Description

Ron just found his own copy of advanced potion making, but its been corrupted by some kind of spell. Help him recover it!

Challenge Endpoints	
Download advanced-potion-making	advanced-potion-making

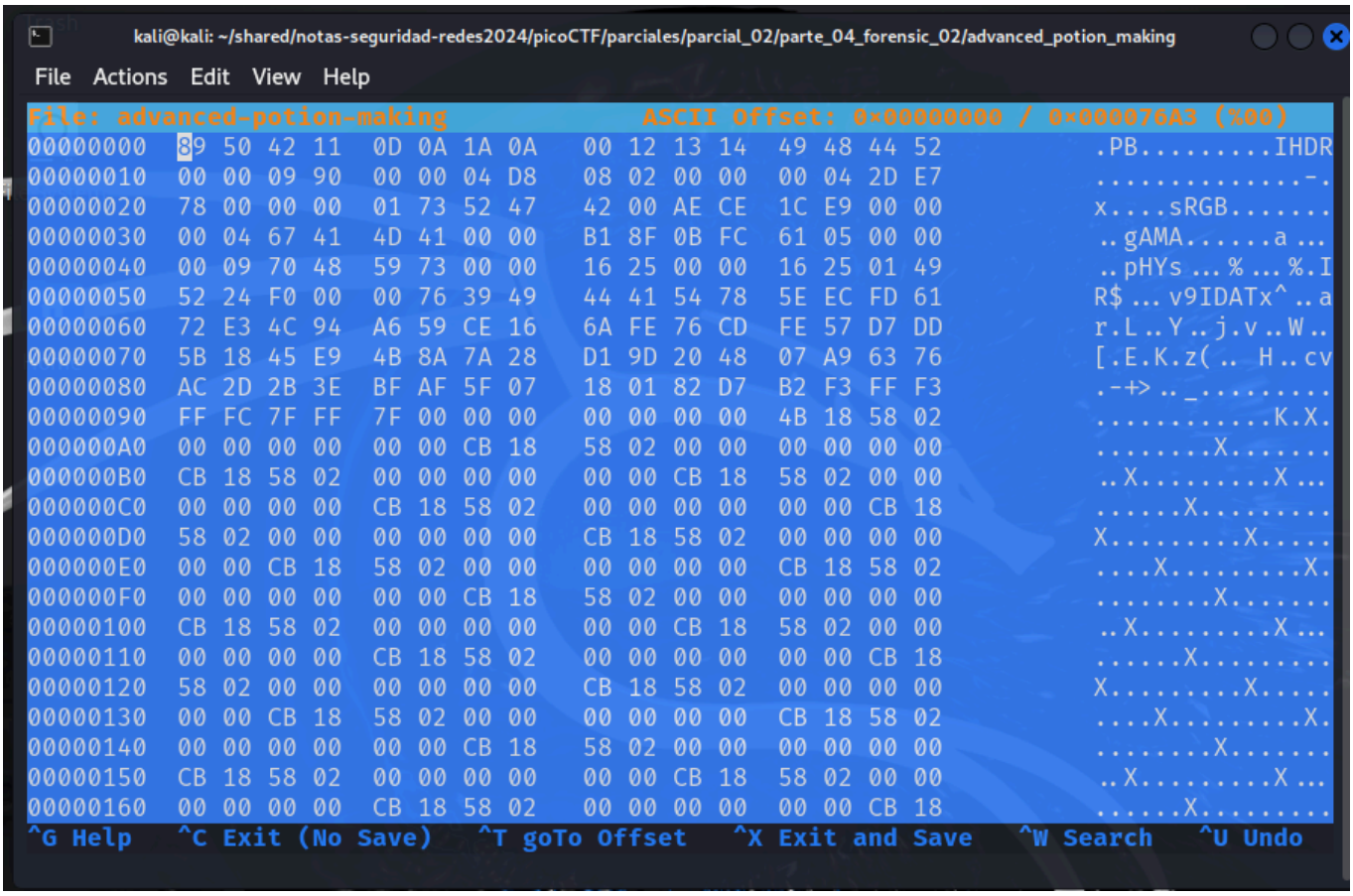
Hints

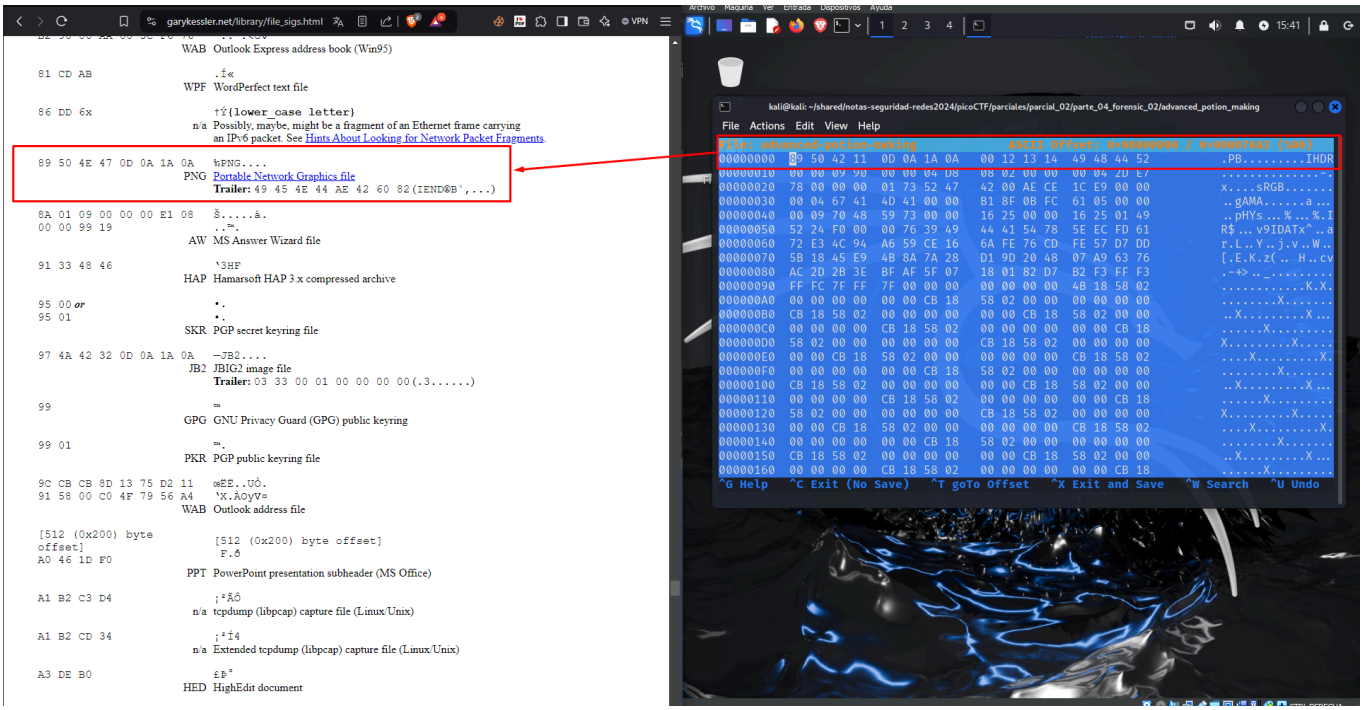
- (None)

Solución

```
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ ls
advanced-potion-making  advanced-potion-making.md

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ file advanced-potion-making
advanced-potion-making: data

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ hexeditor advanced-potion-making

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ file advanced-potion-making
advanced-potion-making: data

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ mv advanced-potion-making advanced-potion-making.png

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ ls
 advanced-potion-making.md         'Pasted image 20241107154151.png'
```

