

LinkedIn: [Kelvin Kimotho](#)

GitHub: [Kelvin Kimotho](#)

extensions

Medium

Forensics

picoCTF 2019

AUTHOR: SANJAY C/DANNY

Description

This is a really weird text file **TXT**? Can you find the flag?

Hints ?

1

2

How do operating systems know what kind of file it is?
(It's not just the ending!)

Solution

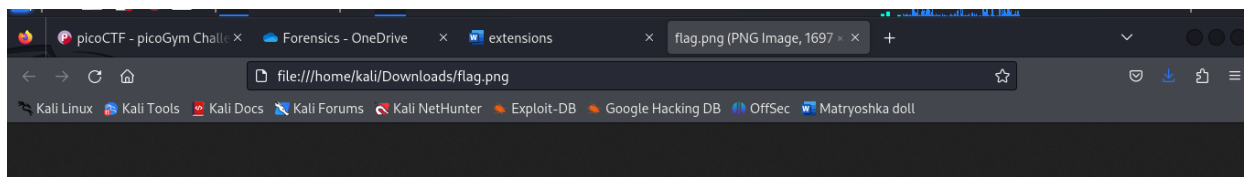
I downloaded the file for this analysis, it had a **.txt** file extension. It is good practice to confirm the file type because file extensions are deceiving. I use the **file** tool which tells what type a file is irregardless of the file extension.

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ ls
flag.txt
(kali@kali)-[~/Downloads]
$ file flag.txt
flag.txt: PNG image data, 1697 x 608, 8-bit/color RGB, non-interlaced
(kali@kali)-[~/Downloads]
$
```

The toll identifies the file as a **PNG image** despite of it having a **.txt** extension. I went ahead and changed the extension to **.png** first.

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ mv flag.txt flag.png
(kali@kali)-[~/Downloads]
$ ls
flag.png
(kali@kali)-[~/Downloads]
$
```

I then opened the file as an image and that's how I retrieved the flag.



picoCTF{now_you_know_about_extensions}

