

Category: Forensics**Date:** 11 October 2025**Difficulty:** EasyDISKO 1 **Easy** **Forensics** **picoGym Exclusive**

AUTHOR: DARKRAICG492

Hints **Description**

1

Can you find the flag in this disk image?

Download the disk image [here](#).

Challenge Overview: The challenge provides a compressed file named 'disko-1.d.gz'

Stage 1 – Verify file name and type (Quick file check)

Start by identifying what kind of file i'm dealing with:

File disko-1.d.gz

```
(kali㉿kali)-[~]  
$ ls -lh /home/kali/Downloads/disko-1.dd*  
-rw-r--r-- 1 kali kali 20M Oct 11 18:04 /home/kali/Downloads/disko-1.dd.gz
```

Stage 2 – Inspect without full extraction

Instead of decompressing the entire image, we can stream its contents and search directly for readable strings.

This saves time and avoids creating unnecessary files.

`zcat disko-1.d.gz | strings | grep picoCTF`

```
(kali㉿kali)-[~]  
$ sudo zcat -f /home/kali/Downloads/disko-1.dd.gz 2>/dev/null | strings | grep -i "picoCTF" -n  
287931:picoCTF{[REDACTED]}  
  
(kali㉿kali)-[~]  
$
```

Cryptography

Why this works:

The file is gzip-compressed, but the flag text is stored in plain ASCII inside the image.

zcat decompresses the data stream on the fly, and strings extracts human-readable text, while grep filters for the CTF flag pattern.

Result

Running the command reveals a string matching the CTF flag format:

picoCTF{REDACTED}

Flag redacted to comply with CTF rules.