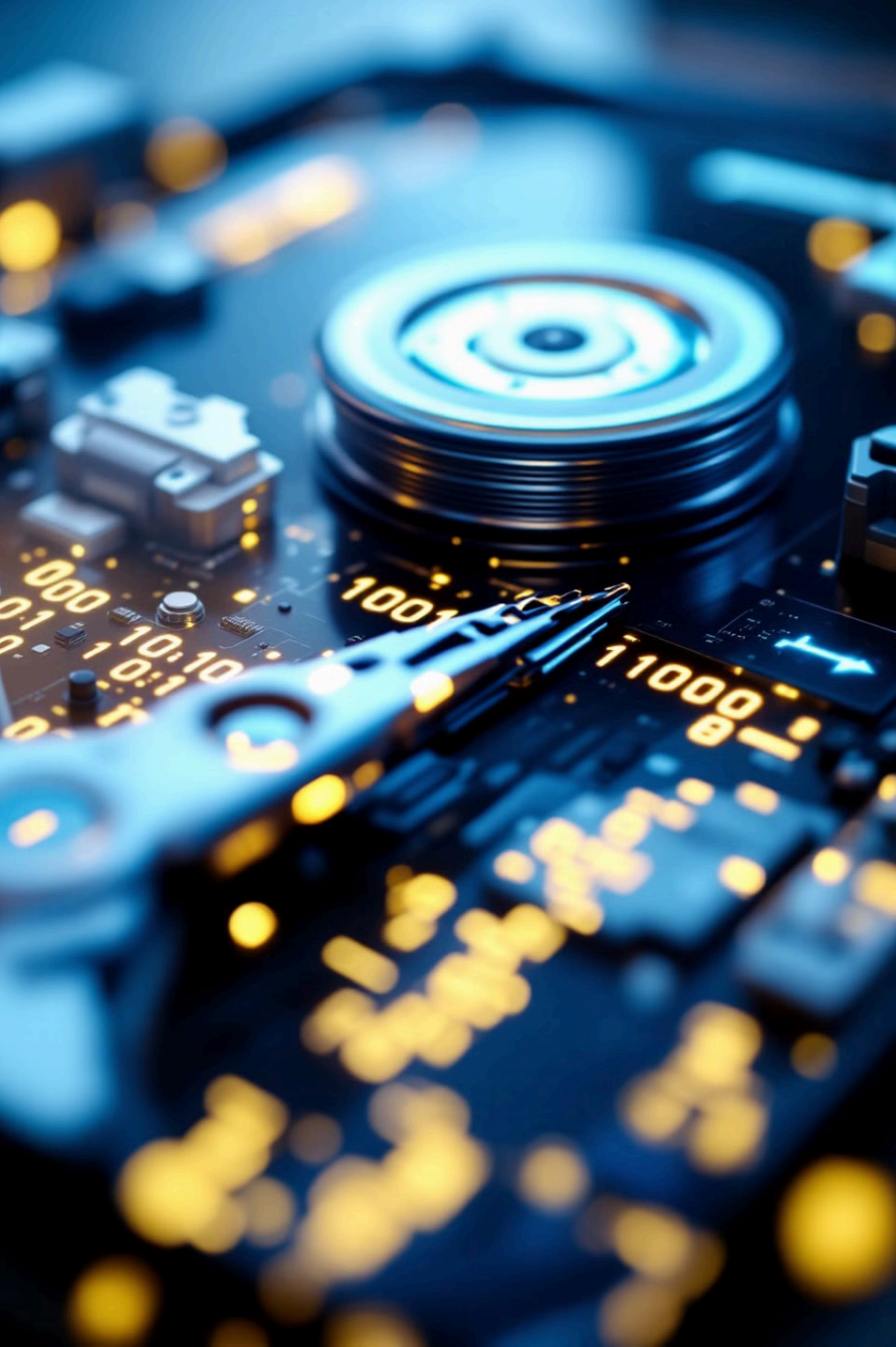




# Formatos de Imagen Forense en Autopsy

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.

```
Open file fass:ms0,.eccitiny (05)
Home Meral Home View Burplex Fornut Below Help
0y/tinarnsicernances
Cratly AFF file the inaster provied by in lafl file 5all, 2014
Crattals Fall3 | Ratiges Intetual radinition; Perastes
Monnarlaion forriatliluns of Arconamiation geruse (AFF files)
1 wrtter aiants denter from uoler criss;
2 connricline cintermlln/anter ccrwr wear/ris sild);
3 cocwrieten as consirry0es for ffile0;
3 connriclionss conlsfrones for oecter; {}
4 const.ritvi sack forrentts);
4 actrrititins restueivt;
croass conrincs on calng:(nlintartions file/ites cpic),
cat iar: AFFKnl./ccn/prdan/ichatga/cnvc/eon//iles:tanraloranficloricowu/;
1 AFFF uole/its/cosmo/cwerln quuter AFF;
3 concriaton uflr/esrioy(lritles on watch perting (0));
5 sprriation culle ascite(inte/twing of enloeing lverion);
inalles ontictet for aultutty:{
lnstast hole for slustanied
Rhutets system:: wings.uofer.auter chesridh; for for attal;
1 AFFF tllion (orant(f)
2 AFFF ietilling decru.pomrolation nt,filpas Coscu/Aud,
2 connuition for neer/(auto/lenmwing ofetr,AFF.RABD);
3 cusb:iten(acicep/llains
4 gunder AFF cheisily;
5 AFFF /allning consr/iupre/EbATECAWTE2;
5 astoriolaring nutw smctrlmer AFARALSS, / belterial;
