Mason Competitive Cyber

Host Based Forensics

Upcoming Competitions & Events

- Angstrom CTF
  - online April 19-26
  - #angstormctf

General Process

Scope → Collect Data → Process Data → Analysis → Report

- Don’t forget to scope!
- Different collection philosophies
  - On-site vs. Remote
  - Imaging vs. Live Response
- Analysis
  - Timelining
- Sometimes legal action

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
- PCI compliance
- Timelining

- Ransomware
- Business Email Compromise

Windows: Quick Wins

- Terminal Services Event Log
  - RDP
  - Time
  - IP Geolocation
- Autoruns
- Shimcache
  - Evidence of execution
- Amcache
  - Own registry hive
  - Shimcache with hashes

Windows: Important Artifacts

- $MFT
  - Created, Modified, Last Accessed
  - $STDINFO vs $FILENAME
- Memory
  - RAM
  - Fileless malware
  - Collecting is tricky for LR

Windows: File Download

- Browser History
  - Direct
  - Edge WebcacheV01.dat
  - FF downloads.sqlite
- Skype history
  - Chat sessions
  - Files transferred
- Shellbags
  - USRCLASS.dat
  - Explorer viewing preferences
- MRU keys

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
  - Watch out for DLL Injection
- Search hashes of suspicious ones on VT

Forensics tools

- Scoping
- Collection
  - FTK Imager
  - KAPE
  - Automactc
- Processing
  - Regripper
  - Encase/FTK/X-ways
  - Volatility
  - Log2timeline
- Analysis
  - SIEM
- Reporting

Linux

- /var/log
- .bash_history for each user
- Application logs
  - Probably some kind of server
  - Logmein

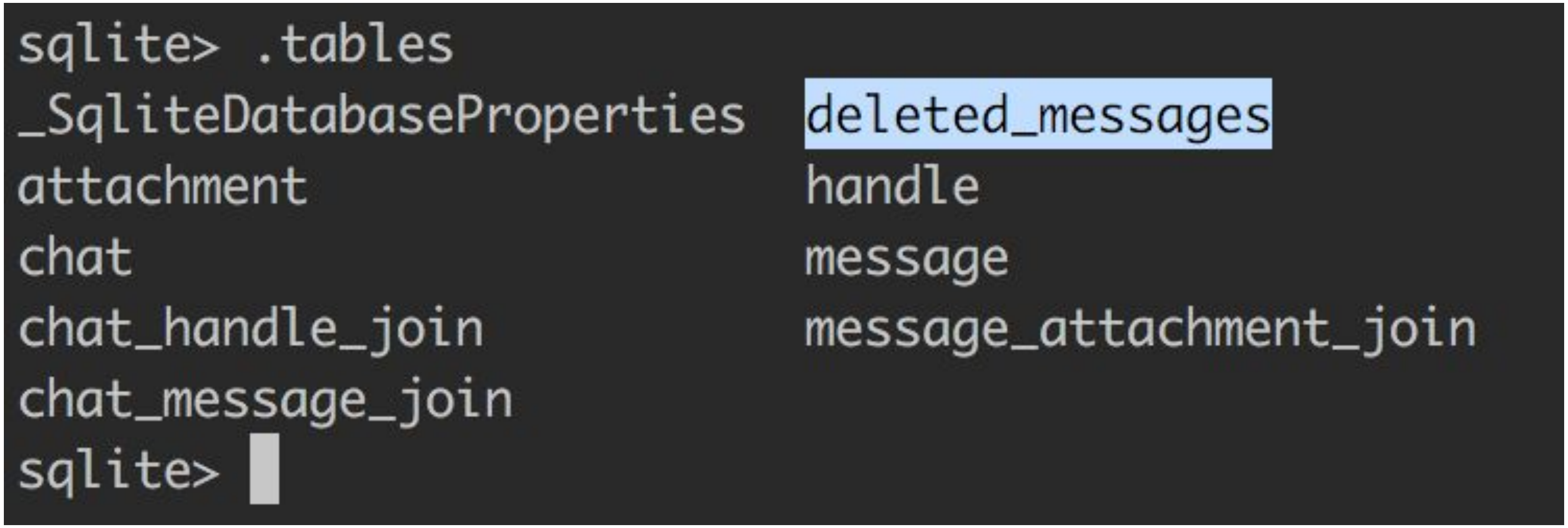
- Process tree
- List of open files and network connections
  - lsof -i -n -P

