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

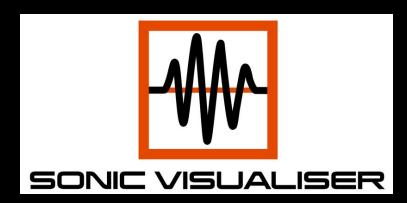
Audio Steganography

Recommended tools

Audacity https://www.audacityteam.org/



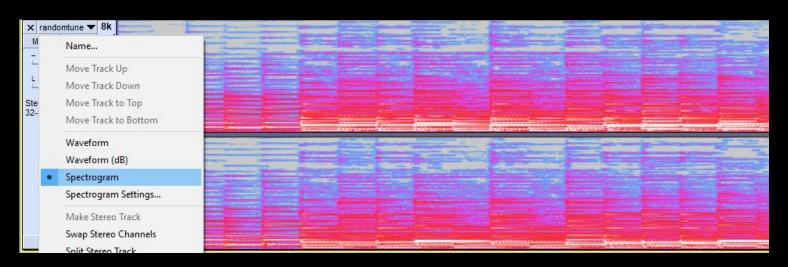
Sonic Visualiser https://sonicvisualiser.org/



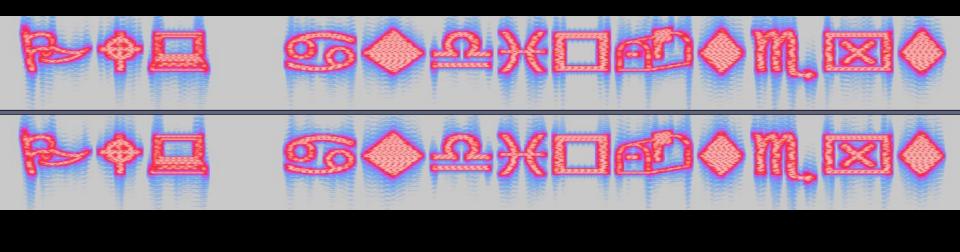
Spectrogram

Visually shows the spectrum of frequencies

Can be used to visually hide messages

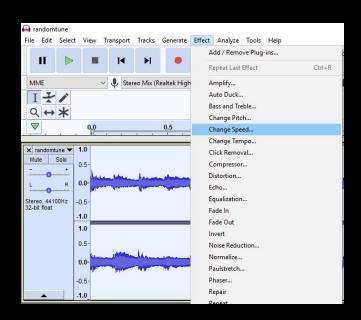


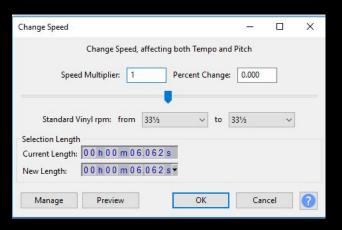
Example of spectrogram hiding messages



Speed Altering

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





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)

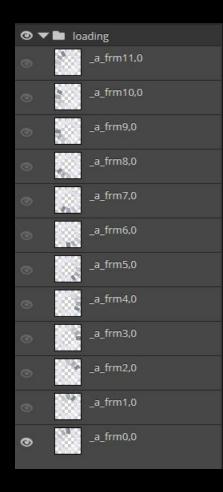
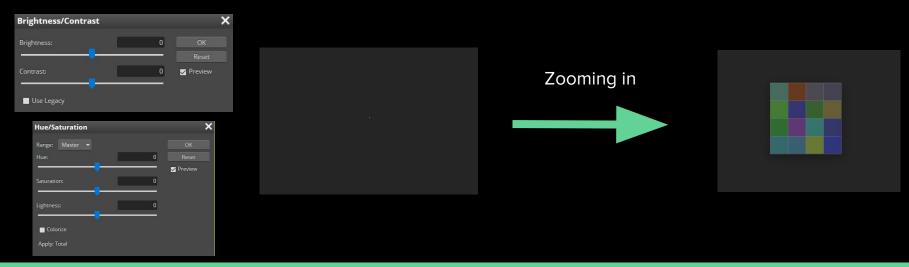


