Report on “Enhance” picoCTF project.

This practice assignment was a very interesting one. Just like a treasure hunt I was task to find the flag and report back.

Short description.

Evaluate the image provided and find the hidden flag.

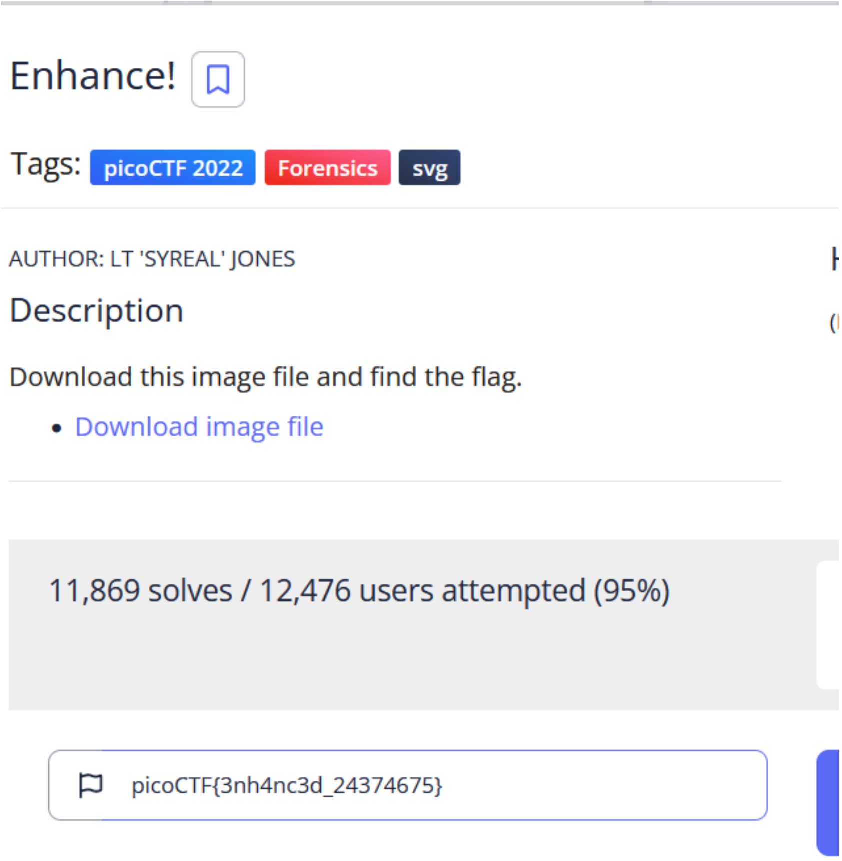
Skills needed.

Inspection skills, vigilance and pattern recognition.

Methodology of solving

1. I downloaded the file from the picoCTF website.
2. Then from reference to the class prior, I opened the file in edge and used the Ctrl+U key combination to view the source code of the page containing the picture.
3. After inspection I noticed a pattern that actually spells out picoCTF{. This prompted me to look further and notice the complete flag as required.
4. But the picoCTF indicated that the flag was incorrect so I actually had to make further observations and finally removed the whitespaces manually (although time inefficient 😁) which was my problem.

Screenshot of the flag.



Enhance!

