Description

The Network Operations Center (NOC) of your local institution picked up a suspicious file, they're getting conflicting information on what type of file it is. They've brought you in as an external expert to examine the file. Can you extract all the information from this strange file? Download the suspicious file [here](#).

Hints

- This problem can be solved by just opening the file in different ways

Solución

```
┌──(kali㊨kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ ls
flag2of2-final.pdf  secret-of-polyglot.md

┌──(kali㊨kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ file flag2of2-final.pdf
flag2of2-final.pdf: PNG image data, 50 x 50, 8-bit/color RGBA, non-interlaced

┌──(kali㊨kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ exiftool flag2of2-final.pdf
ExifTool Version Number         : 12.76
File Name                       : flag2of2-final.pdf
Directory                       : .
File Size                       : 3.4 kB
File Modification Date/Time     : 2024:02:07 12:50:38-05:00
File Access Date/Time           : 2024:11:07 12:13:54-05:00
File Inode Change Date/Time     : 2024:11:07 12:13:01-05:00
File Permissions                : -rwxrwx---
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 50
Image Height                    : 50
Bit Depth                       : 8
Color Type                      : RGB with Alpha
```

```
Compression                   : Deflate/Inflate
Filter                        : Adaptive
Interlace                     : Noninterlaced
Profile Name                  : ICC profile
Profile CMM Type              : Little CMS
Profile Version               : 4.3.0
Profile Class                 : Display Device Profile
Color Space Data              : RGB
Profile Connection Space      : XYZ
Profile Date Time             : 2023:11:02 17:42:31
Profile File Signature        : acsp
Primary Platform              : Apple Computer Inc.
CMM Flags                     : Not Embedded, Independent
Device Manufacturer           :
Device Model                  :
Device Attributes             : Reflective, Glossy, Positive, Color
Rendering Intent              : Perceptual
Connection Space Illuminant   : 0.9642 1 0.82491
Profile Creator               : Little CMS
Profile ID                    : 0
Profile Description           : GIMP built-in sRGB
Profile Copyright             : Public Domain
Media White Point             : 0.9642 1 0.82491
Chromatic Adaptation          : 1.04788 0.02292 -0.05022 0.02959 0.99048
