Steganography

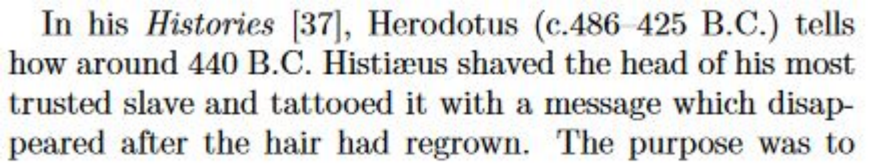
The art of hiding secrets

So what is steganography???

Steganography (‘stego’ for short) is essentially concealing things.

Things include:

- Messages
- Files
- Your assignment



In his *Histories* [37], Herodotus (c.486–425 B.C.) tells how around 440 B.C. Histiæus shaved the head of his most trusted slave and tattooed it with a message which disappeared after the hair had regrown. The purpose was to

Audio Steganography

Recommended tools

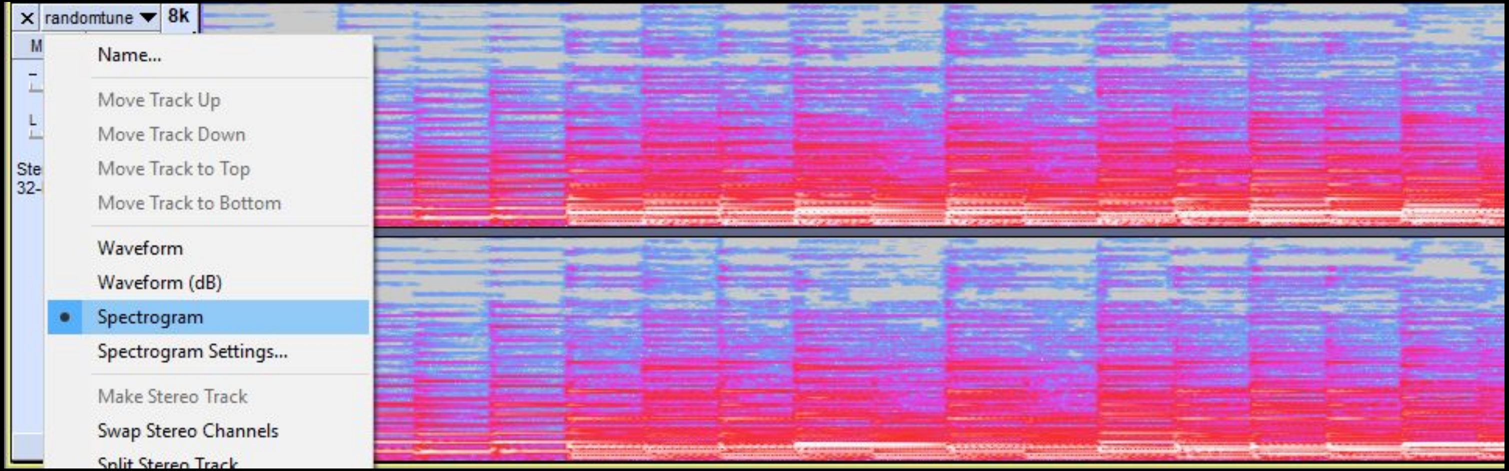
Audacity https://www.audacityteam.org/

Sonic Visualiser https://sonicvisualiser.org/

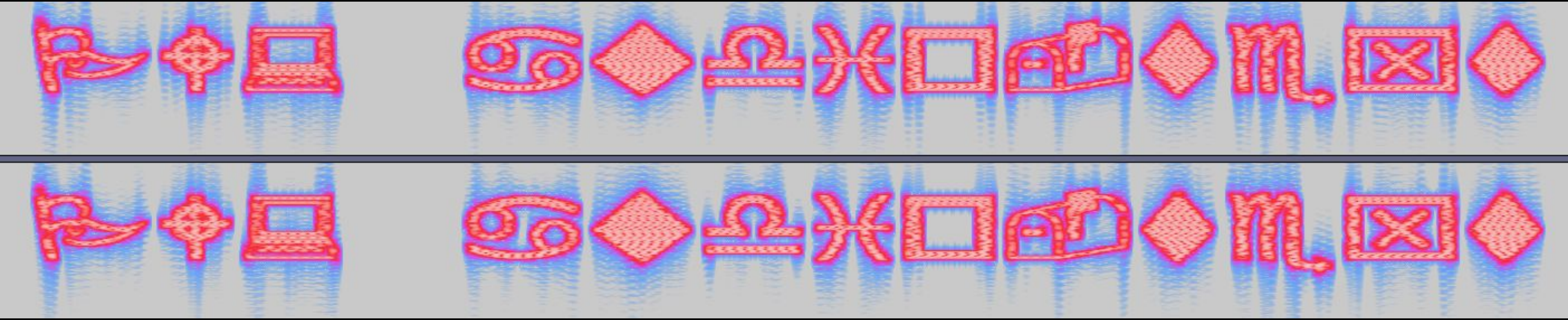
Spectrogram

Visually shows the spectrum of frequencies

Can be used to visually hide messages

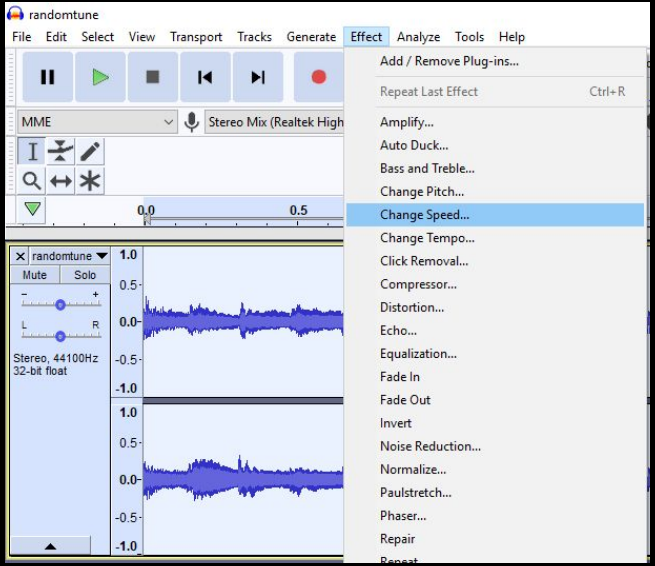


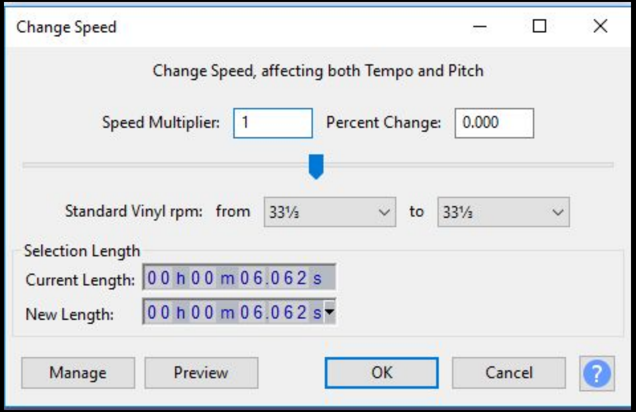
Example of spectrogram hiding messages



Speed Altering

Sometimes audio may need a tad bit of speed adjustments (faster or slower)




