Steganography

The art of hiding in plain sight.

- What is steganography?
- Why is steganography?
- Where is steganography?
- Who is, just kidding, we're doing examples :p

What is Steganography

If encryption can be thought of as the encoding of data for confidentiality, then steganography is the encoding of data to obscure the fact that the data is there at all.

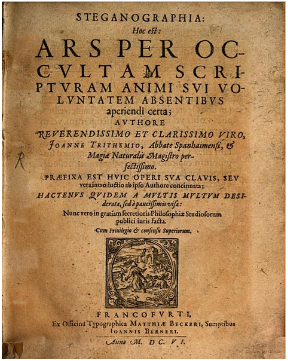
How

- Physically hiding the data/information has been used for centuries
- Digitally altering a file to insert data while retaining the original information expected has proven to be be very easy
  - Humans cant tell the difference between a `<tab>` character and 8 `<space>` characters
  - Humans cant hear over ∼20kHz
  - Humans cant tell the difference between #00ff00 and #00ff01

But why?

- Encryption can be noisy / obvious.
- So are most backdoors, remote commands, random network ports
- How can we transmit data between two parties when we know that even the *detection* of a transmission could cause harm?

When



STEGANOGRAPHIA:
Hoc eſt:
ARS PER OCCVLTAM SCRIPTVRAM ANIMI SVI VOLVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
JOANNE TRITHEMIO, *Abbate Spanhaimenſi, &*
Magiæ Naturalis Magiſtro perfectiſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipſo Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DESIderata, ſed à pauciſſimis viſa:
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.

R

FRANCOFVRTI,
Ex Officina Typographica MATTHIÆ BECKERI, Sumptibus
IOANNIS BERNERI.
Anno M. DC. VI.

Figure 1: Steganographia

First recorded use 1499, although writings from ancient Greece (∼440 BC) mention ways to pass messages unseen.

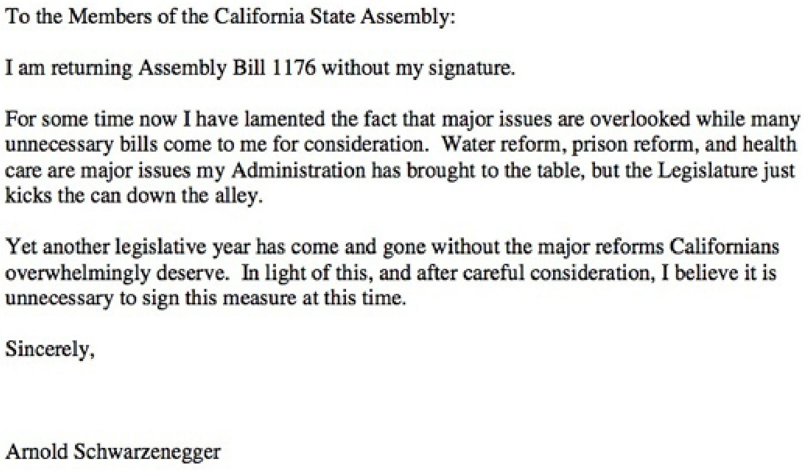
Where

Anywhere we can think to hide data.

- On a messengers scalp, allowing hair to regrow before sending ~440 BC
- Written on the wood of a wax tablet before wax was applied ~440 BC
- Published in a major work ~Steganographia 1499
- Written to an alternate track mode on a floppy ~1970s
  - 40 track mode
  - Robert Hanssen

Where else, text!

- Encoded in the first letter of each line:



To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked while many
unnecessary bills come to me for consideration. Water reform, prison reform, and health
care are major issues my Administration has brought to the table, but the Legislature just
kicks the can down the alley.

Yet another legislative year has come and gone without the major reforms Californians
overwhelmingly deserve. In light of this, and after careful consideration, I believe it is
unnecessary to sign this measure at this time.

Sincerely,

Arnold Schwarzenegger

Figure 2: Arnold

Where else, more text!!

- In a plain text file

```
--------------------------------------------
| Great work, you've found my secret lair! |
| the flag is nananananananana+batman      |
--------------------------------------------
   \      .  .
    \     |\_|\
     \    | a_a\
          | | "]
      ____| '-\___
     /.----.___.-'\
    //        _    \
   //   .-. (~v~) /|
  |'|  /\:  .--  / \
 // |-/  \_/____/\/~|
|/  \ |  []_|_|_] \ |
| \  | \ |___   _\ ]_}
| |  '-' /   ' '  |
```

Whitespace encoding with `stegsnow`

Notice anything weird about the previous slide?

