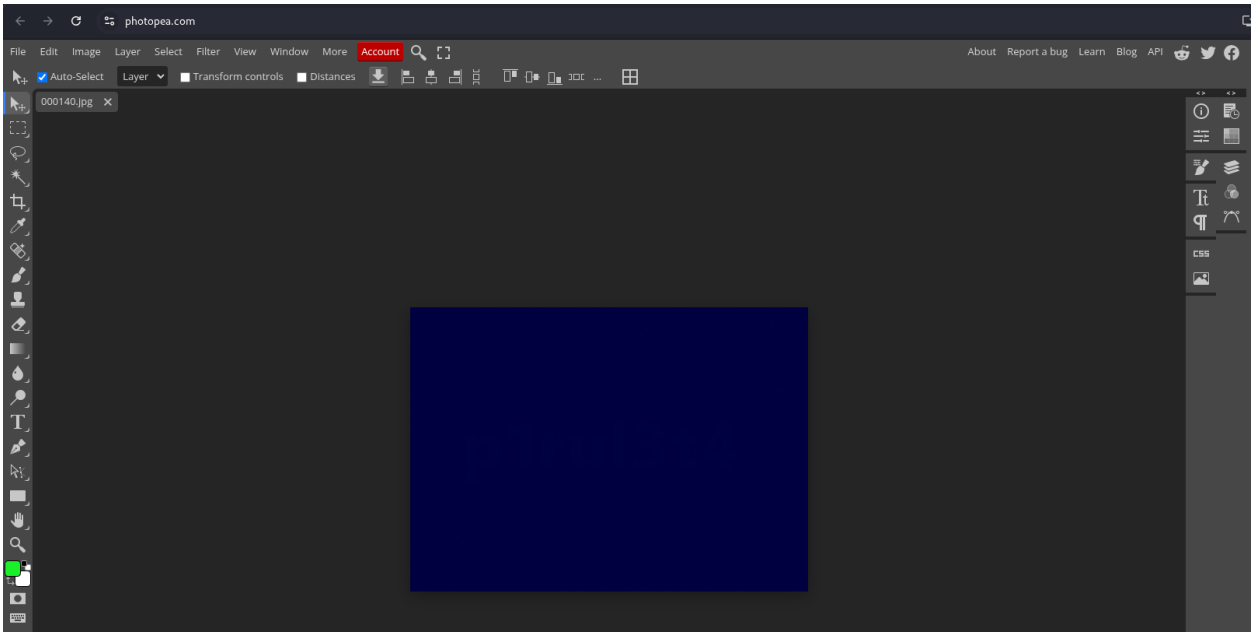
Pixels y pergaminos

El reto nos brinda una imagen jpg, al intentar extraer algún embebido nos pide una contraseña.