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

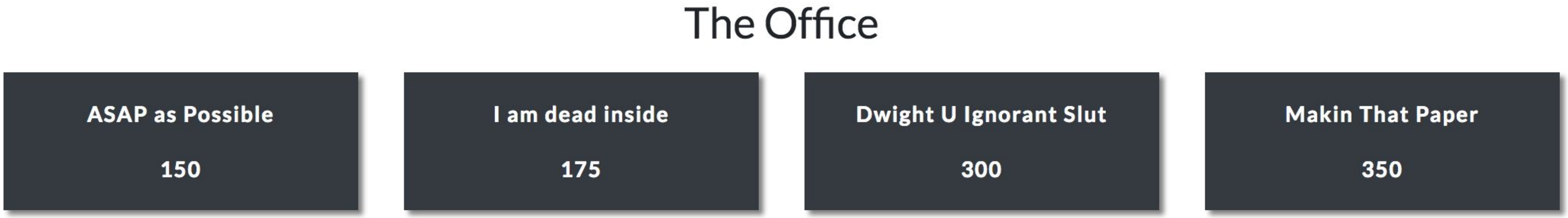
- iMessage chat logs
  - Users/<username>/Library/Messages/chat.db



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

Scenario

- tctf.competitivecyber.club



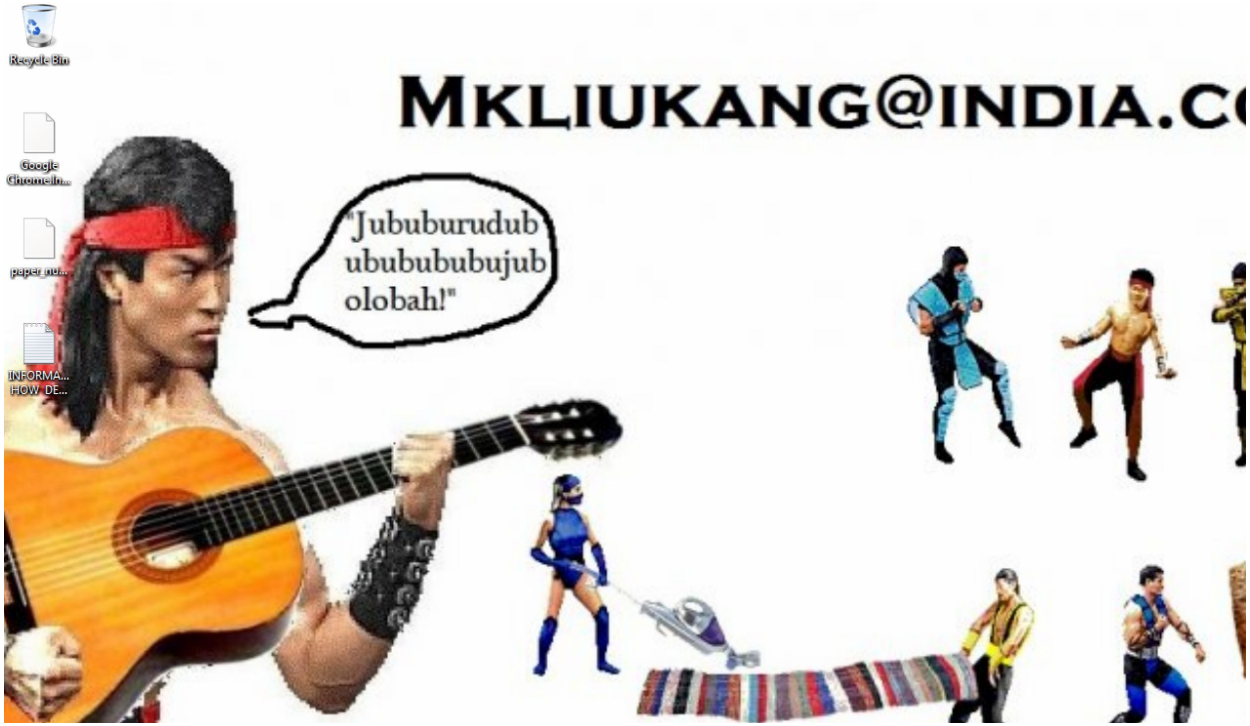
The Office

ASAP as Possible
150

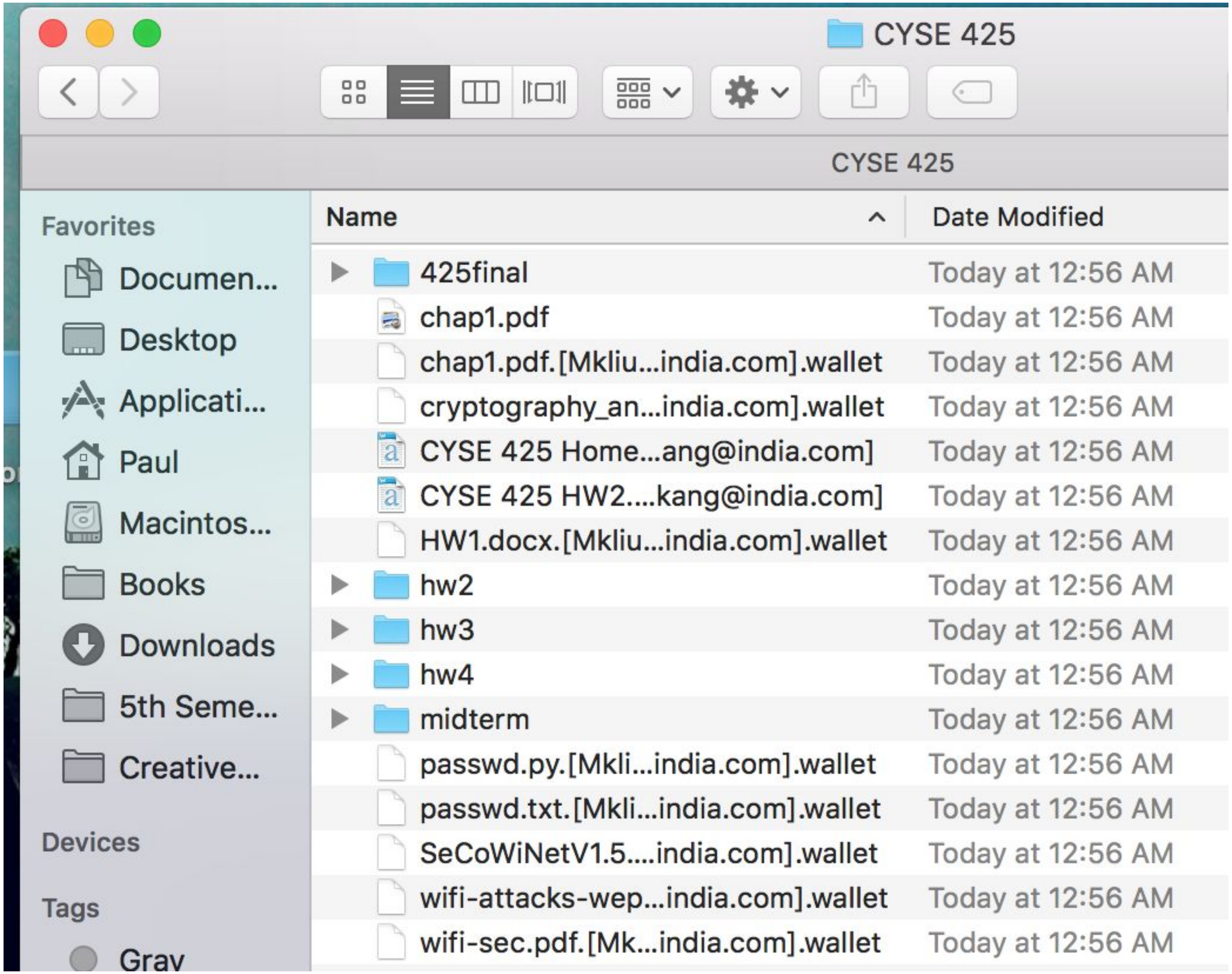
I am dead inside
175

Dwight U Ignorant Slut
300

Makin That Paper
350



Don’t be me



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