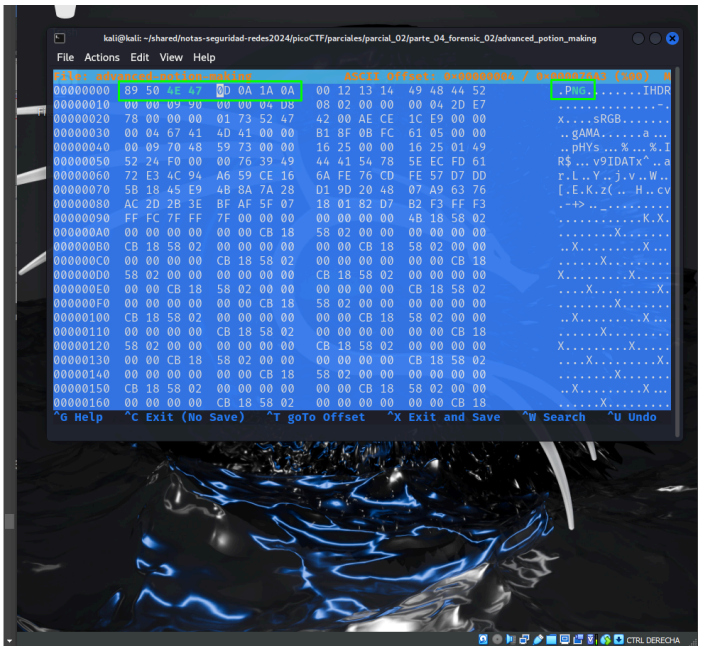
```
 advanced-potion-making.png        'Pasted image 20241107154418.png'
'Pasted image 20241107153950.png'

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ eog advanced-potion-making.png &
[1] 13518

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/advanced_potion_making]
└─$ eog advanced-potion-making.png &
