A few minutes with
sysDiagnose

Mitch Cohen

August 17, 2020

mitch@mitchcohen.com
Twitter: @mitchcohen
Micro.blog: mitch.micro.blog

github.com/mitchcohen/360iDev2020-sysDiagnose

sysWhat?

- sysDiagnose is a tool primarily for reporting bugs to Apple
- Includes tons of info about the device and recent operations to help Apple diagnose the bug
- Available on all Apple platforms, plus Xcode and Mail.app on macOS
- https://developer.apple.com/bug-reporting/profiles-and-logs/?name=sysdiagnose

sysHow?

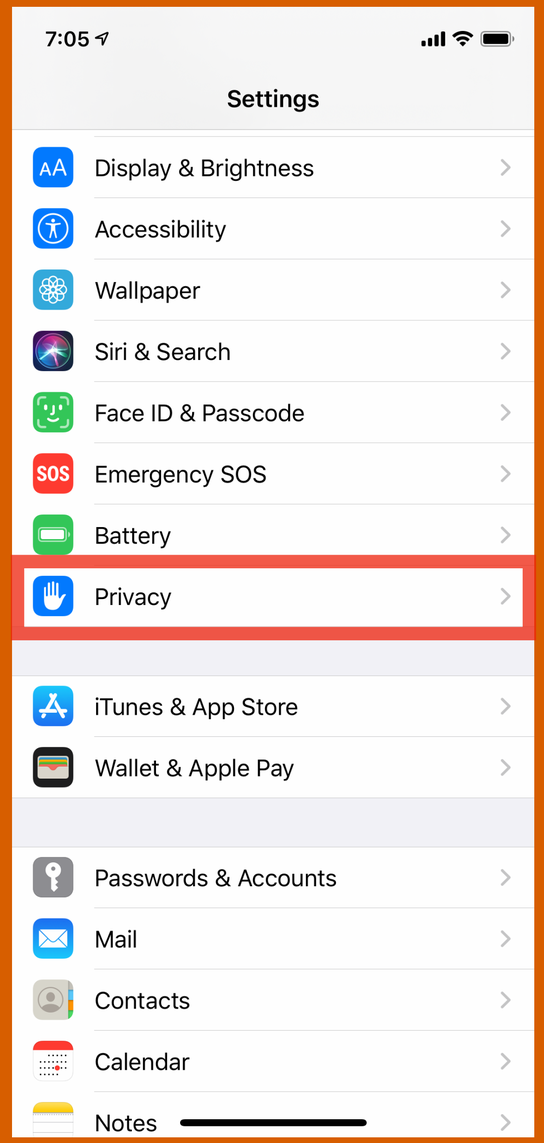
- Press and hold *both* volume buttons *and* side or top button for 1.0 to 1.5 seconds, then release.
- Press too long and iPhone will restart. Oops!

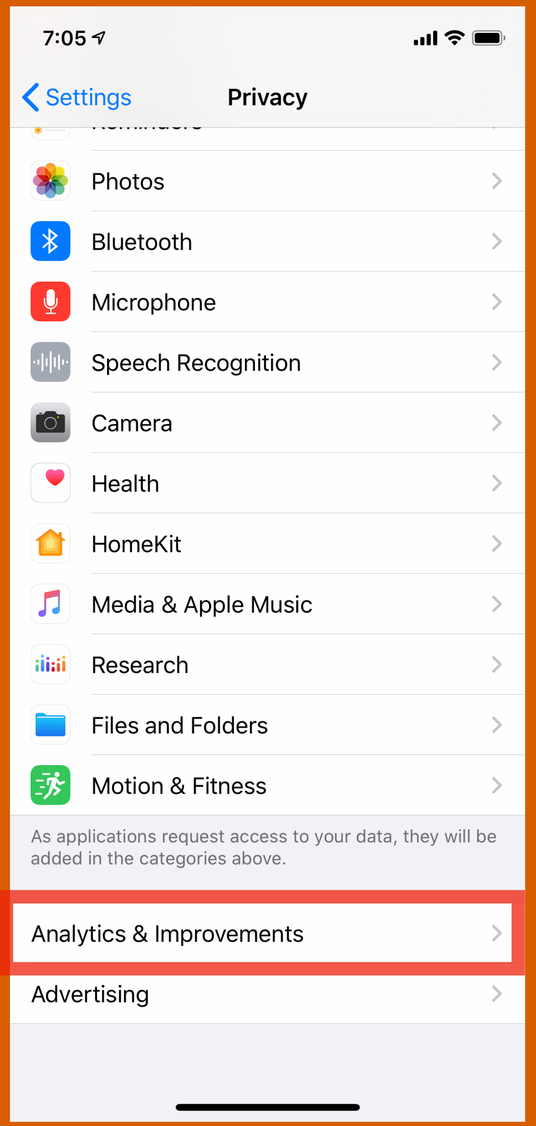
- Upon releasing buttons, iPhone will vibrate briefly.
- Same steps for iPad, but no vibrating.