Change Speed

Change Speed, affecting both Tempo and Pitch

Speed Multiplier: 1 Percent Change: 0.000

Standard Vinyl rpm: from 33⅓ to 33⅓

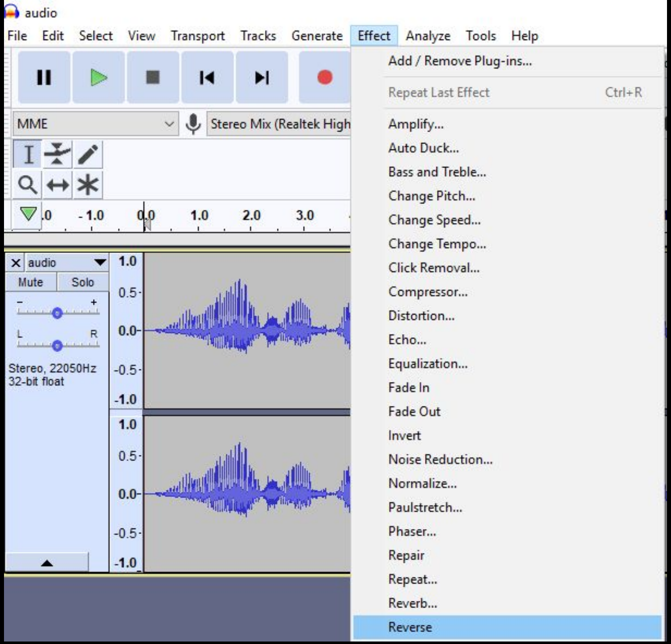
Selection Length

Current Length: 00 h 00 m 06.062 s

New Length: 00 h 00 m 06.062 s

Reversing

Perhaps the gibberish is just reversed audio



Visual Steganography

Recommended tools

Photoshop

GIMP https://www.gimp.org/

Photopea (Online tool) https://www.photopea.com/

Media Player Classic (Windows only) https://mpc-hc.org/

VLC https://www.videolan.org/vlc/

Frame by frame

Some things appear and disappear faster than you can say “Misc Cat”

For videos:

In VLC use ‘e’ to go to the next frame. Other programs may use arrow keys

For YouTube videos, use , and . to go back and forth between frames

For gifs:

Opening in an image editor actually reveals each frame as layers (except ms paint, or anything that doesn’t deal with layers)

Gifs frame by frame example

Each frame of a gif as displayed as layers when opened

in an image editor (in this case, photopea)

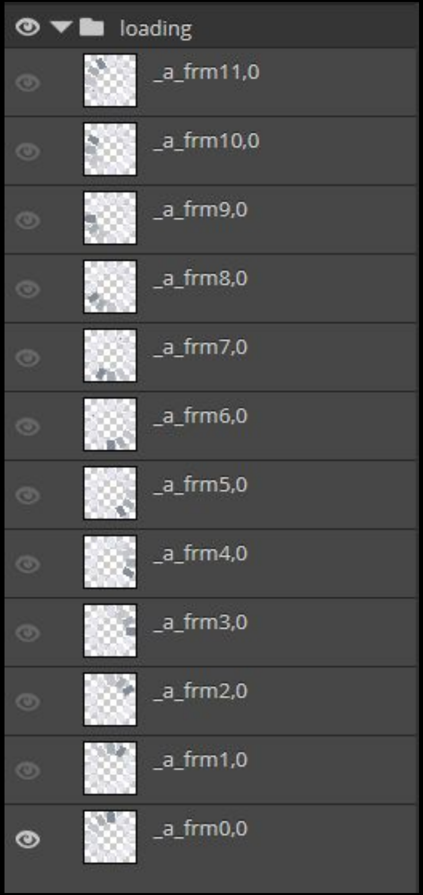
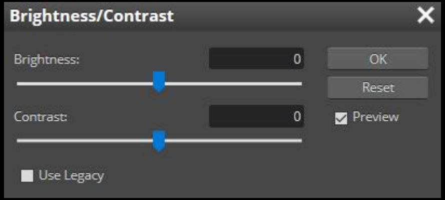


Image adjustments

Brightness / Contrast / Hue / Saturation / Zooming

Just slide the sliders till you see stuff (sometimes using paint bucket tool works)

