

Esta es una lista simple (pero útil) de las herramientas más usadas:

PARA OBTENCIÓN DE DATOS

exiftool y jExifToolGUI

Extrae, edita y borra metadatos EXIF, IPTC, XMP, etc. Muy completo.

Instalación:

```
sudo apt -y install libimage-exiftool-perl
curl -sL
https://raw.githubusercontent.com/nipegun/dh-scripts/refs/heads/main/SoftInst/ParaGUI/jExifToolGUI-Instalar.sh |
bash
```

Uso:

exiftool archivo.jpg

binwalk

Analiza binarios e imágenes en busca de cabeceras incrustadas (útil para CTFs).

Instalación:

sudo apt -y install binwalk

Uso:

binwalk archivo.jpg

foremost

Extrae archivos embebidos en imágenes (y otros formatos).

Instalación:

sudo apt -y install foremost

Uso:

foremost archivo.jpg

strings

Busca texto legible en imágenes (a veces aparecen pistas).

Instalación:

sudo apt -y install binutils

Uso:

strings archivo.jpg



PARA ESTEGANOGRAFÍA

steghide

Inserta o extrae datos en imágenes y archivos de audio. Soporta cifrado.

Instalación:

sudo apt -y install steghide

Uso:

steghide extract -sf archivo.jpg

outguess

Inserta datos en imágenes JPEG.

Instalación:

sudo apt -y install outguess

Uso:

outguess -k "contraseña" -r archivo.jpg extraido.txt

stegsolve

Herramienta gráfica en Java para CTFs, permite ver imágenes en distintos planos de color. (No siempre en los repos oficiales, pero suele estar en stegsolve.jar descargable).

Instalación:

```
mkdir -p ~/HackingTools/Esteganografía/StegSolve/
cd ~/HackingTools/Esteganografía/StegSolve/
wget http://www.caesum.com/handbook/Stegsolve.jar -0 stegsolve.jar
```

Uso:

java -jar ~/HackingTools/Esteganografía/StegSolve/stegsolve.jar

zsteg

Detecta esteganografía en imágenes PNG y BMP (muy usada en CTF).

Instalación:

sudo apt-y install ruby ruby-dev build-essential
sudo gem install zsteg

Uso:

zsteg archivo.png



openstego

Suite completa de esteganografía en Java.

Instalación:

curl -

 $\verb|sl| https://raw.githubusercontent.com/nipegun/dh-scripts/refs/heads/main/SoftInst/ParaGUI/OpenStego-Instalar.sh| bash | bash$

Uso:

Lanzar la app gráfica

stegsnow

Esteganografía en espacios en blanco (aunque más textual que de imágenes).

Instalación:

sudo apt -y install stegsnow

Uso:

stegsnow -C -p "contraseña" archivo.txt