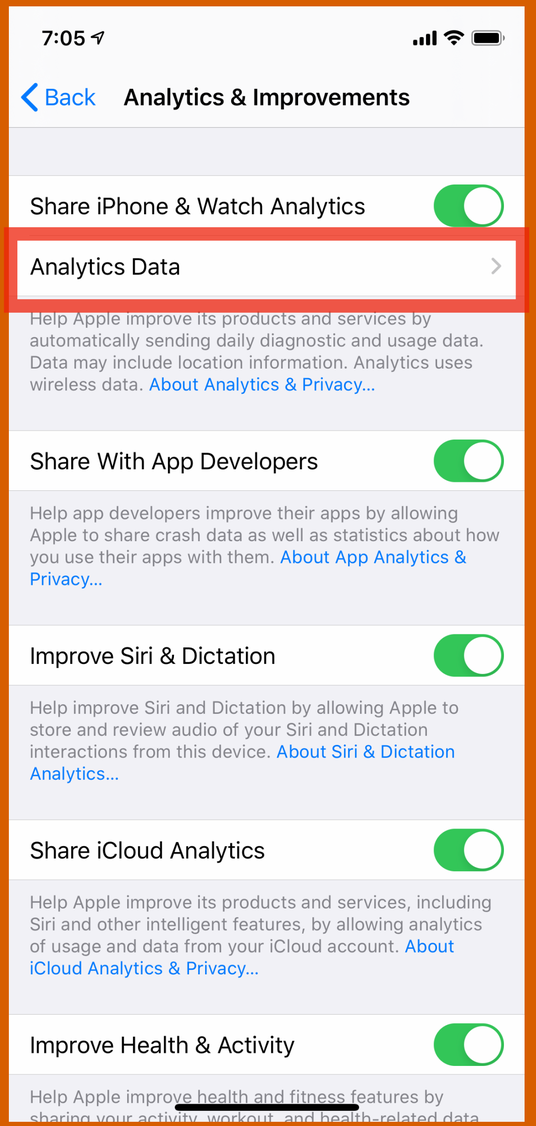
Wait 5-10 minutes

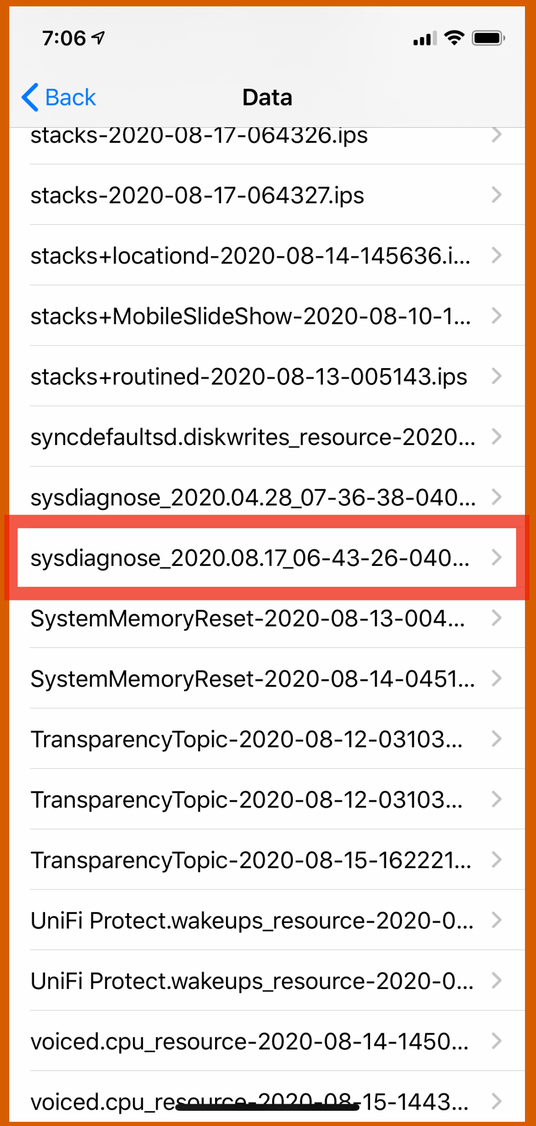
(hopefully, if you pressed it right)

