Mason Competitive Cyber

Forensics

News since last meeting

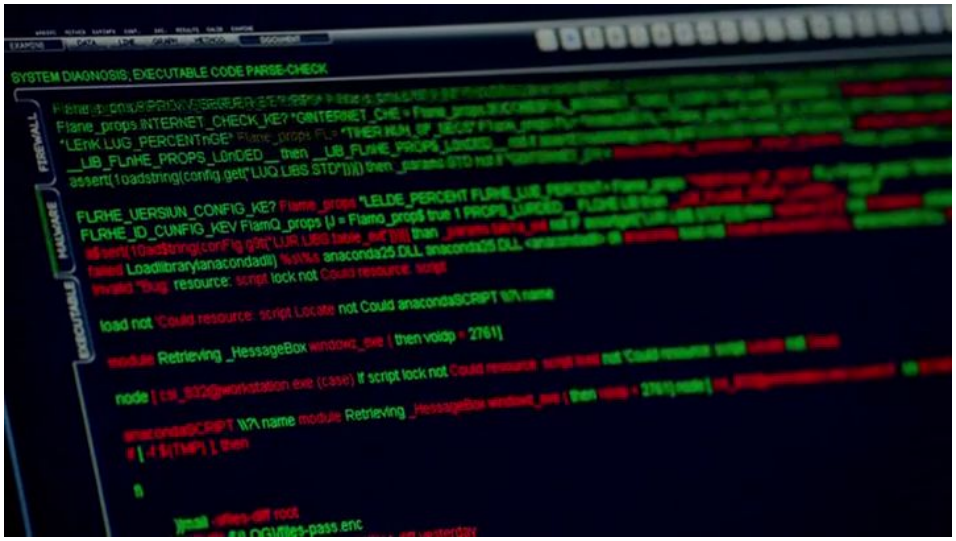
- Bad Rabbit ransomware
  - Affecting Russia & Ukraine
  - Pretends to be Adobe Flash installer
    - doesn’t use EternalBlue

Upcoming CTFs & Events

- HITCON CTF Quals
  - November 3rd 10pm - November 5th 10pm
  - Online
  - Finals in Taiwan

Forensics in the real world

- DFIR = Digital Forensics Incident Response
- Data Recovery
- Law Enforcement
- Expert Witness
- Incident Response
  - SOC
  - CERT



Host Based Forensics

- Can’t modify evidence if want it to be used in court
  - write blocker
  - make image

- $MFT
  - List of all files and their metadata
- Event Logs
  - RDP
- Browser history
- Shimcache
  - track compatibility issues with executed programs
  - list of exe’s and dll’s run (or browsed to)

- Parsers

Forensics in CTFs

- Solvable with strings
  - Not really forensics

- Network forensics
- Steganography

- “Broken” file formats
- Disk or VM images
  - needle in haystack

Strings

- Outputs printable characters in file
  - Simple reverse engineering challenges
  - pcap files

```
sharknado ❯ strings file.pcap | grep -i flag
```

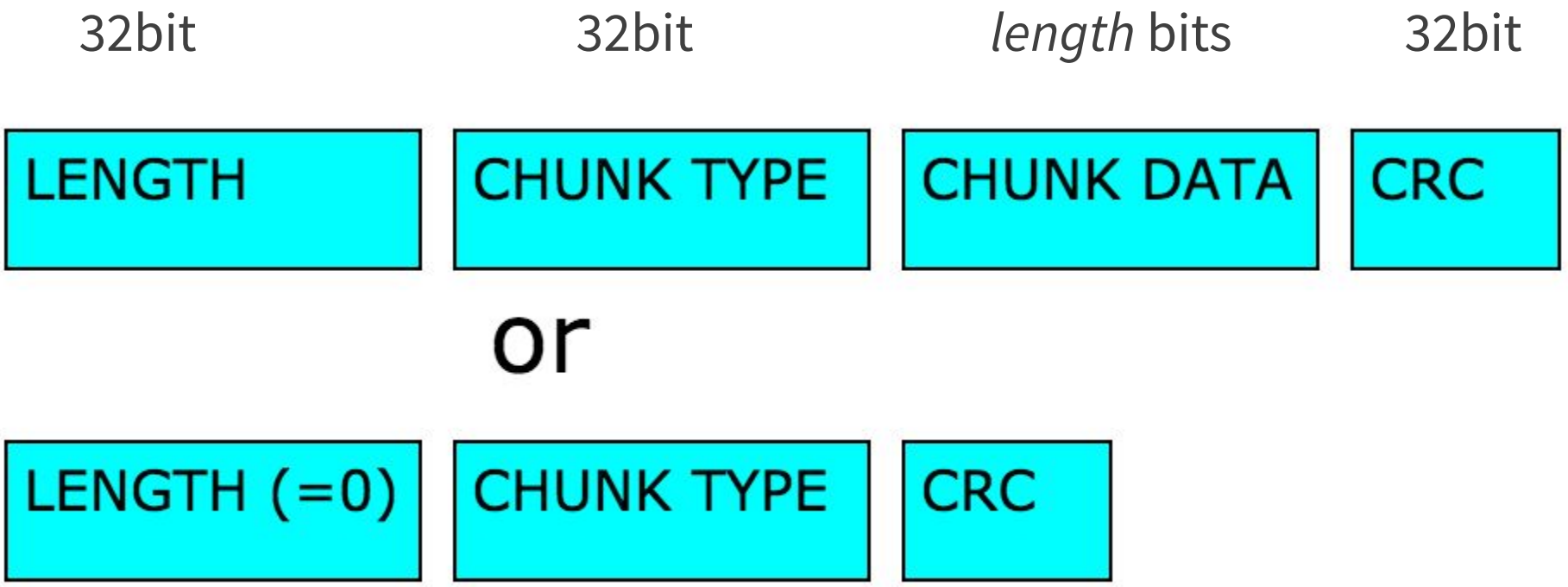
EXIF data

- Exchangeable Image File format
- Metadata about photo
  - Size
  - **Author**
  - Timestamp
  - **Geotags**
  - Encoding
  - Resolution

- Exiftool
- Online tools

Corrupted PNG

- PNG format
- Header
  - 8950 4e47 0d0a 1a0a “magic number”
  - .PNG



Corrupted PNG Solutions

- Actually jpeg
  - Revealed in exiftool or “file” command
  - change extension
- Missing/Corrupted Header
  - Look at working PNG
  - Add correct header with Hex editor
- Incorrect CRCs
  - PNGCSum

Practical Challenges

- go.gmu.edu/tctf or 52.205.150.185:8000
  - MasonCC's training CTF
  - make a team if you don't have one
  - added forensics and trivia categories

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™