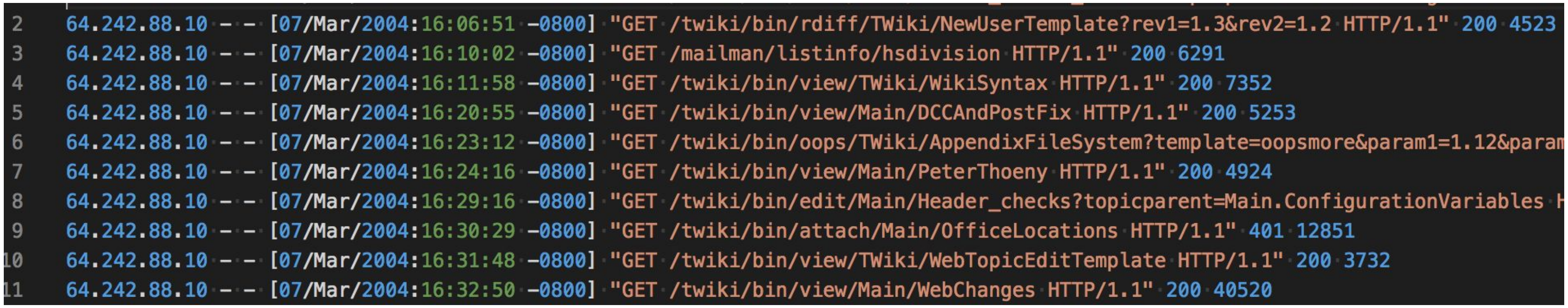
Mason Competitive Cyber

MacOS Security

Quick Problem

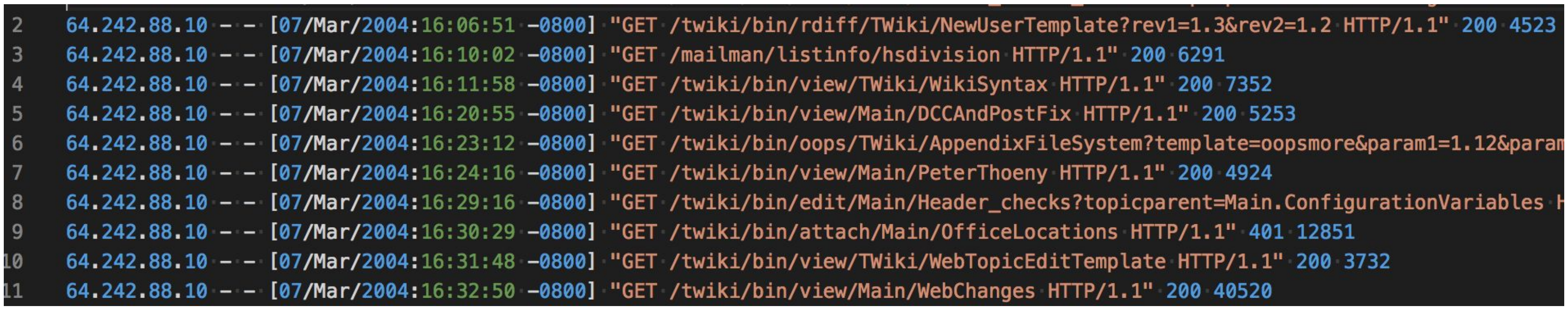
- Given an apache log, find 400 and 500 errors, upload those lines to a REST API



