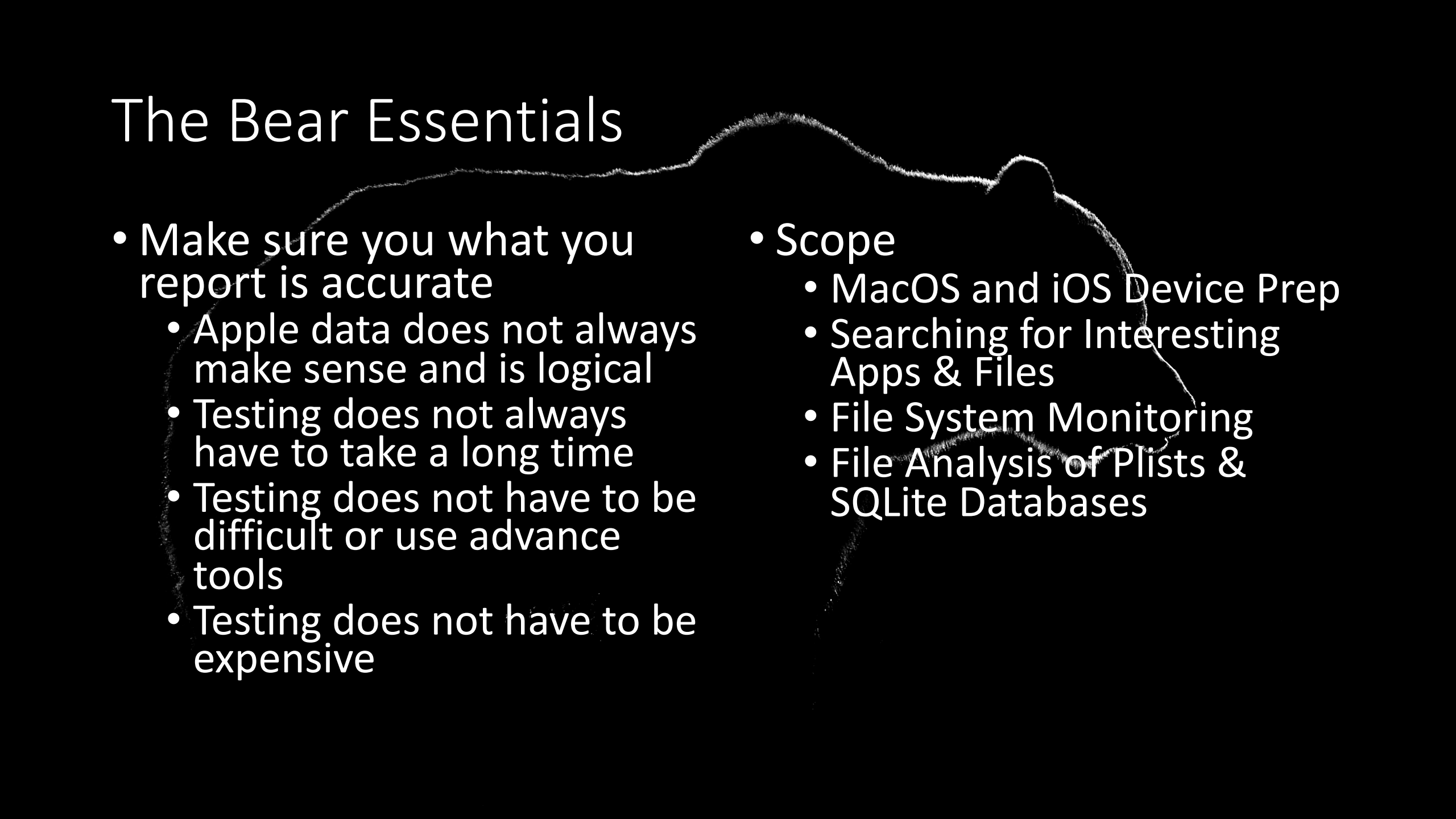
Poking the Bear

Teasing Out Apple's Secrets Through Dynamic Forensic Testing and Analysis

Sarah Edwards | @iamevltwin | mac4n6.com | for518.com

The Bear Essentials



- Make sure you what you report is accurate
  - Apple data does not always make sense and is logical
  - Testing does not always have to take a long time
  - Testing does not have to be difficult or use advance tools
  - Testing does not have to be expensive
- Scope
  - MacOS and iOS Device Prep
  - Searching for Interesting Apps & Files
  - File System Monitoring
  - File Analysis of Plists & SQLite Databases

macOS and iOS Device Prep

(iOS makes macOS seem easy peasy.)

MacOS Device Prep

- Live Machine or Virtual Machines
- Virtual Machines
  - VMWare Fusion
  - Parallels
  - VirtualBox
- Disable SIP (Recovery Mode –> csrutil disable)
- Create Clean Snapshots (VM or tmutil)
- “Clean” User Account
  - Create test accounts for apps too!
- Download binaries

```
Sarahs-Mac:~ oompa$ tmutil localsnapshot
Created local snapshot with date: 2019-10-09-210538
Sarahs-Mac:~ oompa$ tmutil listlocalsnapshots /
com.apple.TimeMachine.2019-10-09-210538
```