Dive into Settings

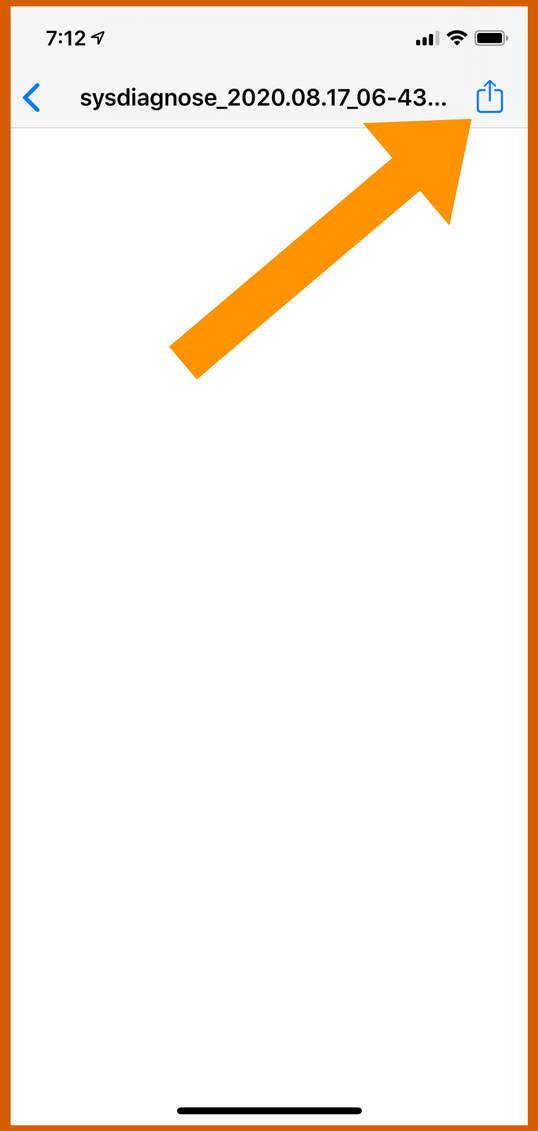


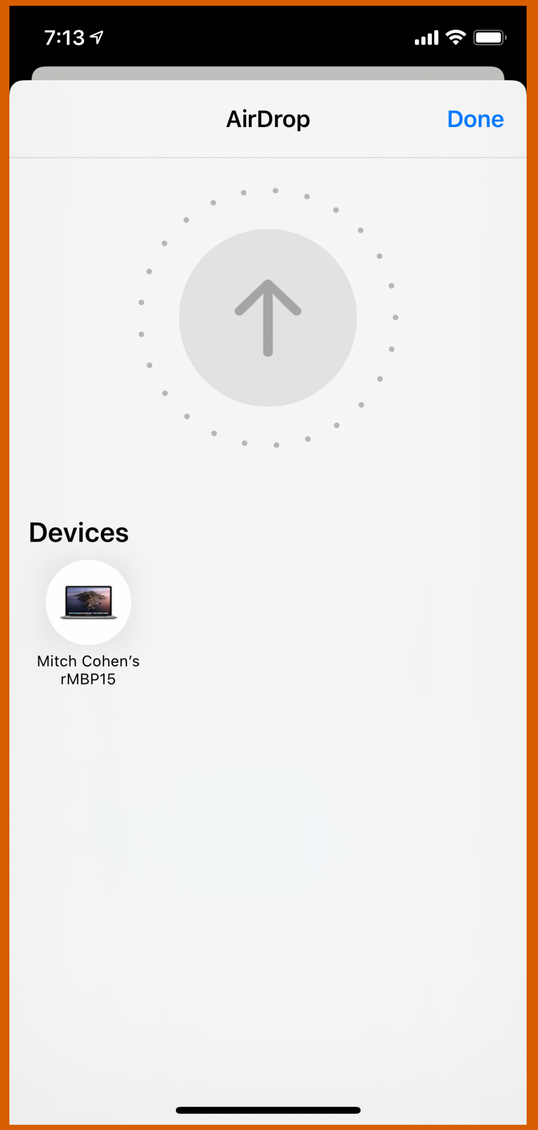


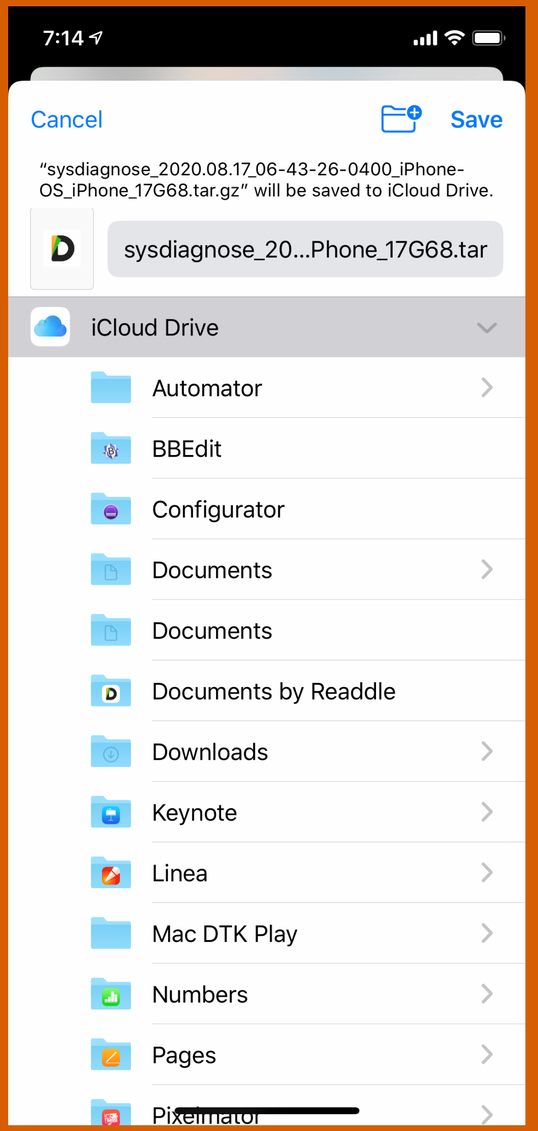




AirDrop, save to Files, DropBox…







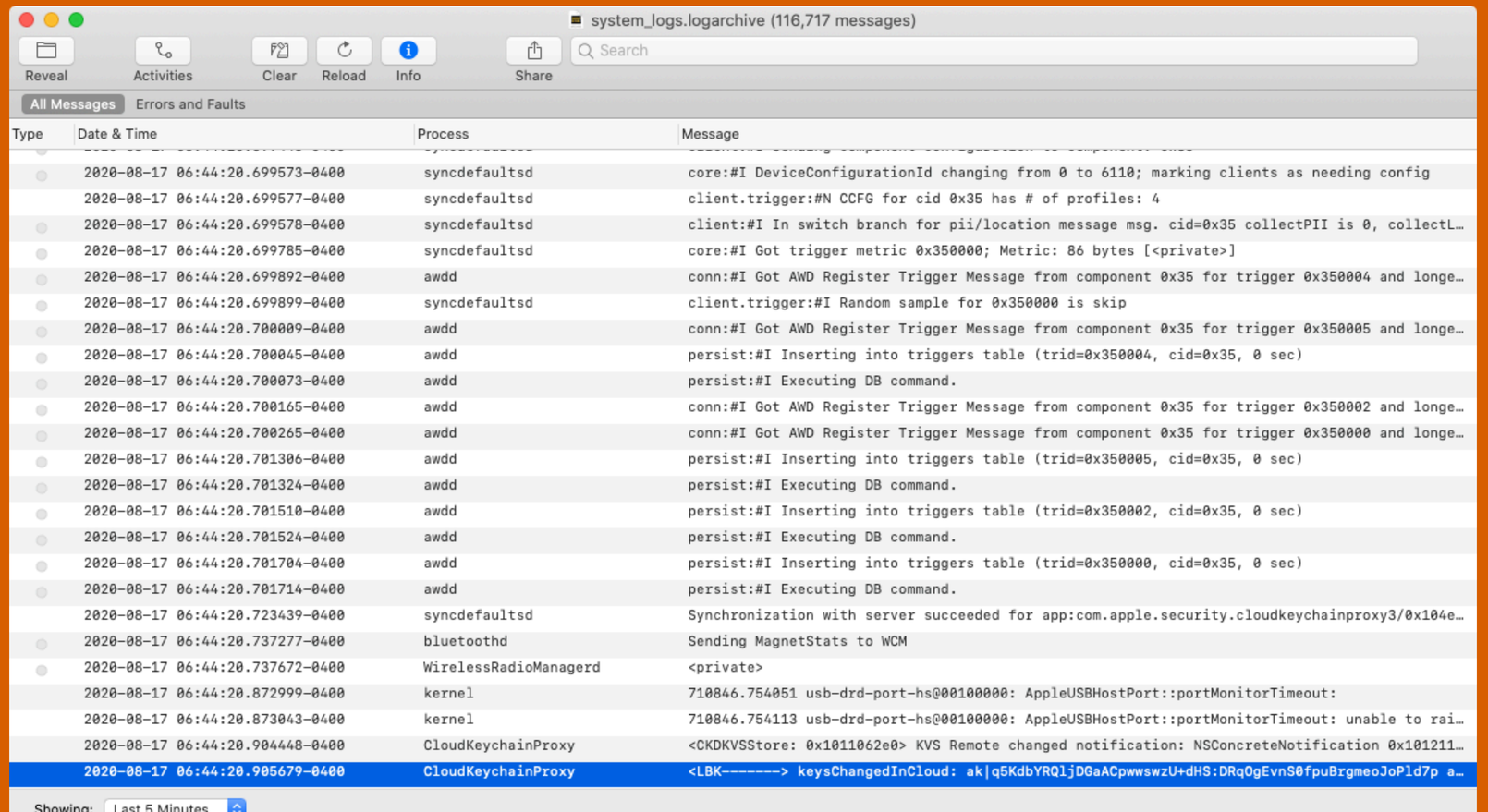
- apfs_stats.txt
- ASPSnapshots
- brctl
- ckksctl_status.txt
- crashes_and_spins
- disks.txt
- error_log.txt
- errors
- fileproviderctl_check.log
- fileproviderctl_dump.log
- fileproviderctl.log
- hidutil.plist
- hpmDiagnose.txt
- ioreg
- kbdebug.txt
- logs
- lsaw.csstoredump
- microstackshots
- mount.txt
- mount.txt
- night-shift.log
- oslog_archive_error.log
- otctl_status.txt
- pcsstatus.txt
- Personalization
- Preferences
- Proximity
- ps_thread.txt
- ps.txt
- README.txt
- RunningBoard
- security-sysdiagnose.txt
- smcDiagnose.txt
- spindump-nosymbols.txt
- summaries
- swcutil_show.txt
- sysdiagnose.log
- system_logs.logarchive
- Preferences
- Proximity
- ps_thread.txt
- ps.txt
- README.txt
- RunningBoard
- security-sysdiagnose.txt
- smcDiagnose.txt
- spindump-nosymbols.txt
- summaries
- swcutil_show.txt
- sysdiagnose.log
- system_logs.logarchive
- tailspin-info.txt
- taskinfo.txt
- taskSummary.csv
- TimezoneDB
- vm_stat.txt
- WiFi

