

CTF Write-up — Elf's Snapshot

Category: Forensics

Points: 25

Author: p3f0rm3r ({x0x} Team)

Challenge Description

A tiny file hides a message for Santa's eyes only. A souvenir file from the North Pole. Something's inside it.

File: elfsnapshot.png

Analysis

The challenge provides a single PNG image. In forensic challenges, metadata analysis is often the first step. Therefore, exiftool was used to inspect the file.

Solution

Step 1 — Metadata Analysis

The image metadata was analyzed using the following command:

```
exiftool elfsnapshot.png
```

The output revealed a hidden comment containing the flag.

Evidence — ExifTool Output

```
Session Actions Éditer Vue Aide
p3rf0rm3er@p3rf0rm3er: ~/ATC_CTF
(p3rf0rm3er@p3rf0rm3er)~[~/ATC_CTF]
$ exiftool elfsnapshot.png
ExifTool Version Number      : 13.44
File Name                    : elfsnapshot.png
Directory                   : .
File Size                    : 121 bytes
File Modification Date/Time   : 2026:01:31 13:20:01+01:00
File Access Date/Time        : 2026:02:01 22:22:31+01:00
File Inode Change Date/Time   : 2026:02:01 22:22:31+01:00
File Permissions              : -rw-rw-r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                  : 1
Image Height                  : 1
Bit Depth                    : 8
Color Type                    : RGB with Alpha
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
Comment                      : shake it gently: atcctf_snowglobe
Image Size                   : 1x1
Megapixels                   : 0.000001

(p3rf0rm3er@p3rf0rm3er)~[~/ATC_CTF]
$
```

Flag

atcctf_snowglobe

Conclusion

This challenge demonstrates how sensitive information can be hidden inside file metadata. Tools like exiftool allow quick extraction of such data, making metadata analysis an essential forensic skill.