# Mason Competitive Cyber

## Host Based Forensics

# News since last meeting

- Fedex exposed user information from AWS S3 Bucket
  - Left public
  - Scanned documents (passports, DLs, etc.)
- US Department of Energy creates Cybersecurity Office
- AMSI null character vuln patched
  - ASMI = Anti-Malware Secure Interface
  - Truncates files after null character

# Upcoming Competitions & Events

- CyberFusion
  - Friday/Saturday
  - In-person @ VMI
  - Registration locked
- BSides NoVA CTF
  - Saturday
  - Herndon
  - Conference
- CryptoParty
  - March 3rd 10:30am-6pm
  - HUB

# LE Side

- Data Integrity & Chain of Custody
- Write Blockers, Air Gapped computers
- Encase/FTK/X-Ways

# Private Incident Response Side

- Less concern with data integrity & chain of custody
- Cyber Insurance
- PPI compliance
- Timelining

- Ransomware
- O365 compromise

# Windows

- $MFT
  - Created, Modified, Last Accessed
  - $STDINFO vs $FILENAME
- Shellbags
  - NTUSER.dat and USRCLASS.dat
  - Explorer viewing preferences

# Windows: File Download

- Browser History
  - Direct
  - Edge WebcacheV01.dat
  - FF downloads.sqlite
- Skype history
  - Chat sessions
  - Files transferred
- Shellbags
  - Open/Save MRU → files opened or saved in explorer

# Windows: Program Execution

- Shellbags
  - UserAssist → GUI programs launched from desktop
  - RunMRU → Start,Run
  - LastVisitedMRU → Executable used to open Open/Save MRU
- AppCompat
  - Check for potential application compatibility issues
  - Amcache.hve or Shimcache
  - ONLY written to when system is rebooted
- Prefetch
  - Preloads pages of commonly used applications

# Windows: File Use & Knowledge

- Shellbags
  - Open/Save MRU → files opened or saved in explorer
  - LastVisitedMRU → Executable used to open ^
  - RecentDocs → Last 150 opened
  - Folder → Recent folders opened
  - BagMRU → Folder and folder settings

- Jump Lists
- LNK Files
  - Shortcut files
  - Many Timestamps
- Prefetch

# Windows: Event Logs

- EVT vs EVTX
- Event IDs may differ based on windows version
- Useful logs
  - Security
  - Terminal Services

- Event messages not stored in raw event logs

# Windows: Autoruns

- Make CSV
- Filter by test on signature column to find unverified
- Search hashes of suspicious ones on VT

# Forensics tools

- Encase/FTK/X-way
- Log2timeline
- Volatility
- Regripper

- Parsers

# Linux

- /var/log
- .bash_history for each user
- Application logs
  - Logmein

- Process tree
- List of open files and network connections
  - lsof -i -n -P

# OSX

- Changes Based on Version
  - Apple: “Upgrade or be left to die”
- Linux Crossover
  - /var/log/
  - .bash_history
- Knock Knock
  - Detects persistence mechanisms
  - Lists things set to autostart, looks up on VT
- Non app store downloads
  - ~/Library/Preferences/com.apple.LaunchServices.QuarantineEvents

# OSX

- iMessage chat logs
  - Users/<username>/Library/Messages/chat.db
  - Think your partner is cheating? Use this one weird trick to find out!  (don't actually)

```
sqlite> .tables
_SqliteDatabaseProperties   deleted_messages
attachment                  handle
chat                        message
chat_handle_join            message_attachment_join
chat_message_join
sqlite>
```

