

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

The screenshot shows the challenge interface for 'flags are stepic'. At the top, the title is followed by a bookmark icon and a user icon. Below the title are four tags: 'Medium' (orange), 'Forensics' (red), 'picoCTF 2025' (blue), and 'browser_webshell_solvable' (dark blue). The main content area is split into two columns. The left column contains the author 'RICKY', a 'Description' section with the text 'A group of underground hackers might be using this legit site to communicate. Use your forensic techniques to uncover their message', and a note that 'Additional details will be available after launching your challenge instance.' The right column contains a status message 'This challenge launches an instance on demand. Its current status is: NOT_RUNNING' and a 'Launch Instance' button. Below this is a 'Hints' section with a question mark icon and a single hint numbered '1'. At the bottom, a grey bar shows '3,083 users solved' and '30% Liked'. Below that is a flag submission area with a text input containing 'picoCTF{FLAG}' and a 'Submit Flag' button.

flags are stepic

Medium Forensics picoCTF 2025 browser_webshell_solvable

AUTHOR: RICKY

Description

A group of underground hackers might be using this legit site to communicate. Use your forensic techniques to uncover their message

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.
Its current status is: NOT_RUNNING

Launch Instance

Hints ?

1

3,083 users solved 30% Liked

picoCTF{FLAG} Submit Flag

Files and Tools Used

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

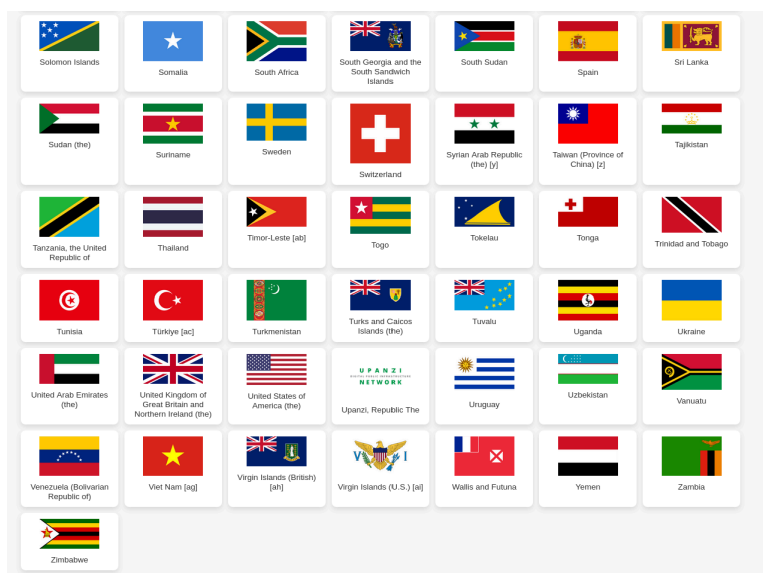
• Tools Used:

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

Step-by-Step Process

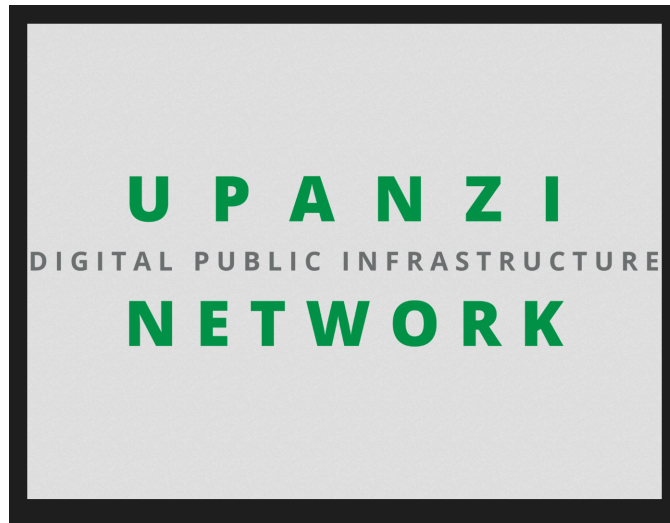
Step 1: Inspect Webpage and Identify Image

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.

Find in page							
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application							
Status	Method	Domain	File	Initiator	Type	Transformed	Size
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	330 B
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	276 KB
200	GET	standard-pizza.plc.cf.net:63730	tg.png	img	png	cached	1,39 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	2,63 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	452 B
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	8,30 KB
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	276 KB
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	276 KB
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	8,30 KB
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	378 KB
200	GET	standard-pizza.plc.cf.net:63730	fr.png	img	png	cached	3,44 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	3,44 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	268 B
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	330 B
200	GET	standard-pizza.plc.cf.net:63730	gh.png	img	png	cached	1,65 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	2,67 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	3,44 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	880 B
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	8,30 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	2,62 KB
200	GET	standard-pizza.plc.cf.net:63730	kg.png	img	png	cached	1,65 KB



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`:

```
main.py x
home > gurleen > ctf > main.py
1  from PIL import Image
2  import stepic
3
4  im1 = Image.open('upz.png')
5  s = stepic.decode(im1)
6  print(s)
```

Step 3: Run Script and Extract the Flag

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

```
(gurleen@kali)~/ctf
$ python3 main.py
/usr/lib/python3/dist-packages/PIL/Image.py:3402: DecompressionBombWarning: Image size (150658990 pixels) exceeds limit of 89478485 pixels, could be decompression bomb DOS attack.
warnings.warn(
picoCTF{fl4g_h45_fl4g16aa94cf}
(gurleen@kali)~/ctf
$
```

Flag Submitted

picoCTF{fl4g_h45_fl4g16aa94cf}

The flag was correct and successfully submitted.

Forensics



Medium

flags are stepic

3,083 solves

30%