[2] 13652

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



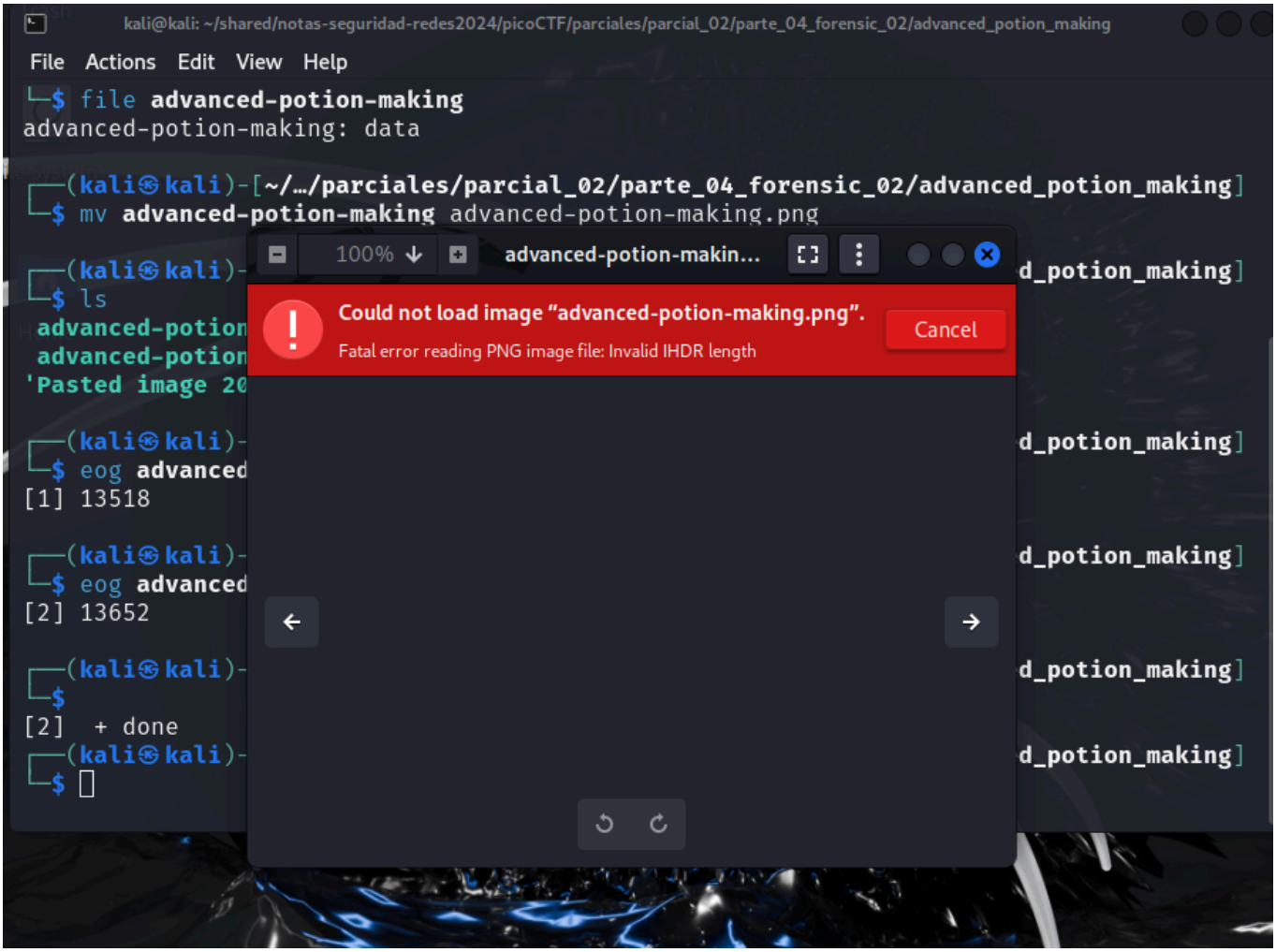


Se observa que el header no es el mismo al utilizar la herramienta de `exiftools`. Por lo que se procede a corregirlas:

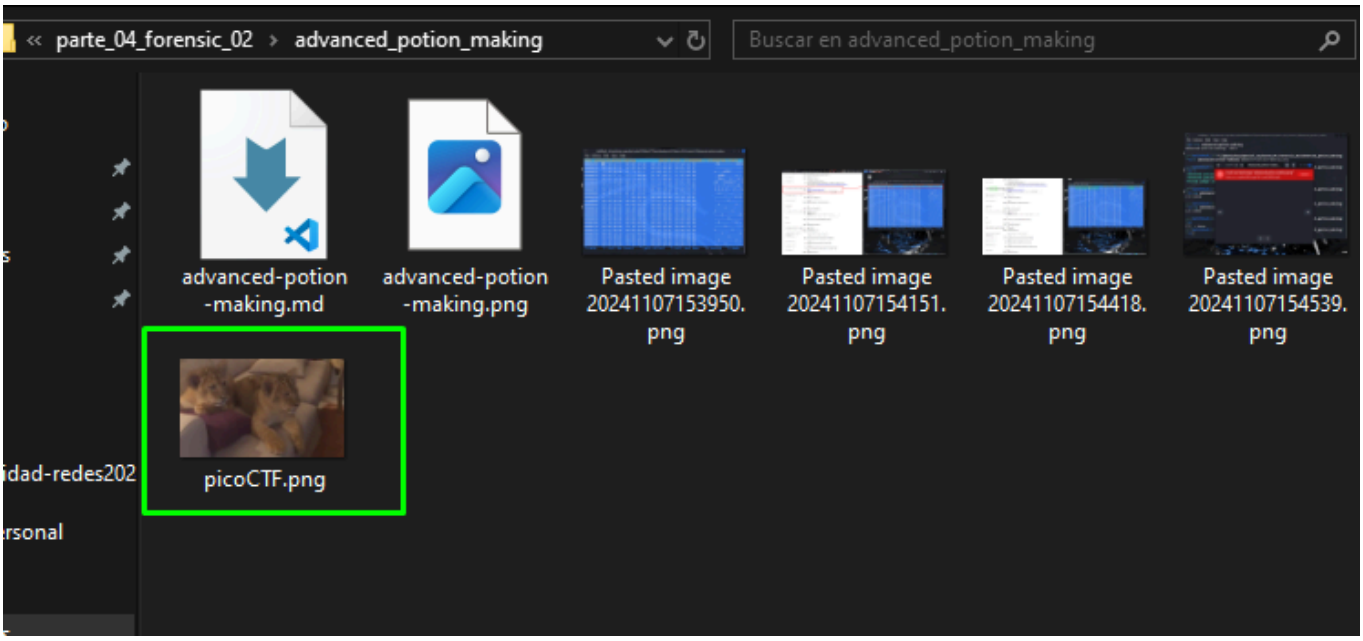
```
                        WPF  WordPerfect text file