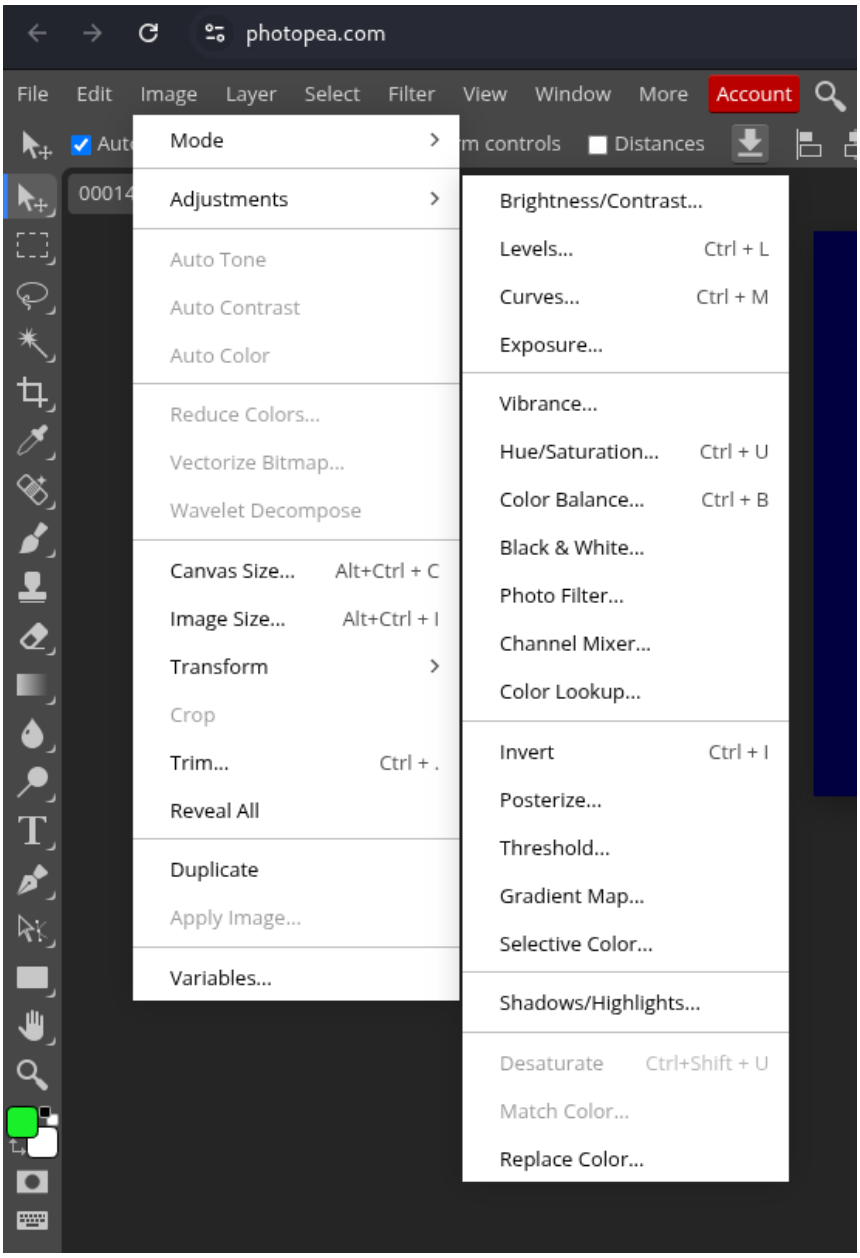
```
┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1
└─$ steghide extract -sf 000140.jpg
Enter passphrase:
```

Al analizar la imagen entregada, se observa que presenta un fondo de color casi uniforme, lo cual es un indicio común de información oculta mediante variaciones mínimas de color. A simple vista no se aprecia ningún texto, pero esto sugiere que el contenido puede estar oculto mediante diferencias de luminosidad o contraste.