Some things though, need you to look really really closely



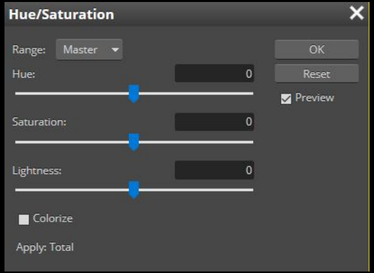
Brightness/Contrast

Brightness: 0

Contrast: 0

☑ Preview

□ Use Legacy



Hue/Saturation

Range: Master

Hue: 0

Saturation: 0

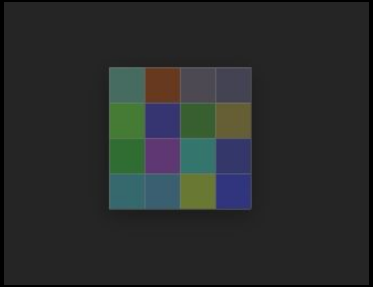
Lightness: 0

☑ Preview

□ Colorize

Apply: Total

Zooming in



Hidden in plain sight

In a giant wall of text

Invisible (ink)

Italics/Bold

Capitals (maybe even punctuation)

Acrostic

Font changes

Challenge: http://bit.ly/PlainSightFun (hint: this page is your key)

Other Steganography

Colour codes

An innocent set of pixels can hide a secret message that can change the whole world

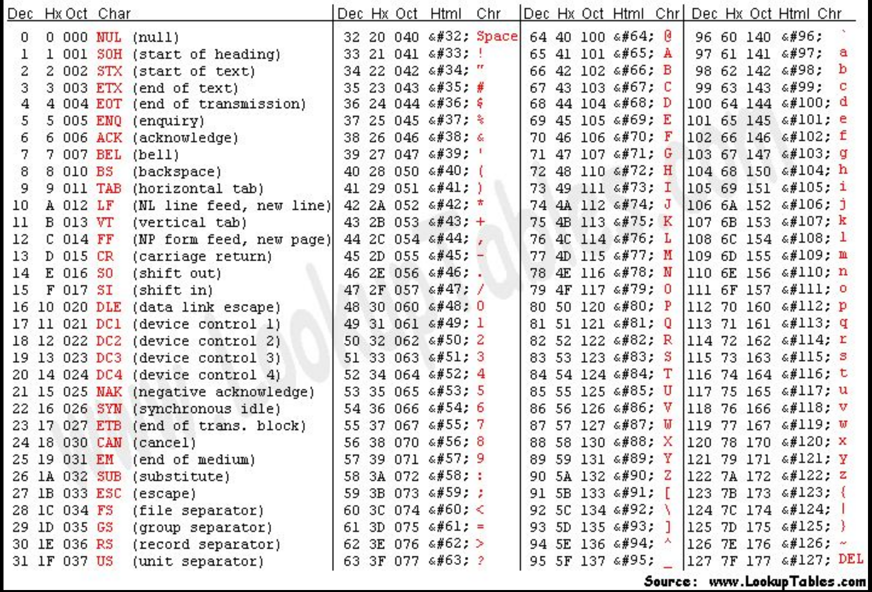
Images are made up of tiny pixels. Essentially small dots that make up a large image. Each of those pixels are set to a certain colour, represented using colour codes.

Short explanation of RGB system and mess around with colours:

https://www.rapidtables.com/web/color/RGB_Color.html

From colours to ASCII

All english characters are encoded into a system called “ASCII” - which is essentially a way for computers to represent text.



