y empaquetan datos para transferencia.

2

Análisis

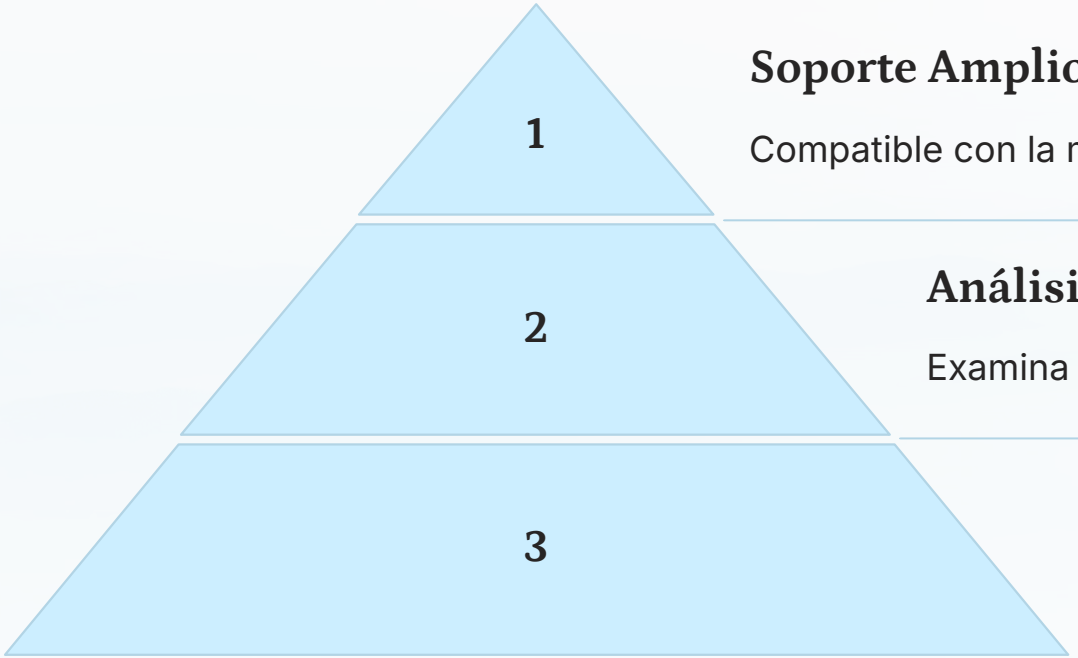
Autopsy puede explorar su contenido y recuperar archivos eliminados.

3

Limitaciones

No son formatos de imagen forense propiamente dichos.

Capacidades de Autopsy



Soporte Amplio

Compatible con la mayoría de formatos mencionados.

Análisis Avanzado

Examina particiones, sectores no asignados y datos eliminados.

Verificación de Integridad

Utiliza hashes para verificar la integridad de los datos.

Elección del Formato

1

RAW/DD

Para simplicidad y acceso directo a los datos.

2

E01

Para compresión, integridad de datos y auditoría.

3

AFF

Para un formato abierto con compresión y cifrado.

Conclusiones

Versatilidad

Cada formato tiene sus propias ventajas y casos de uso.

Compatibilidad

Autopsy soporta una amplia gama de formatos forenses.

Elección informada

Selecciona el formato según las necesidades específicas del caso.