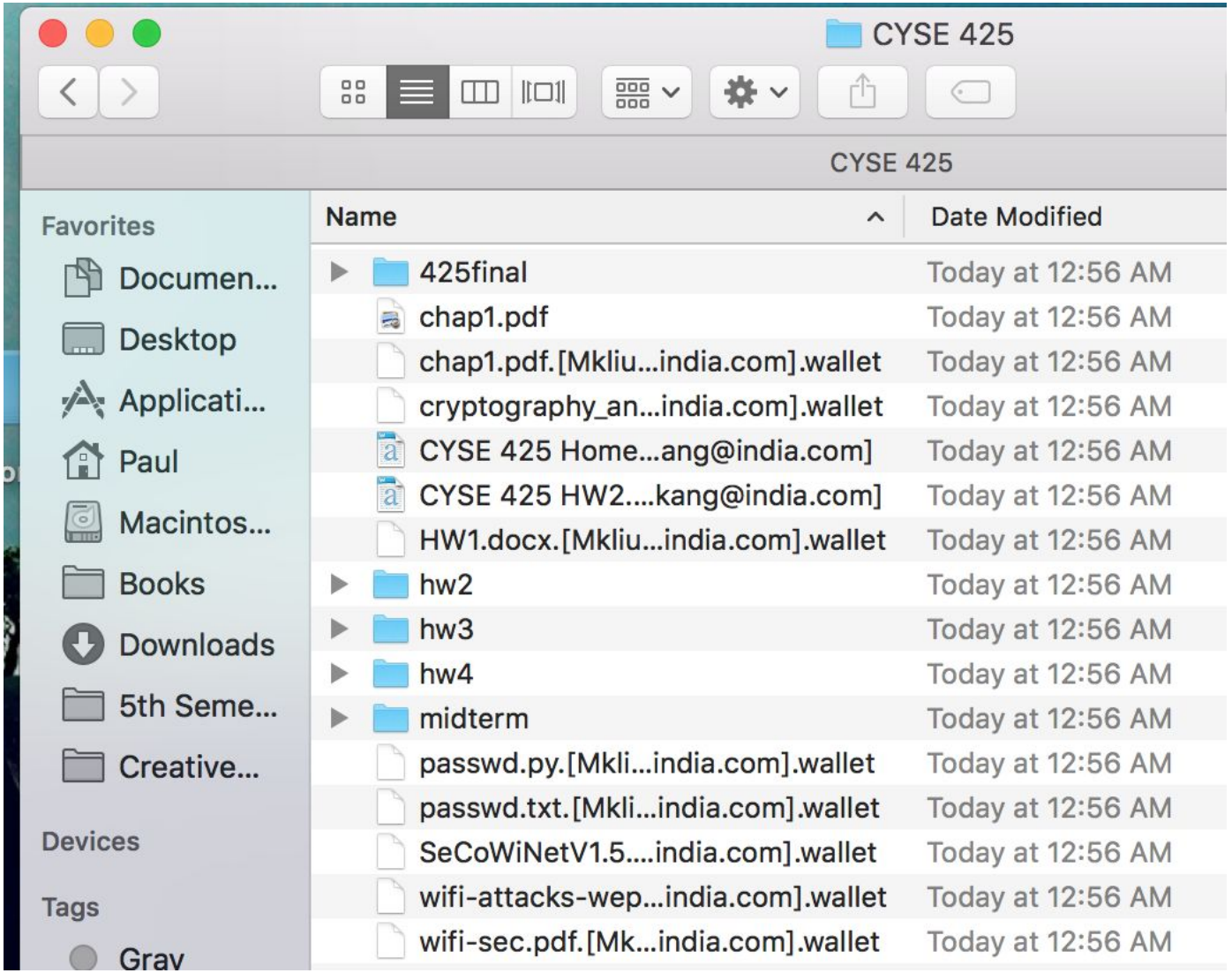
# Scenario

- tctf.competitivecyber.club

The Office

| ASAP as Possible | I am dead inside | Dwight U Ignorant Slut | Makin That Paper |
|---|---|---|---|
| 150 | 175 | 300 | 350 |

# Don’t be me


CYSE 425
CYSE 425
Favorites
Documen...
Desktop
Applicati...
Paul
Macintos...
Books
Downloads
5th Seme...
Creative...
Devices
Tags
Gray
Name
Date Modified
425final
Today at 12:56 AM
chap1.pdf
Today at 12:56 AM
chap1.pdf.[Mkliu...india.com].wallet
Today at 12:56 AM
cryptography_an...india.com].wallet
Today at 12:56 AM
CYSE 425 Home...ang@india.com]
Today at 12:56 AM
CYSE 425 HW2....kang@india.com]
Today at 12:56 AM
HW1.docx.[Mkliu...india.com].wallet
Today at 12:56 AM
hw2
Today at 12:56 AM
hw3
Today at 12:56 AM
hw4
Today at 12:56 AM
midterm
Today at 12:56 AM
passwd.py.[Mkli...india.com].wallet
Today at 12:56 AM
passwd.txt.[Mkli...india.com].wallet
Today at 12:56 AM
SeCoWiNetV1.5....india.com].wallet
Today at 12:56 AM
wifi-attacks-wep...india.com].wallet
Today at 12:56 AM
wifi-sec.pdf.[Mk...india.com].wallet
Today at 12:56 AM

# Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™