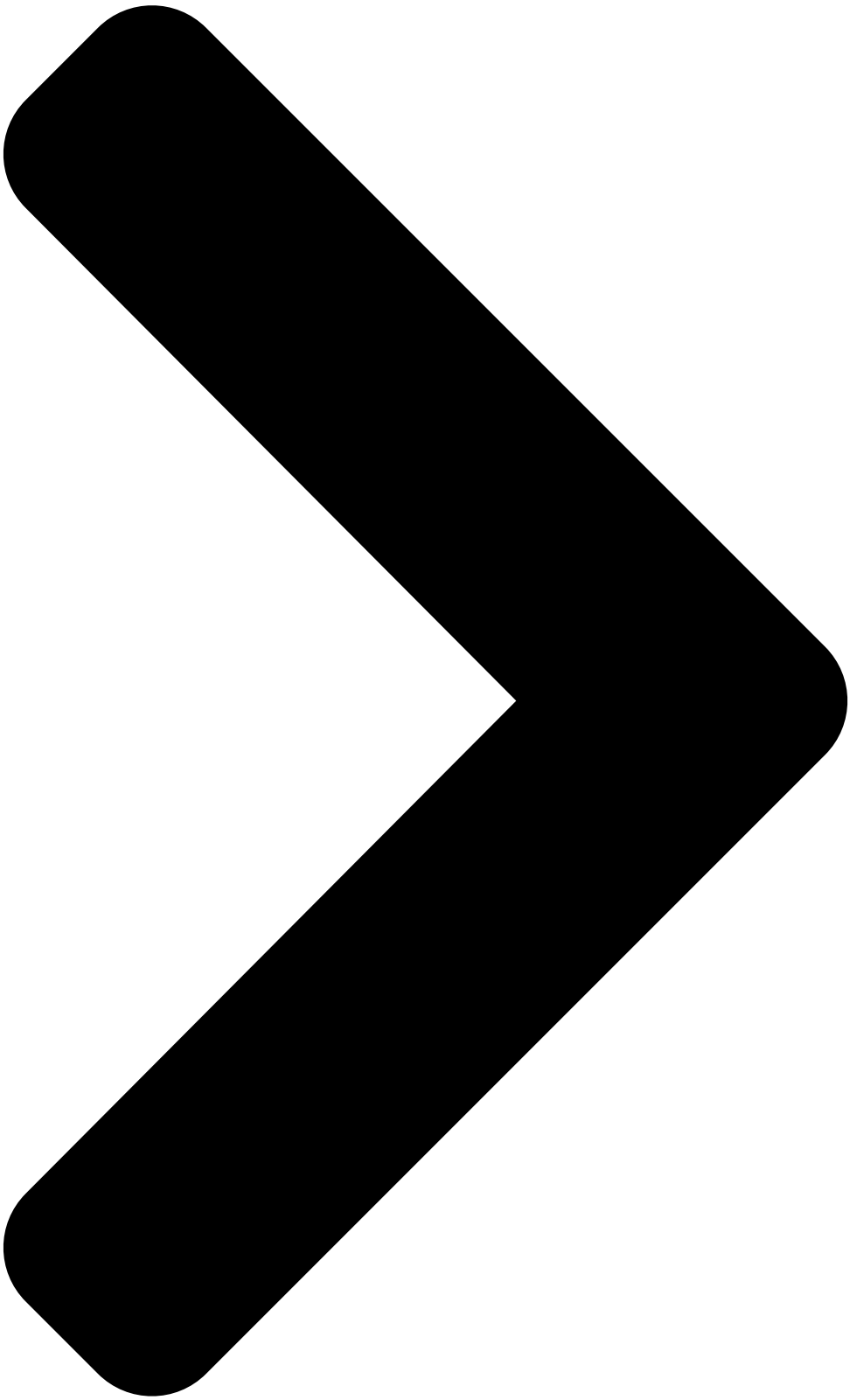
Steganography - A list of useful tools and resources

