STEGANOGRAPHY: HIDDEN IN PLAIN SIGHT

BY: KEVIN R. MEDINA SANTIAGO

COMPUTER FORENSICS

- Investigation of information found in computers and digital storage media
- Focuses on:
  - Identifying
  - Preserving
  - Recovering
  - Analyzing

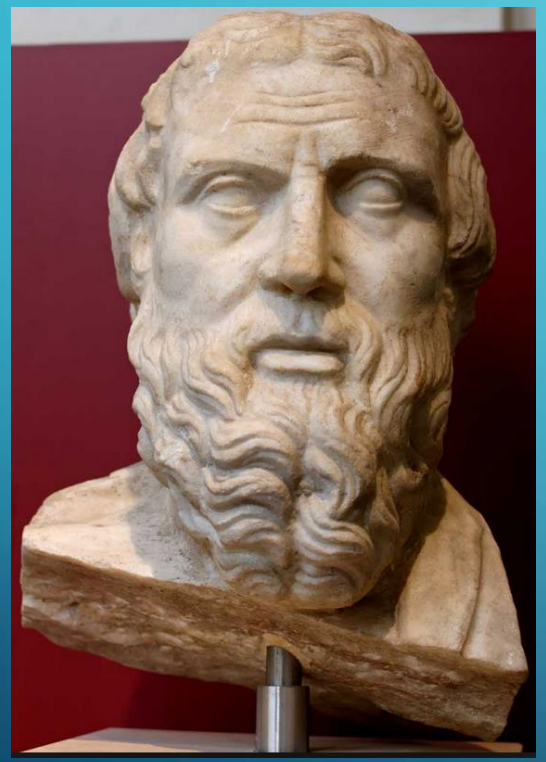
WHAT IS STEGANOGRAPHY?