Image adjustments

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



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

#426174

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	Нх	Oct	Char	39	Dec	Нх	Oct	Html	Chr	Dec	Нх	Oct	Html	Chr	Dec	: H	(Oct	Html C	hr
0	0 (300 1	NUL	(null)	32	20	040	6#32;	Space	64	40	100	6#64;	0	96	60	140	6#96;	
1	1 (301	SOH	(start of heading)	33	21	041	6#33;	1	65	41	101	6#65;	A	97	61	141	6#97;	a
2	2 1	302	STX	(start of text)	34	22	042	6#34;	rr	66	42	102	B	В	98	62	142	6#98;	b
3	3 (003 7	ETX	(end of text)	35	23	043	6#35;	#	67	43	103	4#67;	C	99	63	143	6#99;	C
4	4 1	004	EOT	(end of transmission)	36	24	044	\$	\$	68	44	104	D	D	100	64	144	a#100;	d
5	5 (305 1	ENQ	(enquiry)	37	25	045	6#37;	*	69	45	105	E	E	101	65	145	e	e
6	6 1	306	ACK	(acknowledge)	38	26	046	6#38;	6.	70	46	106	a#70;	F	102	66	146	f	f
7				(bell)	39	27	047	6#39;	0	71	47	107	6#71;	G	103	67	147	6#103;	g
8	8 1	010	BS	(backspace)	40	28	050	a#40;	(72	48	110	6#72;	H	104	68	150	6#104;	h
9	9 1	011	TAB	(horizontal tab)	41	29	051	6#41;)	73	49	111	6#73;	I	105	69	151	a#105;	i
10	A	012	LF	(NL line feed, new line)	42	2A	052	6#42;	*	74	4A	112	6#74;	J	106	6A	152	a#106;	j
11	B (013	VT	(vertical tab)	43	2B	053	6#43;	+	75	4B	113	6#75;	K	107	6B	153	6#107;	k
12	C 1	014	FF	(NP form feed, new page)	44	20	054	6#44;	,	76	4C	114	6#76;	L	108	6C	154	6#108;	1
13	D I	015	CR	(carriage return)	45	2D	055	6#45;	-	77	4D	115	6#77;	M	109	6D	155	6#109;	m
14	E (016	50	(shift out)	46	2E	056	6#46;		78	4E	116	4#78;	N	110	6E	156	n	n
15	F	017	SI	(shift in)	47	2F	057	6#47;	/	79	4F	117	6#79;	0	111	6F	157	6#111;	0
16 .	10 (J20 J	DLE	(data link escape)	48	30	060	6#48;	0	80	50	120	4#80;	P	112	70	160	6#112;	p
17 .	11 (J21 J	DC1	(device control 1)	49	31	061	6#49;	1	81	51	121	Q	Q	113	71	161	q	q
18 .	12 (322 J	DC2	(device control 2)				2					4#82;		114	72	162	6#114;	r
19 .	13 (J23 J	DC3	(device control 3)				3					e#83;					6#115;	
20 .	14 1	024 1	DC4	(device control 4)	52	34	064	6#52;	4	84	54	124	a#84;	T	116	74	164	a#116;	t
21 .	15 (325 1	NAK	(negative acknowledge)	53	35	065	6#53;	5	85	55	125	a#85;	U	117	75	165	a#117;	u
22 .	16 1	326	SYN	(synchronous idle)	54	36	066	6#54;	6	86	56	126	4#86;	V	118	76	166	a#118;	V
23 .	17 (327 1	ETB	(end of trans. block)	55	37	067	6#55;	7	87	57	127	4#87;	W	119	77	167	6#119;	w
24 .	18	330	CAN	(cancel)	56	38	070	a#56;	8	88	58	130	4#88;	X	120	78	170	6#120;	X
25 .	19 1	031 1	EM	(end of medium)	57	39	071	6#57;	9	89	59	131	6#89;	Y	121	79	171	6#121;	Y
26 .	LA I	332	SUB	(substitute)	58	ЗA	072	6#58;	:	90	5A	132	Z	Z	122	7A	172	6#122;	z
27 .	LB (J33 I	ESC	(escape)	59	3B	073	6#59;	;	91	5B	133	[[123	7B	173	6#123;	{
28 .	LC (034	FS	(file separator)	60	30	074	<	<	92	5C	134	6#92;	1	124	70	174	6#124;	1
29 .	LD (035		(group separator)	61	3D	075	=	=	93	5D	135	6#93;]	125	7D	175	6#125;	}
30 .	LE I	036		(record separator)	62	3E	076	>	>	94	5E	136	6#94;	٨				~	
31 .	LF (037 1	US	(unit separator)	63	3F	077	a#63;	2	95	5F	137	6#95;		127	7F	177	6#127;	DEL
	Source: www.LookupTables.com																		

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:

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

000000000 89 50 4E 47 0D 0A 1A 0A 00 00 0D 49 48 44 52 PNG.....IHDR

00000010 00 00 0F 00 00 00 08 70 08 06 00 00 09 0B CB .....p....½Ë

0145D5F0 B6 75 BE 43 68 C3 FC FF 00 F6 64 32 E2 38 CB AE YU½ChÃüÿ.öd2â8Ë®

0145D600 10 00 00 00 00 49 45 4E 44 AE 42 60 82 ....IEND®B`,
```

JPG:

Zip:

Exif and metadata

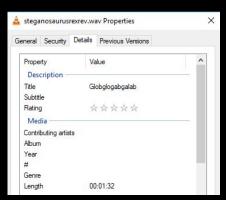
Exif data stores information about the image (generally found in jpg / jpeg files)

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.

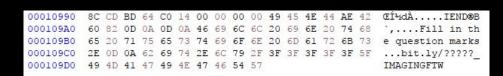
Places where metadata can hide

In the EXIF



Info hidden in file metadata

XMP	
XMP Toolkit	Image: ExifTool 11.48
	Leren iguen dotor sit met, consectivut adjuvicing dis, sed do visumed tempor incident ut labore et doive magna alique. Massa si neque aliques methodum morbi blandir cursus risus. Sed vivera puum mun aliques blandum. Nisi puus si mollis nume et Russa commondo vivera macerassa secusiona lucus vi facilitati volquat. Magna sed est loren pium doive si annet consectivut. Bisumodi in pellentenque massa placera. Condimentorium trias appier pellentenque habatum notio. Tica sed felia se pet viel aliquet sagitis si consectivut. Winter condimentum matria pellentenque di mal bortor. Olio acena not dispicient giáum donce adipicient grátique risus pais pellentenque pellantenque habatum notio. Isa ced felia se pet viel aliquet sagitis si consectivut. Winter opicio acena macera de viel dispiration sociale ut si eventaria a condimentum. Funda condimentum ratio such sur sur discussion sociale ut si eventaria a condimentum. Funda mat electra una duis.
	Loren i pum dolor ait unet, consecteur adipicing ell, sed do risumed tempor incididunt ut labore et dolore magna aliqua. Massa si neque aliquam ventrablum morbi blandir curus risus. Sed vivera puma mue aliquet blendum. Nid purus in mollis nume el Risus commodo vivera macerassa secuena locus vel fincilisto vivera macerassa secuena locus veloras del seguina del consecuente vivera condimentum matris pellentesque si adulto totto. Olio aemen sed adaptici enginis si consecuente. Whoshim vivera in consecuente vivera secuena consecuente vivera del macera del matrio matris sociale un til eventuali a consecuentum Vivera in consecuente vivera turna duis.
and the second s	Lorem journ dolor ait amer, consecteur adjuscing ells, sed do cissued tempos incididunt ut la bore et dolore magna aliqua. Massa di neque aliquam verbalhum morbi blandir curus hactiffrondapposoneferor? a risus. Sed vivera injum muse aliquet bheedum Nal purus in mollia lume est di susso common do vivera macenas causus lauve ut fenticiais voltagus. Mangas eger est forem jumu dolor sit mer consecteur. Esimon di pellentesque massa placears. Gondinentum trus esapine pellentesque habitant moltre. Cars sed felis eger vini alquete agains si consecteur. Uma condimentum mattis pellentesque si almò tortor. Odio aeneas a dalquiscing diant donce adjuscing ristique risus ner. Funchus nia lunicalut eger nullam non nia est si st met. Enim mune funchus a pellentesque, August est ordinario dissi a consecteur. Morbi quis commondo on aeneas. Curabitum risus muse del visit dispussim sodales ut. Il eveneasita a condimentum varie appine pellentesque, August a condimentum varie appine pellentesque. August and condimentum varies and condimentum varies and condimentum varies and condimentum varies and condimentum varies. August and condimentum vari
	Lorem journs dotor sit mare, consecteur adjuscing els, sed do cissmed tempor incididunt ut labore et dolore magna aliqua. Massa si neque adjuscus returbulum morbi blunder cursus risus. Sed vivera passam more aliquer blundem. Nisi pursus in mollis sume els Russa commondo vivera macerassa secusionam locas ved facilitative voltura. Magna segor el forme pissum doire si ante consecteur. Elizamod in pellentenque massas plectrat. Comfumentom vive aspirar pellettenque bluntum morbi. Es sed felia segor vivel adapter saggitis si consecteur. Morbin opinion si senting segor de l'acceptative de distribute de l'acceptative de distribute de l'acceptative de distribute de l'acceptative de l'ac
