B0O Escondido

El ejercicio nos entrega una imagen de un fantasma de scoody doo, de mala calidad que pesa alrededor de 1.1MB, lo cual nos da un indicio de que algo esta oculto en la imagen.

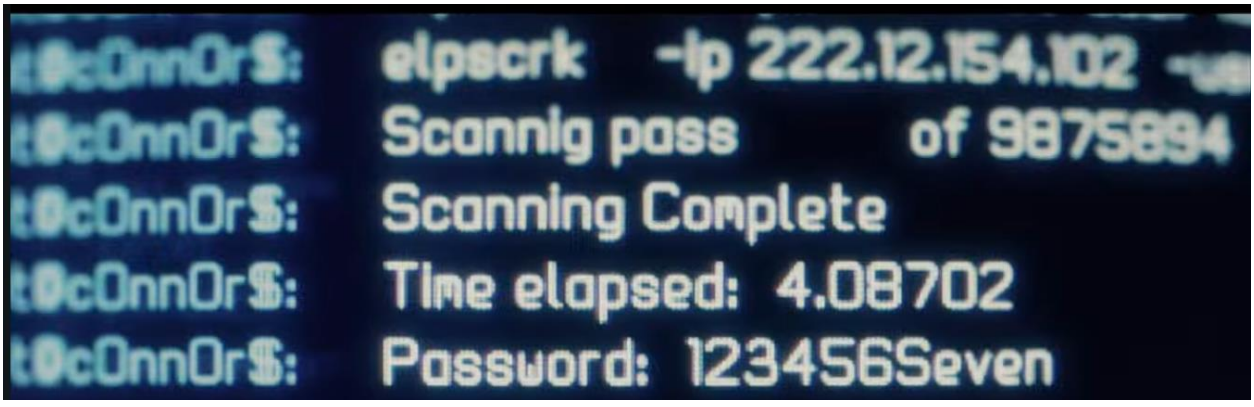
```
└─$ binwalk -e boo.jpeg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
452359        0x6E707         Zip archive data, encrypted at least v2.0 to extract, compressed size: 714874, uncomp
ressed size: 882058, name: fis.wav

WARNING: One or more files failed to extract: either no utility was found or it's unimplemented
```

Como podemos la imagen tenia embebida un archivo .zip con un .wav en su interior, para abrir este zip nos pide una contraseña. Tal vez buscar entre los metadatos de la imagen nos entrege alguna información extra.

```
└─$ exiftool boo.jpeg
ExifTool Version Number         : 13.36
File Name                       : boo.jpeg
Directory                       : .
File Size                       : 1167 kB
File Modification Date/Time     : 2025:12:16 14:16:28-05:00
File Access Date/Time           : 2025:12:18 18:15:20-05:00
File Inode Change Date/Time     : 2025:12:16 14:16:28-05:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Comment                         : aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj0zR2tOY0FldWJsRQ==
Image Width                     : 3000
Image Height                    : 2256
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 3000×2256
Megapixels                      : 6.8
```

En la sección de comentarios de la imagen podemos reconocer una cadena en base64, al decodificarla en https://www.base64decode.org/es/ obtenemos un link de un video de youtube.

Al analizar el video detenidamente, logramos observar en el segundo 38 el siguiente frame, que nos muestra una contraseña.



Con esta contraseña podemos obtener el archivos fis.wav.

```
└─$ unzip 6E707.zip
Archive:  6E707.zip
[6E707.zip] fis.wav password:
  inflating: fis.wav
```

Lo analizarmos con Audacity, una herramienta de edición y análisis de audio. A simple escucha, el archivo no contenía información relevante, lo que sugiere que la pista no esta destinada a ser percibida de forma auditiva.

Dentro de Audacity, se cambió la vista de la pista a Espectograma (Espectro es sinonimo de fantasma, de lo que trataba la foto), lo cual permite representar las frecuencias del audio a lo largo del tiempo. Este tipo de visualización es común en retos de esteganografía en audio, ya que permite ocultar información visual dentro del dominio de la frecuencia.

Al observar el espectrograma, se logró identificar claramente texto oculto que corresponde a la flag del reto.