bt3gl / **My-Gray-Hacker-Resources**

My-Gray-Hacker-Resources / **Steganography** /

bt3gl del ~ Latest commit `424908f` on Dec 2, 2014

..		
Images	Reorganized	4 years ago
README.md	readmes	4 years ago

README.md

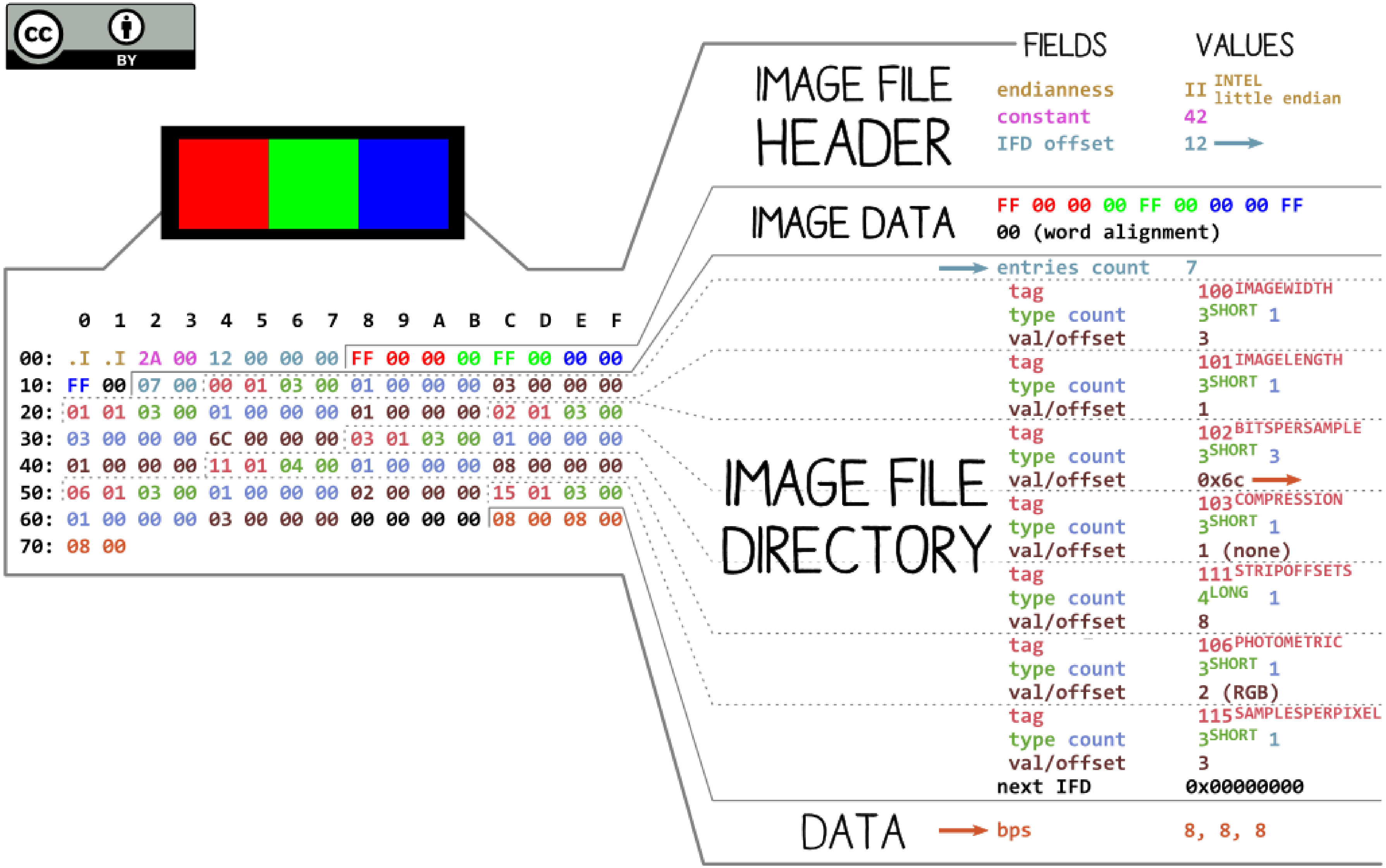
Steganography

Images

- Adding two images
- xor_bytes
- color crypto

TAGGED IMAGE FILE FORMAT

ANGE ALBERTINI
http://www.corkami.com



```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F

00: .I .I 2A 00 12 00 00 00 FF 00 00 00 FF 00 00 00
10: FF 00 07 00 00 01 03 00 01 00 00 00 03 00 00 00
20: 01 01 03 00 01 00 00 00 01 00 00 00 02 01 03 00
30: 03 00 00 00 6C 00 00 00 03 01 03 00 01 00 00 00
40: 01 00 00 00 11 01 04 00 01 00 00 00 08 00 00 00
50: 06 01 03 00 01 00 00 00 02 00 00 00 15 01 03 00
60: 01 00 00 00 03 00 00 00 00 00 00 00 08 00 08 00
70: 08 00
```

IMAGE FILE HEADER

FIELDS	VALUES
endianness	II INTEL little endian
constant	42
IFD offset	12 →

IMAGE DATA

FF 00 00 00 FF 00 00 00 FF
00 (word alignment)

IMAGE FILE DIRECTORY

FIELDS	VALUES
→ entries count	7
tag	100 IMAGEWIDTH
type count	3 SHORT 1
val/offset	3
tag	101 IMAGELENGTH
type count	3 SHORT 1
val/offset	1
tag	102 BITSPERSAMPLE
type count	3 SHORT 3
val/offset	0x6c →
tag	103 COMPRESSION
type count	3 SHORT 1
val/offset	1 (none)
tag	111 STRIPOFFSETS
type count	4 LONG 1
val/offset	8
tag	106 PHOTOMETRIC
type count	3 SHORT 1
val/offset	2 (RGB)
tag	115 SAMPLESPERPIXEL
type count	3 SHORT 1
val/offset	3
next IFD	0x00000000

DATA

→ bps 8, 8, 8

Command Line:

- Pull out the audio with ffmpeg:

```
$ ffmpeg -i windows.mp4 windows.wav
```

- Make a gif from video using ffmpeg

```
$ ffmpeg -i windows.mp4 windows.gif
```

- Online tool for images:
  - utilitymill
  - pngcheck
  - Paranoid.jar

Metadata

Image metadata

- To find information inside a picture, we can use package pnginfo or pngcheck.
- If we need base64 decoding (for example a PGP key with a picture).
- Weird pieces of bytes may need to be XORed.
- If we have a decrypted message and a key:

i. Import the private key to use it to decrypt the message with `gpg --allow-secret-key-import --import private.key`

ii. Decrypt with `gpg --decrypt message.pgp`.

- ExifTool

Other Tools

- OpenStego
- OutGuess
- Gimp
- Audacity
- MP3Stego
- ffmpeg
- pngcheck
- StegFS
- Steghide

Terms Privacy Security Status Help

Contact GitHub API Training Shop Blog About