AUTHOR: LT 'SYREAL' JONES

Description

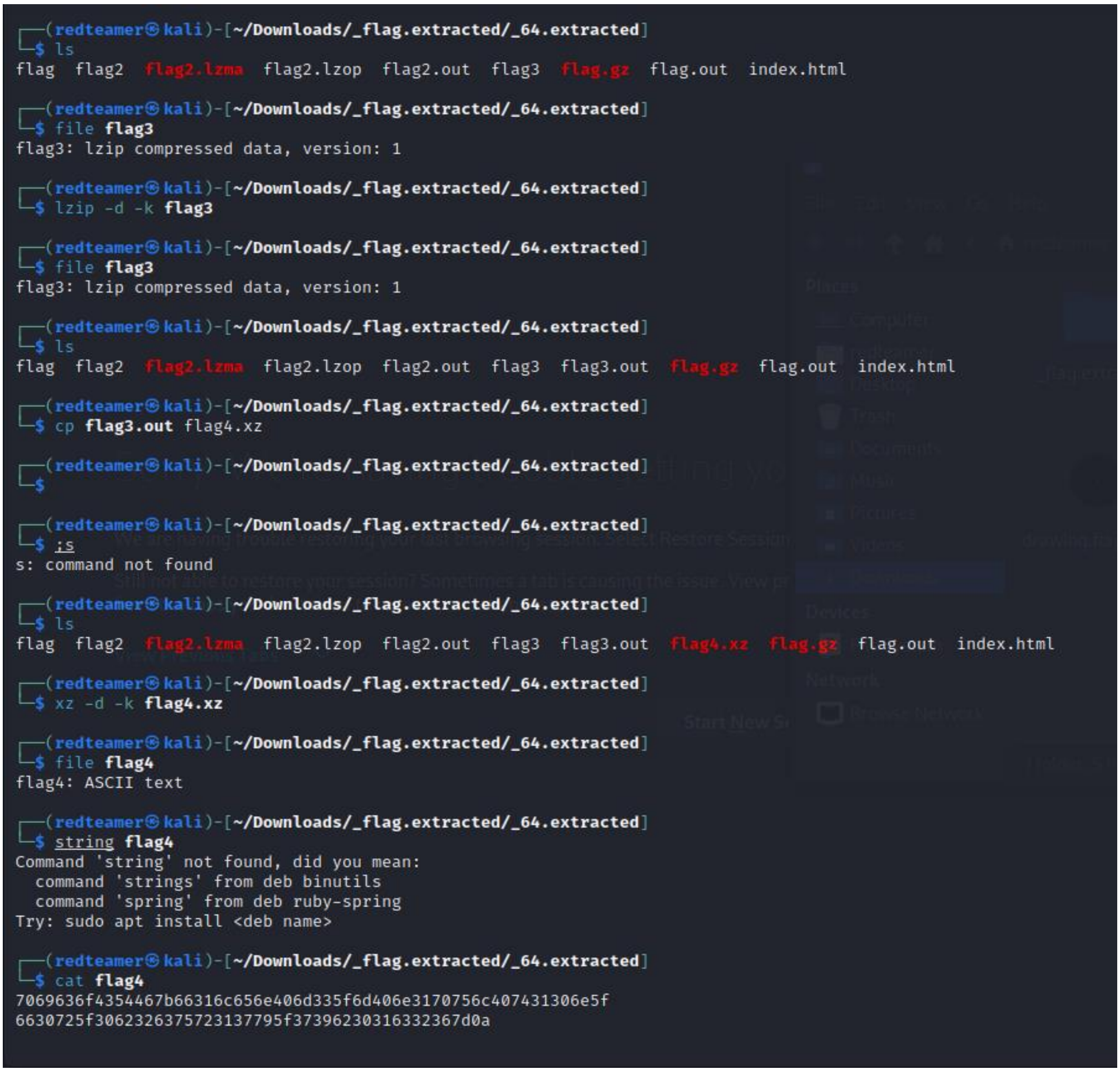
Download this image file and find the flag.