iOS Device Prep – Device Selection & Jailbreak

Pick a Jailbreak-able Device - www.theiphonewiki.com/wiki/

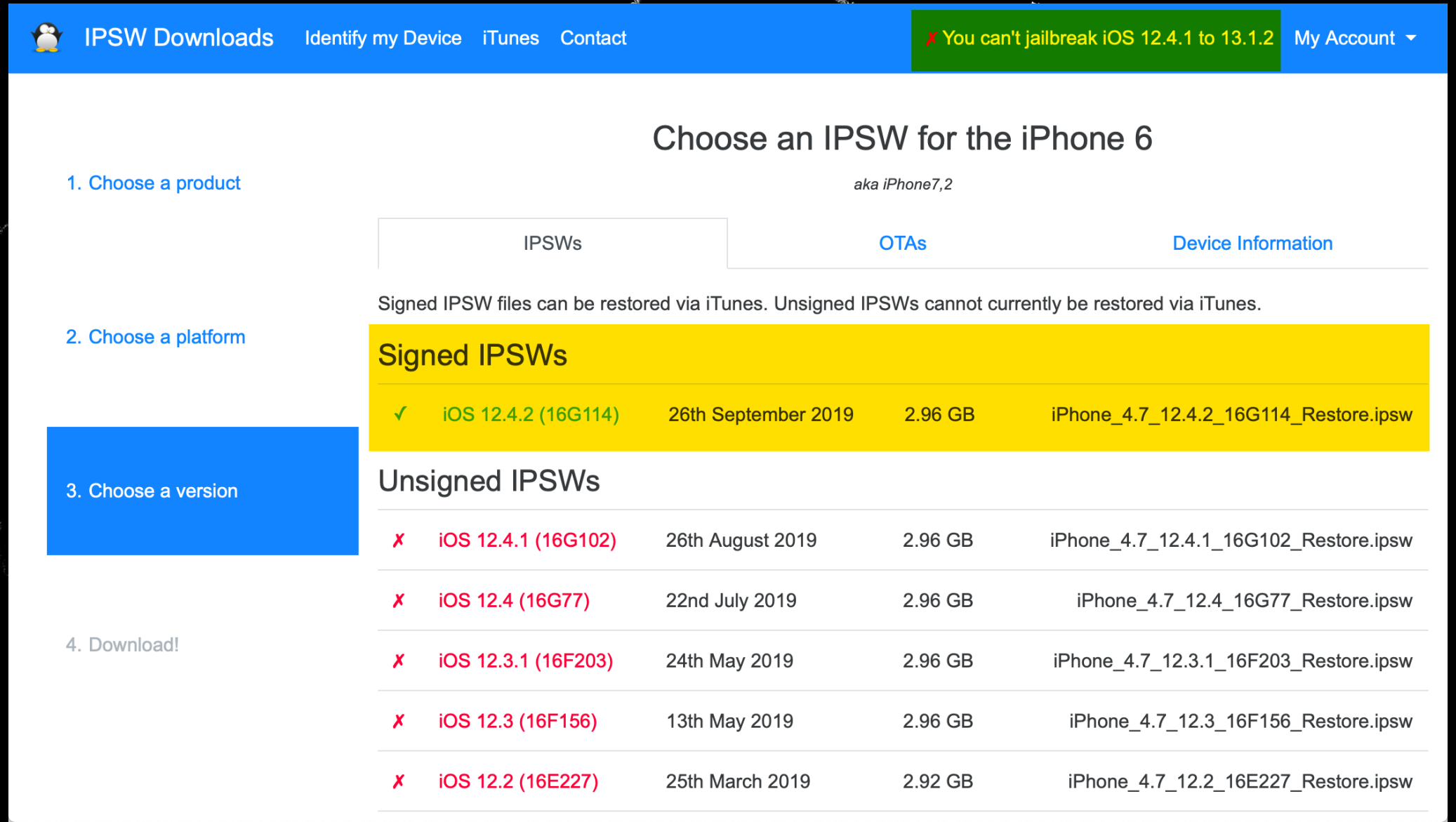
iOS	Jailbreak Tool	Tool Version	iPhone 5s	iPhone 6	iPhone 6 Plus	iPhone 6s	iPhone 6s Plus	iPhone SE	iPhone 7	iPhone 7 Plus	iPhone 8	iPhone 8 Plus	iPhone X	iPhone XR	iPhone XS	iPhone XS Max	iPod touch (6th generation)	iPod touch (7th generation)
12.0	Chimera	1.3.9	Yes															N/A
	unc0ver	3.7.0b1	Yes															
12.0.1	Chimera	1.3.9	Yes															
	unc0ver	3.7.0b1	Yes															
12.1	Chimera	1.3.9	Yes															
	unc0ver	3.7.0b1	Yes															
12.1.1	Chimera	1.3.9	Yes															
	unc0ver	3.7.0b1	Yes															
12.1.2	Chimera	1.3.9	Yes														N/A	
	unc0ver	3.7.0b1	Yes														N/A	
12.1.3	Chimera	1.3.9	Yes											Partial			Yes	
	unc0ver	3.7.0b1	Yes															
12.1.4	Chimera	1.3.9	Yes											Partial			Yes	
	unc0ver	3.7.0b1	Yes															
12.2	Chimera	1.3.9	Yes											Partial			Yes	
	unc0ver	3.7.0b1	Yes															
12.3	No Tool Available		No															
12.3.1	No Tool Available		No															
12.3.2	No Tool Available		N/A									No	N/A					
12.4	Chimera	1.3.9	Yes											Partial			Yes	
	unc0ver	1.7.0b1	Yes															
12.4.1	No Tool Available		No															

13.x

iOS	Jailbreak Tool	Tool Version	Device													
			iPhone 6s	iPhone 6s Plus	iPhone SE	iPhone 7	iPhone 7 Plus	iPhone 8	iPhone 8 Plus	iPhone X	iPhone XR	iPhone XS	iPhone XS Max	iPhone 11	iPhone 11 Pro	iPhone 11 Pro Max
13.0	No Tool Available		No													

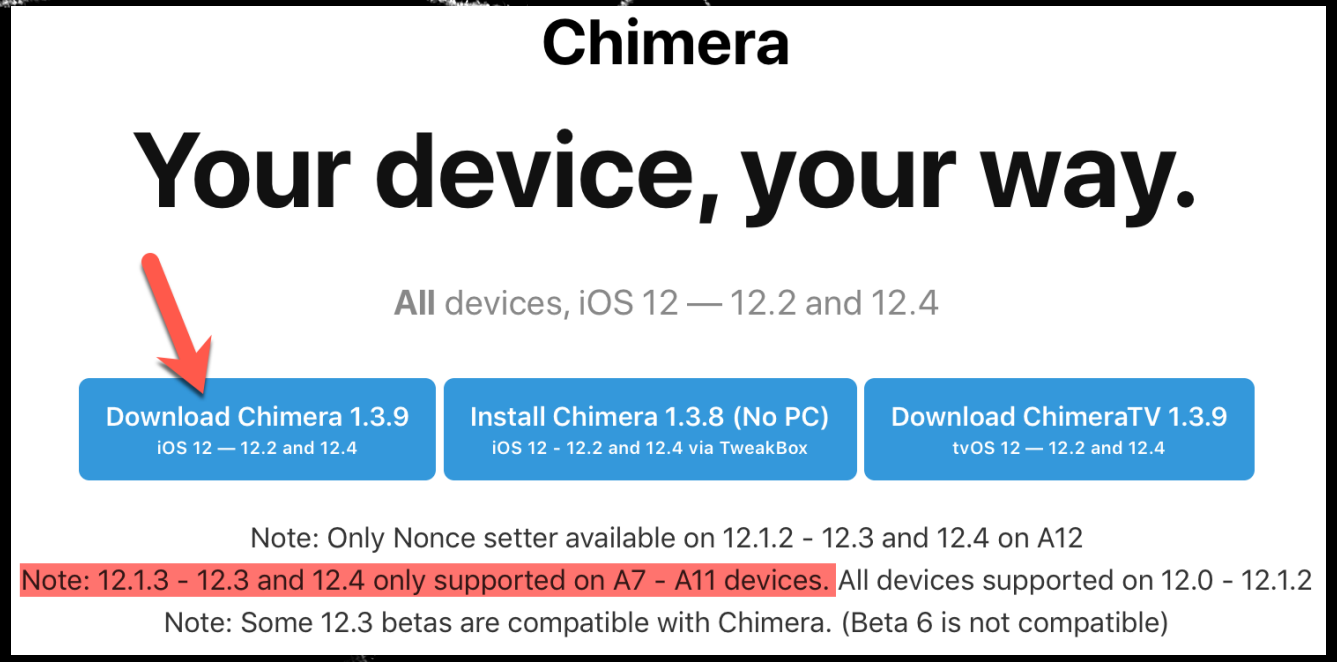
iOS Device Prep – Device Selection

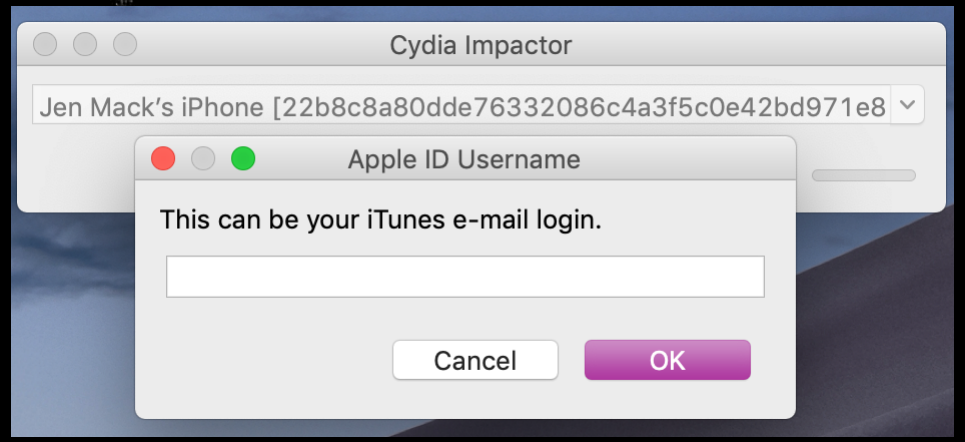
iOS Signing Window - ipsw.me



iOS Device Prep – Jailbreak!

