Mason Competitive Cyber

Steganography

News since last meeting

- Firefox Quantum
- 19/50 states have cyber insurance
- Amazon Echo vulnerable to BlueBorne
  - Bluetooth vuln disclosed in September
- Popular wordpress plugin vulnerable
  - Formidable Forms
    - Blind SQL injection
    - Reflected & Stored XSS

Upcoming CTFs & Events

- Hack the Box
  - Now (advanced room)
  - Online
  - Attack

- RC3 CTF 2017
  - Nov 17 9pm - Nov 19 11:59pm
  - Online
  - Jeopardy style

Steganography

- Steganography = hiding messages in a way that nobody would suspect there is a hidden message
  - Different from cryptography

- 90% of the time in CTFs they will be images
  - Lower layers
  - Shift colors of image
  - Two files concatenated together
  - Message hidden in pixels

- Can be own category or be in Forensics or Cryptography

Steganography

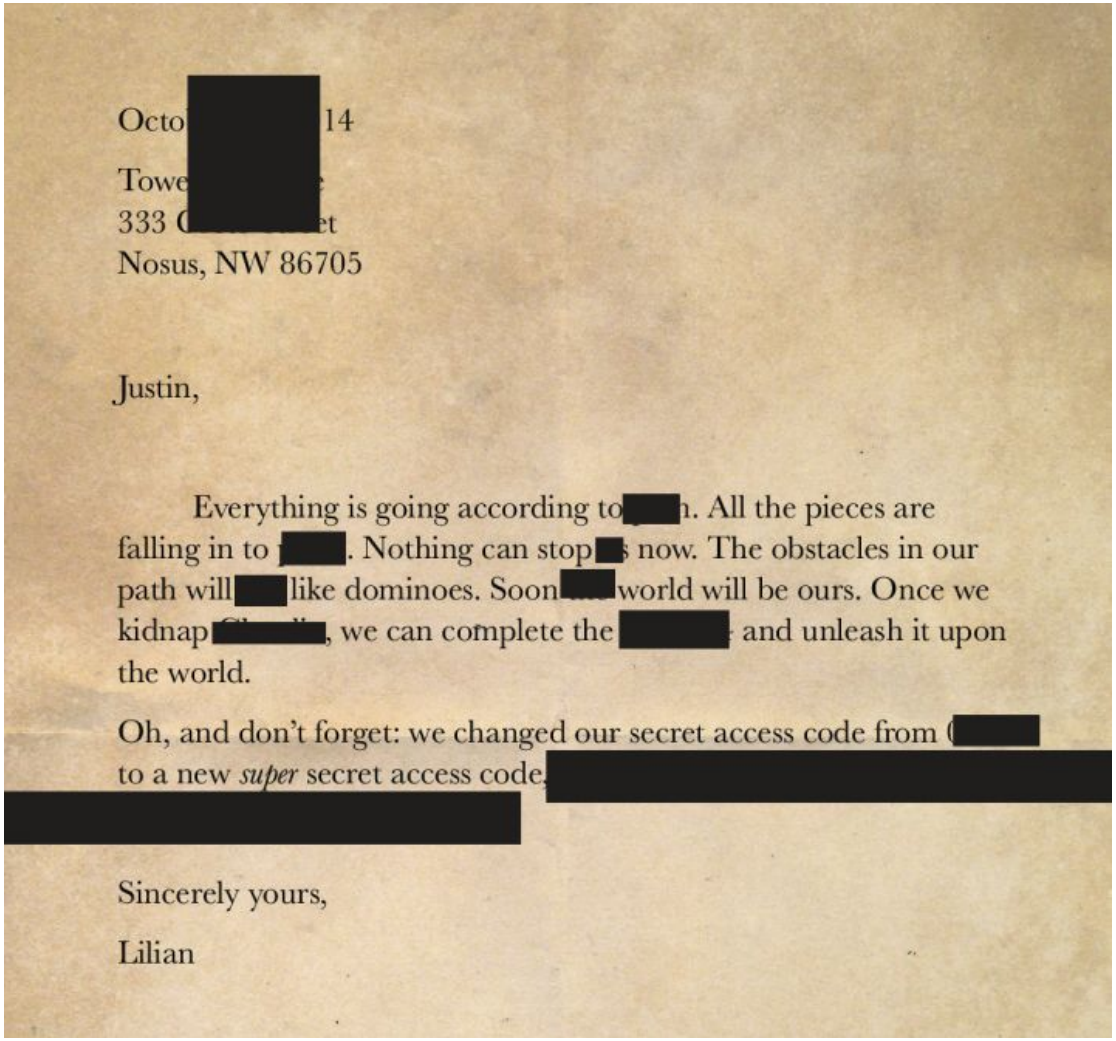
- Steganography = hiding messages in a way that nobody would suspect there is a hidden message
  - Different from cryptography

- 90% of the time in CTFs they will be images
  - Lower layers
  - Shift colors of image
  - Two files concatenated together
  - Message hidden in pixels

- Can be own category or be in Forensics or Cryptography

Layers

- Adobe Illustrator
- GIMP
- Photoshop



Octo[redacted]14

Towe[redacted]
333 C[redacted]et
Nosus, NW 86705

Justin,

Everything is going according to [redacted]n. All the pieces are falling in to [redacted]. Nothing can stop [redacted]s now. The obstacles in our path will [redacted] like dominoes. Soon [redacted] world will be ours. Once we kidnap [redacted], we can complete the [redacted] and unleash it upon the world.

