

Steganography

Horem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Iaucibus ornare suspendisse sed nisi lacus sed viverra tellus in. Dalesuada nunc vel risus commodo viverra maecenas accumsan lacus. Da metus vulputate eu scelerisque felis. Elementum pulvinar etiam non quam lacus suspendisse faucibus interdum posuere. Ni ultrices mi tempus imperdiet nulla malesuada pellentesque elit eget. Iondimentum mattis pellentesque id nibh tortor id. Narius vel pharetra vel turpis nunc eget lorem. Paim diam vulputate ut pharetra sit. Loci eu lobortis elementum nibh tellus molestie. Agestas dui id ornare arcu odio. Ionsectetur a erat nam at lectus urna duis convallis. Nhoncus dolor purus non enim praesent elementum facilisis leo. Susto eget magna fermentum iaculis eu non diam phasellus. Illamcorper velit sed ullamcorper morbi tincidunt. Gibendum enim facilisis gravida neque convallis a cras. Huspendisse sed nisi lacus sed viverra tellus in hac. Th fermentum posuere urna nec tincidunt. Odio eu feugiat pretium nibh ipsum. Sed risus ultricies tristique nulla. Purus gravida quis blandit turpis cursus.ignissim sodales ut eu sem integer vitae justo eget magna. Vestibulum morbi blandit cursus risus at ultrices mi. Mattis molestie a iaculis at erat pellentesque adipiscing commodo. Molestie a iaculis at erat pellentesque adipiscing commodo. Integer quis auctor elit sed vulputate mi sit. Viverra suspendisse potenti nullam ac. Vitae turpis **HIDDEN IN PLAIN SIGHT** sed sed risus. Aliquet risus feugiat in ante metus dictum at tempor commodo. Proin nibh nisl condimentum id venenatis a condimentum vitae. Tortor pretium viverra suspendisse potenti nullam ac tortor vitae. Sed viverra ipsum nunc aliquet. Sit amet volutpat conseq



Disclaimer

Anything you learn in these sessions is FOR EDUCATIONAL PURPOSES ONLY and we are NOT RESPONSIBLE FOR YOUR ACTIONS! The tools we will show you aren't illegal but using them against a network you don't own or where you don't have the explicit written permission to use them is HIGHLY ILLEGAL and almost always against the terms of service. DO NOT UNDER ANY CIRCUMSTANCES USE THE TOOLS AND TECHNIQUES SHOWN AGAINST ANY UNIVERSITY OWNED PRODUCT, WEBSITE OR NETWORK, YOU WILL BE PUNISHED BY THE DEPARTMENT/UNIVERSITY AND COULD BE PROSECUTED IN SOME CASES. There are hundreds of websites where you can practice these techniques in a safe, legal environment without the risk of causing real damage or facing prosecution.



What is Steganography?

why does Harlan hate it?

~ Modern Steganography

Hiding messages within public messages so that it is not apparent to any observer

1. Data is encrypted
2. Data is then inserted then hidden
3. Unrecognisable end result that can only be recovered by intended receiver

Carrier Files:

- BMP / JPEG
- GIF
- WAV

~ Is everything Steg?

NO; RULE SETS ARE KEY

The Bible Code:

When the rules are constantly changing and broad you will find whatever you want

- Michael Drosnin

Equidistant word spaces:

can 'show' hidden messages that are not intended.

Hidden Message + Carrier File = Hidden Message in Carrier

Carrier File > Hidden Message

~ Common Hiding Techniques

There are many different tools that have varying algorithms with hiding techniques but some common approaches are:

Appending to the end of carrier

```
000172f0: 0eb7 5d72 e779 023a e54d 4cf0 5e98 07c7  ..]r.y.:.ML.^...
00017300: 1391 922a 949c d83b 6c9b c509 f8be 12d7  ...*...;l.....
00017310: a411 030c 2a51 0f45 c40e 9e77 4a84 fd0c  ...*Q.E...wJ...
00017320: 3cc3 0436 befef283 efbf fae6 87ef befdf <..6.....
00017330: fce5 3bc1 e72f 3f7f f1e3 4fbf fcfc ebe3  ..;./?...0....
00017340: e5c6 cb7b bf7a f9fe bbeb ddb8 e69f 3f9f  ...{.z.....?.
00017350: ff05 ce43 ed85 3c08 32fb 0000 0000 4945  ...C.<.<.2.....IE
00017360: 4e44 ae42 6082                                ND.B`.
```

```
~/Steg
> dd if=hidden_message bs=1 >> image.png
7+0 records in
7+0 records out
7 bytes copied, 2.5759e-05 s, 272 kB/s
```

```
00017310: a411 030c 2a51 0f45 c40e 9e77 4a84 fd0c  ...*Q.E...wJ...
00017320: 3cc3 0436 befef283 efbf fae6 87ef befdf <..6.....
00017330: fce5 3bc1 e72f 3f7f f1e3 4fbf fcfc ebe3  ..;./?...0....
00017340: e5c6 cb7b bf7a f9fe bbeb ddb8 e69f 3f9f  ...{.z.....?.
00017350: ff05 ce43 ed85 3c08 32fb 0000 0000 4945  ...C.<.<.2.....IE
00017360: 4e44 ae42 6082 5345 4352 4554 0a        ND.B`.SECRET.
```