- Pick a Jailbreak
  - Chimera - chimera.sh
  - Unc0ver - github.com/pwn20wndstuff/Undecimus
- Download legitimate Jailbreak
- Follow the directions! Each jailbreak works a bit different.
- Sideload via Cydia Impactor
  - cydiaimpactor.com
  - Semi-untethered jailbreaks
  - Apple Developer Credentials (7 days or 365 days)





iOS Device Prep - Jailbreak!

- Review Jailbreak Settings (per-JB)
- Click the Jailbreak button
- Cross Fingers & Have Patience!
  - It may crash and reboot multiple times

iOS Device Prep – SSH Setup

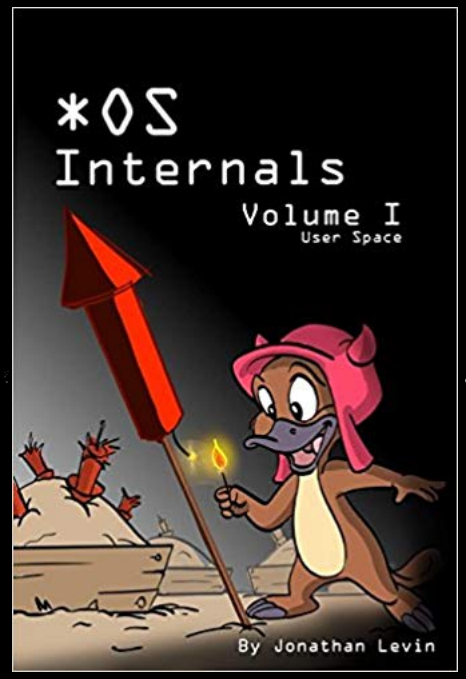
- SSH may or may not come with Jailbreak
- If not, install via Cydia/Sileo
- OpenSSH & Dropbear are common
  - It may or may not run on 22, also try 2222
- Change passwords immediately!
  - ….for root AND mobile
  - iOS password is still ‘alpine’
  - Remember new password
- Can use Wi-Fi or local lightning cable tether via iproxy
  - libimobiledevice.org
  - brew install libimobiledevice

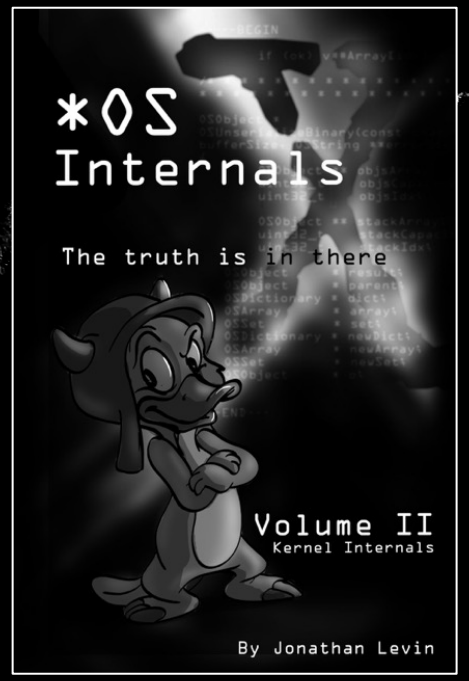
```
Sarahs-Mac:~ oompa$ iproxy 4242 22
waiting for connection
accepted connection, fd = 4
waiting for connection
Number of available devices == 1
Requesting connecion to device handle == 51 (serial:
22b8c8a80dde76332086c4a3f5c0e42bd971e840), port 22
```

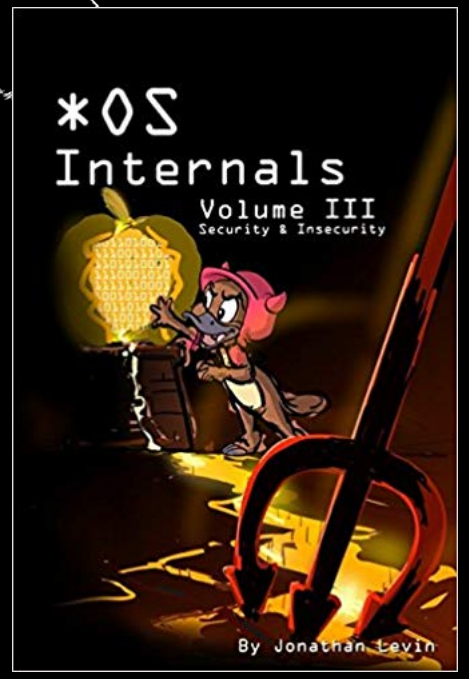
```
Sarahs-Mac:~ oompa$ ssh -p 4242 root@127.0.0.1

root@127.0.0.1's password:
Jen-Macks-iPhone:~ root# passwd root
Changing password for root.
New password:
```

iOS Device Prep – iOS Binpack

- Jailbreak may or may not come with Jonathan Levin's iOS binpack
- newosxbook.com/tools/iOSBinaries.html
- scp -P 4242 binpack64-256.tar root@127.0.0.1:
- Many useful binaries!
  - jtool
  - jlutil
  - fs_usage
  - xxd
  - sqlite3
  - & more!

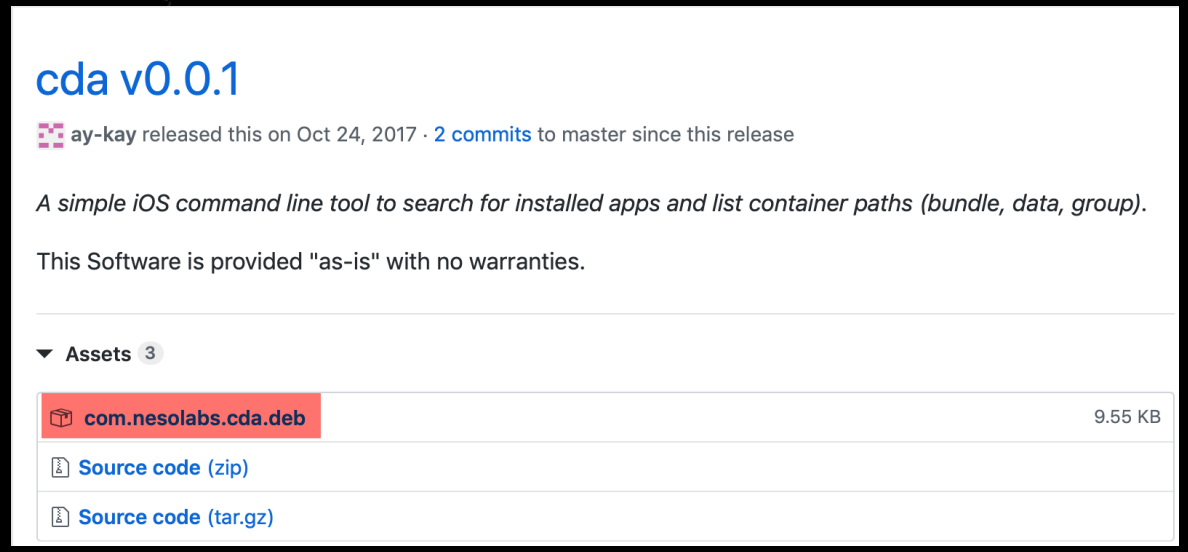


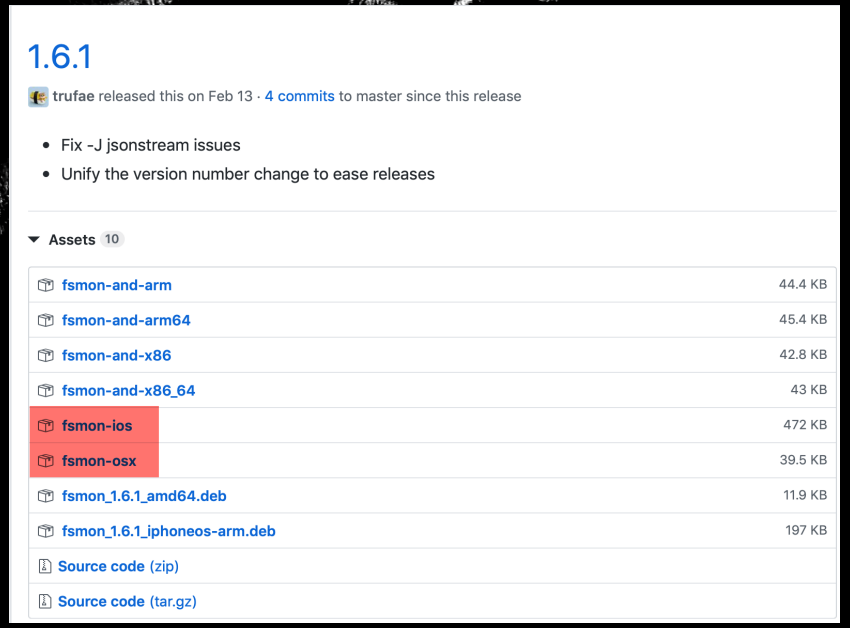




iOS Device Prep – Other Tools

- cda - github.com/ay-kay/cda
  - Lists app container paths
  - Extract ‘cda’ binary from .deb file
    - The Unarchiver
- fsmon - github.com/nowsecure/fsmon
  - File system monitor
  - Build or use pre-compiled binaries
    - iOS and macOS (and Android 🤭)





iOS Device Prep – Thinning Fat Binaries

- Fat (Universal) Mach-O Binaries - Need to be thinned to arm64

```
Sarahs-Mac:Downloads oompa$ file com.nesolabs.cda/usr/bin/cda
com.nesolabs.cda/usr/bin/cda: Mach-O universal binary with 2 architectures: [arm_v7:Mach-O executable arm_v7] [arm64:Mach-O 64-bit executable arm64]
com.nesolabs.cda/usr/bin/cda (for architecture armv7):  Mach-O executable arm_v7
com.nesolabs.cda/usr/bin/cda (for architecture arm64):  Mach-O 64-bit executable arm64
Sarahs-Mac:Downloads oompa$ file fsmon-ios.dms
fsmon-ios.dms: Mach-O universal binary with 2 architectures: [arm_v7:Mach-O executable arm_v7] [arm64:Mach-O 64-bit executable arm64]
fsmon-ios.dms (for architecture armv7): Mach-O executable arm_v7
fsmon-ios.dms (for architecture arm64): Mach-O 64-bit executable arm64
```

- lipo (macOS)
  - lipo <binary> -thin arm64 -output <new_binary>
- jtool (MacOS or iOS)
  - jtool -arch arm64 -e arch <binary>

iOS Device Prep – Thinning Fat Binaries

- lipo - Native to macOS

```
Sarahs-Mac:ios_binaries oompa$ lipo cda -thin arm64 -output cda64
Sarahs-Mac:ios_binaries oompa$ file cda64
cda64: Mach-O 64-bit executable arm64
```

- jtool (Jonathan Levin's otool replacement)
  - newosxbook.com/tools/jtool.html

```
Jen-Macks-iPhone:~ root# jtool -arch arm64 -e arch fsmon-ios
Selected architecture (arm64) starts at 245760 and spans 237760 bytes - written to fsmon-ios.arch_arm64
```

iOS Device Prep – Permissions & Location

- SCP files to iOS device
  - scp -P 4242 cda64 root@127.0.0.1:cda
- Permissions & Location
  - “operation not permitted”
    - Check location of executable
    - Can only run in system partition (/)
  - “permission denied”
    - Check Permissions
    - chmod as needed

```
Jen-Macks-iPhone:~ root# pwd
/var/root
Jen-Macks-iPhone:~ root# ls -l cda fsmon
-rwxr-xr-x  1 root  wheel   52720 Oct  9 22:23 cda
-rw-------  1 root  wheel  237760 Oct  9 22:20 fsmon
Jen-Macks-iPhone:~ root# ./cda
zsh: operation not permitted: ./cda
Jen-Macks-iPhone:~ root# ./fsmon
zsh: permission denied: ./fsmon
```

```
Jen-Macks-iPhone:~ root# cp cda fsmon /bin
Jen-Macks-iPhone:~ root# which cda fsmon
/bin/cda
/bin/fsmon
```

iOS Device Prep – Entitlements & Codesign

- Test the new binaries

```
Jen-Macks-iPhone:~ root# fsmon /
FSE_CREATE_FILE 620      "timed" /priv
FSE_CONTENT_MODIFIED     620     "time
FSE_CREATE_FILE 620      "timed" /priv
FSE_CHOWN       620      "timed" /priv
FSE_CONTENT_MODIFIED     620     "time
```

```
Jen-Macks-iPhone:~ root# jtool --sig --ent /bin/fsmon
Blob at offset: 216144 (21616 bytes) is an embedded signature
Code Directory (1299 bytes)
                Version:     20400
                Flags:       adhoc (0x2)
                CodeLimit:   0x34c50
                Identifier:  fsmon-ios-55554944dc6381f374203b8c9669175be32f15c5 (0x58)
                Executable Segment: Base 0x00000000 Limit: 0x00000000 Flags: 0x00000000
                CDHash:      fa0900ef5ba08d654ee25ca8e1701139c4121768 (computed)
                # of Hashes: 53 code + 5 special
                Hashes @239 size: 20 Type: SHA-1
 Empty requirement set (12 bytes)
Entitlements (242 bytes) :
--
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
 <dict>
  <key>platform-application</key>
  <true/>
 </dict>
</plist>
--
Code Directory (1995 bytes)
                Version:     20400
                Flags:       adhoc (0x2)
                CodeLimit:   0x34c50
                Identifier:  fsmon-ios-55554944dc6381f374203b8c9669175be32f15c5 (0x58)
                Executable Segment: Base 0x00000000 Limit: 0x00000000 Flags: 0x00000000
                CDHash:      ee39181b4dc6a3a7b8317eac91b953df7425b27225ad01d42237ae1ab1c613de (computed)
                # of Hashes: 53 code + 5 special
                Hashes @299 size: 32 Type: SHA-256
Blob Wrapper (8 bytes) (0x10000 is CMS (RFC3852) signature)
```

iOS Device Prep – Entitlements & Codesign

- “killed”
- No entitlements & signature for cda

```
[Jen-Macks-iPhone:~ root# cda
zsh: killed     cda
[Jen-Macks-iPhone:~ root# jtool --sig --ent cda
Blob at offset: 52304 (416 bytes) is an embedded signature
Code Directory (366 bytes)
                Version:     20001
                Flags:       none
                CodeLimit:   0xcc50
                Identifier:  cda.47ba6b93.unsigned (0x2c)
                CDHash:      76c1358263ccde65f3146cc045b623f1acf4627b (computed)
                # of Hashes: 13 code + 2 special
                Hashes @106 size: 20 Type: SHA-1
 Empty requirement set (12 bytes)
```

iOS Device Prep – Entitlements & Codesign

- Extract entitlements from another binary
- Sign and provide entitlements to cda
- Still doesn't work? Reboot and Re-jailbreak!

```
Jen-Macks-iPhone:~ root# jtool --ent /bin/fsmon > ~/ent.xml
Jen-Macks-iPhone:~ root# jtool --sign --inplace --ent ~/ent.xml /bin/cda
Jen-Macks-iPhone:~ root# cda
zsh: killed     cda
Jen-Macks-iPhone:~ root# Connection to 127.0.0.1 closed by remote host.
Connection to 127.0.0.1 closed.
Sarahs-Mac:~ oompa$ ssh -p 4242 root@127.0.0.1
ssh_exchange_identification: read: Connection reset by peer
Sarahs-Mac:~ oompa$ ssh -p 4242 root@127.0.0.1
ssh_exchange_identification: read: Connection reset by peer
Sarahs-Mac:~ oompa$ ssh -p 4242 root@127.0.0.1
root@127.0.0.1's password:
Jen-Macks-iPhone:~ root# cda
Syntax: cda searchTerm
```

Analysis Time!

(Setup wasn’t so bad…right?)

Warning: Possible demo fail ahead!

iOS App Search – cda
Find those pesky app paths

```
Jen-Macks-iPhone:~ root# cda whatsapp
[1] WhatsApp (57T9237FN3.net.whatsapp.WhatsApp)
Bundle: /private/var/containers/Bundle/Application/AF9C1B29-4930-4D07-A568-5A1ED1D02434
Data: /private/var/mobile/Containers/Data/Application/A39EC9F4-AAC7-4606-AFA4-855513B9A3E8
Group: /private/var/mobile/Containers/Shared/AppGroup/B6FB9243-C2B1-4860-93A4-DE4F9AEE49F4 (group.com.facebook.family)

Group: /private/var/mobile/Containers/Shared/AppGroup/AFE677A4-78A2-4DC4-8A50-A4D38D7B3175 (group.net.whatsapp.WhatsApp.shared)
```

```
Jen-Macks-iPhone:~ root# cda wegmans
[1] Wegmans (K6N5Z67FH2.com.wegmans.wegmansapp)
Bundle: /private/var/containers/Bundle/Application/0FF0BA84-5EF5-4BC0-A036-6B60A75DE19C
Data: /private/var/mobile/Containers/Data/Application/BE05C07C-651E-4E06-BFD8-6E0DDD2E6CE5
```

```
Jen-Macks-iPhone:~ root# cda photos
[1] Photos (com.apple.mobileslideshow)
Bundle: /Applications/MobileSlideShow.app

[2] PhotosViewService (com.apple.PhotosViewService)
Bundle: /Applications/PhotosViewService.app
```

macOS App Search – find
Find those pesky app paths

- It’s all about the App name or Bundle ID (org.whispersystems.signal)

```
Sarahs-Mac:~ oompa$ find ~/Library/ -ipath '*signal*'
/Users/oompa/Library//Application Support/CrashReporter/Signal_40C7325D-6F93-53CA-8D13-CEBF2505C302.plist
/Users/oompa/Library//Application Support/CloudDocs/session/containers/iCloud.org.whispersystems.signal
/Users/oompa/Library//Application Support/CloudDocs/session/containers/iCloud.org.whispersystems.signal.plist
/Users/oompa/Library//Application Support/Signal
/Users/oompa/Library//Application Support/Signal/attachments.noindex
/Users/oompa/Library//Application Support/Signal/attachments.noindex/61
/Users/oompa/Library//Application Support/Signal/attachments.noindex/61/61b98de0ee3ef4c2650740b7efbea3709684087f825356968889ba0763dfbba8
/Users/oompa/Library//Application Support/Signal/attachments.noindex/0d
/Users/oompa/Library//Application Support/Signal/attachments.noindex/0d/0dbfcb53f66674bc0592e920dbfa433a607a1f243ab390d3650d11fcd21d5450
/Users/oompa/Library//Application Support/Signal/attachments.noindex/0d/0d80198ed0f2f86f30f46a237c717e280eb62cfd6db18db8431c6c5a68b742cc
```

MacOS and iOS File Monitoring - fsmon

- iOS Example

```
FSE_CREATE_FILE 431     "Camera"        /private/var/mobile/Media/PhotoData/takingphoto
FSE_CREATE_FILE 431     "Camera"        /private/var/mobile/Media/DCIM/.MISC/Incoming/59237015732__59769BD6-2472-4CA0-B985-E93C2AE8B96D.JPG
FSE_CONTENT_MODIFIED    431     "Camera"        /private/var/mobile/Media/DCIM/.MISC/Incoming/59237015732__59769BD6-2472-4CA0-B985-E93C2AE8B96D.JPG
FSE_XATTR_MODIFIED      431     "Camera"        /private/var/mobile/Media/DCIM/.MISC/Incoming/59237015732__59769BD6-2472-4CA0-B985-E93C2AE8B96D.JPG
FSE_STAT_CHANGED        431     "Camera"        /private/var/mobile/Media/DCIM/.MISC/Incoming/59237015732__59769BD6-2472-4CA0-B985-E93C2AE8B96D.JPG
FSE_CREATE_FILE 336     "analyticsd"    /private/var/db/analyticsd/aggregate_persist_temp
FSE_CONTENT_MODIFIED    336     "analyticsd"    /private/var/db/analyticsd/reservoir_persist_temp
FSE_RENAME      336     "analyticsd"    /private/var/db/analyticsd/reservoir_persist_temp -> /private/var/db/analyticsd/reservoirs/1a052925-de52-4455-a885-65816831d534
FSE_CREATE_FILE 319     "assetsd"       /private/var/mobile/Media/PhotoData/MISC/.dat.nosync013f.0WO3gI
FSE_CONTENT_MODIFIED    319     "assetsd"       /private/var/mobile/Media/PhotoData/MISC/.dat.nosync013f.0WO3gI
FSE_CREATE_FILE 319     "assetsd"       /private/var/mobile/Media/PhotoData/MISC/.dat.nosync013f.0WO3gI
FSE_CHOWN       319     "assetsd"       /private/var/mobile/Media/PhotoData/MISC/DCIM_APPLE.plist
FSE_CREATE_FILE 319     "assetsd"       /private/var/mobile/Media/PhotoData/imagewriter
FSE_XATTR_MODIFIED      319     "assetsd"       /private/var/mobile/Media/DCIM/.MISC/Incoming/59237015732__59769BD6-2472-4CA0-B985-E93C2AE8B96D.JPG
FSE_CREATE_FILE 319     "assetsd"       /private/var/mobile/Media/DCIM/100APPLE/IMG_0065.JPG
FSE_STAT_CHANGED        319     "assetsd"       /private/var/mobile/Media/DCIM/.MISC/Incoming
FSE_CREATE_FILE 319     "assetsd"       /private/var/mobile/Media/PhotoData/Caches/ClientServerTransactions/C5BBC303-EF16-464B-B374-B091D7FC2827
FSE_XATTR_MODIFIED      319     "assetsd"       /private/var/mobile/Media/DCIM/100APPLE/IMG_0065.JPG
```

MacOS and iOS File Monitoring - fsmon

- macOS Example

```
Sarahs-Mac:fsmon-master oompa$ fsmon
open /dev/fsevents: Operation not permitted
Sarahs-Mac:fsmon-master oompa$ sudo fsmon
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_CREATE_FILE 12120   ""      /Users/oompa/test.txt
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_CHOWN       2861    "cfprefsd"      /Users/oompa/Library/Preferences/com.apple.Terminal.plist.jCHoFnv
FSE_CHOWN       2861    "cfprefsd"      /Users/oompa/Library/Preferences/com.apple.Terminal.plist.jCHoFnv
FSE_CONTENT_MODIFIED    2861    "cfprefsd"      /Users/oompa/Library/Preferences/com.apple.Terminal.plist.jCHoFnv
FSE_CREATE_FILE 2861    "cfprefsd"      /Users/oompa/Library/Preferences/com.apple.Terminal.plist.jCHoFnv
FSE_XATTR_MODIFIED      62      "logd"  /private/var/db/diagnostics/Persist/0000000000000379.tracev3
FSE_CREATE_FILE 380     "Little Snitch Ne"      /Users/oompa/Library/Application Support/Little Snitch/ConnectionsCache.sqlite-journal
FSE_CONTENT_MODIFIED    380     "Little Snitch Ne"      /Users/oompa/Library/Application Support/Little Snitch/ConnectionsCache.sqlite-journal
FSE_DELETE      380     "Little Snitch Ne"      /Users/oompa/Library/Application Support/Little Snitch/ConnectionsCache.sqlite-journal
```

MacOS and iOS File Monitoring – fs_usage
Built in macOS, iOS from Jonathan Levin's binpack

```
Jen-Macks-iPhone:~ root# fs_usage
23:21:21.421598  read              F=17   B=0x2d                                                                                0.000016   CommCenter.10454
23:21:21.421681  write             F=17   B=0xa                                                                                 0.000015   CommCenter.10454
23:21:21.426021  read              F=17   B=0x6d                                                                                0.000010   CommCenter.10454
23:21:21.426066  read              F=17   B=0x68                                                                                0.000003   CommCenter.10454
```

- …every system call ever…

```
23:21:23.867154  open              F=10       (_WC__E)  private/var/mobile/Media/PhotoData/takingphoto                        0.002056   Camera.9953
23:21:23.867521  lstat64                [  2]           ile/Media/DCIM/.MISC/Incoming/59237048440__4B0DF05F-0C44-4B4B-8CDF-C5349F0CC64F.JPG    0.000081   Camera.9958
23:21:23.868575    RdData[AT1]     D=0x0012192c  B=0x1000   /dev/disk0s1                                                        0.000300 W analyticsd.7266
23:21:23.869007    RdData[AT1]     D=0x0012192d  B=0x6000   /dev/disk0s1                                                        0.000295 W analyticsd.7266
23:21:23.869612  PAGE_IN_FILE      A=0x0100490000                                                                                0.001563   analyticsd.7266
23:21:23.870074  open              F=11       (_WC_T_)  ile/Media/DCIM/.MISC/Incoming/59237048440__4B0DF05F-0C44-4B4B-8CDF-C5349F0CC64F.JPG    0.000511   Camera.9958
23:21:23.870092  fcntl             F=11  <CACHING OFF>                                                                          0.000004   Camera.9958
23:21:23.870094  fcntl             F=11  <CMD=62>                                                                               0.000002   Camera.9958
23:21:23.870224  lstat64                           private/var/db/analyticsd/aggregates/fcb171d4-781b-4783-87f4-31b95e20e97f      0.000096   analyticsd.7266
23:21:23.870344  open                   [  2] (R_____)  private/var/mobile/Media/PhotoData/disableICloudPhotos                 0.000055   cloudphotod.7853
23:21:23.870397  open              F=13       (R_____)  private/var/mobile/Media/PhotoData/pauseICloudPhotos                  0.000022   cloudphotod.7853
23:21:23.870404  fstat64           F=13                                                                                          0.000006   cloudphotod.7853
23:21:23.870417  close             F=13                                                                                          0.000012   cloudphotod.7853
23:21:23.870460  open                   [  2] (R_____)  private/var/mobile/Media/PhotoData/pauseSyncMarker                   0.000027   cloudphotod.7853
23:21:23.870477  unlink                            private/var/db/analyticsd/aggregates/fcb171d4-781b-4783-87f4-31b95e20e97f      0.000251   analyticsd.7266
23:21:23.870528  lstat64                [  2]      private/var/db/analyticsd/aggregate_persist_temp                           0.000047   analyticsd.7266
23:21:23.870774  open              F=8        (_WC_T_)  private/var/db/analyticsd/aggregate_persist_temp                    0.000135   analyticsd.7266
23:21:23.870803  fstat64           F=8                                                                                           0.000005   analyticsd.7266
23:21:23.873051  write             F=8    B=0x4                                                                                  0.002225   analyticsd.7266
23:21:23.873142  write             F=8    B=0x63                                                                                 0.000034   analyticsd.7266
23:21:23.873150  lseek             F=8    O=0x00000067        <SEEK_SET>                                                         0.000005   analyticsd.7266
23:21:23.873153  lseek             F=8    O=0x00000067        <SEEK_SET>                                                         0.000002   analyticsd.7266
23:21:23.873296  close             F=8                                                                                           0.000141   analyticsd.7266
23:21:23.873549  rename                            private/var/db/analyticsd/aggregate_persist_temp                           0.000238   analyticsd.7266
23:21:23.875272    WrData[AT1]     D=0x004f6210  B=0x1000   /dev/disk0s1  private/var/db/analyticsd/aggregate_persist_temp     0.002082 W analyticsd.7266
23:21:23.876322  write             F=11   B=0x1f1a55                                                                             0.006220   Camera.9958
23:21:23.877023  close             F=11                                                                                          0.000693   Camera.9958
23:21:23.877428  open              F=11       (_W____)  ile/Media/DCIM/.MISC/Incoming/59237048440__4B0DF05F-0C44-4B4B-8CDF-C5349F0CC64F.JPG    0.000262   Camera.9958
```

MacOS File Monitoring – watch

- brew install watch
- Watch directories for changes

```
Sarahs-Mac:~ oompa$ touch /private/tmp/hello_there
```

```
Every 2.0s: ls -l /private/tmp          Sarahs-Mac.                : Wed Oct  9 23:28:34 2019

total 16
-rwxrw-rw-@ 1 oompa  wheel    5 Oct  7 17:04
-rw-r-----  1 oompa  wheel   68 Oct  9 21:23 adb.log
drwx------  3 oompa  wheel   96 Oct  7 17:03 com.apple.launchd.A1uOm163O2
drwx------  3 oompa  wheel   96 Oct  7 17:03 com.apple.launchd.THPdcoNYKD
-rw-r--r--  1 oompa  wheel    0 Oct  9 23:17 default.profraw
d----w--w-  2 oompa  wheel   64 Oct  7 17:05 devio_semaphore_devio_0xb503
-rw-r--r--  1 oompa  wheel    0 Oct  9 23:28 hello_there
-rw-r--r--  1 root   wheel    0 Oct  7 17:03 mcu.err.log
-rw-r--r--  1 root   wheel    0 Oct  7 17:03 mcu.out.log
drwxr-xr-x  2 root   wheel   64 Oct  7 17:03 powerlog
```

File Analysis – iOS Plist Files – jlutil (binpack)

```
Jen-Macks-iPhone:/private/var/mobile/Containers/Data/Application/BE05C07C-651E-4E06-BFD8-6E0
DDD2E6CE5/Library/Preferences root# jlutil com.wegmans.wegmansapp.plist
   kGMSMapsUserClientLegalCountry: US
   ADBMOBILE_PERSISTED_MID_HINT: 7
   OMCK5: 2017-12-17T19:19:53Z
   ADOBEMOBILE_STOREDDEFAULTS_OS: iOS 11.0.1
   LatestPassVersion: 1.0
   ADBMOBILE_PERSISTED_MID_BLOB: 6G1ynYcLPuiQxYZrsz_pkc
   OMCK1: 2017-12-17T19:19:53Z
   GMSMapsUserClientZwiebackCookie: 119=sye3ozm4HI566gf
B19O-Udr6Pzv141aObMvWaRCWclodoE1P8TaWKtQjmRu1A6ZJ4grWkR
   GMSMapsUserCookie: AAAAAAAAAAAiNpSU++a/QWDHAjZCKKd66
   com.facebook.sdk:lastInstallResponse110555019105039:
      success: true
   com.google.Maps.GMSSDKLastVersion: 2.3.30035
   ADMS_START: 2017-12-17T19:19:53Z
   UserFirstName: Jen
   PotentialUser:
      accountProfile:
         Loyalty:
            Keytag: 101408058509
            Number: 14080585
         Address:
            Street: 123 Elm
            PostalCode: 22203
            City: Arlington
            Country: USA
            State: VA
         Name:
            Surname: Mack
            GivenName: Jen
         EmailAddress: 1337jmack@gmail.com
      store:
         Title: Alexandria
         LocationDetails:
            Name: Alexandria
            Latitude: 38.7418
            State: VIRGINIA
```

File Analysis – macOS Plist Files – Xcode, plutil –p

```
Sarahs-Mac:Preferences oompa$ plutil -p com.suavetech.0xED.plist
{
  "DecimalNumbersMode" => 1
  "FixedPitchFontName" => "Menlo-Regular"
  "FixedPitchFontSize" => 14
  "HexatorAutoSaveSplitViewName" => [
    0 => "{{0, 0}, {1280, 64}}"
    1 => "{{0, 73}, {1280, 526}}"
  ]
  "HexatorSearchType" => 0
  "LastNewVersionCheck" => "2019-09-27 12:13:05 +0000"
  "LittleEndianMode" => 0
  "NSNavLastRootDirectory" => "~/Desktop/protobufs/maps"
  "NSNavLastUserSetHideExtensionButtonState" => 1
  "NSNavPanelExpandedSizeForSaveMode" => "{841, 448}"
  "NSNavPanelExpandedStateForSaveMode" => 1
  "NSTableView Columns v2 HexatorValueTableView" => <62706c69 73743030 d4010203 04050636 37582476 65727369 6f6e5824 6f626a
65 63747359 24617263 68697665 72542474 6f701200 0186a0ae 07080f1a 1b1c1d1e 1f202630 31325524 6e756c6c d2090a0b 0e5a4e53 2e
6f626a 65637473 5624636c 617373a2 0c0d8002 800a800d d310090a 11151957 4e532e6b 657973a3 12131480 03800480 05a31617 1880068
0 07800880 095a4964 656e7469 66696572 55576964 74685648 69646465 6e565479 70436f6c 23405dc0 00000000 0008d221 2223245a 246
36c61 73736e61 6d655824 636c6173 7365735c 4e534469 6374696f 6e617279 a2232558 4e534f62 6a656374 d310090a 272b19a3 12131480
 03800480 05a32c2d 18800b80 0c800880 09565661 6c436f6c 23408f40 00000000 00d22122 33345e4e 534d7574 61626c65 41727261 79a3
3335 25574e53 41727261 795f100f 4e534b65 79656441 72636869 766572d1 38395541 72726179 80010008 0011001a 0023002d 00320037
0046004c 0051005c 00630066 0068006a 006c0073 007b007f 00810083 00850089 008b008d 008f0091 009c00a2 00a900b0 00b900ba 00bf0
0ca 00d300e0 00e300ec 00f300f7 00f900fb 00fd0101 01030105 01070109 01100119 011e012d 01310139 014b014e 01540000 00000000 0
2010000 00000000 003a0000 00000000 00000000 00000000 0156>
```

File Analysis – macOS or iOS - SQLite

- CLI – sqlite3 (binpack)
- GUI – DB Browser for SQLite (sqlitebrowser.org)
  - MacOS or scp database from iOS

```
Jen-Macks-iPhone:~ root# find /private/var -iname knowledge
/private/var/mobile/Library/CoreDuet/Knowledge
Jen-Macks-iPhone:~ root# cd /private/var/mobile/Library/CoreDuet/Knowledge
Jen-Macks-iPhone:/private/var/mobile/Library/CoreDuet/Knowledge root# ls
knowledge.plist         knowledgeC.db           knowledgeC.db-shm       knowledgeC.db-wal
Jen-Macks-iPhone:/private/var/mobile/Library/CoreDuet/Knowledge root# sqlite3 knowledgeC.db
SQLite version 3.11.0 2016-02-15 17:29:24
Enter ".help" for usage hints.
sqlite> .tables
ZADDITIONCHANGESET              ZOBJECT
ZCONTEXTUALCHANGEREGISTRATION   ZSOURCE
ZCONTEXTUALKEYPATH              ZSTRUCTUREDMETADATA
ZCUSTOMMETADATA                 ZSYNCPEER
ZDELETIONCHANGESET              Z_4EVENT
ZHISTOGRAM                      Z_METADATA
ZHISTOGRAMVALUE                 Z_MODELCACHE
ZKEYVALUE                       Z_PRIMARYKEY
sqlite>
```

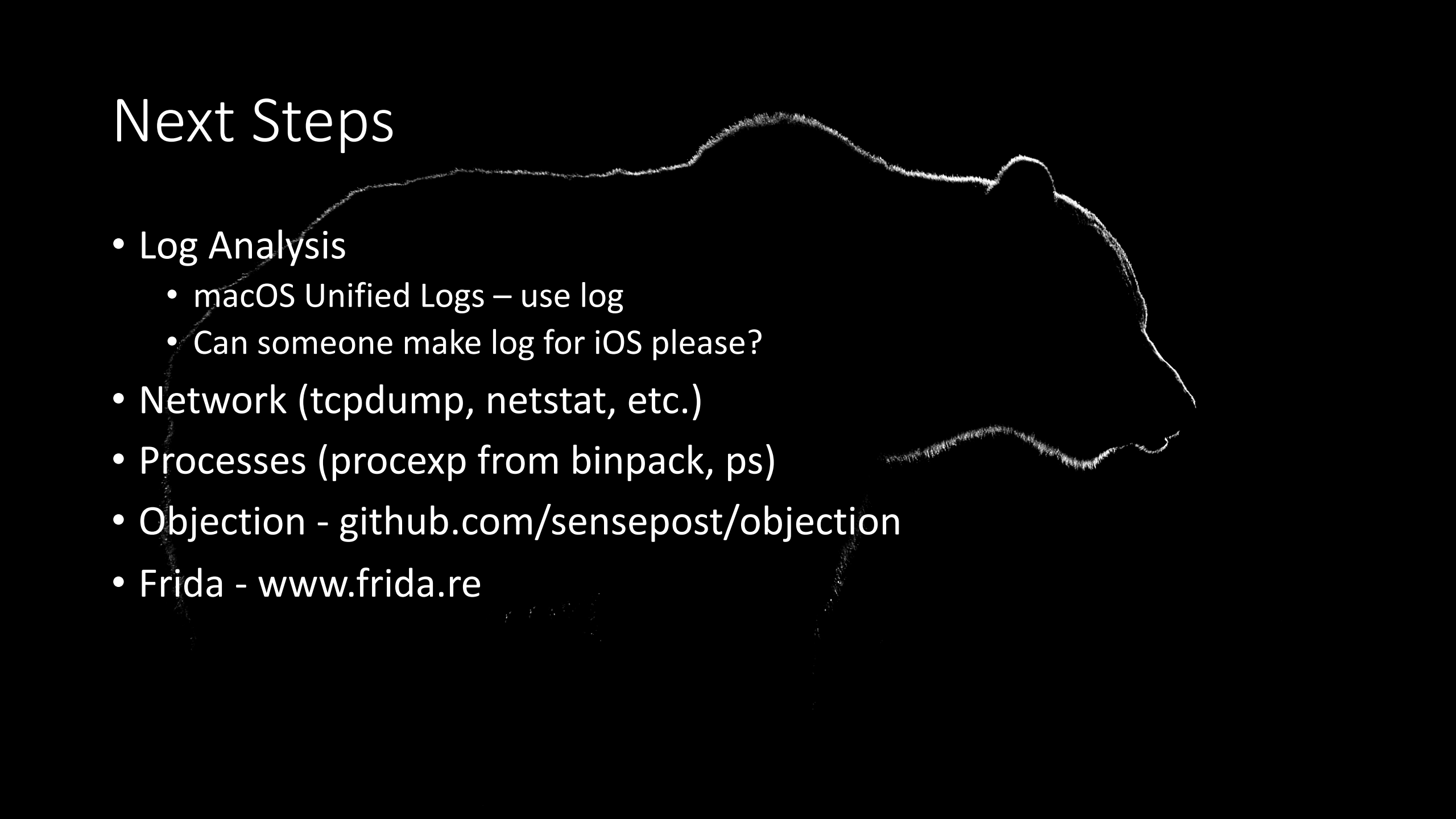
File Analysis – macOS or iOS - SQLite

- Use queries for quick dynamic analysis
- Check out APOLLO! (github.com/mac4n6/APOLLO)

```
Jen-Macks-iPhone:/private/var/mobile/Library/CoreDuet/Knowledge root# sqlite3 -header -column knowledgeC.db < ~/knowledge_app_focus.sql
BUNDLE ID                                    USAGE IN SECONDS  DAY OF WEEK  GMT OFFSET  START                END                  ENTRY CREATION       ZOBJECT TABLE ID
-------------------------------------------  ----------------  -----------  ----------  -------------------  -------------------  -------------------  ----------------
com.apple.mobilemail.MailCacheDeleteExtension  1               Wednesday    -4          2019-09-12 03:46:09  2019-09-12 03:46:10  2019-09-12 03:46:10  8197
com.apple.mobilemail.MailCacheDeleteExtension  1               Thursday     -4          2019-09-12 09:53:44  2019-09-12 09:53:45  2019-09-12 09:53:45  8220
com.apple.mobilemail.MailCacheDeleteExtension  1               Thursday     -4          2019-09-12 21:47:28  2019-09-12 21:47:29  2019-09-12 21:47:29  8243
com.apple.mobilemail.MailCacheDeleteExtension  1               Friday       -4          2019-09-13 21:51:50  2019-09-13 21:51:51  2019-09-13 21:51:51  8266
com.apple.mobilemail.MailCacheDeleteExtension  1               Saturday     -4          2019-09-14 21:53:16  2019-09-14 21:53:17  2019-09-14 21:53:17  8289
com.apple.mobilemail.MailCacheDeleteExtension  1               Thursday     -4          2019-09-19 07:02:22  2019-09-19 07:02:23  2019-09-19 07:02:23  8321
com.apple.mobilemail.MailCacheDeleteExtension  1               Thursday     -4          2019-09-19 13:02:49  2019-09-19 13:02:50  2019-09-19 13:02:50  8349
com.apple.mobilemail.MailCacheDeleteExtension  1               Thursday     -4          2019-09-19 19:03:18  2019-09-19 19:03:19  2019-09-19 19:03:19  8372
com.apple.mobilemail.MailCacheDeleteExtension  1               Friday       -4          2019-09-20 07:08:16  2019-09-20 07:08:17  2019-09-20 07:08:17  8395
com.apple.mobilemail.MailCacheDeleteExtension  1               Saturday     -4          2019-09-21 07:28:28  2019-09-21 07:28:29  2019-09-21 07:28:29  8418
com.apple.Preferences                          9               Saturday     -4          2019-09-21 14:45:10  2019-09-21 14:45:19  2019-09-21 14:45:19  8426
com.apple.MobileStore                          2               Saturday     -4          2019-09-21 14:45:19  2019-09-21 14:45:21  2019-09-21 14:45:21  8429
com.apple.Preferences                          3               Saturday     -4          2019-09-21 14:45:22  2019-09-21 14:45:25  2019-09-21 14:45:25  8431
com.apple.Preferences                          60              Saturday     -4          2019-09-21 14:45:34  2019-09-21 14:46:34  2019-09-21 14:46:35  8434
```

```
Jen-Macks-iPhone:/private/var/containers/Shared/SystemGroup/296FB310-80D4-431C-AA5F-0A5E06E543AD/Library/BatteryLife root#
sqlite3 -column -header CurrentPowerlog.PLSQL < ~/powerlog_torch.sql
ADJUSTED_TIMESTAMP   BUNDLE_ID   STATUS      ORIGINAL_TORCH_TIMESTAMP  OFFSET_TIMESTAMP     TIME_OFFSET        TORCH_ID
-------------------  ----------  ----------  ------------------------  -------------------  -----------------  ----------
2019-08-20 23:17:47              OFF         1970-01-01 23:45:12       1970-02-21 03:15:19  1566257554.81345   1
2019-10-10 04:47:38              ON          1970-02-21 05:15:03       1970-02-21 03:15:19  1566257554.81345   2
2019-10-10 04:47:44              OFF         1970-02-21 05:15:10       1970-02-21 03:15:19  1566257554.81345   3
```

Next Steps



- Log Analysis
  - macOS Unified Logs – use log
  - Can someone make log for iOS please?
- Network (tcpdump, netstat, etc.)
- Processes (procexp from binpack, ps)
- Objection - github.com/sensepost/objection
- Frida - www.frida.re

Thanks!

- TL;DR
  - Testing is not difficult, you need to do it.
- Thank a jailbreaker, tool developer, or researcher - all of this is free* because of them.
  - *with purchase of Mac or iOS Device
- SANS Mac and iOS Forensic Analysis and IR – for518.com
- Twitter: @iamevltwin
- Blog: mac4n6.com
- Github: github.com/mac4n6
- Apple Pattern of Life Lazy Output’er (APOLLO) - github.com/mac4n6/APOLLO