- You can decode a secret message using a tool called `stegsnow`

```
Nothing fishy here...  The flag is wealthy+philanthropist
```

Text (printed to paper)

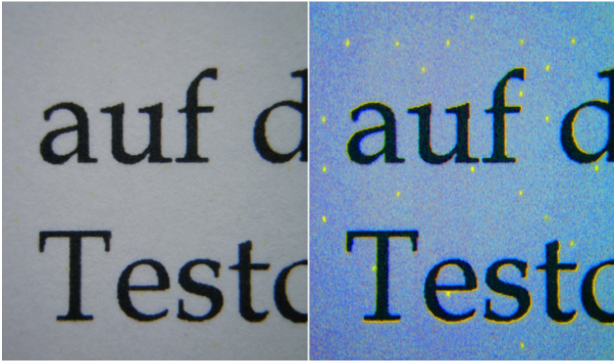
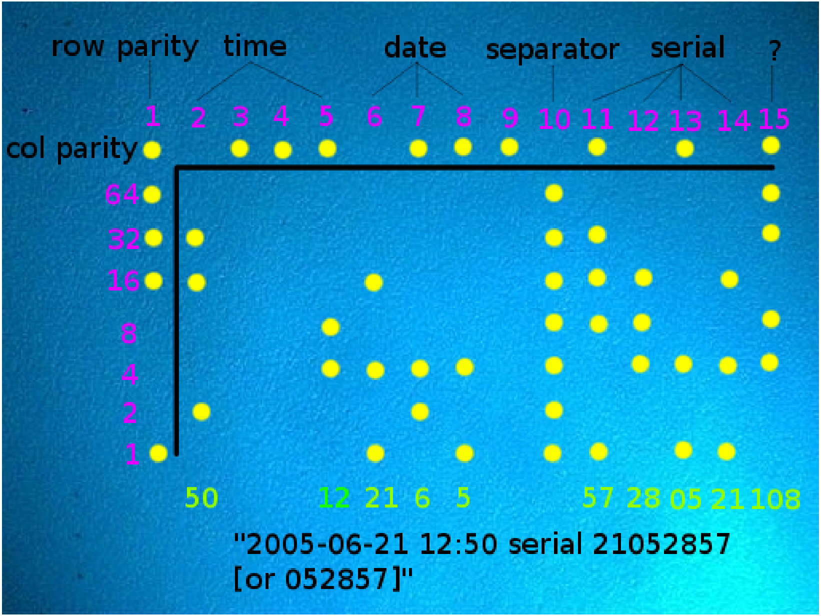


Figure 3: printer fingerprinting

In 2015 it was discovered that all major printer manufacturers entered into a secret agreement with governments to ensure that the output of their printers was forensically traceable. *-Wikipedia*

Machine Identification Code (MIC)



"2005-06-21 12:50 serial 21052857
[or 052857]"

Images

Figure 5: Shakespeare

- Contains the entire work of William Shakespeare.
- done by fiddling with `.zip` and `.jpg` headers

Images of Cats

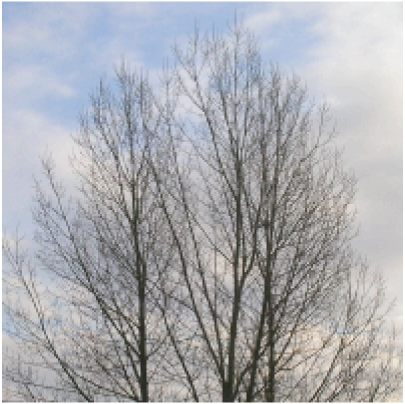


Figure 6: Not a cat

- Contains a picture of a cat
- Picture is encoded in the two Least Significant Bits (LSB)

The actual cat pic

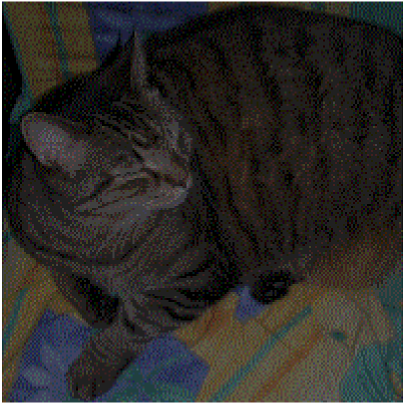


Figure 7: Is a cat

- Is a picture of a cat
- Probably hates me