

RECUPERACIÓN DE ARCHIVOS MEDIANTE CARVING (PHOTOREC)



¿Qué es el carving en informática forense?

Carving (o data carving) es una técnica que permite **recuperar archivos directamente del contenido binario de un disco, sin depender del sistema de archivos ni de las entradas MFT o inodos.**

Definición clara para tu guía:

Carving es el proceso de **extraer archivos perdidos o eliminados directamente de sectores del disco**, buscando patrones específicos en los datos (como cabeceras y pies de archivo), **sin utilizar información de las tablas de archivos.**

¿Cuándo se usa?

Se utiliza cuando:

- El sistema de archivos está dañado o formateado.
 - Las entradas MFT han sido eliminadas o sobrescritas.
 - Solo queda el contenido crudo del disco (espacio no asignado).
 - Queremos recuperar fragmentos de archivos eliminados.
-

¿Cómo funciona?

1. Se escanean los sectores del disco o imagen en bruto.
2. Se buscan **firmas de cabecera y pie** de tipos de archivos conocidos:

- JPG → empieza con FFD8 y termina con FFD9
- PDF → empieza con %PDF y termina con %%EOF
- DOCX, ZIP, PNG... etc.

3. Al encontrar esas firmas, el programa intenta **reconstruir el archivo** aunque no haya entrada en la MFT.


Herramientas comunes para carving:

- foremost
- scalpel
- photorec
- bulk_extractor (aunque más orientado a extracción de datos que a reconstrucción de archivos)

Montaje de una imagen E01 en formato RAW para usar con PhotoRec

¿Por qué necesitamos convertir .E01 a RAW?

PhotoRec **no trabaja directamente con imágenes en formato .E01 (Expert Witness Format)**. Por eso, antes de usar `photorec`, necesitamos montar la imagen .E01 y convertirla temporalmente a un formato RAW legible por herramientas de recuperación, como si fuera un disco físico.

 Paso 1: Usar `ewfmount` para montar la imagen .E01

```
root@caine:/# ewfmount /media/sda1/windows_001_10.E01 imagenEWFRAW
```

¿Qué es ese archivo ewf1?

Es un acceso virtual a la imagen .E01, pero con formato compatible RAW, listo para herramientas como `photorec`, `scalpel`, `mount`, etc.

🔑 Configurar imagen .E01 como dispositivo de bloques con losetup

Después de montar una imagen .E01 como RAW usando ewfmount, podemos **asociar ese archivo (ewf1) a un dispositivo de loop** para tratarlo como un disco físico real dentro del sistema.

```
root@caine:/# losetup -fP imagenEWFRAW/ewf1
```

🧠 ¿Qué hace este comando?

Parte del comando	Función
losetup	Asocia archivos como dispositivos de bloque (tipo /dev/loopX)
-f	Busca el primer dispositivo de loop libre disponible
-P	Detecta y crea automáticamente particiones del dispositivo loop
imagenEWFRAW/ewf1	Es el archivo RAW simulado creado con ewfmount

🌀 ¿Para qué sirve?

- Permite que el sistema operativo **vea el contenido de la imagen como un disco real con particiones**.
- Crea dispositivos como /dev/loop0, /dev/loop0p1, /dev/loop0p2, etc.
- Es útil para:
 - **Montar particiones manualmente** (por ejemplo, /dev/loop0p1)
 - Acceder a sistemas de archivos directamente con mount
 - **Usar herramientas de análisis directamente sobre particiones reales dentro de la imagen**

El comando `losetup -fP imagenEWFRAW/ewf1` permite **convertir una imagen montada en RAW a un dispositivo de bloques tipo /dev/loopX**, con todas sus particiones accesibles. Esto facilita el montaje manual de particiones y el análisis forense con herramientas como `mount`, `photorec`, o exploración directa.

```
root@caine:/# photorec
```

Seleccionamos el disco del cual queremos recuperar archivos:

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 85 GB / 80 GiB (R0) - VBOX HARDDISK
Disk /dev/sdb - 53 GB / 50 GiB (R0) - VBOX HARDDISK
Disk /dev/sr0 - 4169 MB / 3976 MiB (R0) - VBOX CD-ROM
Disk /dev/loop0 - 4059 MB / 3871 MiB (R0)
>Disk /dev/loop1 - 53 GB / 50 GiB (R0)
Disk /dev/loop1p1 - 53 GB / 49 GiB (R0)

>[Proceed ] [ Quit ]
```

Y por ejemplo solo de la parte que está vacía que es la que nos interesa:

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

1 * HPFS - NTFS          2048  0  1 104855551  0  1 104853504

Please choose if all space needs to be analysed:
>[ Free ] Scan for file from NTFS unallocated space only
[ Whole ] Extract files from whole partition
```

☒ Opción: [Free]

- ◇ **Analiza solo el espacio no asignado** (unallocated)
- ◇ Es decir, **busca archivos eliminados** que podrían estar en zonas del disco donde el sistema operativo ya no asigna archivos nuevos.

☞ Ideal cuando:

- Solo quieres recuperar archivos **borrados**.
- No quieres analizar archivos existentes (para ahorrar tiempo y espacio).
- Estás en un contexto forense y quieres ver **lo que el usuario intentó eliminar**.

☐ Opción: [Whole]

- ◇ Analiza **toda la partición**, tanto el espacio ocupado como el libre.
- ◇ Recupera archivos **borrados y actuales** (aunque estén intactos o sobrescritos).

☞ Ideal cuando:

- Buscas **la mayor cantidad posible de archivos**, sin importar su estado.
- Estás ante una imagen sospechosa con **archivos ocultos o camuflados**.
- Tienes tiempo y espacio suficiente para recuperar todo el contenido.

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/loop1 - 53 GB / 50 GiB (R0)
  Partition      Start      End      Size in sectors
  1 * HPFS - NTFS    2048      0 1 104855551    0 1 104853504

Destination /media/sda1/recup_dir

Pass 1 - Reading sector 51647552/104853504, 214 files found
Elapsed time 0h00m23s - Estimated time to completion 0h00m23
exe: 111 recovered
tx?: 58 recovered
png: 32 recovered
txt: 8 recovered
bmp: 4 recovered
lnk: 1 recovered
```

Stop

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/loop1 - 53 GB / 50 GiB (R0)
  Partition      Start      End      Size in sectors
  1 * HPFS - NTFS    2048      0 1 104855551    0 1 104853504

214 files saved in /media/sda1/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

[Quit]

Los archivos recuperados se extraen al sitio donde indiquemos:

```
caine@caine:/media/sda1/recup_dir.1$ ls
f0083448.dll
f0726056.png
f0726072.png
f0726080.png
f0726088.png
f0726096.png
f0726112.png
f0726120.png
f0726128.png
f0726136.png
f0726152.png
f0726200.png
f0726208.png
f0726224.png
f0726240.png
f0726264.png
f0726312.png
f0726320.png
f0726328.png
f0726336.png
f0726344.png
f0726352.png
f0726360.png
```