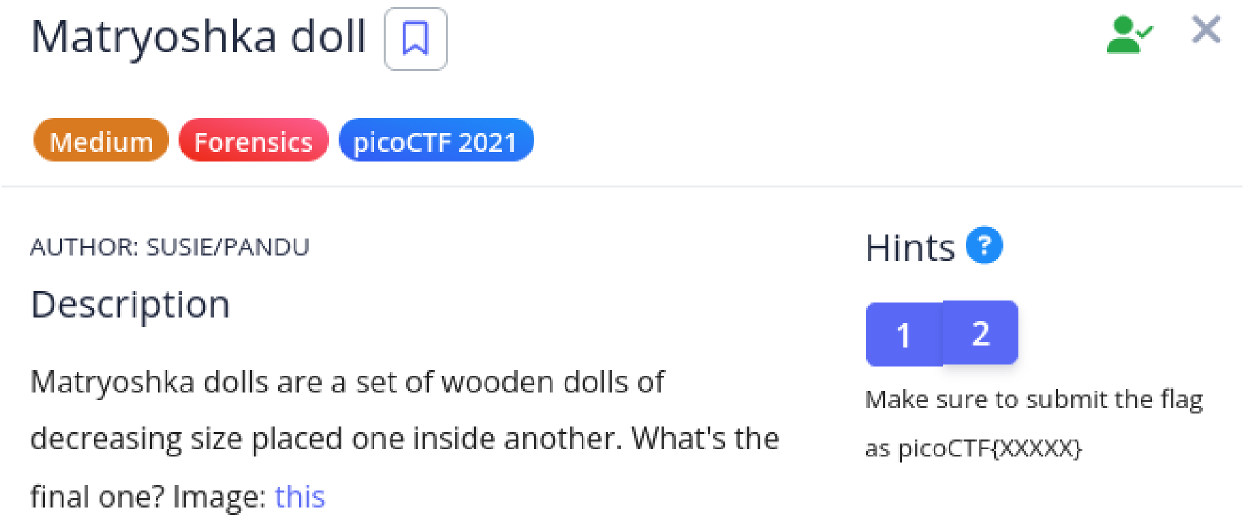
LinkedIn: Kelvin Kimotho

GitHub: Kelvin Kimotho



Matryoshka doll

Medium Forensics picoCTF 2021

AUTHOR: SUSIE/PANDU

Description

Matryoshka dolls are a set of wooden dolls of decreasing size placed one inside another. What's the final one? Image: this

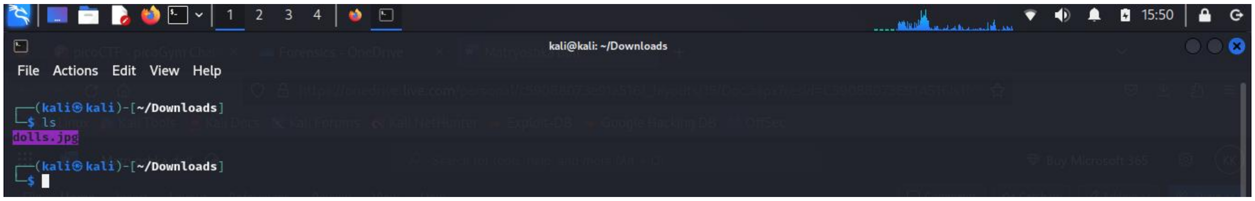
Hints ?

1 2

Make sure to submit the flag as picoCTF{XXXXX}

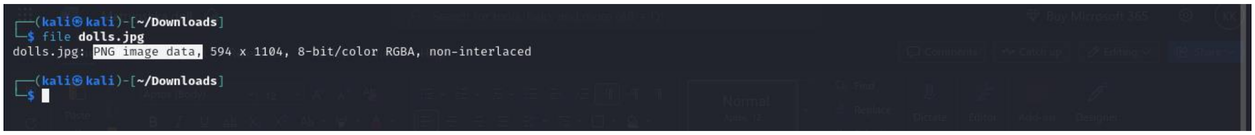
Solution

I downloaded the dolls.jpg file for analysis.



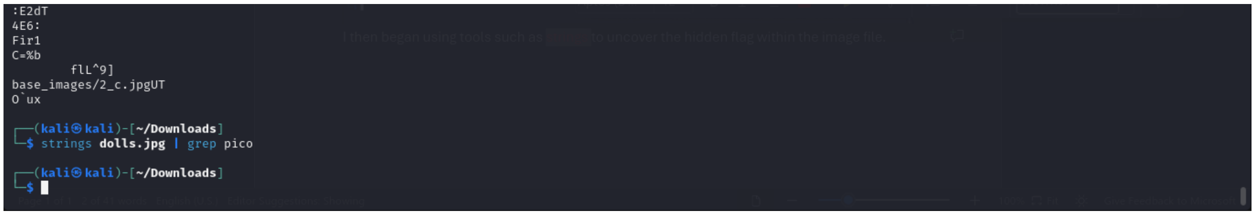
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
dolls.jpg