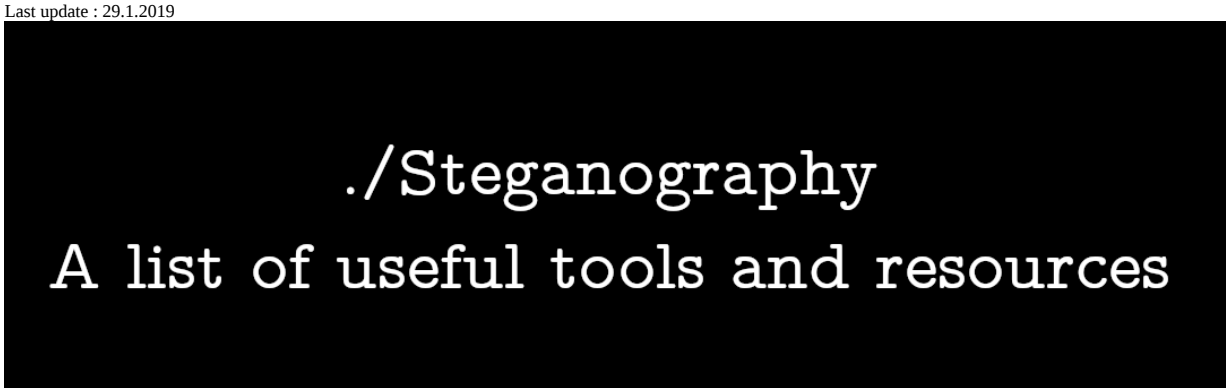
Published on 25 Jan 2019



a list of tools and resources for steganography CTF challenges.

Steganography

Steganography is hiding a file or a message inside of another file , there are many fun steganography CTF challenges out there where the flag is hidden in an image , audio file or even other types of files. Here is a list of the most tools I use and some other useful resources.
Note : This list will be updated regularly , feel free to pm if you have any suggestions
Last update : 29.1.2019



Steghide

Steghide is a steganography program that hides data in various kinds of image and audio files , only supports these file formats : `JPEG, BMP, WAV and AU`. but it's also useful for extracting embedded and encrypted data from other files.
It can be installed with `apt` however the source can be found on github.

Useful commands:
`steghide info file` : displays info about a file whether it has embedded data or not.
`steghide extract -sf file` : extracts embedded data from a file

Foremost

Foremost is a program that recovers files based on their headers , footers and internal data structures , I find it useful when dealing with png images.
It can be installed with `apt` however the source can be found on github.

Useful commands:
`foremost -i file` : extracts data from the given file.

Stegsolve

Sometimes there is a message or a text hidden in the image itself and in order to view it you need to apply some color filters or play with the color levels. You can do it with GIMP or Photoshop or any other image editing software but stegsolve made it easier. it's a small java tool that applies many color filters on images. Personally i find it very useful
You can get it from github

Strings

Strings is a linux tool that displays printable strings in a file. That simple tool can be very helpful when solving stego challenges. Usually the embedded data is password protected or encrypted and sometimes the password is actaully in the file itself and can be easily viewed by using strings
It's a default linux tool so you don't need to install anything.

Useful commands:
`strings file` : displays printable strings in the given file.

Sometimes important stuff is hidden in the metadata of the image or the file , exiftool can be very helpful to view the metadata of the files.
You can get it from here

Useful commands:
`exiftool file` : shows the metadata of the given file

Exiv2

A tool similar to exiftool.
It can be installed with `apt` however the source can be found on github.
Official website

Useful commands:
`exiv2 file` : shows the metadata of the given file

Binwalk

Binwalk is a tool for searching binary files like images and audio files for embedded files and data.
It can be installed with `apt` however the source can be found on github.

Useful commands:
`binwalk file` : Displays the embedded data in the given file
`binwalk -e file` : Displays and extracts the data from the given file

Zsteg

zsteg is a tool that can detect hidden data in png and bmp files.
to install it : `gem install zsteg` , The source can be found on github

Useful commands:
`zsteg -a file` : Runs all the methods on the given file
`zsteg -E file` : Extracts data from the given payload (example : zsteg -E b4,bgr,msb,xy name.png)

Wavsteg

WavSteg is a python3 tool that can hide data and files in wav files and can also extract data from wav files.
You can get it from github

Useful commands:
`python3 WavSteg.py -r -s soundfile -o outputfile` : extracts data from a wav sound file and outputs the data into a new file

---

Sonic visualizer

Sonic visualizer is a tool for viewing and analyzing the contents of audio files, however it can be helpful when dealing with audio steganography. You can reveal hidden shapes in audio files.
Offical Website

Unicode Text Steganography

A web tool for unicode steganography , it can encode and decode text.

---

npiet online

an online interpreter for piet. piet is an esoteric language , programs in piet are images. read more about piet here

---

dcode.fr

Sometimes when solving steganography challenges you will need to decode some text. dcode.fr has many decoders for a lot of ciphers and can be really helpful.

Bruteforcers

StegCracker

A tool that bruteforces passwords using steghide

Fcrackzip

Sometimes the extracted data is a password protected zip , this tool bruteforces zip archives.
It can be installed with `apt` however the source can be found on github.

Useful commands:
`fcrackzip -u -D -p wordlist.txt file.zip` : bruteforces the given zip file with passwords from the given wordlist

---

Challenges

Some platforms to solve stego challenges
Hack The Box
root me
RingerZeroCTF