-0.01707 -0.00925 0.01508 0.75168
Red Matrix Column             : 0.43604 0.22249 0.01392
Blue Matrix Column            : 0.14305 0.06061 0.71393
Green Matrix Column           : 0.38512 0.7169 0.09706
Red Tone Reproduction Curve   : (Binary data 32 bytes, use -b option to
extract)
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to
extract)
Blue Tone Reproduction Curve  : (Binary data 32 bytes, use -b option to
extract)
Chromaticity Channels         : 3
Chromaticity Colorant         : Unknown
Chromaticity Channel 1        : 0.64 0.33002
Chromaticity Channel 2        : 0.3 0.60001
Chromaticity Channel 3        : 0.15001 0.06
Device Mfg Desc               : GIMP
Device Model Desc             : sRGB
Pixels Per Unit X             : 11811
Pixels Per Unit Y             : 11811
Pixel Units                   : meters
Modify Date                   : 2023:11:02 17:57:06
Comment                       : Created with GIMP
```

```
Warning                         : [minor] Trailer data after PNG IEND chunk
Image Size                      : 50x50
Megapixels                      : 0.003


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ eog flag2of2-final.pdf


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ mv flag2of2-final.pdf flag2of2-final.png


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ ls
flag2of2-final.png  secret-of-polyglot.md


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ eog flag2of2-final.png
^C


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ ls
flag2of2-final.png  secret-of-polyglot.md


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ cp flag2of2-final.png flag2of2-final.pdf


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ ls
flag2of2-final.pdf  flag2of2-final.png  secret-of-polyglot.md


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$ open flag2of2-final.pdf &
[1] 4715


┌──(kali㊉kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└─$
[1]  + done       open flag2of2-final.pdf
┌──(kali㊉kali)-
```
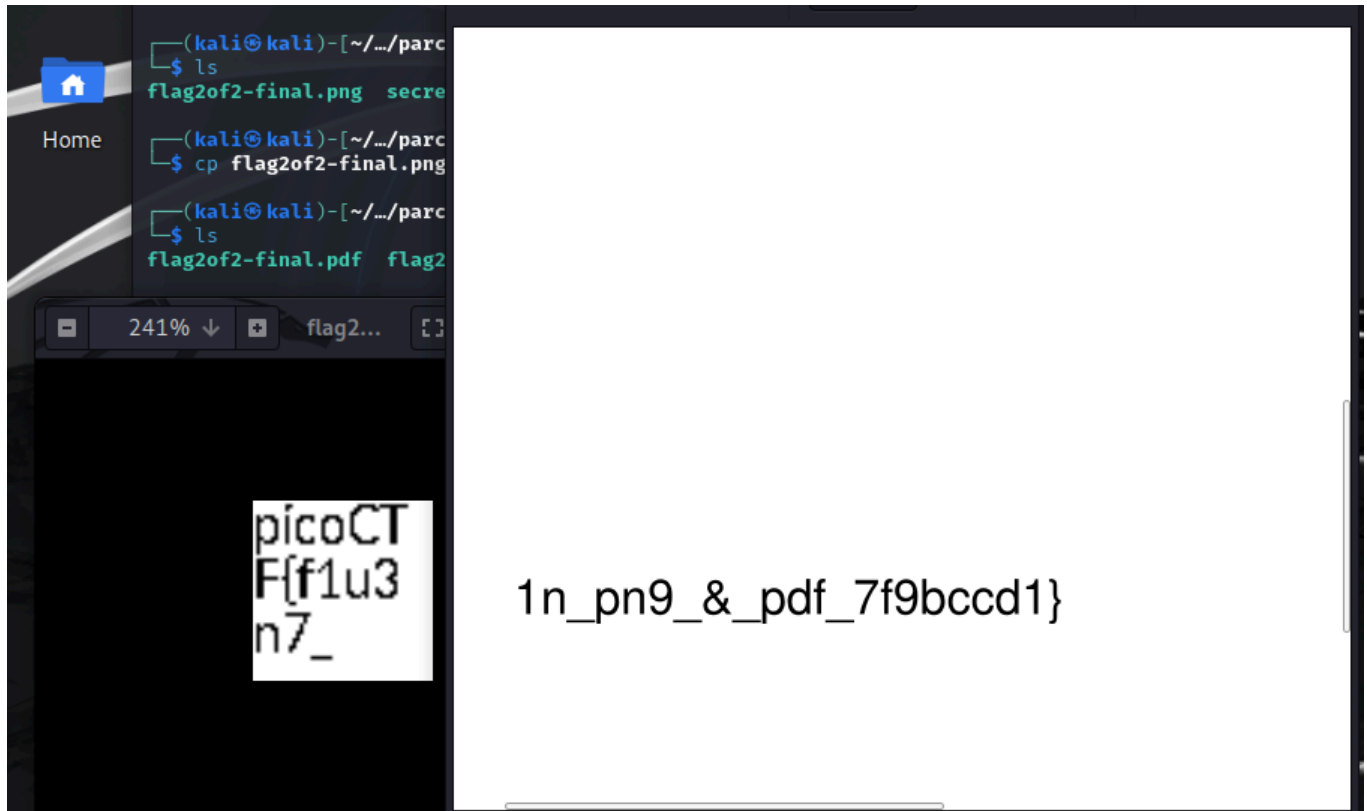
```
[~/.../parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└$ eog flag2of2-final.png &
[1] 4846

┌──(kali㉿kali)-
[~/.../parciales/parcial_02/parte_04_forensic_02/secret_of_the_polyglot]
└$
```


Bandera

```
flag: picoCTF{f1u3n7_1n_pn9_&_pdf_7f9bccd1}
```

Notas Adicionales

Sólo se tuvo que hacer una copia del documento pero en extensión `.png` y abrirlos por separado a ambos y de este modo podemos ver ambas partes de la `flag`.

Referencias

·