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH (start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX (start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX (end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT (end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ (enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK (acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL (bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS (backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB (horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF (NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT (vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF (NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR (carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO (shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI (shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE (data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1 (device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2 (device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3 (device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4 (device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK (negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN (synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB (end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN (cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM (end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB (substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC (escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS (file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS (group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS (record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US (unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

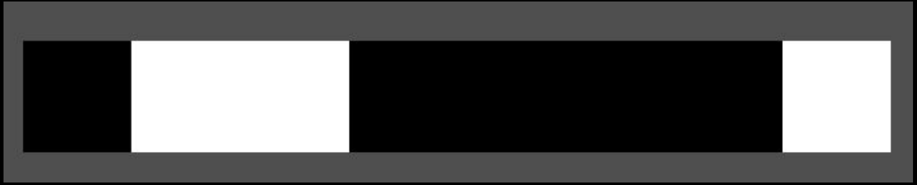
#426174 = Bat

First, split into R,G,B (42,61,74)
Since these colour codes use hex(adecimal) codes, use the Hx column on the ascii table to the left to get B,a,t

Binary everywhere

Sometimes, an image with seemingly random image with black and white dots may turn out to be a binary string (or vice versa, where a random binary string may turn out to be a meaningful image).

E.g. Where black = 0, and white = 1:



= 01100001 = ASCII code for ‘a’

Binary (and even morse) can appear anywhere when there are only two states / options (e.g. Left/Right, Up/Down, Upper/Lower case, and other creative scenarios)

Least Significant Bit

Each pixel of an image can be represented with binary (RGB has 3 bytes, grey scale only has one byte)

E.g. in a black and white image, a set of pixels could have the value:

00110100 10101011 01001001 00010010 01101101 01010100 00111011 010110111

By taking the ‘least significant bit’ (right most bit), you get the binary: ‘01101011’ - the ascii value for ‘k’

For RGB, it’s the same logic, just done with each of the colour channels.

File signatures

Every file has a signature that lets the computer know what kind of file it is

https://en.wikipedia.org/wiki/List_of_file_signatures

https://www.garykessler.net/library/file_sigs.html

Recommended tool: HxD (love it - windows only)

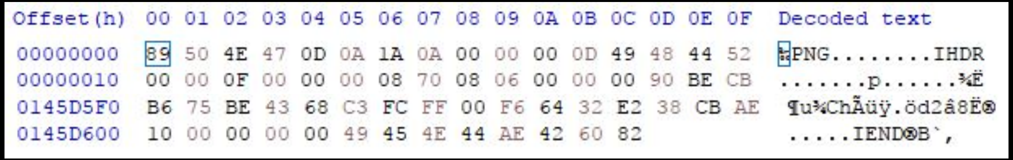
Mac: 0xED

Linux: okteta / hexedit

(any other hex editor should work fine)

Common file types:

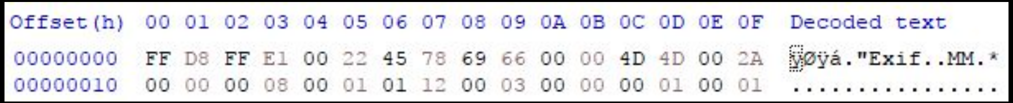
PNG:



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000   89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ‰PNG........IHDR
00000010   00 00 0F 00 00 00 08 70 08 06 00 00 00 90 BE CB  .......p......¾Ë
0145D5F0   B6 75 BE 43 68 C3 FC FF 00 F6 64 32 E2 38 CB AE   ¶u¾ChÃüÿ.öd2â8Ë®
0145D600   10 00 00 00 00 49 45 4E 44 AE 42 60 82            .....IEND®B`‚
```

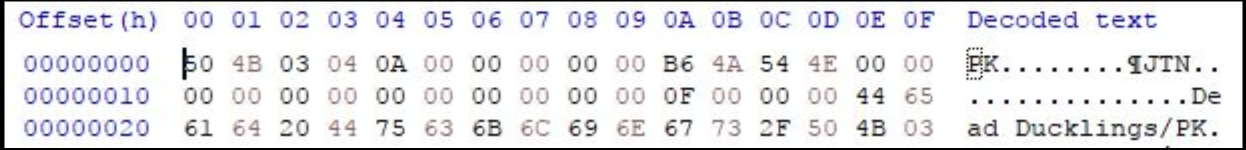
JPG:



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000   FF D8 FF E1 00 22 45 78 69 66 00 00 4D 4D 00 2A  ÿØÿá."Exif..MM.*
00000010   00 00 00 08 00 01 01 12 00 03 00 00 00 01 00 01  ................
```