Folder: crashes_and_spins

- All crashes and spindumps for approx 24 hours
- Not symbolicated
- symbolicatecrash -v <.crash file> <.dSYM file>

  https://www.bugsnag.com/blog/symbolicating-ios-crashes

system_logs.logarchive



Detour: os_log: OS_LOG_TYPE_INFO

Discussion

Logging a message of this type is equivalent to calling the `os_log_info` function. Use this level to capture information that may be helpful, but not essential, for troubleshooting errors.

Info-level messages are initially stored in memory buffers. Without a configuration change, they are purged as memory buffers fill. They are, however, captured in the data store when faults and, optionally, errors occur. When info-level messages are added to the data store, they remain there until a storage quota is exceeded, at which point, the oldest messages are purged.

```
import os.log

os_log("magicNumerator: %{public}@", log:
       OSLog.default, type: .info, "\(magicNumerator)")

os_log("magicDenominator: %{public}@", log:
       OSLog.default, type: .info, "\(magicDenominator)")
```

system_logs.logarchive


```
magicNumerator: 100
magicDenominator: 0
Fatal error: Division by zero: file Swift/arm64-apple-ios.swiftinterface, line 31347
```

User shows you their iPhone:

Device Configuration

HearingAidCompliance	Boolean	NO
DarkenSystemColors	Number	0
SoftwareTTYPreference	Number	0
ReduceMotionEnabled	Number	0
AXSClassicInvertColorsPreference	Number	1
MasterStereoBalance	Number	0
Volume	Number	1
InvertColorsEnabled	Number	0
kVOTOriginaKBAttachedKey	Boolean	NO
PointerEffectScalingEnabled	Number	1
VoiceOverTouchSpeakingRate	Number	0.4
LocalizedStringLookupInfoEnabled	Number	0
BrailleDriverCacheDate	Date	Sep
BrailleMasterStatusCellIndex	Number	0
VoiceOverTouchEnabled	Number	0
PointerAllowAppCustomizationEnabled	Number	1
QuickSpeak	Boolean	YES
FullKeyboardAccessEnabled	Number	0

Text Size

- /Preferences/AppleLocale_CurrentUser.txt

```
{
    UIPreferredContentSizeCategoryName = UICTContentSizeCategoryL;
}
```

Languages

- /Preferences/AppleLocale_CurrentUser.txt

```
{
    AppleLanguages =    (
        "en-US",
        "he-US"
    );
}
```

Locale

- /Preferences/AppleLocale_CurrentUser.txt

```
{
    AppleLocale = "en_US";
}
```