86 DD 6x                     †Ý{lower_case letter}
                        n/a  Possibly, maybe, might be a fragment of an Ethernet frame carrying
                             an IPv6 packet. See Hints About Looking for Network Packet Fragments.

89 50 4E 47 0D 0A 1A 0A      ‰PNG....
                        PNG  Portable Network Graphics file
                             Trailer: 49 45 4E 44 AE 42 60 82(IEND®B`,...)

8A 01 09 00 00 00 E1 08      Š.....á.
00 00 99 19                  ..™.
                         AW  MS Answer Wizard file

91 33 48 46                  '3HF
                        HAP  Hamarsoft HAP 3.x compressed archive

95 00 or                     •.
95 01                        •.
                        SKR  PGP secret keyring file

97 4A 42 32 0D 0A 1A 0A      —JB2....
                         JB2 JBIG2 image file
                             Trailer: 03 33 00 01 00 00 00 00(.3......)

99                           ™
                        GPG  GNU Privacy Guard (GPG) public keyring

99 01                        ™.
                        PKR  PGP public keyring file

9C CB CB 8D 13 75 D2 11      œËË..UÒ.
91 58 00 C0 4F 79 56 A4      'X.ÀOyV¤
                        WAB  Outlook address file

[512 (0x200) byte            [512 (0x200) byte offset]
offset]                       F.ð
A0 46 1D F0
                        PPT  PowerPoint presentation subheader (MS Office)

A1 B2 C3 D4                  ¡²ÃÔ
                        n/a  tcpdump (libpcap) capture file (Linux/Unix)

A1 B2 CD 34                  ¡²Í4
                        n/a  Extended tcpdump (libpcap) capture file (Linux/Unix)