~ Hiding Techniques

Anything can be hidden:

Audio | Video | Images | Packets | Text

- Layout in Documents
- Positions of Lines and Words
- Adding Noise
- Least Significant Bit (LSB)
- Bit Plane Complexity Segmentation
- Interlacing
- Stochastic Modulation
- HTML Steganography

Hiding Techniques

~ Common Hiding Techniques

Hidden inside unused header portions of a carrier

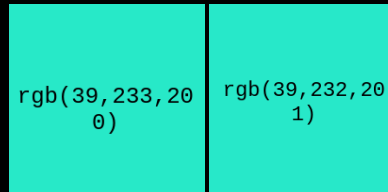
```
> xxd image.png | head
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG.....IHDR
00000010: 0000 0100 0000 0100 0802 0000 00d3 103f  ....?.....?
```

The first eight bytes of a PNG file always contain the following values:

(decimal)	137	80	78	71	13	10	26	10
(hexadecimal)	89	50	4e	47	0d	0a	1a	0a
(ASCII C notation)	\211	P	N	G	\r	\n	\032	\n

Algorithm used to disperse hidden message throughout (LSB)

Hide the binary value 101100101 into 24-bit image			
Original Cover Image			
	Pixel 0	Pixel 1	Pixel 2
R	0 0 1 1 0 0 1 1 1	1 1 1 1 0 1 1 0 0 1	1 1 0 0 1 1 0 0 0 0
G	1 1 1 1 0 1 0 0 1	1 1 0 0 1 1 0 0 0	0 0 1 0 0 1 1 1 1
B	1 1 1 0 0 1 0 0 0	1 1 1 1 0 1 1 0 0 1	1 1 1 1 0 1 1 0 0 1
Stego-image			
	Pixel 0	Pixel 1	Pixel 2
R	0 0 1 1 0 0 1 1 1	1 1 1 1 0 1 1 0 0 1	1 1 0 0 1 1 0 0 0 1
G	1 1 1 1 0 1 0 0 0	1 1 0 0 1 1 0 0 0	0 0 1 0 0 1 1 1 0
B	1 1 1 0 0 1 0 0 1	1 1 1 1 0 1 1 0 0 0	1 1 1 1 0 1 1 0 0 1



Original = (00100111 11101001 11001000)
Steg = (00100111 11101000 11001001)

24-bits colour it would take 3 pixels to hide a hexadecimal letter

~ Hiding Techniques

Anything can be hidden:

Audio | Video | Images | Packets | Text

- Layout in Documents
- Positions of Lines and Words
- Adding Noise
- Least Significant Bit (LSB)
- Bit Plane Complexity Segmentation
- Interlacing
- Stochastic Modulation
- HTML Steganography

Identifying Steganography?

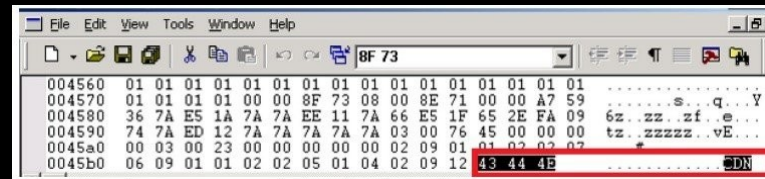
~ Steganalysis

Tools vary in their approach and without knowing which tool is used then it is pretty much impossible to identify existence of hidden data (*this is why Harlan hates it*)

What if we can identify steganography exists

- Find tool used for hiding data (signatures)
- Find the original carrier file (recovered)

Signature-based analysis:



```
File Edit View Tools Window Help
8F 73
004560 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
004570 01 01 01 01 00 00 8F 73 08 00 8E 71 00 00 A7 59 .....s..q..Y
004580 36 7A E5 1A 7A 7A EE 11 7A 66 E5 1F 65 2E FA 09 6z..zz..zf..e...
004590 74 7A ED 12 7A 7A 7A 7A 7A 03 00 76 45 00 00 00 tz..zzzzz..vE...
0045a0 00 03 00 23 00 00 00 00 00 02 09 01 01 02 02 02
0045b0 06 09 01 01 02 02 05 01 04 02 09 12 43 44 4E .....ODN
```

Anomaly Analysis:



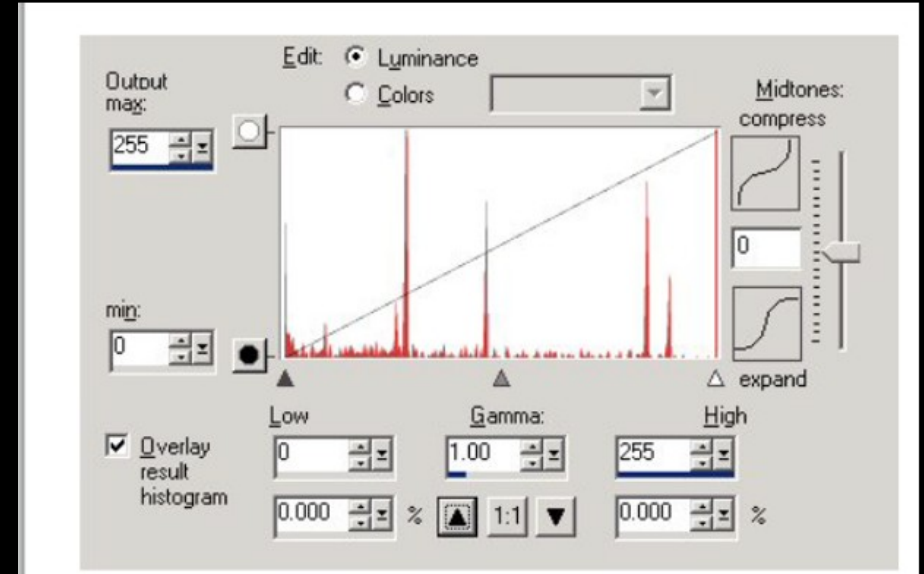
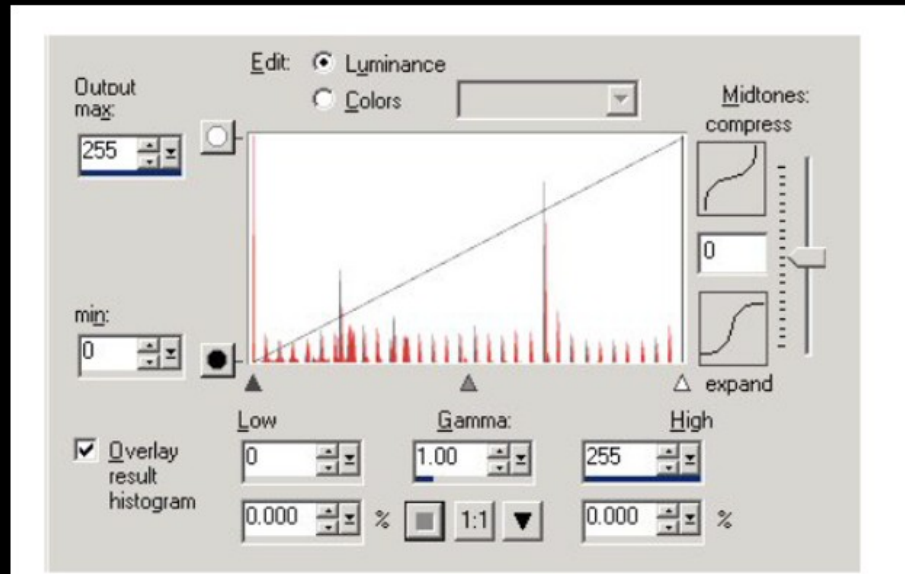
```
~/Steg
> file image.png && du -h image.png
image.png: PNG image data, 256 x 256, 8-bit/color RGB, non-interlaced
2.1M image.png
```

~ Detection

Anything can be hidden:

- Audio | Video | Images | Packets | Text
- Visual Detection
- Audible Detection
- Statistical Detection
 - Histogram
- Structural Detection
 - Size
 - Date (Read | Created | Modified)
 - Checksum
 - Meta-Data
 - Hash

Steganalysis



~ Encryption

This is when messages are encrypted and then hidden, highly common form of anti-forensic as noise and message are undistinguishable

Algorithms commonly based on symmetric secret key

Kerckhoff's principle:

“Cryptographic system should be designed to be secure, even if all its details, except for the key are public”

~ Detection Avoidance

Methods for avoiding the recovery of the message

- Delete original message
- Remove the Steganography program
- Run the Steganography program from a Live Boot / Disk Wiping
- Microwave RAM

~ Alternate Data Streams

One file can link data to many alternate data stream directions with any file sizes. NTFS allows this fork / stream of files and folders:

- Accessed only through the original file
- Can't be seen with C:/dir
- MakeStream software which can move malware to datastreams

~ Detection

- Binwalk
- XDD
- Hexdump
- StegSpy
- Stegbreak
- Knoppix
- LNS
- LADS
- NTFS ADS Check

~ Creation

- DarkCryptTC
- OpenPuff
- StegoShare
- StegFS
- HiderMan
- Jsteg
- MP3stego
- More Tools:
<http://www.jjtc.com/Security/stegtools.htm>