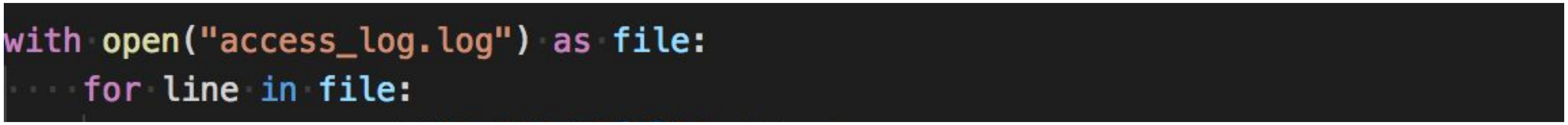
```
64.242.88.10 - - [07/Mar/2004:16:06:51 -0800] "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523
64.242.88.10 - - [07/Mar/2004:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291
64.242.88.10 - - [07/Mar/2004:16:11:58 -0800] "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352
64.242.88.10 - - [07/Mar/2004:16:20:55 -0800] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253
64.242.88.10 - - [07/Mar/2004:16:23:12 -0800] "GET /twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&param1=1.12&param
64.242.88.10 - - [07/Mar/2004:16:24:16 -0800] "GET /twiki/bin/view/Main/PeterThoeny HTTP/1.1" 200 4924
64.242.88.10 - - [07/Mar/2004:16:29:16 -0800] "GET /twiki/bin/edit/Main/Header_checks?topicparent=Main.ConfigurationVariables H
64.242.88.10 - - [07/Mar/2004:16:30:29 -0800] "GET /twiki/bin/attach/Main/OfficeLocations HTTP/1.1" 401 12851
64.242.88.10 - - [07/Mar/2004:16:31:48 -0800] "GET /twiki/bin/view/TWiki/WebTopicEditTemplate HTTP/1.1" 200 3732
64.242.88.10 - - [07/Mar/2004:16:32:50 -0800] "GET /twiki/bin/view/Main/WebChanges HTTP/1.1" 200 40520
```

Quick Problem

- Given an apache log, find 400 and 500 errors, upload those lines to a REST API



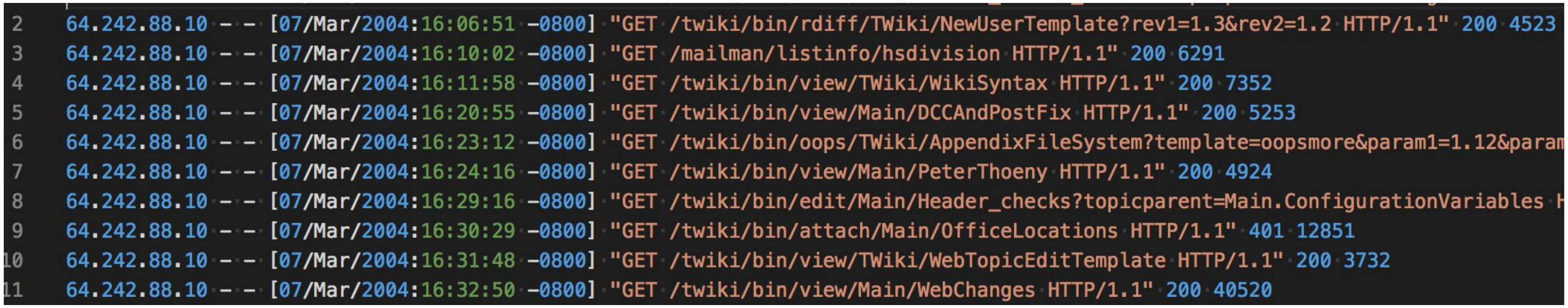
```
64.242.88.10 - - [07/Mar/2004:16:06:51 -0800] "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523
64.242.88.10 - - [07/Mar/2004:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291
64.242.88.10 - - [07/Mar/2004:16:11:58 -0800] "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352
64.242.88.10 - - [07/Mar/2004:16:20:55 -0800] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253
64.242.88.10 - - [07/Mar/2004:16:23:12 -0800] "GET /twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&param1=1.12&param
64.242.88.10 - - [07/Mar/2004:16:24:16 -0800] "GET /twiki/bin/view/Main/PeterThoeny HTTP/1.1" 200 4924
64.242.88.10 - - [07/Mar/2004:16:29:16 -0800] "GET /twiki/bin/edit/Main/Header_checks?topicparent=Main.ConfigurationVariables H
64.242.88.10 - - [07/Mar/2004:16:30:29 -0800] "GET /twiki/bin/attach/Main/OfficeLocations HTTP/1.1" 401 12851
64.242.88.10 - - [07/Mar/2004:16:31:48 -0800] "GET /twiki/bin/view/TWiki/WebTopicEditTemplate HTTP/1.1" 200 3732
64.242.88.10 - - [07/Mar/2004:16:32:50 -0800] "GET /twiki/bin/view/Main/WebChanges HTTP/1.1" 200 40520
```