- Download image file

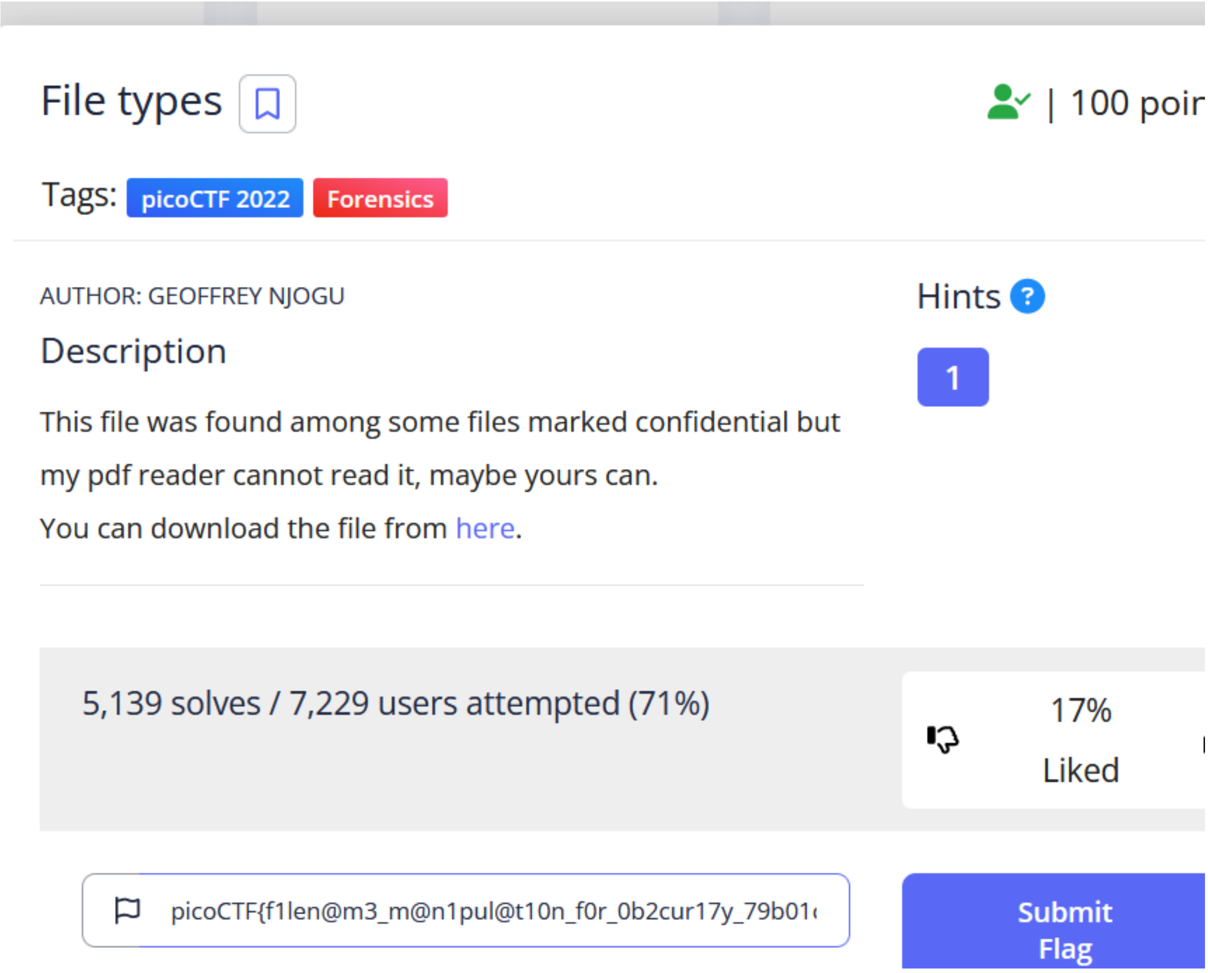
11,869 solves / 12,476 users attempted (95%)

picoCTF{3nh4nc3d_24374675}

For filetypes I went through a whole process of downloading extensions 😓 before finally getting the ACSII code for the flag. Below are screenshots and the flag



```
┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ ls
flag  flag2  flag2.lzma  flag2.lzop  flag2.out  flag3  flag.gz  flag.out  index.html

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ file flag3
flag3: lzip compressed data, version: 1

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ lzip -d -k flag3

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ file flag3
flag3: lzip compressed data, version: 1

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ ls
flag  flag2  flag2.lzma  flag2.lzop  flag2.out  flag3  flag3.out  flag.gz  flag.out  index.html

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ cp flag3.out flag4.xz

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ :s
s: command not found

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ ls
flag  flag2  flag2.lzma  flag2.lzop  flag2.out  flag3  flag3.out  flag4.xz  flag.gz  flag.out  index.html

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ xz -d -k flag4.xz

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ file flag4
flag4: ASCII text

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ string flag4
Command 'string' not found, did you mean:
  command 'strings' from deb binutils
  command 'spring' from deb ruby-spring
Try: sudo apt install <deb name>

┌──(redteamer㉿kali)-[~/Downloads/_flag.extracted/_64.extracted]
└─$ cat flag4
7069636f4354467b66316c656e406d335f6d406e3170756c407431306e5f
6630725f30623263757231377956f37396230316332367d0a
```



File types

Tags:

AUTHOR: GEOFFREY NJOGU

Description

This file was found among some files marked confidential but my pdf reader cannot read it, maybe yours can.

You can download the file from here.

5,139 solves / 7,229 users attempted (71%)

picoCTF{f1len@m3_m@n1pul@t10n_f0r_0b2cur17y_79b01