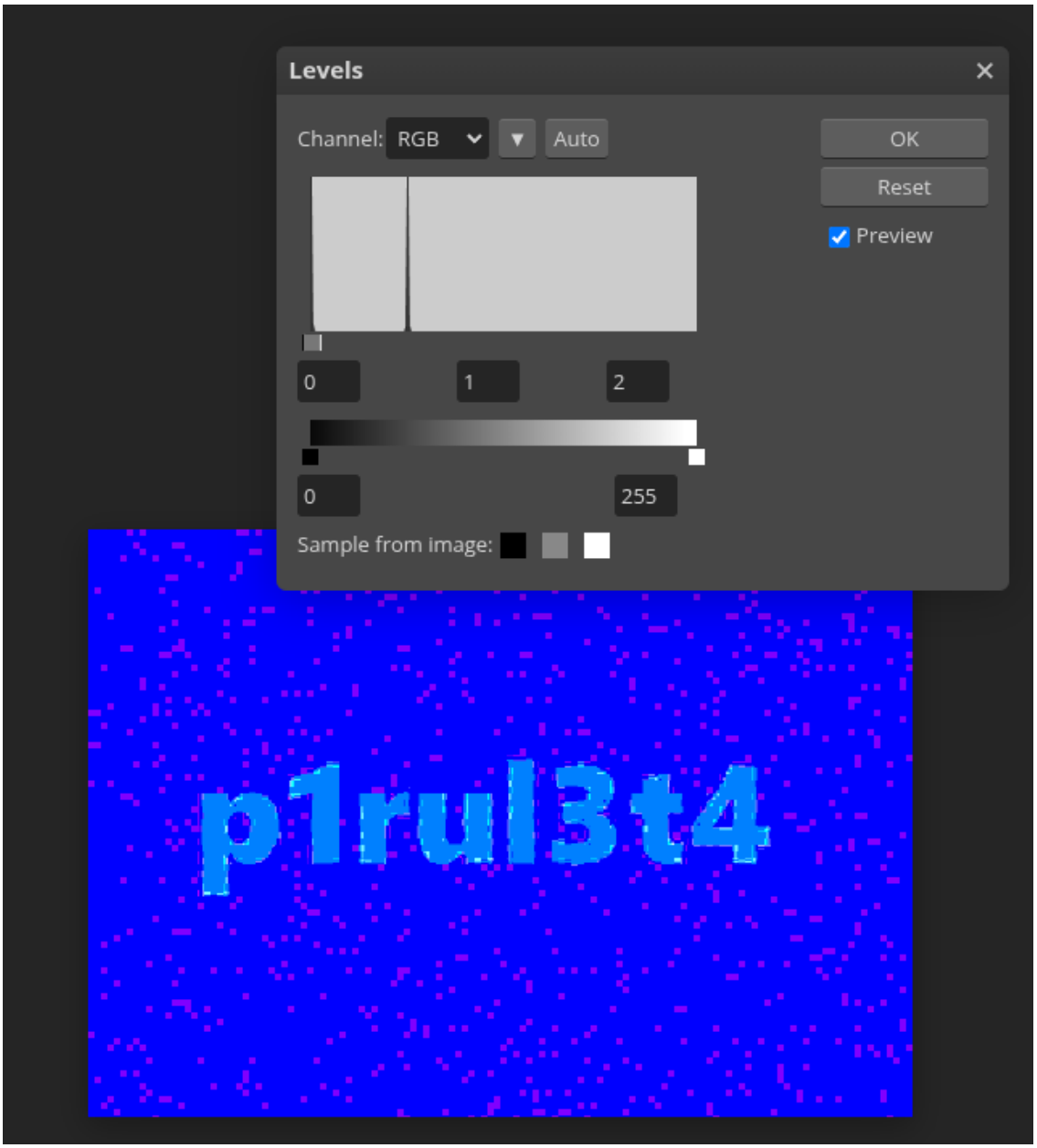
Para confirmar esta hipótesis, se subió la imagen a la herramienta online Photopea (https://www.photopea.com/).



Una vez cargada la imagen, se utilizó la opción **Image → Adjustments → Levels**, modificando los valores de entrada de negro, blanco y el punto medio. Al forzar estos niveles, se amplifican las pequeñas diferencias entre píxeles que originalmente eran imperceptibles para el ojo humano.



Tras aplicar los cambios de niveles, se logró visualizar claramente un texto oculto en el fondo de la imagen, el cual corresponde a una **contraseña**.