S

Covered, concealed, protected

GRAPHEIN

Writing

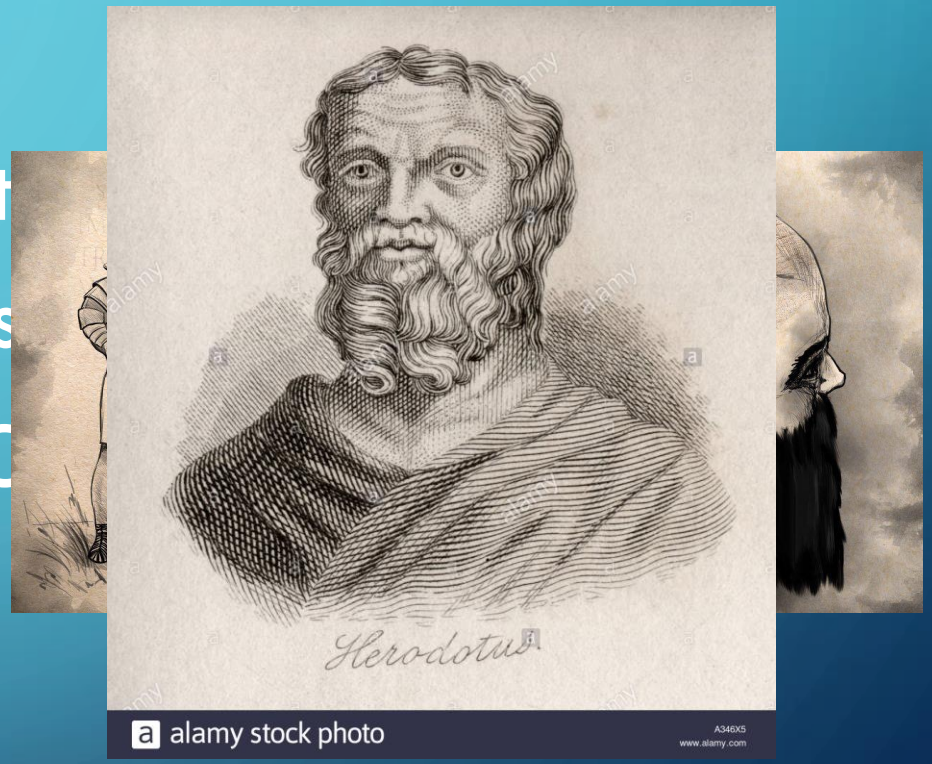


Histiaeus Herodot

Revolution Histories

against the 440 A.C

Persians



PHYSICAL STEGANOGRAPHY

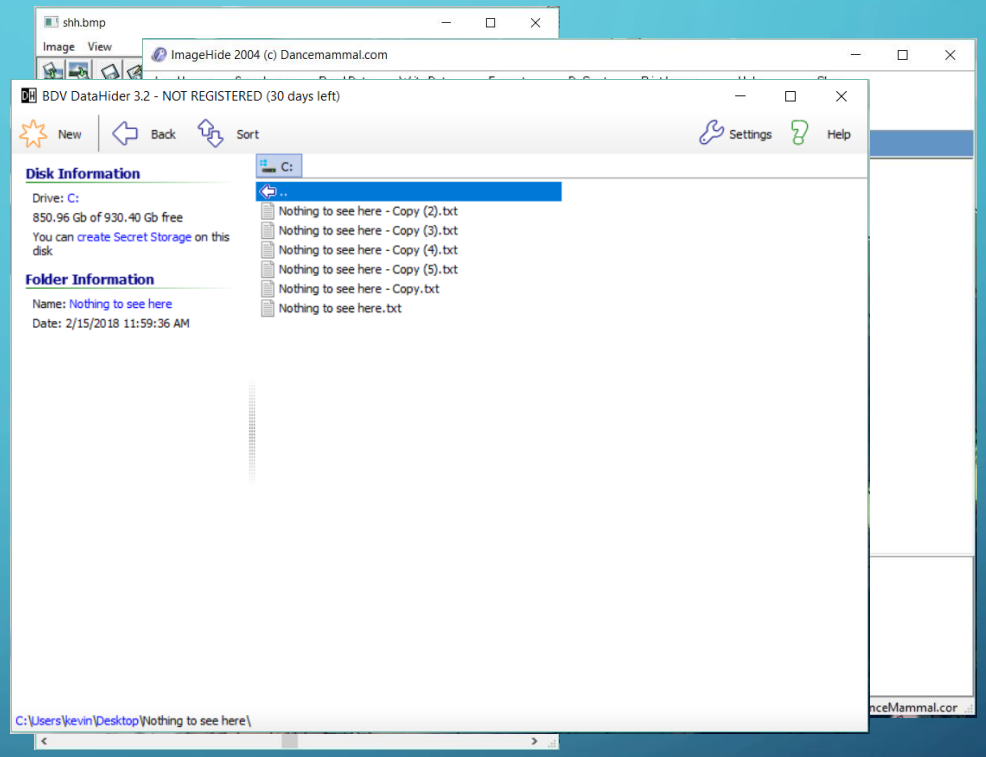
- Invisible Ink
  ISEC
- Message under a postage stamp
  InfoSecurity
- Knitting a message in on clothing
  Tour
- Blinking in Morse code
  2018

DIGITAL STEGANOGRAPHY

- 1975, Personal Computers
- 1985, Barrie Morgan and Mike Barney, Datotek, M2B2
- Steganography tools surfacing
  - Slow at first, followed by a rapid spike

CURRENT STEGANOGRAPHY TOOLS

- TOO MANY TO LIST!!!
- Here are a few:
  - ImageHide
  - Hide in Picture
  - BDV DataHider



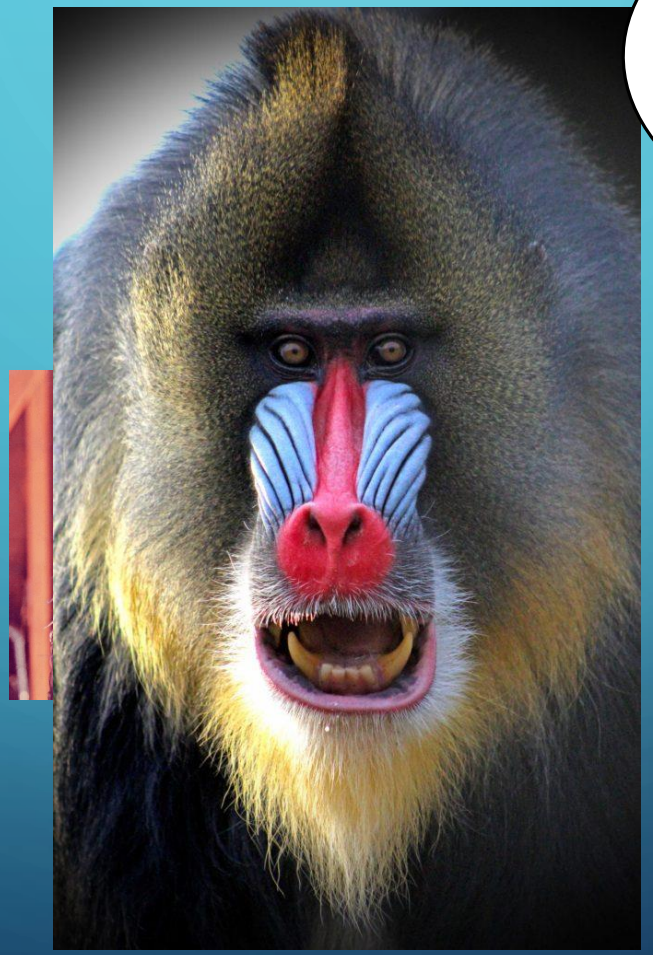
WHAT DO THEY DO?