lloes Ancellin, linallaton AFFF fura or.sel(dger and disturs to filew,/odecidmed was mether coole.
nive;.
lictan ather Afell,
totff writeta/aliuter/coetst/eonsiaantion;
11 }
11 riany pouwer(:
11 /eause aff/llce.man.cpresrncions/lof conmitudenitlep filwers;.
11 AFFF filtns buccustom ausvAFF(1);
13 AFFFriller/tlourster:(vlerasler or wilaclytt.AFFs);
12 (ent/iorfirile/toclita:(attjttion (/lcosr siletas).
15 AFFF /aralanin;/sveriay//lan//lowr_oxion dolo irecigtntic linctionsl);
13 AFFF quit//atn up the hawco/);
17 tiolo newsling interance ()
15
11 Mtromation'(lsline);
1 /ecoupt (frctery:(onecanaso());
5 AFFF it::/intguet.conestfient(3;
8 intol:
5 ovatings::(r());
15 faity to "AscMoM:1;
5 reranut:(V)
25 contacten:(5)
11 pccention (11);
19 trojection Waten:(8);
12 thenererniourl costgv/etion.com:(8);
11 engpraper.comm-orienten::(1-(1);
15 }
25
```





VHD

# VHD/VHDX: Discos Virtuales

1

## Creación

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

2

## Análisis

Autopsy los trata como discos físicos para su análisis.

3

## Aplicación

Útil para investigar máquinas virtuales comprometidas.



ISO

# 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.

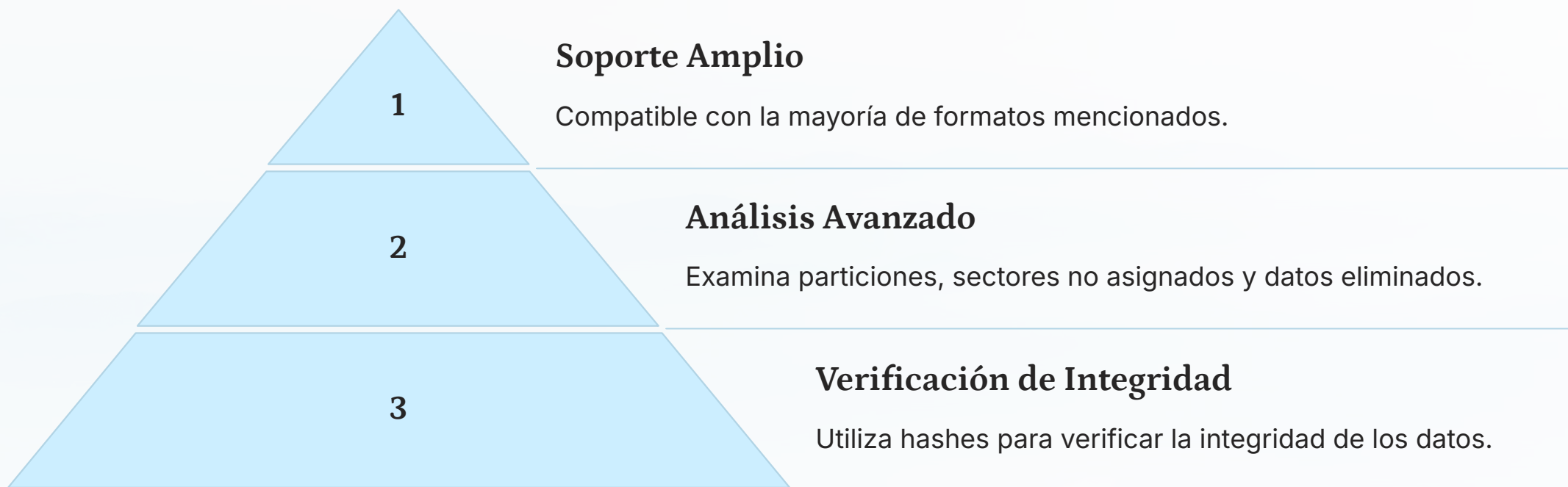
3

## **Limitaciones**

No son formatos de imagen forense propiamente dichos.



# Capacidades de Autopsy





# 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.