A3 DE B0                     £Þ°
                        HED  HighEdit document
```



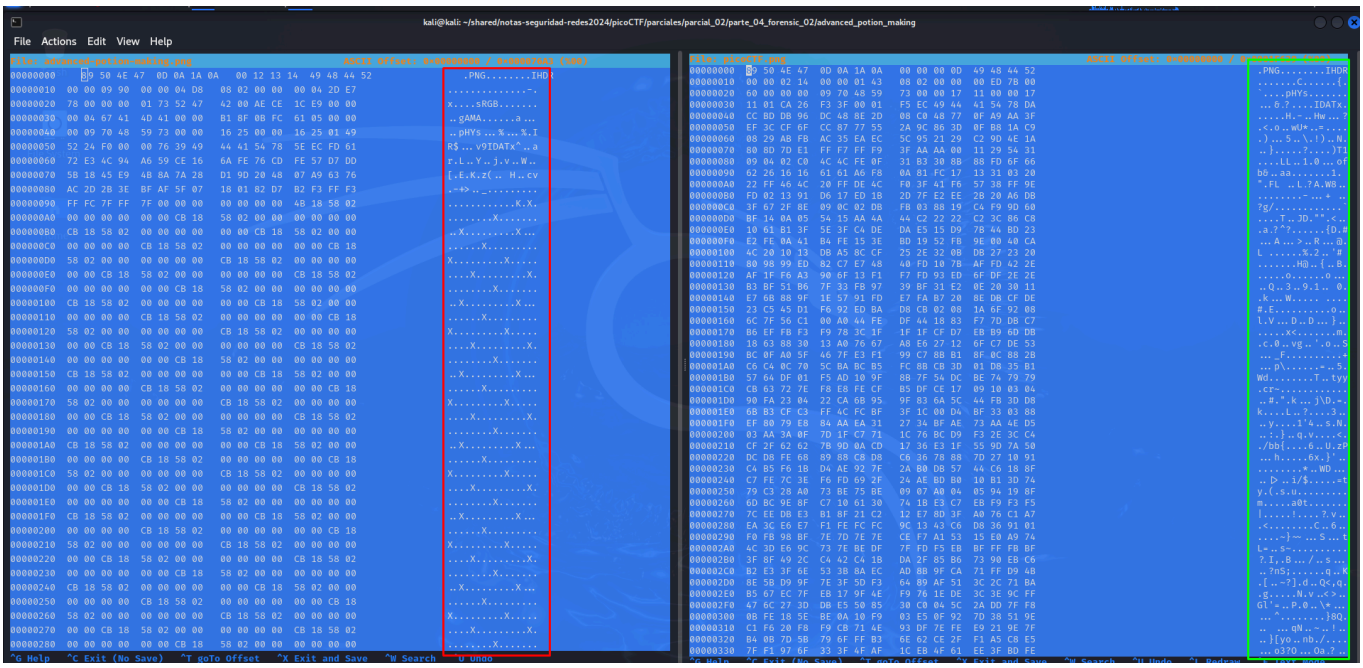
Cambiamos la extensión e intentamos abrir:



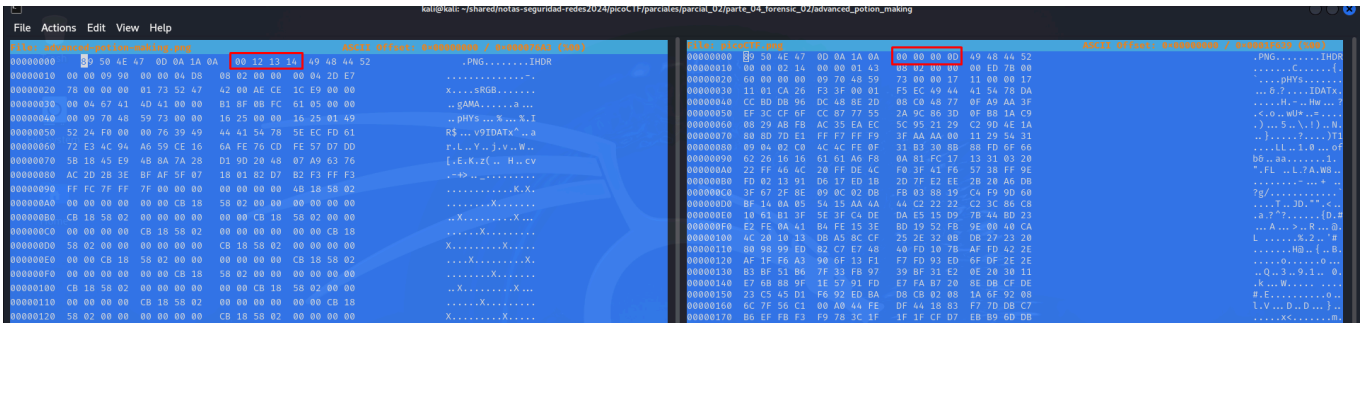
Abrimos otra imagen png que no esté dañada para comparar sus `magic bytes`

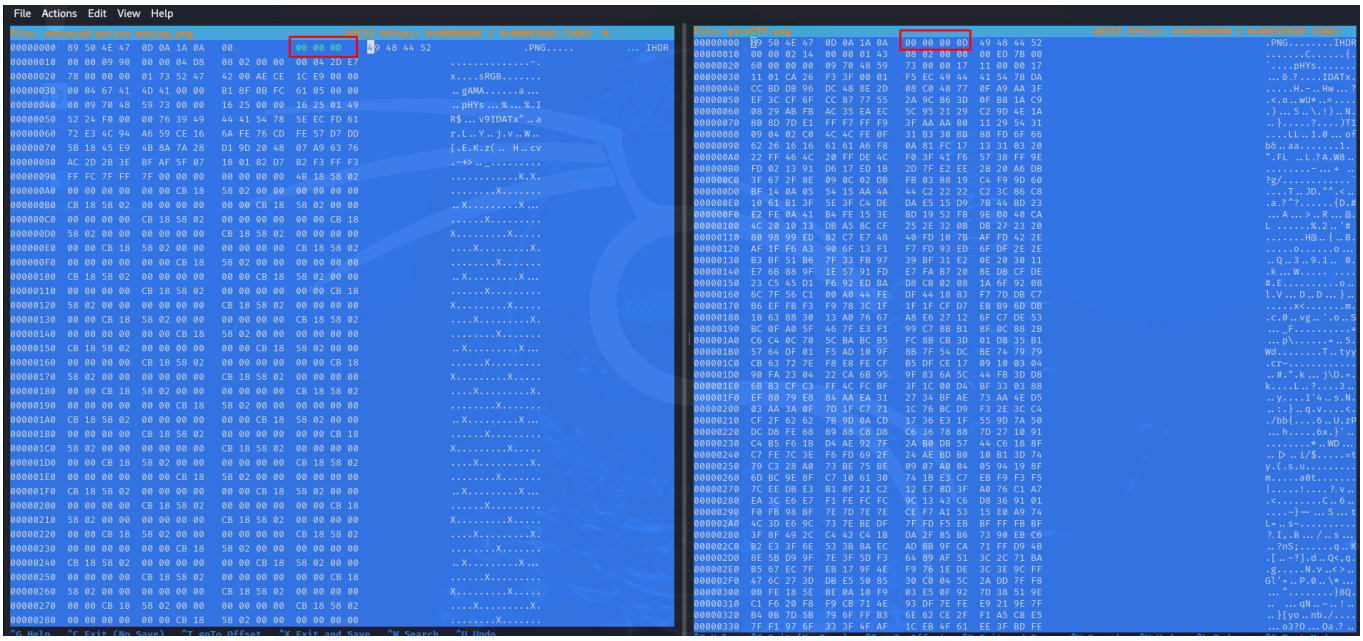


Observamos a la izquierda la imagen corrupta aún y a la derecha la que abrimos para comparar.