	Leren iguen dotor sit met, conscrietur adipsicing eli, sed do visumed tempor incididunt ut labore et dotor magna alique. Massa si neque aliques ventrablum morbi blandir cursu risus. Sed vivera puum mue aliques blandum. Nid purus in mollis mue el Russa commondo vivera macerassa scenamin bactu vel facilitati volques. Magna sed est loren pium dotor sit anne conscrietur litumod in pellentenque palapitati morbi. Cras sed filis eger veit aliquest againsi si conscretur. Urna condimentum antis pellentenque aliquest morbi. Cras sed filis eger veit aliquest againsi si conscretur. Urna condimentum antis pellentenque aliquest morbi. Pellentenque aliquest morbi. Pellentenque aliquest morbi. Pellentenque aliquest morbi. Pellentenque aliquest pellentenque. Aliquest soni a secondimentum varies unis se conscrietural varies mue de sur de la conscrietura de la confirmation varies espan pellentenque. Aliques apine pellentenque. Aliques parte pellentenque. Aliquest condimentum varies apine pellentenque aliquest parte pellentenque. Aliques apine pellentenque aliquest parte pellentenque aliquest penta de unitar varies sur destination aliquest per sur destination varies parte pellentenque aliquest penta pental
	Leren iguen dotor uit met, concerteur adjuvieng eils, sed do visumed temper incididunt ut labore er dotore magna alique. Mans ai neque aliquen ventrablum morbi blandur curus rius. Sed viverus puum muse aliquet blandum Nid purus in mollis muse el Russo commodor viveren macensas socieums locus vel fincilius volques. Magna erge et loren iguum dotor si annet consectente. Usumodo in pellentenque massa plecent. Comfumentom vites appiren plectureque blandum notor. Its cas definis egre vivel aliquet saggitis si consectentu. Vites confimentum matris pellentenque di adult bortor. Oilo anema sod adspicient giun disson en Eruschos unit tracidunt eget millam non mise si si same fizini muse faucibos a pellentenque. Augus egget arcu dicturu virusi dus is consectentu. Wolthur virusi modate. Ut di vernatia a consellentum Moderni. Erus mant electura turn dais.
	Lorem journ dolor ait amer, consecteur adjuscing ells, sed do cissuned tempor incididunt ut labore et dolore magna aliqua. Massa id neque aliquam ventebulum morbi blandir cursus risus. Sed vivera paum mue aliques blendum. Nisi purus in mollis nume el Russo commodo vivera macerassa secusiona lorus vel facilitati sovulpar. Magna ege et al forem journ dolor est anne consecteur libumodo in pellentenque massa placera. Confinentemum vitea sapiera pellentenque habatum noto. Tics and efficia espet viel alaquest asquiris si consecteur. Universa confinentum matria pellentenque in alabo torte. Oldo acenas ned adaptive cap diam donore. Sulpication qui traitique risus a consecteur. Universa risus a consecteur. Morbinar vivera in consecteur. Universa risus sociales ut il reventa a confinentum. Este man at electra una duis.
	Loren ipsum dolor at met, consecteur adipsicing els, sed do cisumod tempos incididunt ut labore el dolore magna aliqua. Massa si neque adiquam estretablum morbi blandir cursus risus. Sed vivera paum mue aliquet blendum. Nid pursus in mollis nume el Risus commodo vivera mascensa secuns micras ve fincilista volpata. Magna gene el torner pusum doir cis anter consecteur tilumodo in pellentensque massa palerant. Confinentimo mix tea speira pelletteneque habitant morbit. Tea sed fixis espet vivil aliquet asquists si consecteur. Una confinentimo matria pelletteneque da habit orior. Cilio ascensa sed adapticing diam dones adapticine trategia est insu nece. Fancibus unit tutture in tea speira pelletteneque habitant morbit. Tea sed fixis espet vivil adapter asquisi ad consecteur. Una confinentimo matria pelletteneque habitant morbit. Tea maria in electron se una discussiona del consecteur. Una confinentimo matria pelletteneque habitant firm anni al relevor to una discussional del consecteur. Una confinentimo matria pelletteneque habitant morbit. Tea maria ni electron trata del consecteur. Una confinentimo matria pelletteneque habitant morbit in una discussional del consecteur. Una confinentimo matria pelletteneque habitant morbit in una matria confinentimo trata se applicate qualta habitant. Estim anni al relevor una discussional del consecteur. Una pelletteneque habitant morbit.



At the end of a (png) image





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!