Forensics CTF 5

Platform: picoCTF 2025

Challenge Name: Flags Are Stepic

Category: Forensics

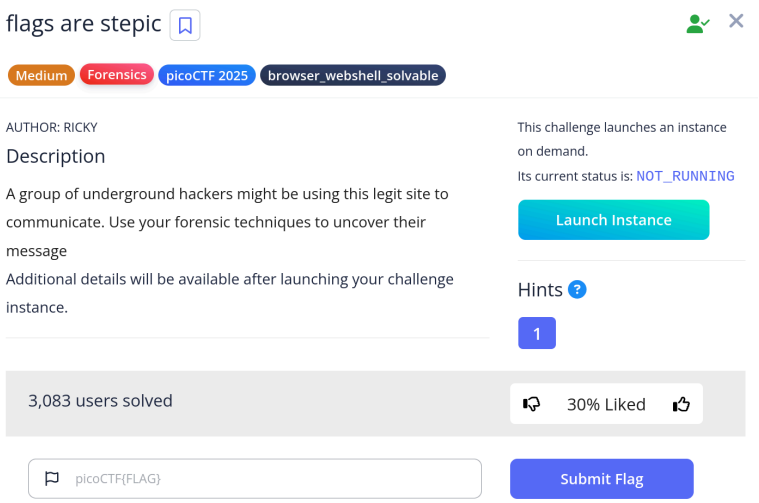
Difficulty: Medium

Submitted By: Gurleen Kaur Brar

Objective

The objective of this challenge was to uncover hidden communication embedded in a legitimate-looking image. The task involved identifying the image in question, detecting hidden data using steganography techniques, and retrieving the embedded message.

Challenge Description



Files and Tools Used

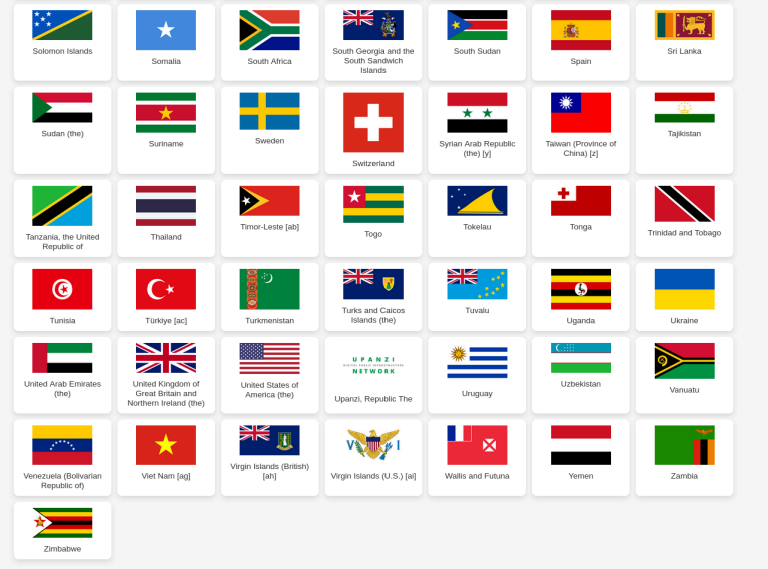
- **Files Provided:** `upz.png` (image from webpage)

- **Tools Used:**
  - Browser Developer Tools (for locating image source)
  - Python with `PIL` and `stepic` libraries
  - VS Code / Kali Linux terminal