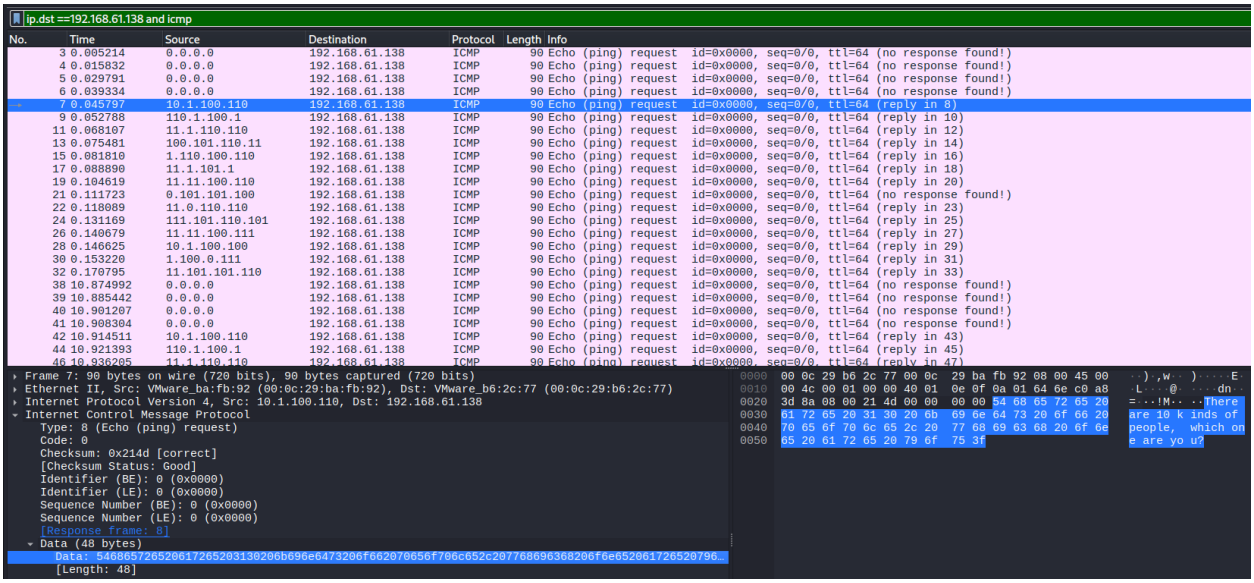
Usamos esa contraseña y logramos obtener un .pcap

```
┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1e
└─$ steghide extract -sf 000140.jpg
Enter passphrase:
wrote extracted data to "captura.pcap".
```

Al usar un editor hexadecimal como xxd “000140.jpg” obervamos una pista.

```
00005c30: 00ea 004a 0028 00a0 4140 c280 0a04 1486  ...J.(..A@.. ...
00005c40: 14c0 2800 a002 800a 0029 0053 1050 30a0  ..(. ... ..).S.P0.
00005c50: 0280 0a00 2800 a002 800a 0028 00a0 6140  ....(. ... ..(..a@
00005c60: 8280 0a00 ffd9 2061 676f 6f64 6669 6c74  ..... agoodfilt
00005c70: 6572 6973 6970 2e64 7374 3d3d 3139 322e  erisip.dst==192.
00005c80: 3136 382e 3631 2e31 3338 616e 6469 636d  168.61.138andicm
00005c90: 70                                       p
```

Al abrir el .pcap se encuentra una gran cantidad de tráfico. A pesar de no ser necesario, es muy útil utilizar el filtro “ip.dst ==192.168.61.138 and icmp”, que se encontraba en los últimos bits de la imagen. Este filtro permite filtrar la captura para ver los paquetes ICMP con destino 192.168.61.138.



Todos los mensaje ICMP llevan el mensaje “There are 10 kind of people, which one are you?” haciendo referencia a que el mundo se divide entre los que saben binario o no, y como pista de que el mensaje se saca de las IP, que están compuestas únicamente por unos y ceros.

De esta forma, por ejemplo 10.1.100.0 sería “010001100000”. Agrupando (en este caso, cada dos IP) nos queda:

010 001 100 110 110 001 100 001 = “Fla”
011 001 110 110 100 101 110 011 = “gis”
001 110 100 110 011 001 101 001 = “:fi”
011 011 100 110 000 101 101 100 = “nal”
011 000 110 110 111 101 110 101 = “cou”
011 011 100 111 010 001 100 100 = “ntd”
001 100 000 111 011 101 101 110 = “0wn”

La flag es finalcountd0wn