┌──(kali㉿kali)-[~/Downloads]
└─$ █
```

I then checked what type of a file it was.



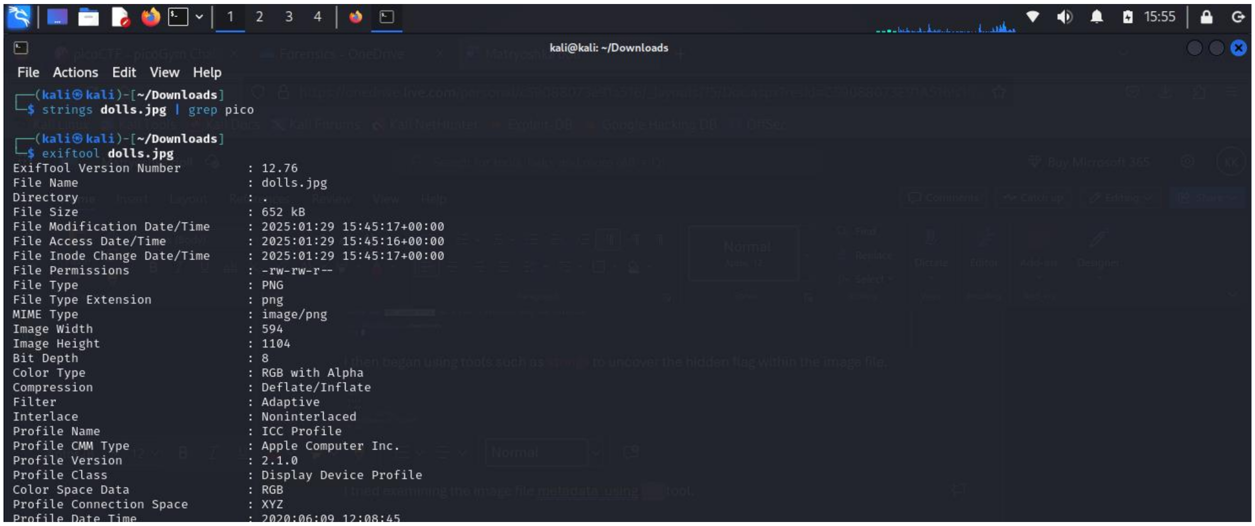
```
┌──(kali㉿kali)-[~/Downloads]
└─$ file dolls.jpg
dolls.jpg: PNG image data, 594 x 1104, 8-bit/color RGBA, non-interlaced

┌──(kali㉿kali)-[~/Downloads]
└─$ █
```

I then began using tools such as strings to uncover the hidden flag within the image file.



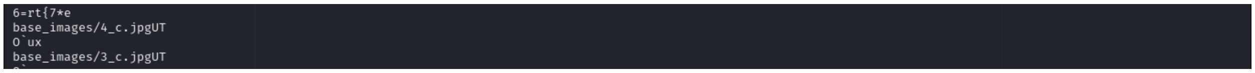
```
:E2dT
4E6:
Fir1
C=%b
        flL^9]
base_images/2_c.jpgUT
O`ux

┌──(kali㉿kali)-[~/Downloads]
└─$ strings dolls.jpg | grep pico

┌──(kali㉿kali)-[~/Downloads]
└─$ █
```

I tried examining the image file metadata using exif tool. I discovered nothing suspicious from the metadata,



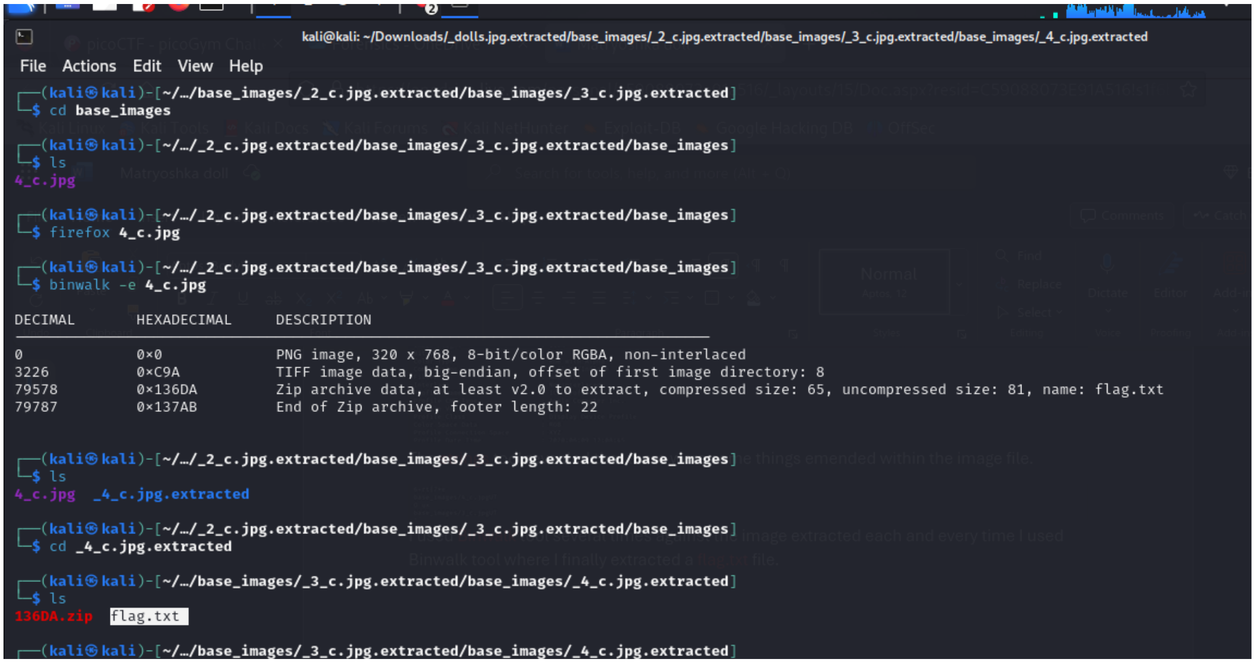
```
┌──(kali㉿kali)-[~/Downloads]
└─$ strings dolls.jpg | grep pico

┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool dolls.jpg
ExifTool Version Number         : 12.76
File Name                       : dolls.jpg
Directory                       : .
File Size                       : 652 kB
File Modification Date/Time     : 2025:01:29 15:45:17+00:00
File Access Date/Time           : 2025:01:29 15:45:16+00:00
File Inode Change Date/Time     : 2025:01:29 15:45:17+00:00
File Permissions                : -rw-rw-r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 594
Image Height                    : 1104
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Profile Name                    : ICC Profile
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2020:06:09 12:08:45
```

The strings tool revealed that there were some things emended within the image file.



```
6=rt{7*e
base_images/4_c.jpgUT
O`ux
base_images/3_c.jpgUT
```

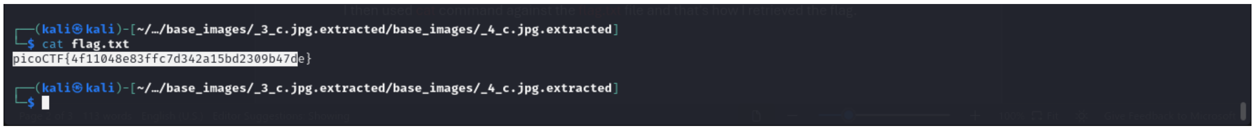
I used Binwalk tool several times against the image extracted each and every time I used Binwalk tool where I finally extracted a flag.txt file.



kali@kali: ~/Downloads/_dolls.jpg.extracted/base_images/_2_c.jpg.extracted/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/…/base_images/_2_c.jpg.extracted/base_images/_3_c.jpg.extracted]
└─$ cd base_images

┌──(kali㉿kali)-[~/…/_2_c.jpg.extracted/base_images/_3_c.jpg.extracted/base_images]
└─$ ls
4_c.jpg

┌──(kali㉿kali)-[~/…/_2_c.jpg.extracted/base_images/_3_c.jpg.extracted/base_images]
└─$ firefox 4_c.jpg

┌──(kali㉿kali)-[~/…/_2_c.jpg.extracted/base_images/_3_c.jpg.extracted/base_images]
└─$ binwalk -e 4_c.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 320 x 768, 8-bit/color RGBA, non-interlaced
3226          0xC9A           TIFF image data, big-endian, offset of first image directory: 8
79578         0x136DA         Zip archive data, at least v2.0 to extract, compressed size: 65, uncompressed size: 81, name: flag.txt
79787         0x137AB         End of Zip archive, footer length: 22


┌──(kali㉿kali)-[~/…/_2_c.jpg.extracted/base_images/_3_c.jpg.extracted/base_images]
└─$ ls
4_c.jpg  _4_c.jpg.extracted

┌──(kali㉿kali)-[~/…/_2_c.jpg.extracted/base_images/_3_c.jpg.extracted/base_images]
└─$ cd _4_c.jpg.extracted

┌──(kali㉿kali)-[~/…/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted]
└─$ ls
136DA.zip  flag.txt

┌──(kali㉿kali)-[~/…/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted]
```

I then used cat command against the flag.txt file and that's how I retrieved the flag picoCTF{4f11048e83ffc7d342a15bd2309b47de}



```
┌──(kali㉿kali)-[~/…/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted]
└─$ cat flag.txt
picoCTF{4f11048e83ffc7d342a15bd2309b47de}

┌──(kali㉿kali)-[~/…/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted]
└─$ 
```