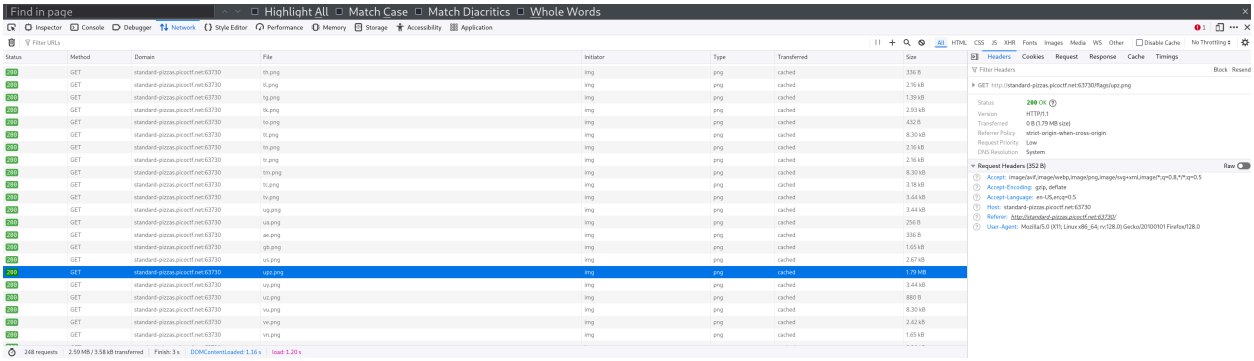
Step-by-Step Process

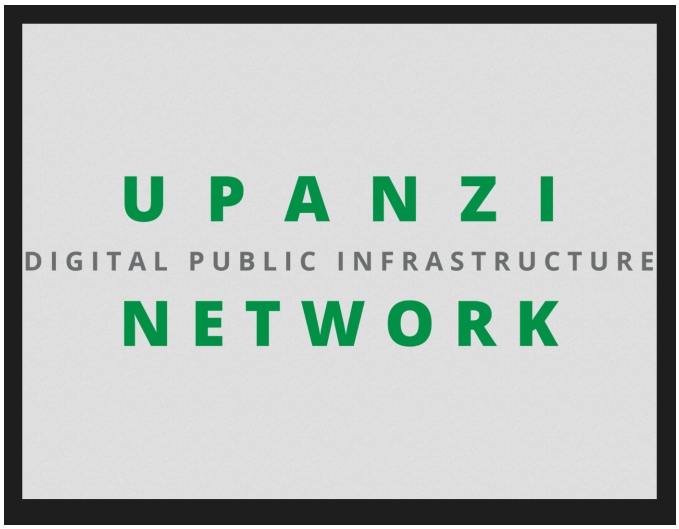
Step 1: Inspect Webpage and Identify Image

Using the browser's developer tools, I examined the elements on the challenge webpage and discovered an image titled `upz.png` labeled "UPANZI NETWORK – Digital Public Infrastructure".



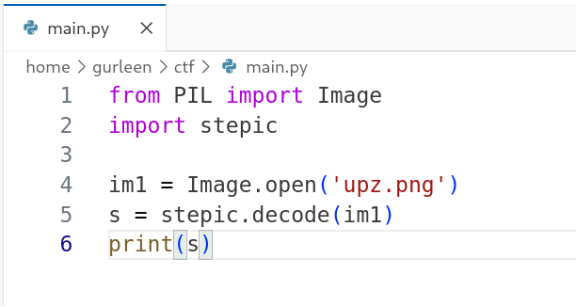
The flag image size was significantly larger than the other flags.





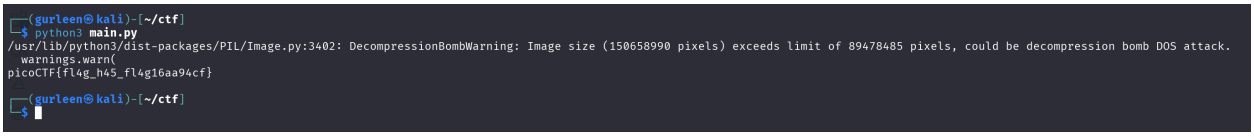
Step 2: Write Python Script to Decode Steganographic Content

Using the `stepic` library, I wrote a simple Python script to extract the hidden data from `upz.png`:



Step 3: Run Script and Extract the Flag

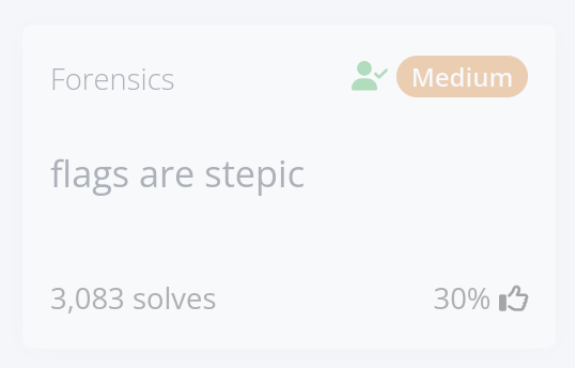
When I ran the script, it printed the decoded flag to the terminal:



Flag Submitted

```
picoCTF{fl4g_h45_fl4g16aa94cf}
```

The flag was correct and successfully submitted.


Forensics
Medium
flags are stepic
3,083 solves
30%