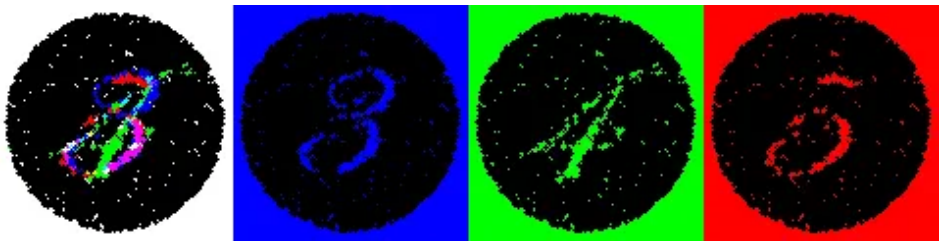
Steganography : Tools & Techniques

Ria Banerjee Follow 3 min read · Mar 27, 2024



The same image viewed by white, blue, green, and red lights reveals different hidden numbers.

What is Steganography?

Steganography is the process of hiding secret data within files that look ordinary, e.g. image, video or audio file, to avoid detection. The hidden data can be extracted only at its destination.

There are several methods and tools for hiding and extracting data to and from files. In this article I'm going to cite a few examples with instructions, which will help you in solving CTFs which involve the use of steganography.

Tools:

1. **Steghide:**

Steghide supports JPEG, BMP, WAV and AU file formats. File formats like PNG are not supported with this tool. But BMP, GIF and JPG are also supported.

Embedding data using steghide:

steghide -ef secret.txt -cf ordinary_image.jpg

You will be asked to set a passphrase, using which the data will be extracted at the destination.

Extracting data:

steghide extract -sf ordinary_image.jpg

Viewing whether the image has a hidden data or not:

steghide info ordinary_image.jpg

Source: https://github.com/StefanoDeVuono/steghide

2. Binwalk:

Binwalk is a tool that searches binary files for hidden files or texts. It is a widely used tool for analyzing, reverse engineering, and extracting firmware images.

Display embedded data in a file:

binwalk <filename>

Extract embedded data in a file:

binwalk -e <filename>

Source: https://github.com/ReFirmLabs/binwalk

3. Strings:

The ‘strings’ command in Linux is used to extract readable strings from a binary file. It is a very useful tool in extracting hidden data from files.

strings <filename>

More about strings:

https://linux.die.net/man/1/strings

4. Exiftool:

Exiftool is used to extract metadata from image files. Sometimes important information is hidden in image metadata, which can be useful.

exiftool <filename>

Source: https://exiftool.org/

5. Foremost:

Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving.

foremost -i <filename>

Source: https://github.com/korczis/foremost

6. StegSeek:

StegSeek is a lightning fast steghide cracker that can be used to extract hidden data from files.

StegSeek can also be used to extract steghide metadata without a password, which can be used to test whether a file contains steghide data.

StegSeek uses a wordlist that you provide to crack hidden data in the file:

stegseek <filename> <wordlist>

Check whether a file contains steghide data without a password:

stegseek — — seed <filename>

Source: https://github.com/RickdeJager/stegseek

7. Zsteg:

Zsteg can find hidden data in .png and .bmp files.

zsteg <filename>

Source: https://github.com/zed-0xff/zsteg

8. WavSteg:

WavSteg is a python3 based tool that hides data in .wav files and extracts the hidden data too. WavSteg uses least significant bit steganography to hide a file in

the samples of a .wav file.

Hide data:

stegolsb wavsteg -h -i sound.wav -s file.txt -o sound_steg.wav

Extract data:

stegolsb wavsteg -r -i sound_steg.wav -o output.txt

Source: https://github.com/ragibson/Steganography#WavSteg

8. Stegsolve:

It is used to analyze images in different planes by taking off bits of the image.

java -jar stegsolve.jar

It will popup a GUI where you will be able to look for a picture to analyze.

Sometimes the data is in the image itself and not visible due to the colour levels or something. Stegsolve is useful in those cases.

Source: https://github.com/eugenekolo/sec-tools/tree/master/stego/stegsolve/stegsolve

9. Exiv2:

This tool is similar to Exiftool. Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata.

exiv2 <filename>

Source: https://github.com/Exiv2/exiv2

10. Sonic Visualizer:

It is a tool that analyzes audio files and can reveal hidden shapes in audio files.

Website: https://www.sonicvisualiser.org/

11. Stegcracker:

Similar to StegSeek, it is a steganography brute-force utility to uncover hidden data inside files.

stegcracker <filename> <wordlist>

12. Fcrackzip:

If the extracted data is a password protected zip file, this tool helps cracking the password.

fcrackzip -v -u -D -p <path_to_wordlist_file> <file_name.zip>

-v : verbose

-u : unzip

-D : dictionary attack

-p : path

Source: https://github.com/hyc/fcrackzip

I hope this information helps. If you know other tools that can be used in Steganography, please mention in the comments. Thanks for reading!