Zip:



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000   50 4B 03 04 0A 00 00 00 00 00 B6 4A 54 4E 00 00  PK........¶JTN..
00000010   00 00 00 00 00 00 00 00 00 00 0F 00 00 00 44 65  ..............De
00000020   61 64 20 44 75 63 6B 6C 69 6E 67 73 2F 50 4B 03  ad Ducklings/PK.
```

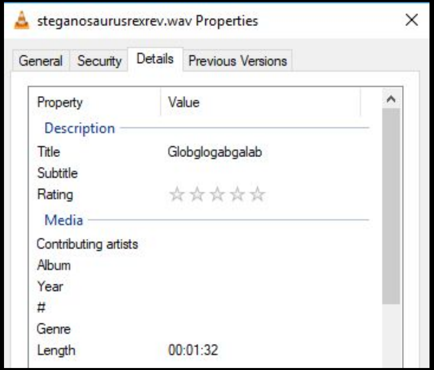
Exif and metadata

Exif data stores information about the image (generally found in jpg / jpeg files)

Metadata shows information about the file, however, someone can edit this data to hide information (audio files, video files, images)

Sometimes, meaningful data can be appended somewhere in the file. Most of the time it’s at the very end of the file, though at times, it can be somewhere in the middle.

Places where metadata can hide

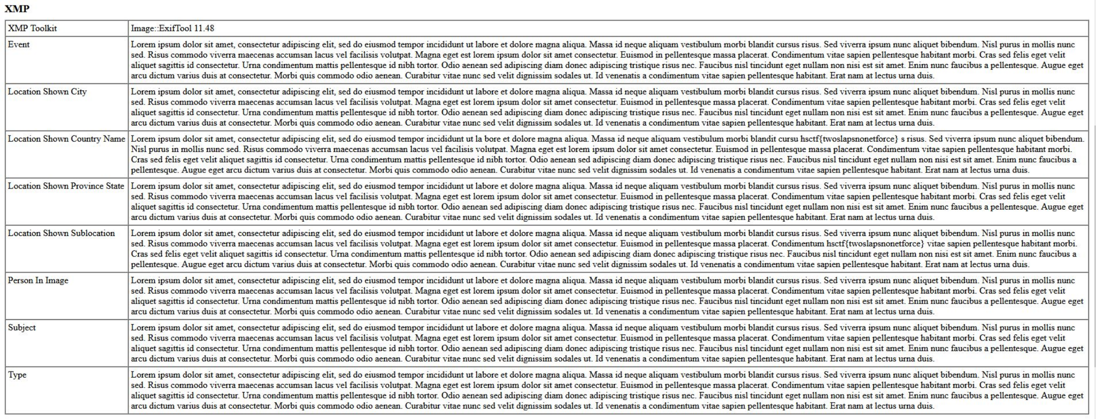


steganosaurusrexrev.wav Properties

Property	Value
Description	
Title	Globglogabgalab
Subtitle	
Rating	☆☆☆☆☆
Media	
Contributing artists	
Album	
Year	
#	
Genre	
Length	00:01:32

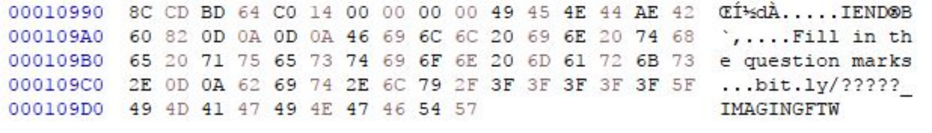
Info hidden in file metadata

In the EXIF



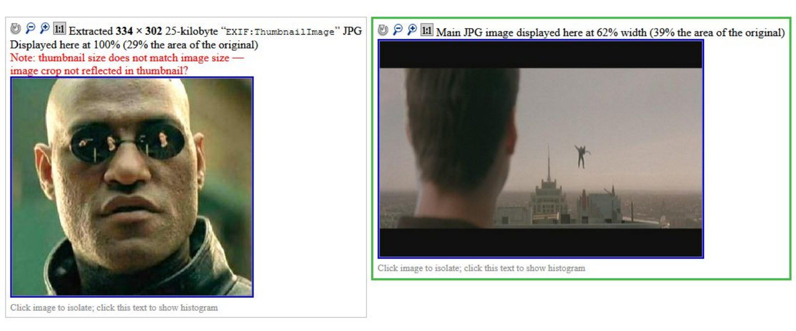
XMP

XMP Toolkit	Image::ExifTool 11.48
Event	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursus risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.
Location Shown City	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursus risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.
Location Shown Country Name	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut la bore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursu hsctf{twoslapsnonetforce} s risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.
Location Shown Province State	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursus risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.
Location Shown Sublocation	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursus risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum hsctf{twoslapsnonetforce} vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.
Person In Image	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursus risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.
Subject	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursus risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.
Type	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam vestibulum morbi blandit cursus risus. Sed viverra ipsum nunc aliquet bibendum. Nisl purus in mollis nunc sed. Risus commodo viverra maecenas accumsan lacus vel facilisis volutpat. Magna eget est lorem ipsum dolor sit amet consectetur. Euismod in pellentesque massa placerat. Condimentum vitae sapien pellentesque habitant morbi. Cras sed felis eget velit aliquet sagittis id consectetur. Urna condimentum mattis pellentesque id nibh tortor. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Faucibus nisl tincidunt eget nullam non nisi est sit amet. Enim nunc faucibus a pellentesque. Augue eget arcu dictum varius duis at consectetur. Morbi quis commodo odio aenean. Curabitur vitae nunc sed velit dignissim sodales ut. Id venenatis a condimentum vitae sapien pellentesque habitant. Erat nam at lectus urna duis.