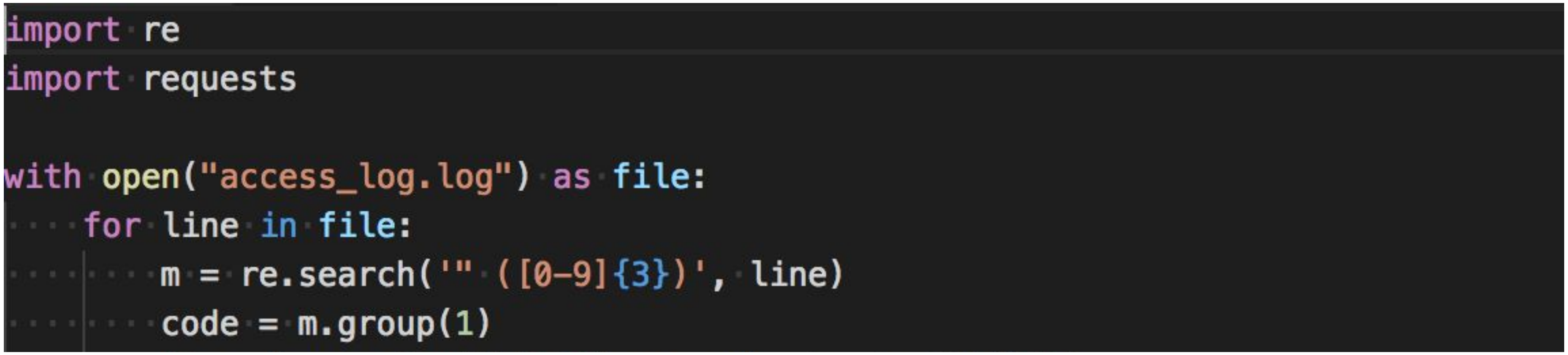
```python
with open("access_log.log") as file:
    for line in file:
```

Quick Problem

- Given an apache log, find 400 and 500 errors, upload those lines to a REST API



```
64.242.88.10 - - [07/Mar/2004:16:06:51 -0800] "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523
64.242.88.10 - - [07/Mar/2004:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291
64.242.88.10 - - [07/Mar/2004:16:11:58 -0800] "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352
64.242.88.10 - - [07/Mar/2004:16:20:55 -0800] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253
64.242.88.10 - - [07/Mar/2004:16:23:12 -0800] "GET /twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&param1=1.12&param
64.242.88.10 - - [07/Mar/2004:16:24:16 -0800] "GET /twiki/bin/view/Main/PeterThoeny HTTP/1.1" 200 4924
64.242.88.10 - - [07/Mar/2004:16:29:16 -0800] "GET /twiki/bin/edit/Main/Header_checks?topicparent=Main.ConfigurationVariables H
64.242.88.10 - - [07/Mar/2004:16:30:29 -0800] "GET /twiki/bin/attach/Main/OfficeLocations HTTP/1.1" 401 12851
64.242.88.10 - - [07/Mar/2004:16:31:48 -0800] "GET /twiki/bin/view/TWiki/WebTopicEditTemplate HTTP/1.1" 200 3732
64.242.88.10 - - [07/Mar/2004:16:32:50 -0800] "GET /twiki/bin/view/Main/WebChanges HTTP/1.1" 200 40520
```