- Hide stuff
  - Images, videos, audio files, documents, text
- Inside other stuff
  - Images, videos, audio files, documents, executables, folders

ENCRYPTION (WHY NOT?)

- Advanced Encryption Standard
- Data Encryption Standard
- Message Digest 5
- Secure Hashing Algorithm

IMAGE STEGANOGRAPHY



IS EVERYTHING FOR SHOW
FOR YOUR EYES ONLY

~~Steganography~~ Pic

Original Pic

DIGITAL WATERMARKING

- Visible Watermarking
  - A logo or text that denotes the owner
- Invisible Watermarking
  - Data embedded into file
    - Invisible and inaudible

STEGANOGRAPHY METHODS

LEAST SIGNIFICANT BIT (LSB)

Data to be hidden:

101101

10000010
01101101
10101000

DISCRETE COSINE TRANSFORM (DCT)

- Technique used to compress JPEG, MJPEG, MPEG

-23	-2	0	0	0	0	0	0
-21	4	2	0	0	0	0	0
6	1	0	0	0	0	0	0
1	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

STEGANALYSIS

- Stego-Only attacks – Stego object available
- Known Cover Attack – Original and Carrier available
- Chosen Stego Attack – Programs used, patterns compared
- Known Stego Attack – Everything is available

HOW TO DETECT?

- EnCase, Guidance Software Inc.
- Ilook Investigator
- StegDetect
- Forensic Toolkit, AccessData

NETWORK STEGANOGRAPHY

- Coined in 2003, Krzysztof Szczypiorski
- Communication Protocols
  - Protocol Logic Manipulation
- Deliberate Packet Delays
- Much harder to detect!

CRYPTOGRAPHY V.S. STEGANOGRAPHY

- Known message passing
- Common technology
- Most algorithms known to governments
- Current algorithms resistant to BFA, but strength reduces while technology increases

- Unknown message passing
- Little Known Technology
- Technology still being developed for certain formats
- Once detected message is known

WHY IS THIS SCARY?

- Mostly used maliciously:
  - Terrorism
  - Hide stolen data
  - Hide illegal videos/images
- Research and Development must go on!

CONCLUSION

- Still being investigated
- Difficult to notice
- Can hide large amounts of data
- Various types of uses, including commercial

REFERENCES

- Funds for foreign cryptology support, 10 USC §412
- Richer, P. (2003). *Steganalysis: Detecting hidden information with computer forensic analysis* (Tech.). Retrieved February 9, 2018, from SANS Institute InfoSec Reading Room website: https://www.sans.org/reading-room/whitepapers/stenganography/steganalysis-detecting-hidden-information-computer-forensic-analysis-1014
- Software, G. (n.d.). EnCase® Forensic. Retrieved February 9, 2018, from https://www.guidancesoftware.com/encase-forensic
- U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes. (n.d.). Retrieved February 9, 2018, from http://www.ilook-forensics.org/

REFERENCES

- Forensic Toolkit. (n.d.). Retrieved February 2, 2018, from https://accessdata.com/products-services/forensic-toolkit-ftk
- Rout, H., & Mishra, B. K. (2014, December). *Pros and Cons of Cryptography, Steganography and Perturbation techniques* (Tech.). Retrieved February 7, 2018, from Research Gate website: https://www.researchgate.net/publication/286092142_Pros_and_Cons_of_Cryptography_Steganography_and_Perturbation_techniques
- Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (n.d.). *Information Hiding—A Survey* (Tech.). Retrieved February 2, 2018, from IEEE website: http://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract award #1563978.

UNIVERSIDAD POLITÉCNICA PUERTO RICO