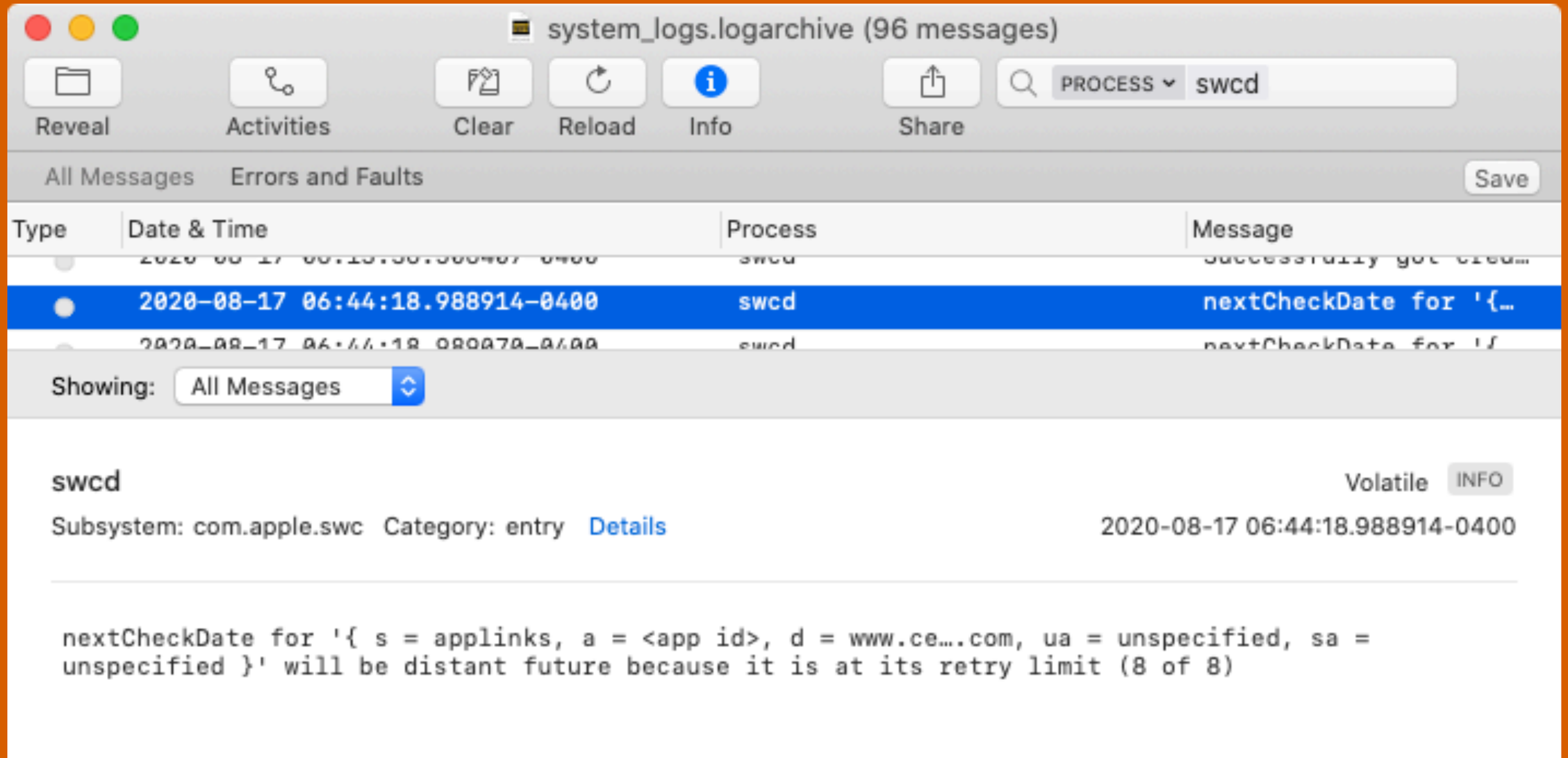
Processes and Threads

- ps.txt has all currently-running processes
- ps_thread.txt has all currently-running processes and their threads

Associated Domains

- Universal Links
- Continuity
- Password AutoFill
- On install, iOS will try fetching https://yourdomain.com/.well-known/apple-app-site-association
- Your app is never told of success or failure!

Associated Domains



More Associated Domains!

- swcutil_show.txt

Service: applinks
App ID: XXX.YYYY.ZZZZ
App Version: 849
Domain: subdomain-inside-VPN.com
User Approval: unspecified
Site/Fmwk Approval: unspecified
Flags:
Last Checked: 2020-07-14 11:06:42 +0000
Error: Error Domain=NSURLErrorDomain Code=-1001 "Timed out waiting for connection to server." UserInfo={Line=226, Function=-[SWCDownloader URLSession:taskIsWaitingForConnectivity:]_block_invoke, PathStatusWhenScheduled=1, NSDebugDescription=Timed out waiting for connection to server.}
Retries: 79

Think about Privacy!

- sysDiagnose contains no user data, but lots of metadata!
- Apps installed
- Hardware details
- Device configuration
- Network connections
- Keychain peers

Thank you for spending a few minutes with sysDiagnose

Mitch Cohen

August 17, 2020

mitch@mitchcohen.com
Twitter: @mitchcohen
Micro.blog: mitch.micro.blog

github.com/mitchcohen/360iDev2020-sysDiagnose