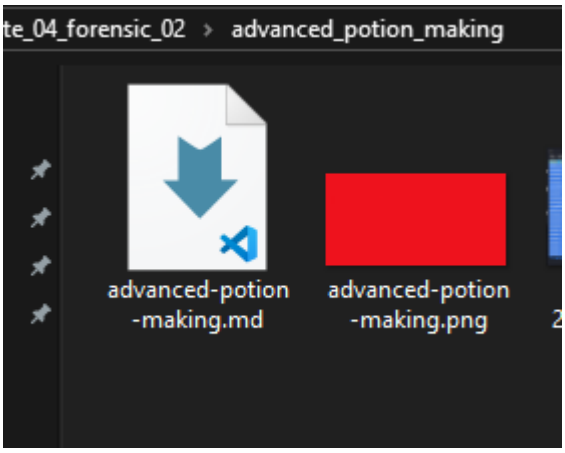


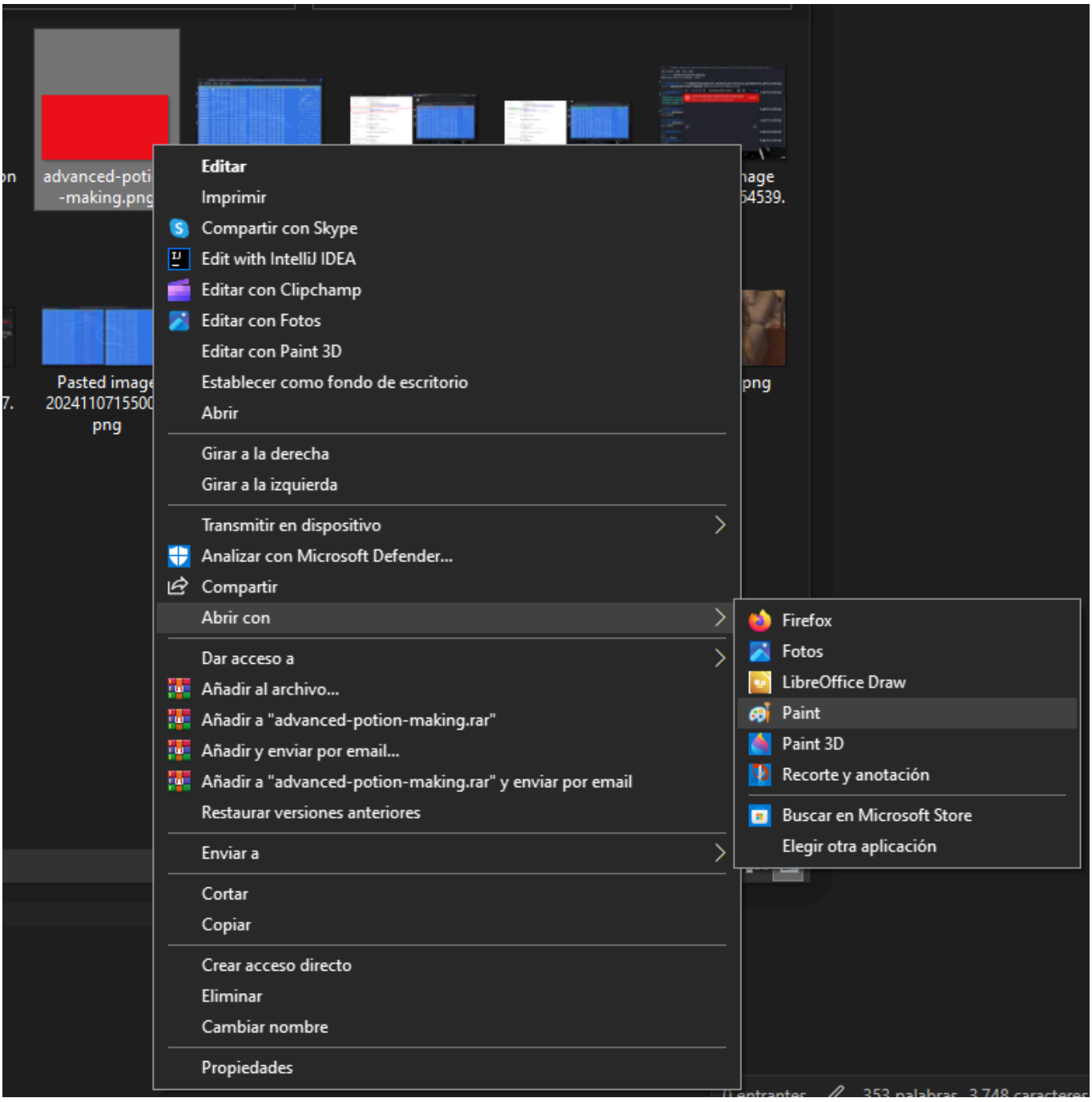
Cambiaremos los seleccionados en rojo para que coincidan con el de la derecha



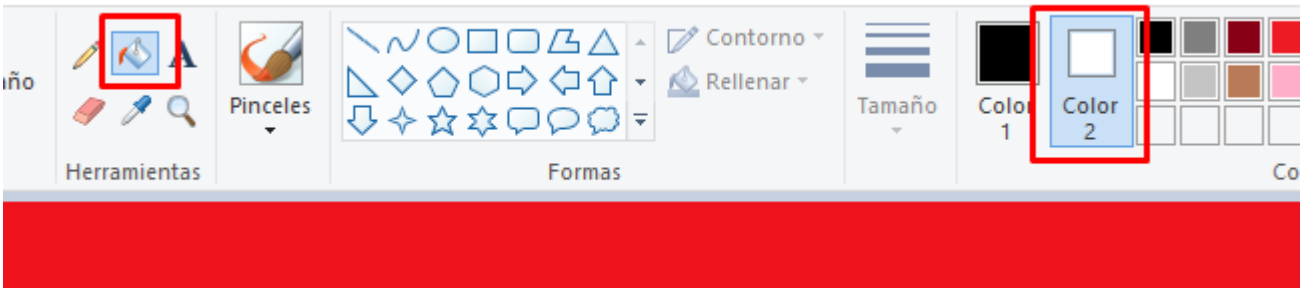


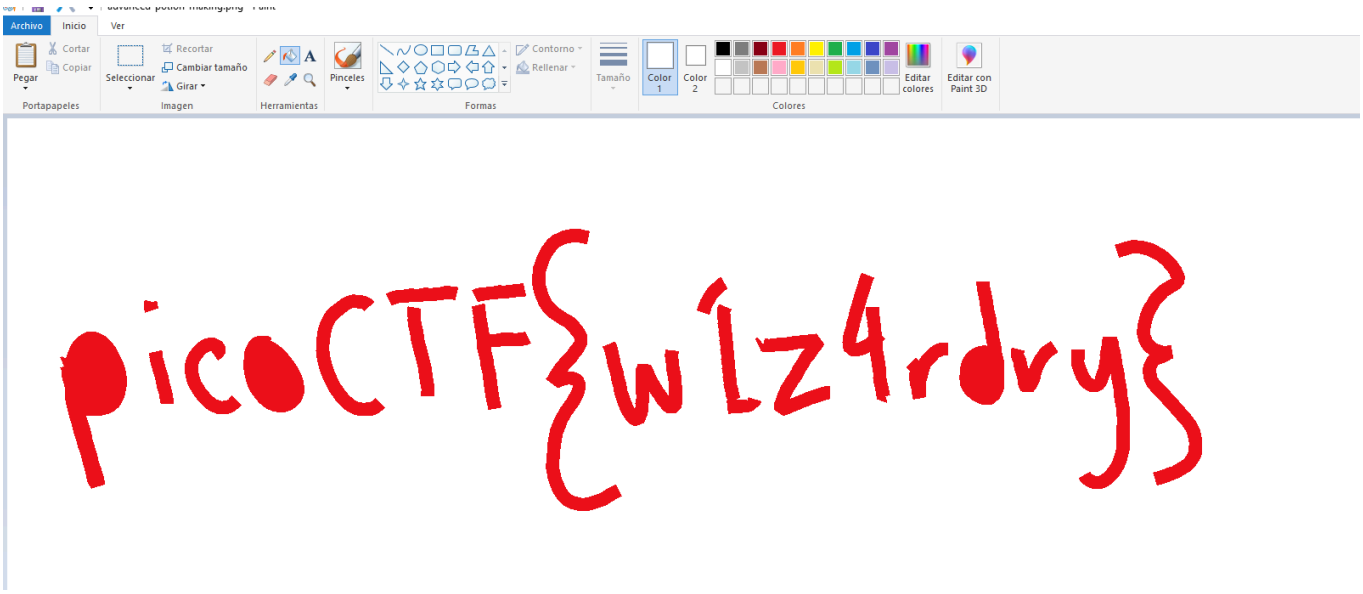
Procederemos a abrir la imagen en `paint` para aplicar la función `floodfill` y ver si encotramos algo que nos pueda interesar.


te_04_forensic_02 › advanced_potion_making
advanced-potion
-making.md
advanced-potion
-making.png


Editar
Imprimir
Compartir con Skype
Edit with IntelliJ IDEA
Editar con Clipchamp
Editar con Fotos
Editar con Paint 3D
Establecer como fondo de escritorio
Abrir
Girar a la derecha
Girar a la izquierda
Transmitir en dispositivo
Analizar con Microsoft Defender...
Compartir
Abrir con
Dar acceso a
Añadir al archivo...
Añadir a "advanced-potion-making.rar"
Añadir y enviar por email...
Añadir a "advanced-potion-making.rar" y enviar por email
Restaurar versiones anteriores
Enviar a
Cortar
Copiar
Crear acceso directo
Eliminar
Cambiar nombre
Propiedades
Firefox
Fotos
LibreOffice Draw
Paint
Paint 3D
Recorte y anotación
Buscar en Microsoft Store
Elegir otra aplicación

Ya estando en `paint` aplicamos `fill` con un color contrastante:





Finalmente encontramos así la bandera

Bandera

```
flag: picoCTF{w1z4rdry}
```

Notas Adicionales

Referencias

- file-signatures