Forensics CTF 2

Platform: picoCTF 2025

Challenge Name: RED

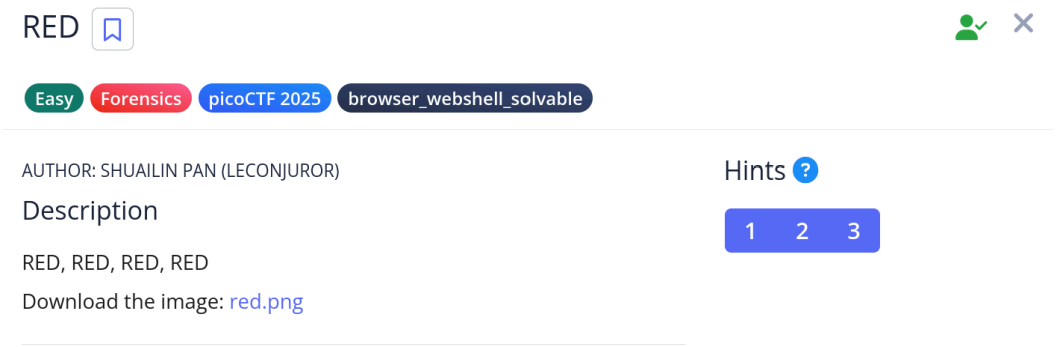
Category: Forensics

Difficulty: Easy

Submitted By: Gurleen Kaur Brar

Objective

The goal of the challenge was to extract hidden data embedded within an image file and decode it to reveal the CTF flag. This task involved detecting steganographic content, identifying encodings, and using the right tools to decode it.



Files and Tools Used

- **File Provided:** `red.png` (image file)
- **Tools Used:**
  - Kali Linux Terminal
  - `zsteg` – for steganographic data extraction
  - CyberChef – for Base64 decoding

Step-by-Step Process

Step 1: Run zsteg on the Image

The image likely contained hidden data using steganography. To analyze it, I ran:

```
zsteg red.png
```

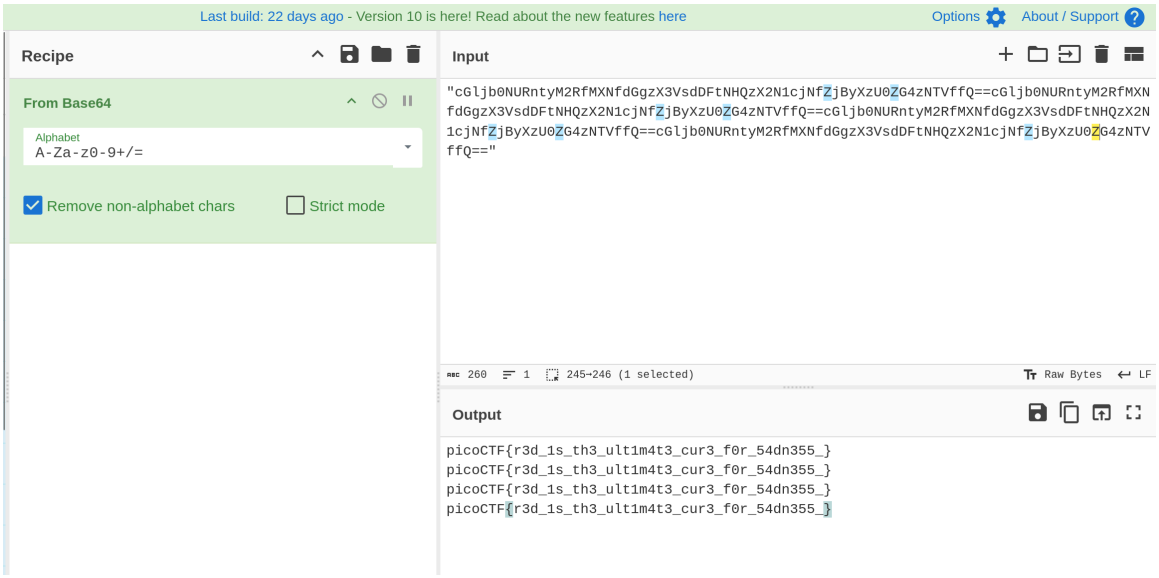
This command listed several embedded data entries in different color channels and bits. One of them included Base64-encoded strings.

Step 2: Copy and Decode Base64 String

I copied one of the longer Base64 strings. To decode it, I used **CyberChef** with the "From Base64" recipe.

Step 3: Get the Flag

The output of the decoded Base64 string in CyberChef revealed the flag:



Flag Submitted

The extracted flag was:

```
picoCTF{r3d_1s_th3_ult1m4t3_cur3_f0r_54dn355_}
```

The flag was successfully submitted and confirmed as correct.