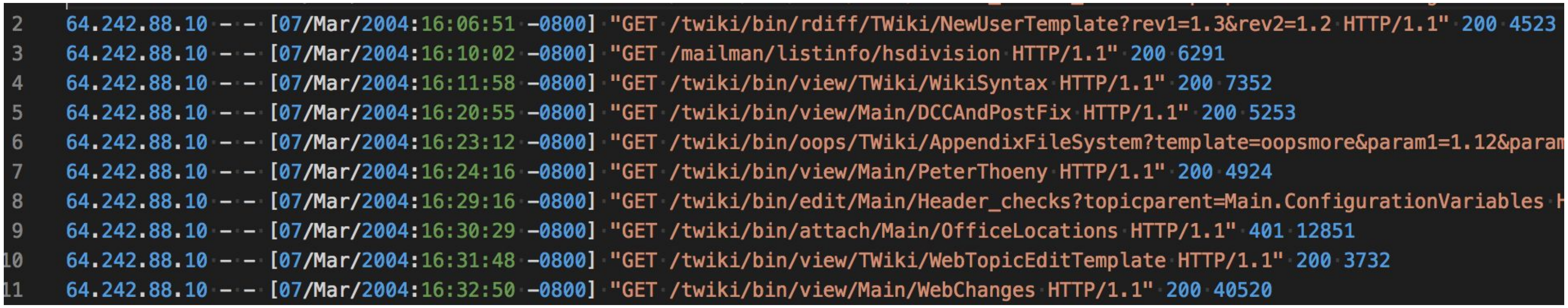
```python
import re
import requests

with open("access_log.log") as file:
    for line in file:
        m = re.search('" ([0-9]{3})', line)
        code = m.group(1)
```

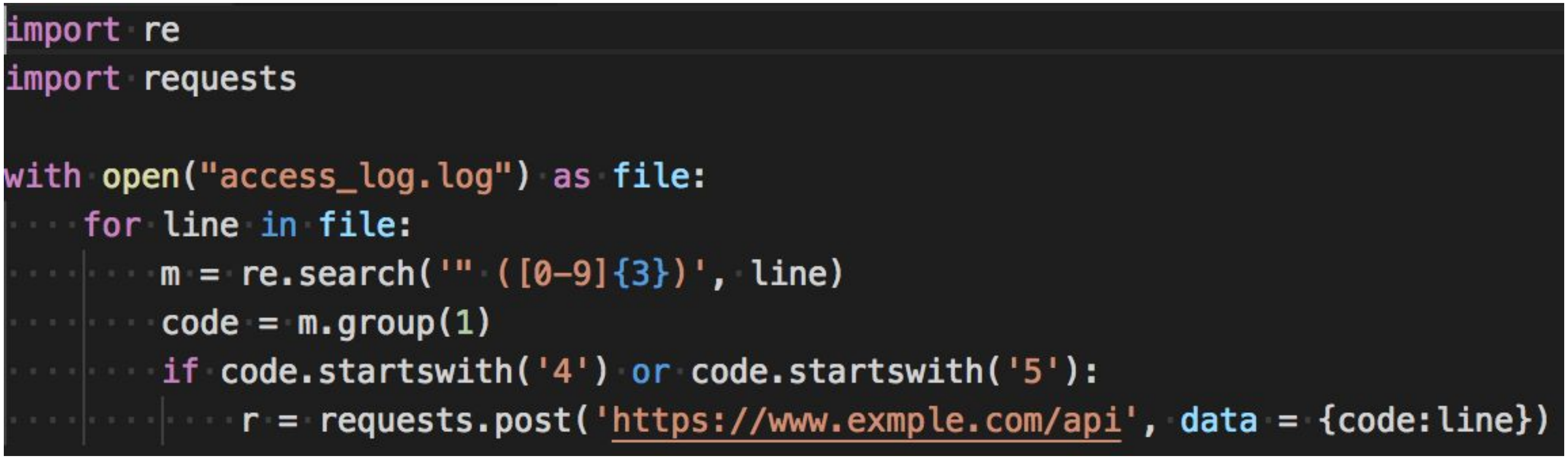
test on regexr.com

Quick Problem

- Given an apache log, find 400 and 500 errors, upload those lines to a REST API



```
64.242.88.10 - - [07/Mar/2004:16:06:51 -0800] "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523
64.242.88.10 - - [07/Mar/2004:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291
64.242.88.10 - - [07/Mar/2004:16:11:58 -0800] "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352
64.242.88.10 - - [07/Mar/2004:16:20:55 -0800] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253
64.242.88.10 - - [07/Mar/2004:16:23:12 -0800] "GET /twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&param1=1.12&param
64.242.88.10 - - [07/Mar/2004:16:24:16 -0800] "GET /twiki/bin/view/Main/PeterThoeny HTTP/1.1" 200 4924
64.242.88.10 - - [07/Mar/2004:16:29:16 -0800] "GET /twiki/bin/edit/Main/Header_checks?topicparent=Main.ConfigurationVariables H
64.242.88.10 - - [07/Mar/2004:16:30:29 -0800] "GET /twiki/bin/attach/Main/OfficeLocations HTTP/1.1" 401 12851
64.242.88.10 - - [07/Mar/2004:16:31:48 -0800] "GET /twiki/bin/view/TWiki/WebTopicEditTemplate HTTP/1.1" 200 3732
64.242.88.10 - - [07/Mar/2004:16:32:50 -0800] "GET /twiki/bin/view/Main/WebChanges HTTP/1.1" 200 40520
```



```python
import re
import requests

with open("access_log.log") as file:
    for line in file:
        m = re.search('" ([0-9]{3})', line)
        code = m.group(1)
        if code.startswith('4') or code.startswith('5'):
            r = requests.post('https://www.exmple.com/api', data = {code:line})
```

MacOS Overview

- Apple’s Operating System
- Closed-source
- Unix-based

- Mac OS X
  - Cheetah-Lion
- OSX
  - Mountain Lion-EL Capitan
- MacOS
  - Sierra-Mojave(current)

- HFS+ vs APFS

MacOS Security

System Hardening

MacOS Install

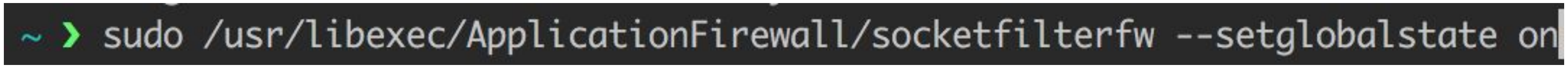
- Installation
  - Create custom image with AutoDMG
- Full disk encryption
  - FileVault
- MacOS and iOS are becoming more similar
  - Sends data to Apple on first boot and more
- Firmware Password
  - Booting from USB
  - Single-user mode
  - Recovery volume
  - Direct Memory Access (DMA) through thunderbolt
    - Use pcileech to read FIleVault passwords and inject kernel modules
    - Fixed as of early 2017

User Accounts

- First user you create has sudo access
  - Mitigate by have user for normal activity and admin user
- Put apps in ~/Applications instead of /Applications when possible
  - Mac App Store installs in /Applications
  - Issues
    - some system preferences & system utilities require root privileges
    - third party apps that require admin

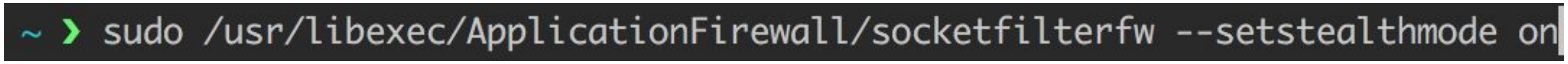
Firewall

- Default application layer firewall
  - Only can block incoming connections



```
~ ❯ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setglobalstate on
```

- Can set it to "stealth mode" which doesn't respond to:
  - ICMP requests
  - connection attempts from a closed TCP port

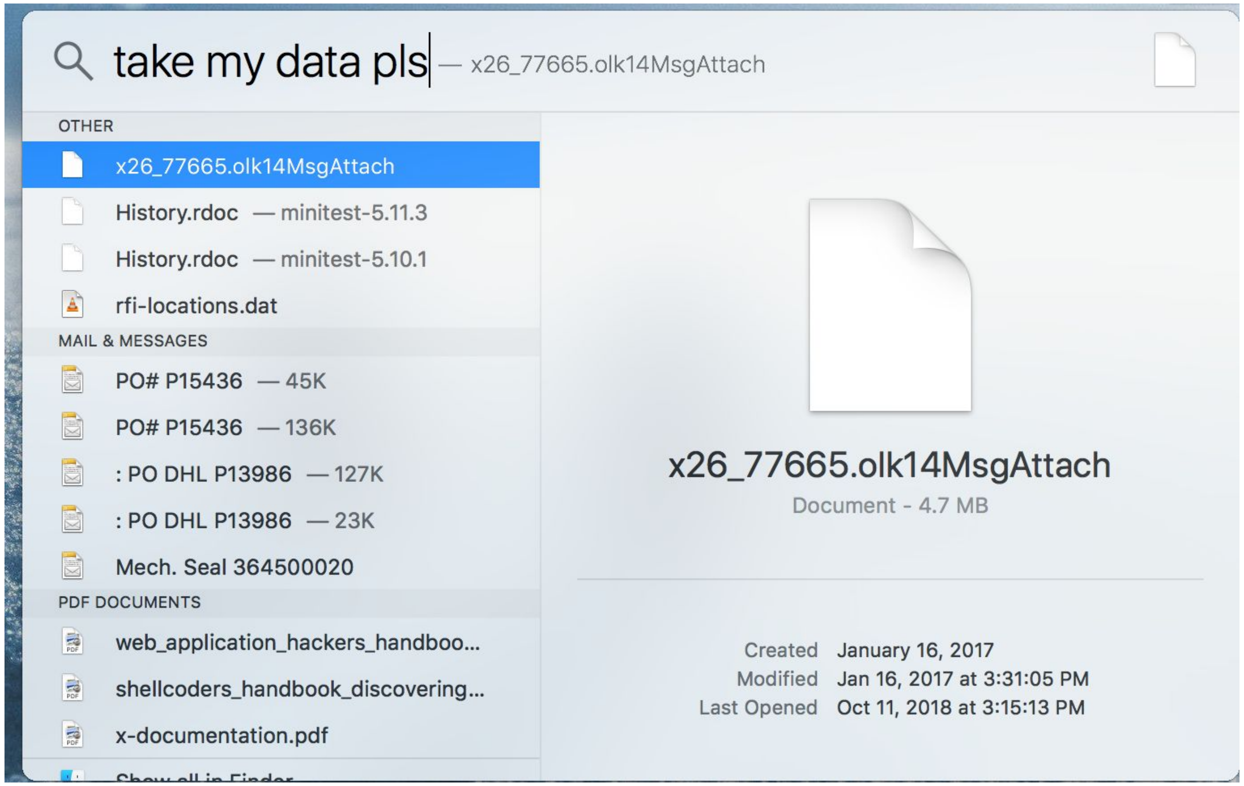


```
~ ❯ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setstealthmode on
```

- pfctl
  - Packet filtering that runs at kernel level
- Third Party Firewall
  - Little Snitch

Spotlight

- Spotlight suggestions
  - Queries sent to Apple
- Bing Web Searches
  - Queries sent to Microsoft



take my data pls — x26_77665.olk14MsgAttach

OTHER
- x26_77665.olk14MsgAttach
- History.rdoc — minitest-5.11.3
- History.rdoc — minitest-5.10.1
- rfi-locations.dat

MAIL & MESSAGES
- PO# P15436 — 45K
- PO# P15436 — 136K
- : PO DHL P13986 — 127K
- : PO DHL P13986 — 23K
- Mech. Seal 364500020

