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 sobreescritas.
- 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/wndows_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`

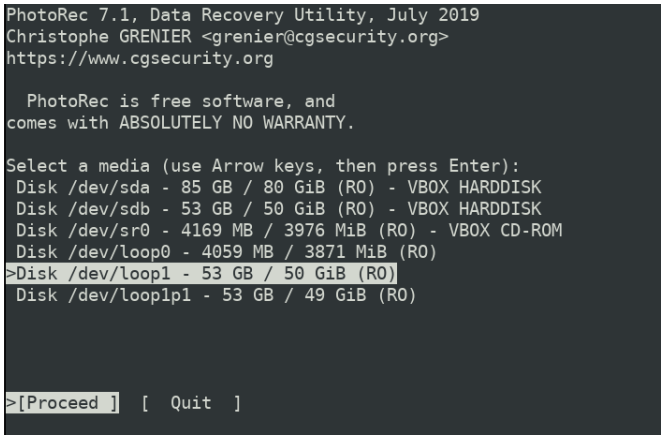
🎯 ¿Para qué sirve?

- 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**

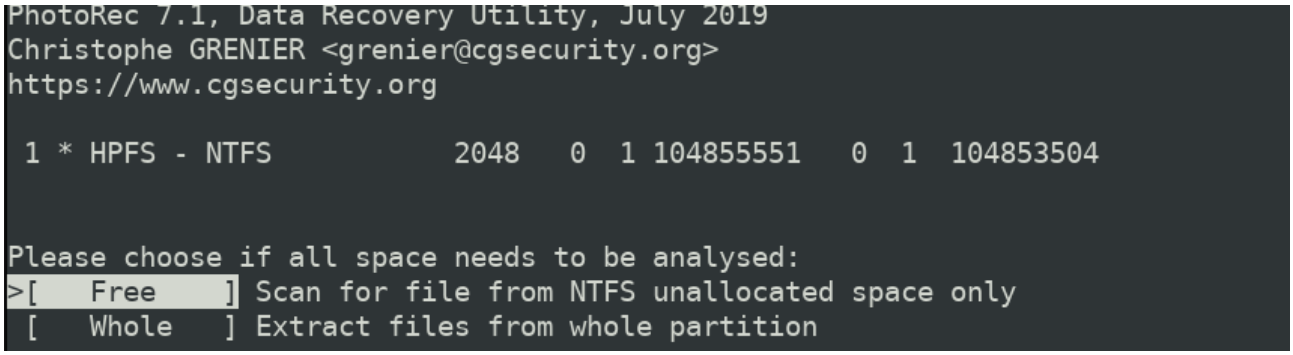
El comando `losetup -fP imagenEWFRaw/ewf1` permite **convertir una imagen montada en RAW a un dispositivo de bloques tipo /dev/loopX**, con todas sus particiones accesibles. Esto facilita el montaje manual de particiones y el análisis forense con herramientas como `mount`, `photorec`, o exploración directa.

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

Seleccionamos el disco del cual queremos recuperar archivos:



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



☑ 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:

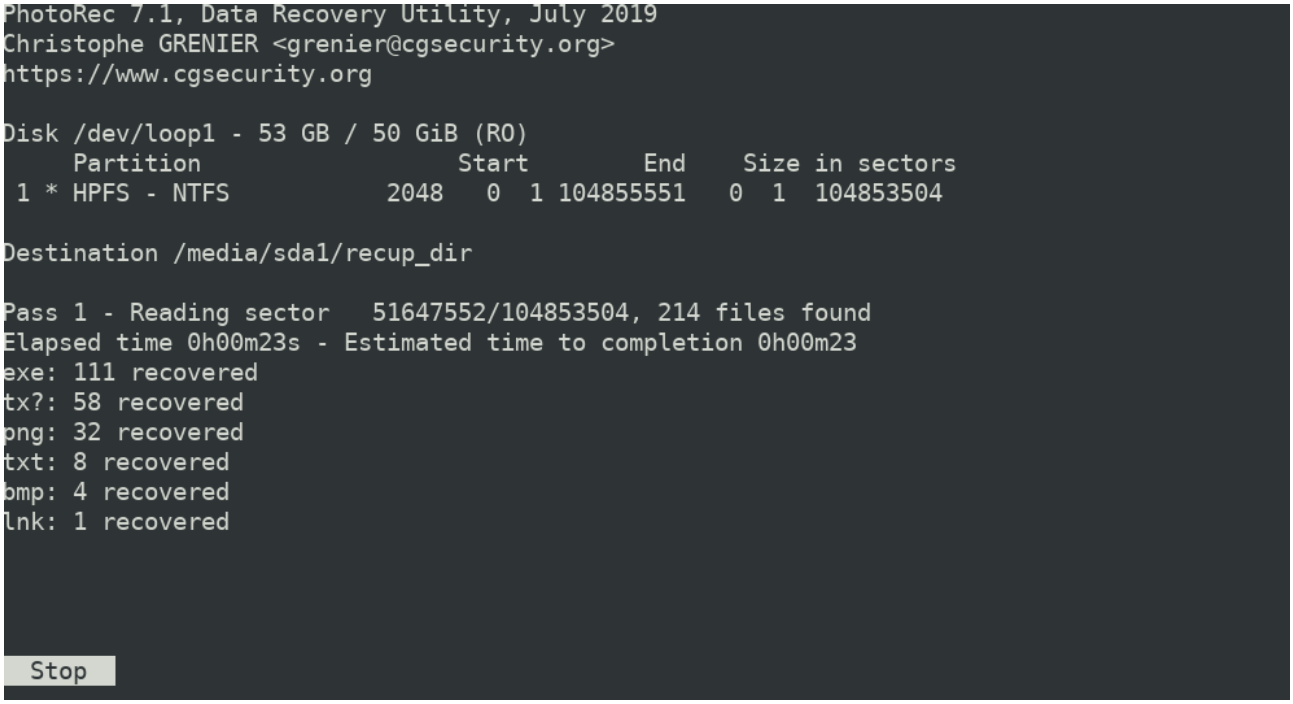
- Solo quieres recuperar archivos **borrados**.
- No quieres analizar archivos existentes (para ahorrar tiempo y espacio).
- Estás en un contexto forense y quieres ver **lo que el usuario intentó eliminar**.

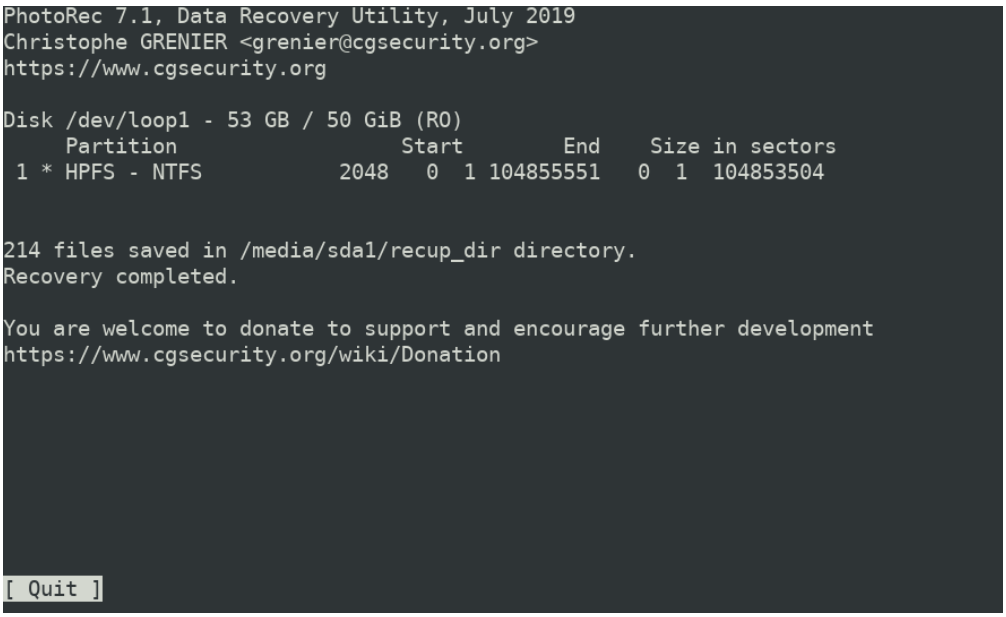
🔁 Opción: `[ Whole ]`

- 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.





Los archivos recuperados se extraen al sitio donde indiquemos: