

«ТУЛЗЫ» ДЛЯ СТЕГАНОГРАФИИ

список основных инструментов для решения задач

LONG STORY SHORT

- › большинство специфических (и не очень) программ консольные и под линух, и это относится почти ко всем категориям ctf. рекомендуется поставить хотя бы виртуалку.
- › все мануалы для консольных тулз, как правило, можно найти `<название_тулзы> --help` в терминале или написать в гугле `<название_тулзы> usage` (скорее всего наткнетесь на github).

> HEX-EDITOR

шестнадцатеричный редактор — используется для редактирования данных представленных как последовательность байтов

> 010 EDITOR

[win/linux/mac]

Один из наиболее удобных
hex-редакторов, позволяет
без проблем
ориентироваться в хексах и
чарах файла.
Отличительной
особенностью является
возможность подгружать
темплейты, позволяющие
разобраться в сигнатурах.

The screenshot displays the 010 Editor application window. The top menu bar includes File, Edit, Search, View, Format, Scripts, Templates, Debug, Tools, Window, and Help. Below the menu is a toolbar with various icons for file operations and editing. The main workspace shows a hex file named 'a8boq1tl5hr11.png'. The hex data is displayed in a grid with columns for address, hex bytes, and ASCII characters. The ASCII column shows the beginning of a PNG file signature: '%PNG.....IHDR'. Below the hex editor, a 'Template Results - PNG.bt' table is visible, listing various PNG chunks and their properties.

Name	Value	Start	Size
> struct PNG_SIGNATURE sig		0h	8h
> struct PNG_CHUNK chunk[0]	IHDR (Critical, Public, Unsafe ...	8h	19h
> struct PNG_CHUNK chunk[1]	bKGD (Ancillary, Public, Unsaf...	21h	12h
> struct PNG_CHUNK chunk[2]	pHYs (Ancillary, Public, Safe t...	33h	15h
> struct PNG_CHUNK chunk[3]	tIME (Ancillary, Public, Unsafe...	48h	13h
> struct PNG_CHUNK chunk[4]	tEXt (Ancillary, Public, Safe to...	5Bh	25h
> struct PNG_CHUNK chunk[5]	IDAT (Critical, Public, Unsafe ...	80h	200Ch
> struct PNG_CHUNK chunk[6]	IDAT (Critical, Public, Unsafe ...	208Ch	200Ch
> struct PNG_CHUNK chunk[7]	IDAT (Critical, Public, Unsafe ...	4098h	200Ch

> XXD

[linux]

Консольная тулза для быстрого анализа данных через терминал.

```
root@yos: ~/Desktop
00035d70: 9573 a182 7462 e34c 3893 5f36 5c48 e76e .s..tb.L8._6\H.n
00035d80: c4c3 50b5 0ec0 e6c7 3a95 a90c 1264 3da8 ..P.....:....d=.
00035d90: 36e2 920d 9e6d 03e5 4665 ecfe b936 81a5 6....m..Fe...6..
00035da0: 2d0c 444b a342 ec19 b530 d30c 8968 6e5f -.DK.B...0...hn_
00035db0: 786b 4ca0 124a 9d64 e322 e603 dca4 cc08 xkL..J.d.".....
00035dc0: d3ba 0c32 b595 9c9e 81c5 9d36 6c9e f633 ...2.....6l..3
00035dd0: 96b1 ea6b c7a9 1de4 deaf 0ef4 694d b315 ...k.....iM..
00035de0: 085c bb2b 517e a7b0 5639 3248 8c36 c61a .\.+Q~..V92H.6..
00035df0: fdf2 766f b3ce 860d b131 29a2 6163 d3d2 ..vo.....1).ac..
00035e00: 9e92 6d32 e295 0e17 6def 30b1 e797 3634 ..m2....m.0...64
00035e10: 784e a2aa 9427 584f 226f 99fa e0e5 9473 xN...'XO"o.....s
00035e20: d08c c5b5 2be0 9d2d 0c5b acbc e346 9586 .....+...-[...F..
00035e30: 514d 9da1 4cc3 4f08 624d c98d 3360 3227 QM..L.O.bM..3`2'
00035e40: a4e2 e841 31cb a937 c167 1cf3 eb46 8618 ...A1..7.g...F..
00035e50: b7e1 9383 2279 3014 66cd b689 9373 2af0 ...."y0.f....s*.
00035e60: e24d f340 d9fa 9f3c c8bb 3eef 163f 222c .M.@...<...?...",
00035e70: c4b8 b8d1 ab36 23d9 478c 34a2 f66d 691c .....6#.G.4..mi.
00035e80: 0651 42ec 9897 35ce 2a4d f376 a5c6 61c3 .QB...5.*M.v..a.
00035e90: 1a07 c70d 4bc9 efcc 7c52 a32e f088 0fcc ....K...|R.....
00035ea0: 3eb6 fa1e 1cc8 50e0 3c1a 98ae 68e0 7a69 >.....P.<...h.zi
00035eb0: 3172 a547 e16e ae5a c6b9 d696 86c3 6831 1r.G.n.Z.....h1
00035ec0: a700 4da3 1eae 5d7c f402 13b3 7bf3 32e4 ..M...]|....{.2.
00035ed0: cf20 4890 db76 cef6 4f08 6ef0 6157 9ba9 . H..v..0.n.aW..
00035ee0: fa4c d93f 8ade 0fd1 7363 5a96 9125 de19 .L.?....scZ..%..
00035ef0: 1b39 c831 fcf3 6048 03f6 ae5e e191 490d .9.1..`H...^..I.
00035f00: 9c6a 63a9 9a7f 3ad8 1ceb 989f 7c88 cdf0 .jc....:....|...
00035f10: 5b64 6199 a76e dc32 0279 8d86 6907 8b85 [da..n.2.y..i...
00035f20: 1bd4 62a1 ea78 f424 62e3 6be8 cd42 8f4e ..h..x.$h.k..R.N
```

ДРУГИЕ РЕДАКТОРЫ

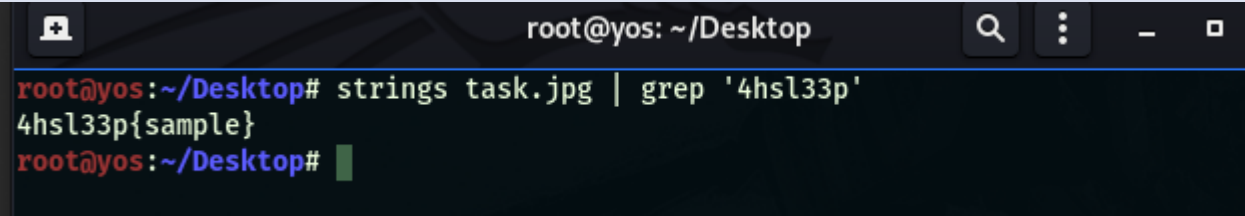
- › Hex editor neo *[win]*
- › Hxd *[win]*
- › Hexcmp *[win]* — редактор + аналогично команде cmp на линуксе позволяет сравнивать файлы
- › HEXEDIT *[linux]* — консольная программа

> СИГНАТУРЫ И ПРОЧЕЕ

> STRINGS

[linux]

Терминальная команда линуха, позволяет просмотреть строки в файле, более-менее похожие на что-то понятное человеку. При помощи регулярок(*regex*) можно очень гибко настроить поиск.

A terminal window with a dark background and light text. The title bar at the top shows 'root@yos: ~/Desktop' and standard window controls. The terminal content shows a command being executed: 'root@yos:~/Desktop# strings task.jpg | grep '4hsl33p''. The output of the command is '4hsl33p{sample}', which is displayed on the line immediately following the command. The prompt 'root@yos:~/Desktop#' is shown again on the next line, followed by a green cursor.

```
root@yos: ~/Desktop
root@yos:~/Desktop# strings task.jpg | grep '4hsl33p'
4hsl33p{sample}
root@yos:~/Desktop#
```


> BINWALK

[linux]

инструмент для поиска файлов и исполняемого кода в бинарнике. Binwalk имеет файл специальных magic-сигнатур, содержащий сигнатуры для файлов, которые часто содержатся в образах встроенных программ, например, сжатые файлы, заголовки, ядра Linux, загрузчики, файловые системы и т.д.

```
root@yos:~/Desktop# binwalk Fork.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
580258	0x8DAA2	RAR archive data, version 5.x

> DEMO

пример решения простейших задач

LONGCAT

- › дан файл longcat.jpg
- › пропускаем его через binwalk
- › видим, что он обнаружил в файле вложенный архив
- › достаем его с помощью команды -e (extract)

```
root@yos: ~/Desktop
root@yos:~/Desktop# binwalk longcat.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
44885	0xAF55	RAR archive data, version 5.x

```
root@yos:~/Desktop# binwalk -e longcat.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
44885	0xAF55	RAR archive data, version 5.x

- › получаем flag.txt

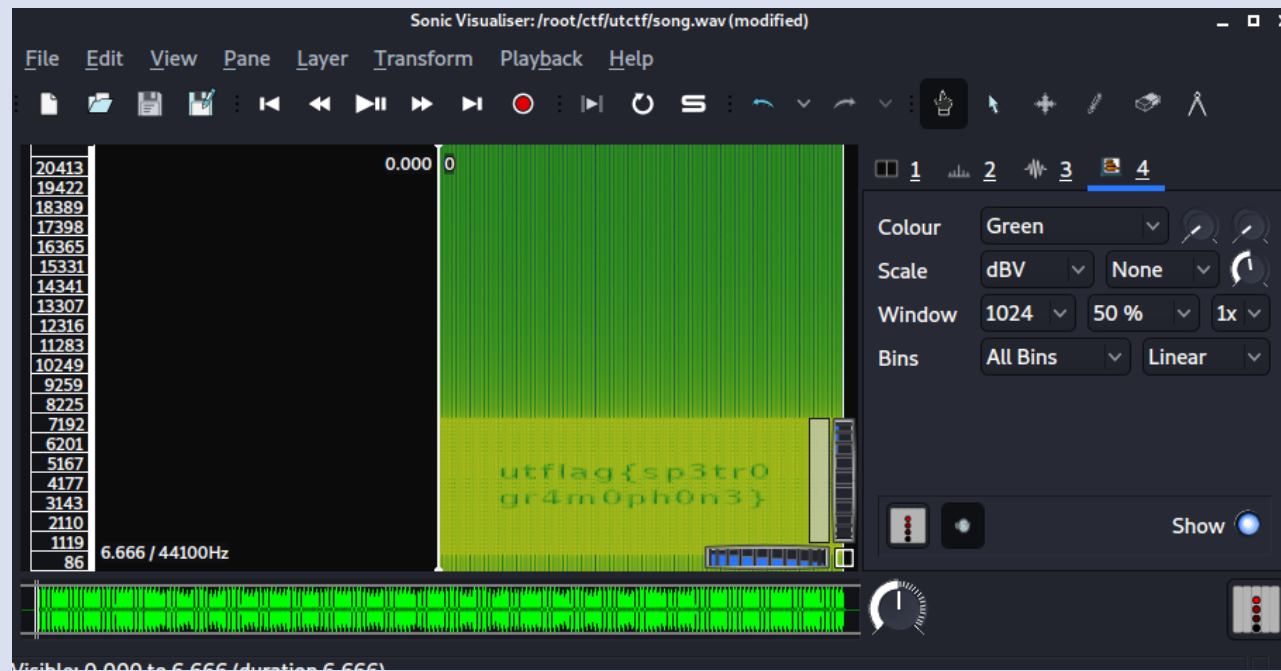
* так же можно увидеть архив в хексах через редактор

> AUDIO

> SONIC VISUALISER

[win/linux/mac]

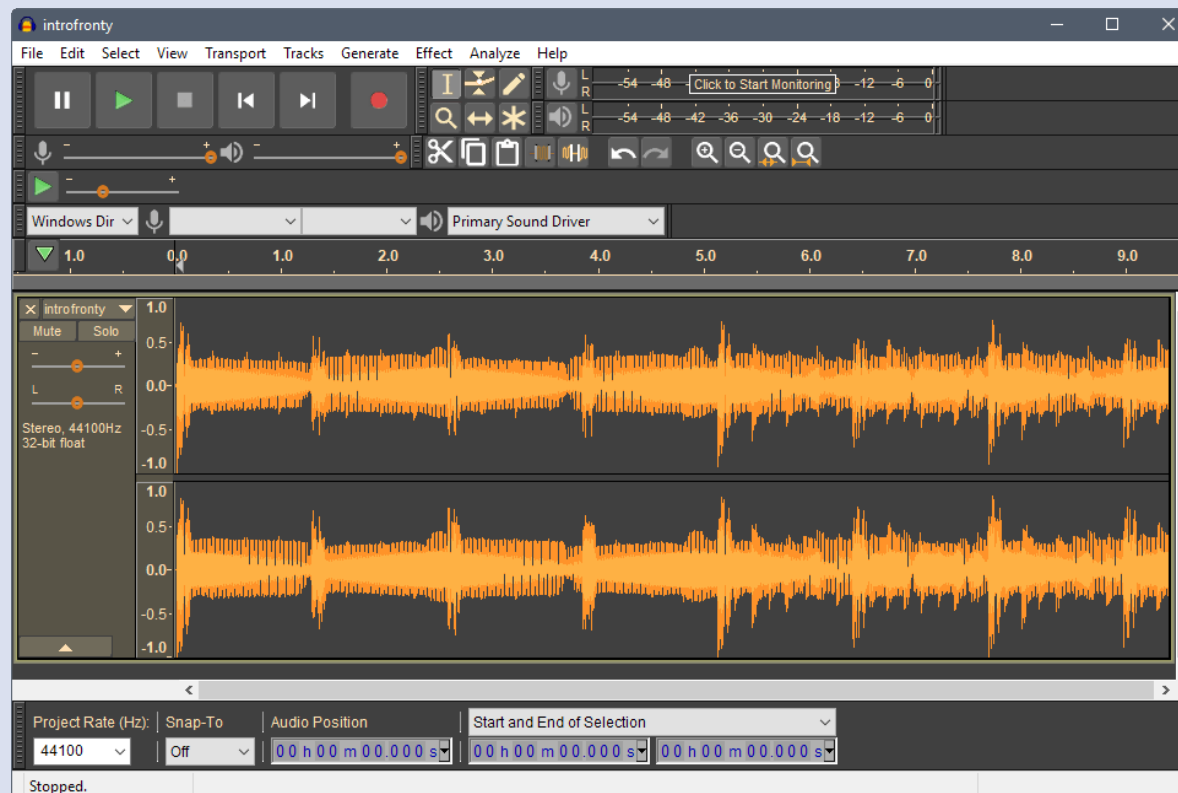
Программа для анализа аудиофайлов, как правило, используется для просмотра спектограмм.



> AUDACITY

[win/linux/mac]

Гибкий звуковой редактор, позволяет изменять и анализировать аудиофайл, и имеет множество настроек для самой звуковой дорожки. Так же умеет импортировать файлы как «сырые данные» (raw).

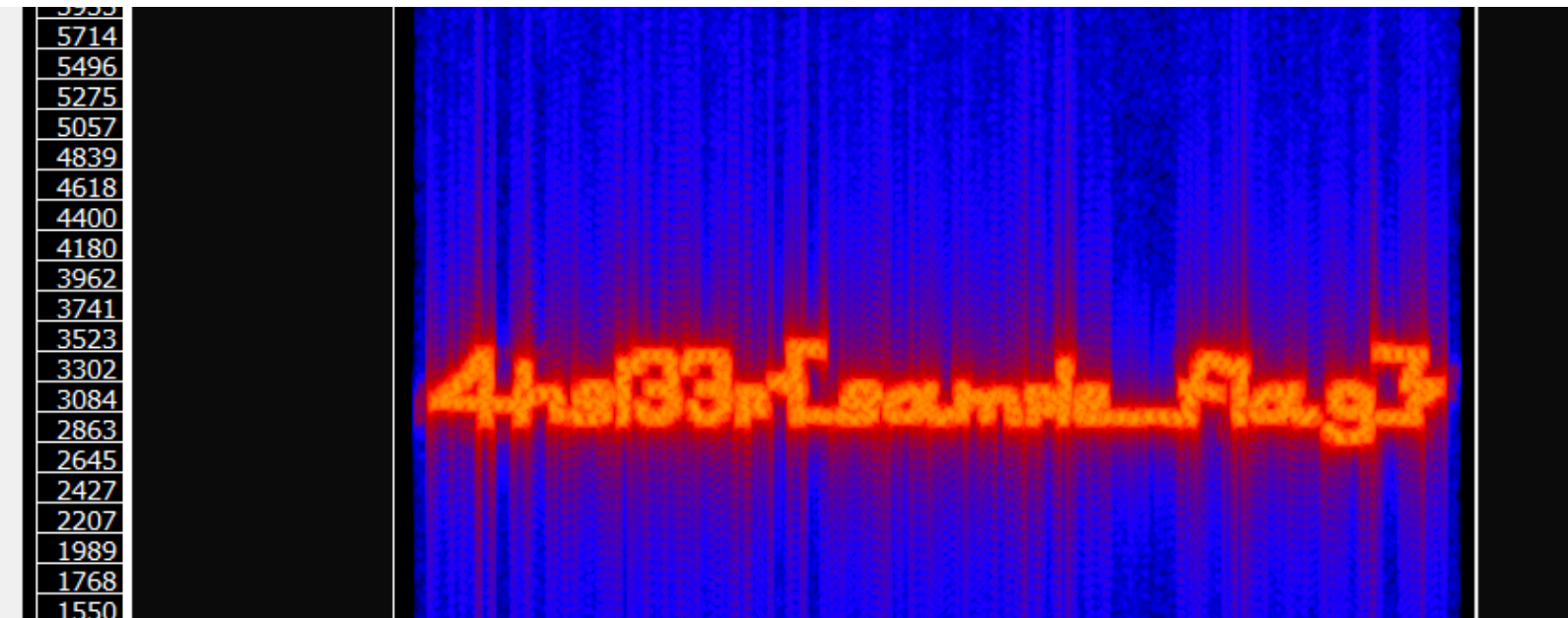


> DEMO

пример решения простейших задач

WAV

- › дан файл task.wav
- › представляет собой жуткий шум
- › открываем sonic visualiser, смотрим спектограмму
- › настраиваем отображение в правом баре



> PICTURES

> ZSTEG

[linux]

Позволяет извлекать данные из изображений (PNG, BMP). zsteg позволяет извлекать все данные в определённом режиме. Это может быть полезно если кто-то спрятал через LSB целый файл и вывод этого файла на экран не представляется возможным.

```
b1,b,msb,xy      .. file: dBase III DBT, version number 0, next free block i
dex 524287
b1,rgb,lsb,xy    .. file: dBase III DBT, version number 0, next free block i
dex 4283273836
b1,rgb,msb,xy     .. file: dBase III DBT, version number 0, next free block i
dex 4289874230
b1,bgr,lsb,xy    .. file: dBase III DBT, version number 0, next free block i
dex 4280633818
b1,bgr,msb,xy     .. file: dBase III DBT, version number 0, next free block i
dex 4288975451
b1,rgba,lsb,xy   .. text: ["D" repeated 45 times]
b1,rgba,msb,xy   .. text: "fDDTwwwwwd"
b1,abgr,lsb,xy   .. text: "fDDEwwwwwb"
b1,abgr,msb,xy   .. file: dBase III DBT, version number 0, next free block i
dex 2720146022
b2,r,lsb,xy      .. file: dBase III DBT, version number 0, next free block i
dex 4294945706
b2,r,msb,xy      .. file: dBase III DBT, version number 0, next free block i
dex 4294956373
b2,g,lsb,xy      .. text: "UUUUUUUUUUUUUUUUUUUUUUUV"
b2,g,msb,xy      .. text: ["U" repeated 33 times]
b2,b,lsb,xy      .. file: dBase III DBT, version number 0, next free block i
```

> STEGHIDE

[linux]

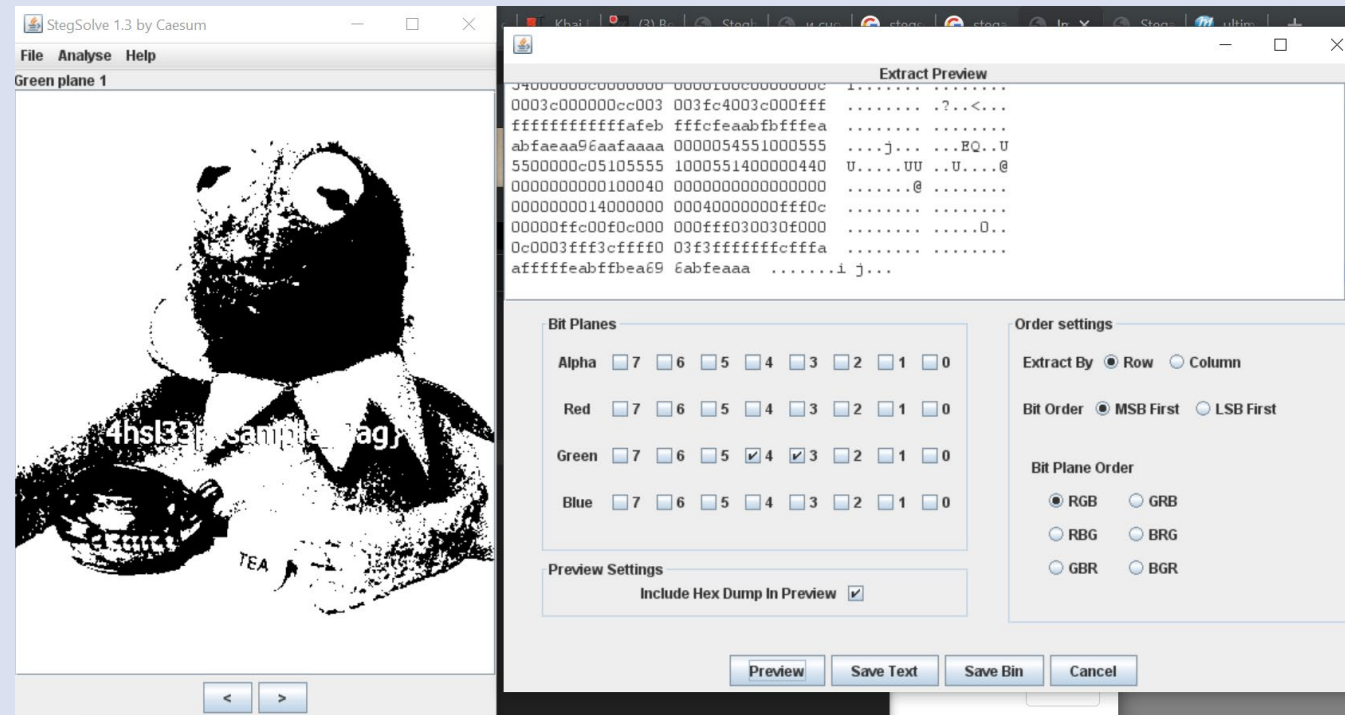
Консольная утилита позволяющая скрывать информацию методом стеганографии в графических или аудио файлах. Поддерживает JPEG, BMP, WAV файлы.

```
root@kali:~/steghide#  
root@kali:~/steghide# steghide info picture.jpg  
"picture.jpg":  
  format: jpeg  
  capacity: 3.1 KB  
Try to get information about embedded data ? (y/n) y  
Enter passphrase:  
  embedded file "secret.txt":  
    size: 590.0 Byte  
    encrypted: rijndael-128, cbc
```

> STEGSOLVE

[win/linux]

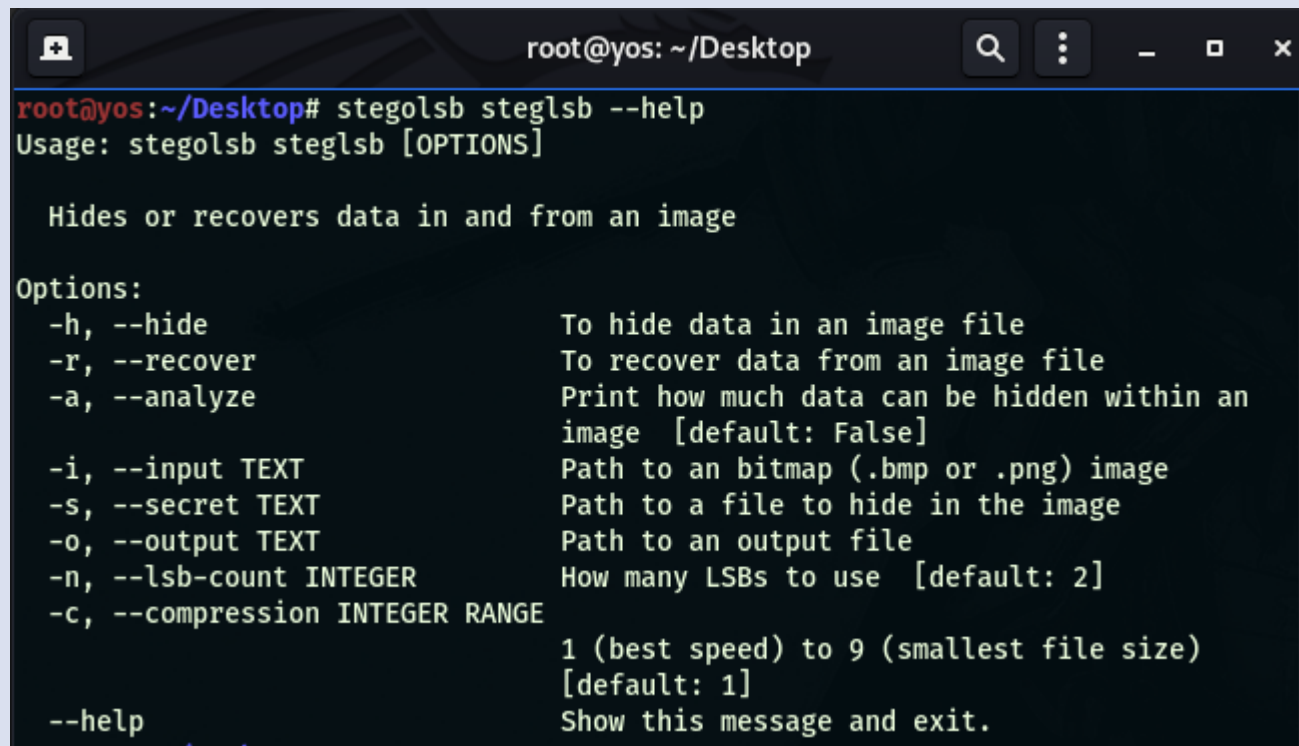
Тулза позволяет просматривать изображения на разных каналах, решать стереограммы, анализировать хексы, накладывать изображения друг на друга с различными параметрами.



> STEGOLSB

[linux]

Консольная тулза для анализа файлов на lsb(*least-significant-bit*). Steglsb — для jpg и bmp изображений. Wavsteg — для wav аудио-файлов.



```
root@yos: ~/Desktop
root@yos:~/Desktop# stegolsb steglsb --help
Usage: stegolsb steglsb [OPTIONS]

Hides or recovers data in and from an image

Options:
  -h, --hide                To hide data in an image file
  -r, --recover             To recover data from an image file
  -a, --analyze             Print how much data can be hidden within an
                             image [default: False]
  -i, --input TEXT          Path to an bitmap (.bmp or .png) image
  -s, --secret TEXT          Path to a file to hide in the image
  -o, --output TEXT          Path to an output file
  -n, --lsb-count INTEGER   How many LSBs to use [default: 2]
  -c, --compression INTEGER RANGE
                             1 (best speed) to 9 (smallest file size)
                             [default: 1]
  --help                    Show this message and exit.
```

> DEMO

пример решения простейших задач

HIDE

- › дан файл longcat.png
- › анализируем его через steghide

```
root@yos:~/Desktop# steghide info longcat.jpg
"longcat.jpg":
  format: jpeg
  capacity: 2.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "flag.txt":
    size: 21.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

- › видим, что внутри спрятан файл flag.txt
- › экстрактируем его

```
root@yos:~/Desktop# steghide extract -sf longcat.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
```

- › получаем флаг

> VIDEO

> FFMPEG

[linux]

Очень мощная программа для работы с видео-файлами, множество дополнительных команд, позволяют делать с файлом разное темное колдунство.

```
root@yos: ~/Desktop
root@yos:~/Desktop# ffmpeg --help
ffmpeg version 4.3.1-2 Copyright (c) 2000-2020 the FFmpeg developers
  built with gcc 10 (Debian 10.2.0-5)
  configuration: --prefix=/usr --extra-version=2 --toolchain=hardened --libdir=/usr/lib/x86_64-linux-gnu --incdir=/usr/include/x86_64-linux-gnu --arch=amd64 --enable-gpl --disable-stripping --enable-avresample --disable-filter=resample --enable-gnutls --enable-ladspa --enable-libaom --enable-libass --enable-libbluray --enable-libbs2b --enable-libcaca --enable-libcdio --enable-libcodec2 --enable-libdav1d --enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribidi --enable-libgme --enable-libgsm --enable-libjack --enable-libmp3lame --enable-libmysofa --enable-libopenjpeg --enable-libopenmpt --enable-libopus --enable-libpulse --enable-librabbitmq --enable-libsrt --enable-libssh --enable-libtheora --enable-libtwolame --enable-libvidstab --enable-libvorbis --enable-libvpx --enable-libwavpack --enable-libwebp --enable-libx265 --enable-libxml2 --enable-libxvid --enable-libzmq --enable-libzvbi --enable-lv2 --enable-omx --enable-openal --enable-opengl --enable-sdl2 --enable-pocketsphinx --enable-libmfx --enable-libdc1394 --enable-libdrm --enable-libiec61883 --enable-chromaprint --enable-frei0r --enable-libx264 --enable-shared
  libavutil      56. 51.100 / 56. 51.100
  libavcodec     58. 91.100 / 58. 91.100
  libavformat    58. 45.100 / 58. 45.100
  libavdevice    58. 10.100 / 58. 10.100
```