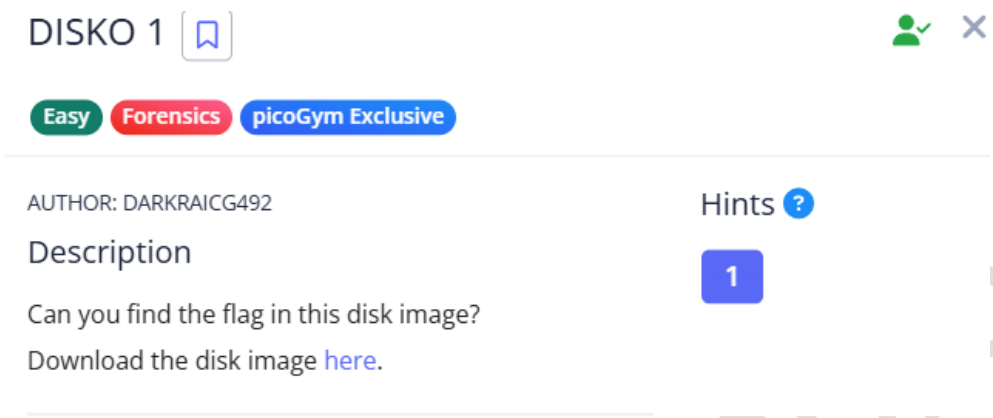
Category: Forensics
Date: 11 October 2025
Difficulty: Easy

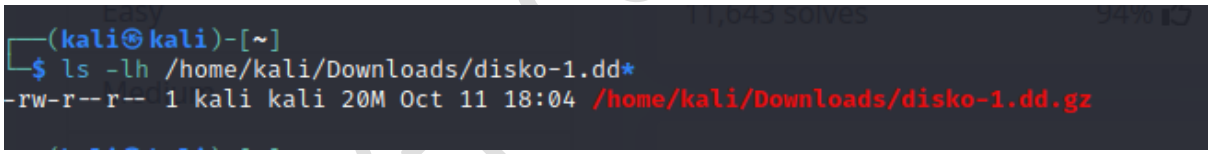


Challenge Overview: The challenge provides a compressed file named 'disko-1.d.gz'

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

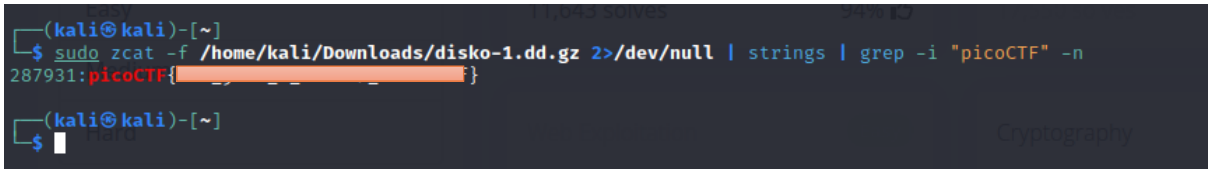


Stage 2 – Inspect without full extraction

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



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.