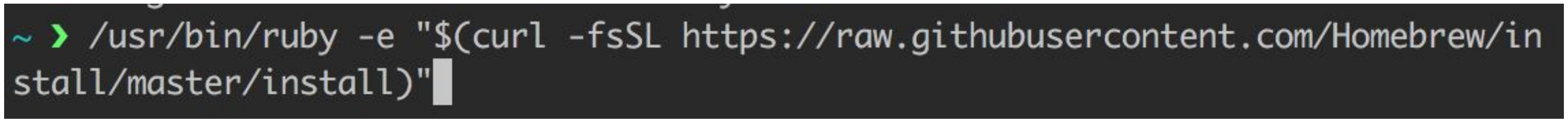
PDF DOCUMENTS
- web_application_hackers_handboo...
- shellcoders_handbook_discovering...
- x-documentation.pdf

x26_77665.olk14MsgAttach
Document - 4.7 MB

Created	January 16, 2017
Modified	Jan 16, 2017 at 3:31:05 PM
Last Opened	Oct 11, 2018 at 3:15:13 PM

Homebrew

- Package manager
- Make updates and installs of tools much easier



```
~ ❯ /usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/in
stall/master/install)"
```

Hosts File

- /etc/hosts
- Hacky approach
  - Block domains by associating them with an invalid IP
  - 0.0.0.0 example.com

Keychain

- MacOS comes with 200+ root authority certificates pre-installed
- In the unlikely event one a root CA was found to be compromised, you can distrust certificates through keychain

Malicious Binaries

- System Integrity Protection
- Binary whitelisting
  - santa
- Behavioral
  - Performance

MacOS Security

Incident Response

Basic Info

- Running processes
  - ps aux
- Loaded kernel extensions
  - kextstat -l
- Logged in users
  - who
- Mounted items
  - mount
- Memory
  - pmem
- Timestamps
  - ctime
  - mtime
  - atime

User Info

- Bash history
- LaunchAgents and LaunchDaemons
  - persistence
  - Knock Knock
- Crontab
- Recent Items
  - plist
    - property list
    - XML
- Finder
  - plist
- Shared File Lists
- System Quarantine Events
- User Quarantine Events

Network Info

- Network interface info
  - ifconfig
- Current network connections
  - netstat
- DNS info
  - scutil --dns
- ARP Table
  - arp -an

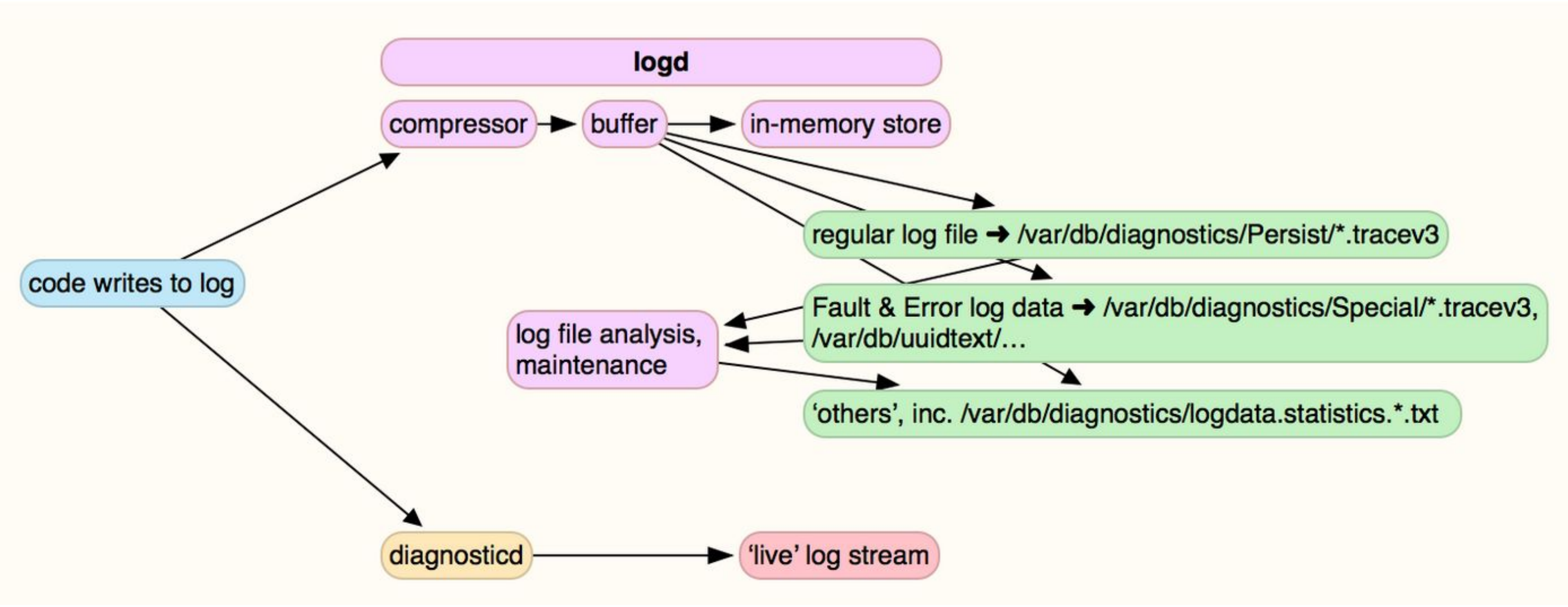
- Hosts file
- Bluetooth
  - /Library/Preferences/com.apple.bluetooth.plist

