Mason Competitive Cyber

Meeting 4: File Carving

Upcoming Events

- iCTF
  - Today 12PM-8PM for academic league
  - 24 hours for public league (can be in both)
- Spring Break- No meeting March 17th
- 0CTF Qualification Round
  - Saturday, March 18th
- Harris Corp visiting us
  - Friday, March 24
  - John deGruyter talking about internships and vulnerability research
  - Food

News

- AWS down for hours on Tuesday
  - Engineer was running command to take down a few servers
  - Ran wrong command
  - Basically took them all down
- Google disclosed unpatched IE and Edge vuln
  - Exceeded 90 days without patch
- Yahoo discovers 3rd data breach in last 6 months
  - Forged cookies
  - 32 million accounts affected
  - CEO Marissa Mayer not receiving bonus
  - Top lawyer resigns

News

- Net Neutrality getting shit on
  - Net Neutrality = same Internet speeds to all websites + access to all websites
  - Trump Admin trying to remove unnecessary regulations from small companies
  - Problem → big ISPs own many smaller companies

What is File Carving?

- File Carving- “reassembling files from fragments in the absence of filesystem metadata”
- Extracting structured data (files) out of raw data, based on format specific characteristics present in the structured data

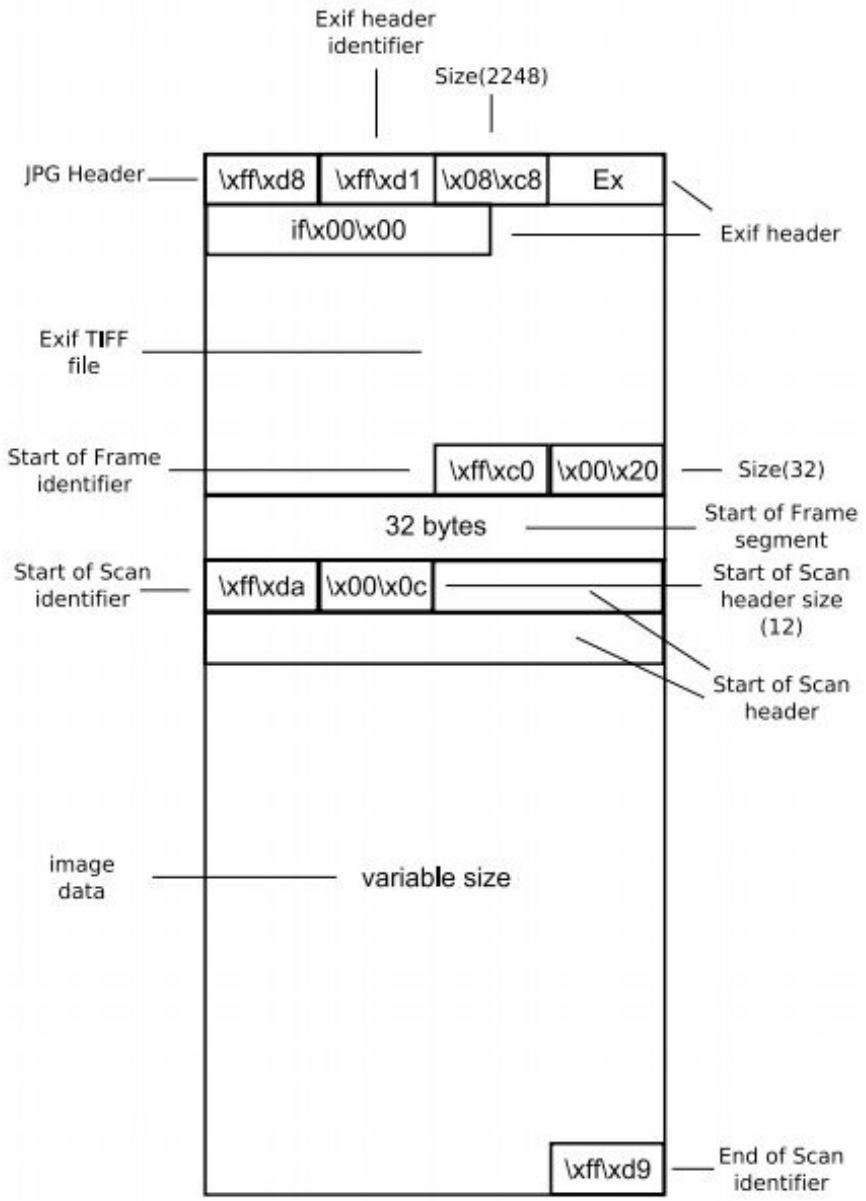
- File Carving Uses:
  - Recovering deleted files
  - Fixing corrupted files
  - Steganography

File Carving without tools

- Use a Hex Editor
  - Notepad++ extension
  - Hex Editor (windows)
  - iHex (OSX)
  - Bless (Ubuntu)
  - xxd (command for OSX and linux)
- Find header and footer
  - JPEG header = FFD8
  - JPEG footer = FFD9
- Fix corrupted headers/trailers
- Look for appended data

JPEG File Structure

- EXIF
  - Exchangeable Image Format
  - Camera settings and shit
  - IF GPS → geotags → $$$$
- Header FFD8
- Footer FFD9



File Carving without tools

- Not all file formats have a default footer
- If no footer, use maximum file size
  - Notepad++ extension
  - Hex Editor (windows)
  - iHex (OSX)
  - xxd (command for OSX and linux)

File Carving

- 2 types of File carving (structure, content)
- Structure
  - Header/footer
  - Identifier strings
  - Max size
- Structure Tools
  - Foremost
  - Scalpel
  - File Finder (part of EnCase)
  - PhotoRec

File Carving

- Content
  - HTML or XML
  - Character count
  - Informational Entropy
    - Uncertainty in how much information is in file
    - Average amount of information in file types

Installing Tools

- Download
- Read readme
- make
- make install

Challenges

- go.gmu.edu/carve