# ESTEGANOGRAFÍA - LISTA DE HERRAMIENTAS Y RECURSOS ÚTILES

## ESTEGANOGRAFÍA

La esteganografía es ocultar un archivo o un mensaje dentro de otro archivo, hay muchos desafíos CTF de esteganografía divertidos por ahí donde la bandera se oculta en una imagen, archivo de audio o incluso otros tipos de archivos.

### HERRAMIENTAS

#### STEGHIDE

Steghide es un programa de esteganografia que esconde datos en varios tipos de archivos de imagen y audio, solo soporta estos formatos de archivo: JPEG, BMP, WAV y AU. pero también es útil para extraer datos incrustados y encriptados de otros archivos.

Se puede instalar con apt sin embargo la fuente se puede encontrar en github.

Comandos útiles:

`steghide info file`: muestra información sobre un archivo si tiene datos incrustados o no.

`steghide extract -sf file`: extrae datos incrustados de un archivo.

#### FOREMOST

Foremost es un programa que recupera archivos basándose en sus cabeceras, pies de página y estructuras de datos internas, lo encuentro útil cuando se trata de imágenes png.

Se puede instalar con apt sin embargo la fuente se puede encontrar en github.

Comandos útiles:

`foremost -i file`: extrae datos del archivo dado.

#### STEGSOLVE

A veces hay un mensaje o un texto oculto en la propia imagen y para poder verlo necesitas aplicar algunos filtros de color o jugar con los niveles de color. Puedes hacerlo con GIMP o Photoshop o cualquier otro software de edición de imágenes, pero stegsolve lo hace más fácil. es una pequeña herramienta java que aplica muchos filtros de color en las imágenes. Personalmente lo encuentro muy útil.

Puedes conseguirlo en github

#### STRINGS

Strings es una herramienta de linux que muestra cadenas imprimibles en un archivo. Esta sencilla herramienta puede ser muy útil a la hora de resolver problemas de stego. Por lo general, los datos incrustados están protegidos por contraseña o cifrados y, a veces, la contraseña es actaully en el propio archivo y se puede ver fácilmente mediante el uso de cadenas. Es una herramienta por defecto de linux así que no necesitas instalar nada.

Comandos útiles:

`strings file`: muestra las cadenas imprimibles en el archivo dado.

### EXIFTOOL

A veces hay cosas importantes ocultas en los metadatos de la imagen o el archivo, exiftool puede ser muy útil para ver los metadatos de los archivos.

Puedes obtenerlo desde aquí.

Comandos útiles:

`exiftool file`: muestra los metadatos del archivo dado

### EXIV2

Una herramienta similar a exiftool.

Se puede instalar con apt aunque el código fuente se puede encontrar en github.

Página oficial

Comandos útiles:

`exiv2 file`: muestra los metadatos del archivo dado

### BINWALK

Binwalk es una herramienta para buscar archivos binarios como imágenes y archivos de audio para los archivos incrustados y los datos.

Se puede instalar con apt, aunque el código fuente se puede encontrar en github.

Comandos útiles:

`binwalk file`: Muestra los datos incrustados en el archivo dado

`binwalk -e file`: Muestra y extrae los datos del archivo dado

### ZSTEG

zsteg es una herramienta que puede detectar datos ocultos en archivos png y bmp.

para instalarlo: gem install zsteg, La fuente se puede encontrar en github

Comandos útiles:

`zsteg -a file`: Ejecuta todos los métodos en el archivo dado

`zsteg -E file`: Extrae los datos de la carga útil dada (ejemplo: `zsteg -E b4,bgr,msb,xy nombre.png){: .align-center}`

### WAVSTEG

WavSteg es una herramienta python3 que puede ocultar datos y archivos en archivos wav y también puede extraer datos de archivos wav.

Puedes conseguirla en github

Comandos útiles:

`python3 WavSteg.py -r -s soundfile -o outputfile`: extrae datos de un archivo de sonido wav y emite los datos en un nuevo archivo

### SONIC VISUALIZER (VISUALIZADOR SÓNICO)

Sonic visualizer es una herramienta para ver y analizar el contenido de archivos de audio, sin embargo, puede ser útil cuando se trata de esteganografía de audio. Puede revelar formas ocultas en archivos de audio.

Sitio web oficial

## HERRAMIENTAS WEB

Esteganografía de texto Unicode

Una herramienta web para esteganografía unicode, puede codificar y decodificar texto.

npiet online

Un intérprete en línea para piet. piet es un lenguaje esotérico, los programas en piet son imágenes. lea más sobre piet aquí

dcode.fr

dcode.fr tiene muchos decodificadores para una gran cantidad de cifrados y puede ser realmente útil.

## BRUTEFORCERS

### STEGCRACKER

Una herramienta que fuerza contraseñas usando steghide, puedes verla aquí.

### FCRACKZIP

A veces los datos extraídos es un zip protegido por contraseña, esta herramienta realiza fuerca bruta en archivos zip.

Se puede instalar con apt sin embargo la fuente se puede encontrar en github.

Comandos útiles:

`fcrackzip -u -D -p wordlist.txt file.zip`: fuerza bruta contra el archivo zip dado con las contraseñas de la lista de palabras dada.