Normal Logs

- /Users/<username>/Library/Logs
- /var/log/
- /private/var/log/

Unified Logging

- Unified Logging
  - log collect
  - Console


logd
compressor
buffer
in-memory store
regular log file ➜ /var/db/diagnostics/Persist/*.tracev3
code writes to log
Fault & Error log data ➜ /var/db/diagnostics/Special/*.tracev3, /var/db/uuidtext/…
log file analysis, maintenance
'others', inc. /var/db/diagnostics/logdata.statistics.*.txt
diagnosticd
'live' log stream

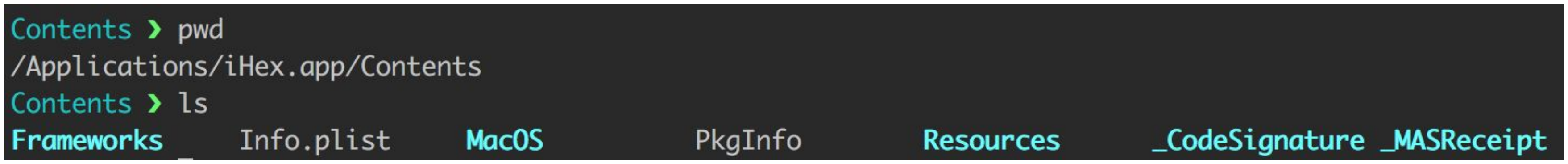
- .tracev3 = proprietary format

Unified Logging

- Log command
  - Log collect
  - Log stream
  - Log show

Misc. MacOS Stuff

- .command file
- caffeinate
- chat.db
- .app “files” are actually folders with a certain format



```
Contents ❯ pwd
/Applications/iHex.app/Contents
Contents ❯ ls
Frameworks      Info.plist      MacOS           PkgInfo         Resources       _CodeSignature _MASReceipt
```

OSXcollector

- https://github.com/Yelp/osxcollector
- Python script that helps do mac forensics
  - no dependencies
- Takes forever

Browser Objects

- Safari
  - /Users/<username>/Library/Caches/com.apple.Safari/WebpagePreviews/
- Use osxcollector to get rest of browser data
  - osxcollector.py -c -l -s chrome

Challenge

- Mac App Reverse Engineering
  - go.gmu.edu/macRE

Links

- https://github.com/google/santa
- https://github.com/google/grr
- https://github.com/yelp/osxcollector
- https://github.com/ufrisk/pcileech

- https://doi.org/10.6028/NIST.SP.800-179
- https://www.mac4n6.com

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™