

Fragments in the dark

We start by identifying what kind of filesystem the image contains

```
(kali㉿kali)-[~]
$ file disk.img
disk.img: Linux rev 1.0 ext4 filesystem data, UUID=8c63b026-7b3a-409a-bbcc-69f28d09113d (extents) (64bit) (large files) (huge files)
```

We find it is ext4

Mount it read-only to safely look around without altering anything

```
(kali㉿kali)-[~]
$ sudo mkdir -p /mnt/ctf
[sudo] password for kali:

(kali㉿kali)-[~]
$ sudo mount -o ro,loop,noauto disk.img /mnt/ctf

(kali㉿kali)-[~]
$ ls -la /mnt/ctf

total 21
drwxr-xr-x 7 kali kali 1024 Sep  2 18:23 .
drwxr-xr-x 5 root root 4096 Sep  2 18:04 ..
drwxrwxr-x 2 kali kali 1024 Sep  2 18:23 .cache
drwxrwxr-x 2 kali kali 1024 Sep  2 18:23 docs
drwxrwxr-x 2 kali kali 1024 Sep  2 18:23 logs
drwx—— 2 root root 12288 Sep  2 18:23 lost+found
drwxrwxr-x 2 kali kali 1024 Sep  2 18:23 tmp
```

Check if any files are visible, especially documentation

```
(kali㉿kali)-[~]
$ ls -la /mnt/ctf/docs

total 3
drwxrwxr-x 2 kali kali 1024 Sep  2 18:23 .
drwxr-xr-x 7 kali kali 1024 Sep  2 18:23 ..
-rw-rw-r-- 1 kali kali 147 Sep  2 18:23 readme.txt

(kali㉿kali)-[~]
$ cat /mnt/ctf/docs/readme.txt
Forensics tip: when listings look empty and strings show nothing interesting,
consider signature-based carving of deleted artifacts in free space.
```

We find a hint in a readme file in documentation

The readme suggests deleted files won't show up with simple listing or strings, so try recovery tools like PhotoRec

```
(kali㉿kali)-[~]
└─$ photorec disk.img
```

Shows a menu select the disk.img

```
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

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

Select a media and choose 'Proceed' using arrow keys:
>Disk disk.img - 50 MB / 48 MiB (RO)
```

Select the filesystem type

```
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk disk.img - 50 MB / 48 MiB (RO)

      Partition          Start          End    Size in sectors
      Unknown            0    0   1        6   30  24       98304 [Whole disk]
>  P ext4              0    0   1        6   30  24       98304
```

Select the ext file type

```
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

P ext4                  0    0   1        6   30  24       98304

To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
>[ ext2/ext3 ] ext2/ext3/ext4 filesystem
  [ Other      ] FAT/NTFS/HFS+/ReiserFS/ ...
```

Select free to scan the unallocated space only since we are looking for deleted files

```
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

P ext4                  0    0   1        6   30  24       98304

Please choose if all space needs to be analysed:
>[ Free     ] Scan for file from ext2/ext3 unallocated space only
  [ Whole    ] Extract files from whole partition
```

Select directory and press c to confirm

```
PhotoRec 7.2, Data Recovery Utility, February 2024

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /home/kali
```

Then quit from photorec

Carve free space for deleted files, the recovered files will be placed in `recup_dir`

```
[kali㉿kali)-[~]
$ cat photorec.log
Using locale 'en_US.UTF-8'.

Tue Sep 2 19:03:58 2025
Command line: PhotoRec /log disk.img

PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
OS: Linux, kernel 6.12.38+kali-amd64 (#1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12)) x86_64
Compiler: GCC 14.2
ext2fs lib: 1.47.2, ntfs lib: libntfs-3g, ewf lib: none, libjpeg: libjpeg-turbo-2.1.5, curses lib: ncurses 6.5
User is not root!
Hard disk list
Disk disk.img - 50 MB / 48 MiB - CHS 7 255 63 (R0), sector size=512

Can't open photorec.ses file: No such file or directory
Partition table type (auto): None
Filesystem created: Tue Sep 2 18:23:37 2025
Last mount time:   Tue Sep 2 18:23:37 2025
    Unknown          0  0  1    6 30 24      98304 [Whole disk]
    P ext4           0  0  1    6 30 24      98304
        ext4 blocksize=1024 Large_file Sparse_SB, 50 MB / 48 MiB
ext2/ext3/ext4 mode activated.
Carve free space only.
ext2_remove_used_space 1-49151
743 first-level signatures enabled

Analyse
    P ext4           0  0  1    6 30 24      98304
        ext4 blocksize=1024 Large_file Sparse_SB, 50 MB / 48 MiB
Pass 0 (blocksize=1024) STATUS_FIND_OFFSET
blocksize=1024, offset=0
Elapsed time 0h00m00s
Pass 1 (blocksize=1024) STATUS_EXT2_ON
/home/kali/recup_dir.1/f0017428.7z      17428-17429
Elapsed time 0h00m00s
Pass 1 +1 file
7z: 1/1 recovered
Total: 1 file found

81760 sectors contain unknown data, 0 invalid files found and rejected.

PhotoRec exited normally.
```

Check what PhotoRec pulled out. Here, it found a .7z archive

```
(kali㉿kali)-[~/recup_dir.1]
$ 7z l f0017428.7z

7-Zip 25.01 (x64) : Copyright (c) 1999-2025 Igor Pavlov : 2025-08-03
64-bit locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 156 bytes (1 KiB)

Listing archive: f0017428.7z

--
Path = f0017428.7z
Type = 7z
Physical Size = 156
Headers Size = 122
Method = LZMA2:12
Solid =
Blocks = 1

Date      Time      Attr          Size   Compressed  Name
-----  -----  -----  -----  -----  -----
2025-09-02 18:23:37  ....A           30        34  flag.txt
-----  -----  -----  -----  -----  -----
2025-09-02 18:23:37                   30        34  1 files
```

Open the recovered archive to see if it contains the flag

```
(kali㉿kali)-[~/recup_dir.1]
$ 7z x f0017428.7z -oextracted

7-Zip 25.01 (x64) : Copyright (c) 1999-2025 Igor Pavlov : 2025-08-03
64-bit locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 156 bytes (1 KiB)

Extracting archive: f0017428.7z
--
Path = f0017428.7z
Type = 7z
Physical Size = 156
Headers Size = 122
Method = LZMA2:12
Solid =
Blocks = 1

Everything is Ok

Size:      30
Compressed: 156
```

Inside the extracted files, locate the hidden flag.txt

```
(kali㉿kali)-[~/recup_dir.1]
$ cd extracted

(kali㉿kali)-[~/recup_dir.1/extracted]
$ ls
flag.txt

(kali㉿kali)-[~/recup_dir.1/extracted]
$ cat flag.txt
SGCTF{ghost_in_deleted_blocks}
```

The real flag is **SGCTF{ghost_in_deleted_blocks}**