```
00010990  8C CD BD 64 C0 14 00 00 00 00 49 45 4E 44 AE 42  ŒÍ½dÀ.....IEND®B
000109A0  60 82 0D 0A 0D 0A 46 69 6C 6C 20 69 6E 20 74 68  `‚....Fill in th
000109B0  65 20 71 75 65 73 74 69 6F 6E 20 6D 61 72 6B 73  e question marks
000109C0  2E 0D 0A 62 69 74 2E 6C 79 2F 3F 3F 3F 3F 3F 5F  ...bit.ly/?????_
000109D0  49 4D 41 47 49 4E 47 46 54 57                    IMAGINGFTW
```

At the end of a (png) image



Extracted **334** × **302** 25-kilobyte “`EXIF:ThumbnailImage`” JPG Displayed here at 100% (29% the area of the original)

Note: thumbnail size does not match image size — image crop not reflected in thumbnail?

Click image to isolate; click this text to show histogram

Main JPG image displayed here at 62% width (39% the area of the original)

Click image to isolate; click this text to show histogram

Also EXIF, but as a hidden thumbnail

Other Stego Tools

Zsteg (https://github.com/zed-0xff/zsteg) - detects stego in PNG/BMP files

stegsolve (http://www.caesum.com/handbook/Stegsolve.jar) allows you to see different colour channels separately

Steghide, StegoSuite, StegSnow, s-tools and thousands of other stego programs: Allows you to hide (and in some cases detect/unhide, but only if it's been hidden with its tool) data in files

Binwalk (https://github.com/ReFirmLabs/binwalk) - Useful for things other than stego as well. Has (file) signature scanning, easily identifying hidden files.

Challenges!!!

Check out MISCCTF Bot on the discord for challenges

In DMs, type $challs, and check out the stego challenges, and give them a crack

Finished them all? I’m working on some challenges soon, and I’m sure a few others are too. Stay tuned for them!