Oh, and don't forget: we changed our secret access code from [redacted] to a new *super* secret access code[redacted]

Sincerely yours,

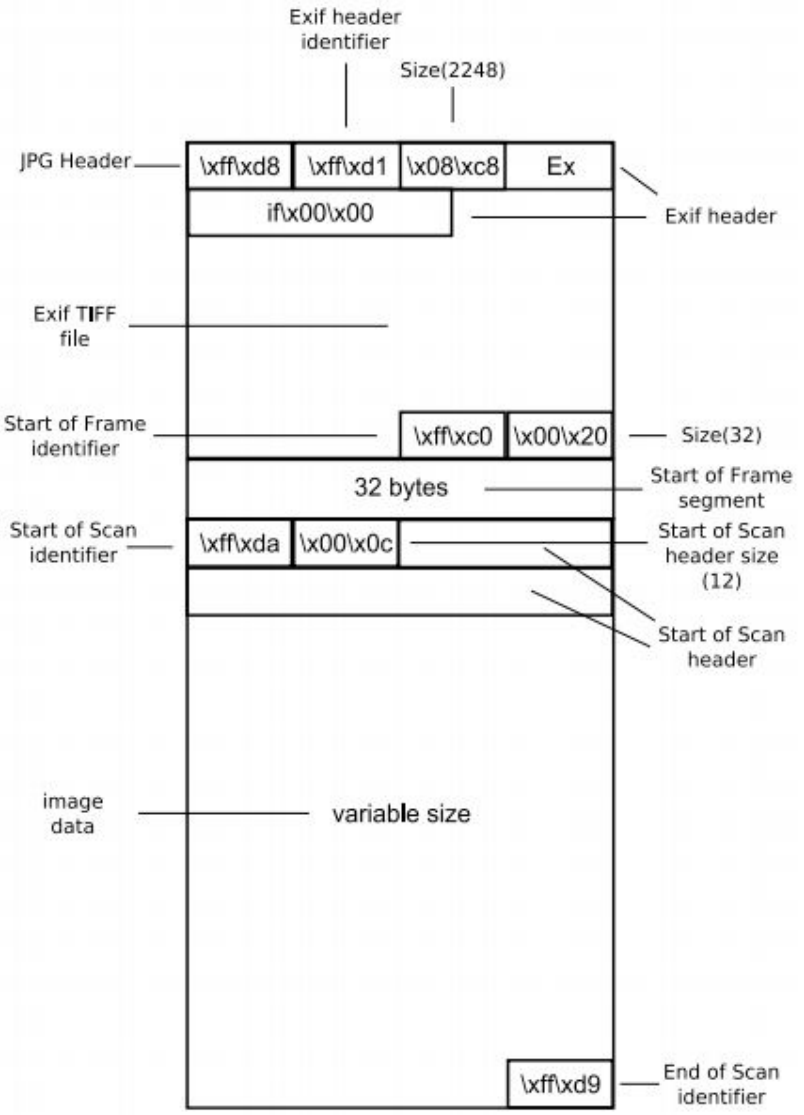
Lilian

Shift Colors of Image

- Use Stegsolve
  - Java app

JPEG Structure

- EXIF
  - Exchangeable Image File Format
  - Author
  - GPS Coordinates
- Header FFD8
- Footer FFD9
- Use tools to File Carve
  - Binwalk
  - Foremost



Two Files Concatenated Together

- If txt you can run strings

- If another file type (like compressed)
  - binwalk -e
  - foremost
  - Rename to .zip and unzip normally

Message Hidden In Pixels

- Least Significant Bit (LSB) Steganography
- Images made of of pixels
  - Each pixel is represented as 3 bytes (0-255)
    - RGB value
    - 00000001 0000001 0000001
- Can hide data in image by changing least significant bit of each byte
    - 11111111 00000000 00000001 → red
    - Hide the message 001 above pixel
    - 1111111**0** 0000000**0** 0000000**1** -> still red

Message Hidden In Pixels

- Use tools or python script to solve LSB steganography
  - For Python use Pillow
  - **OpenStego**
  - Stegsolve
  - Outguess

- Reverse Image search
  - compare with XOR
    - Stegsolve

RC3 CTF 2016

- RC3 CTF 2016 Steganography challenge

Audio Steganography

- Listen to it
  - Maybe it's a cipher or code
- Look at ID3
  - metadata (like EXIF for audio)
- Do Spectrum Analysis of frequency
  - Audacity

Video Steganography

- Similar to GIF Steganography
  - Use ffmpeg or OS X Preview to view frames
- Use Audio Steganography solving techniques

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™