

A few minutes with sysDiagnose



Mitch Cohen

August 17, 2020

mitch@mitchcohen.com

Twitter: @mitchcohen

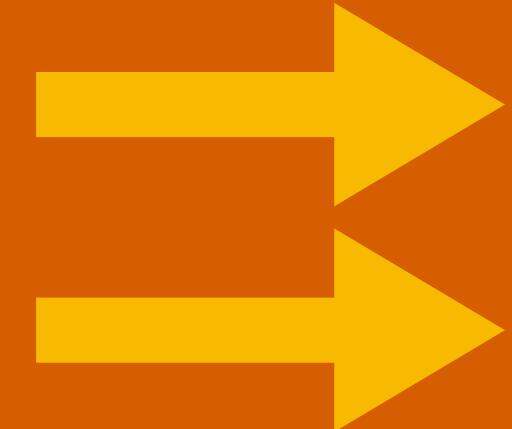
Micro.blog: mitch.micro.blog

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?



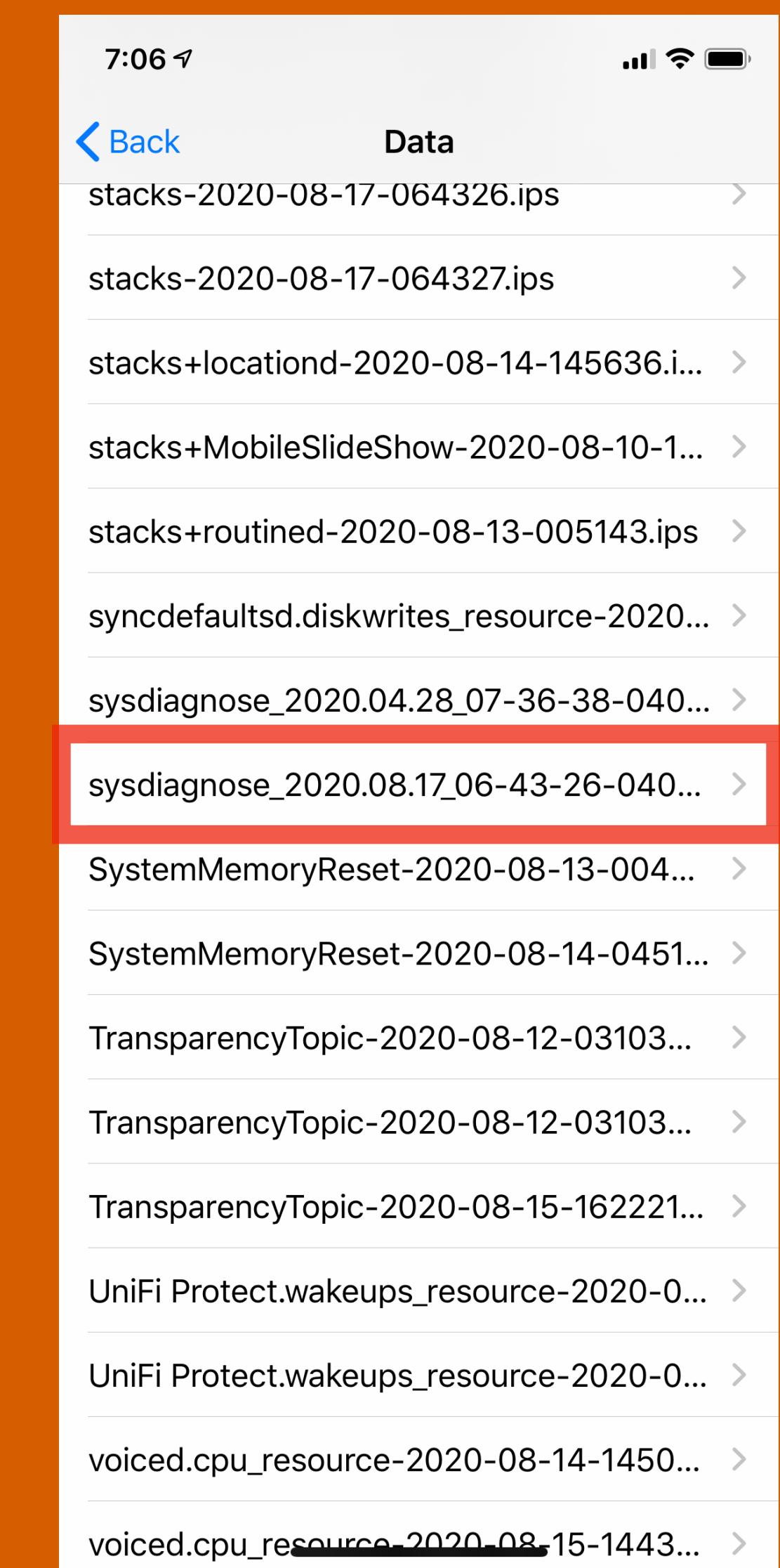
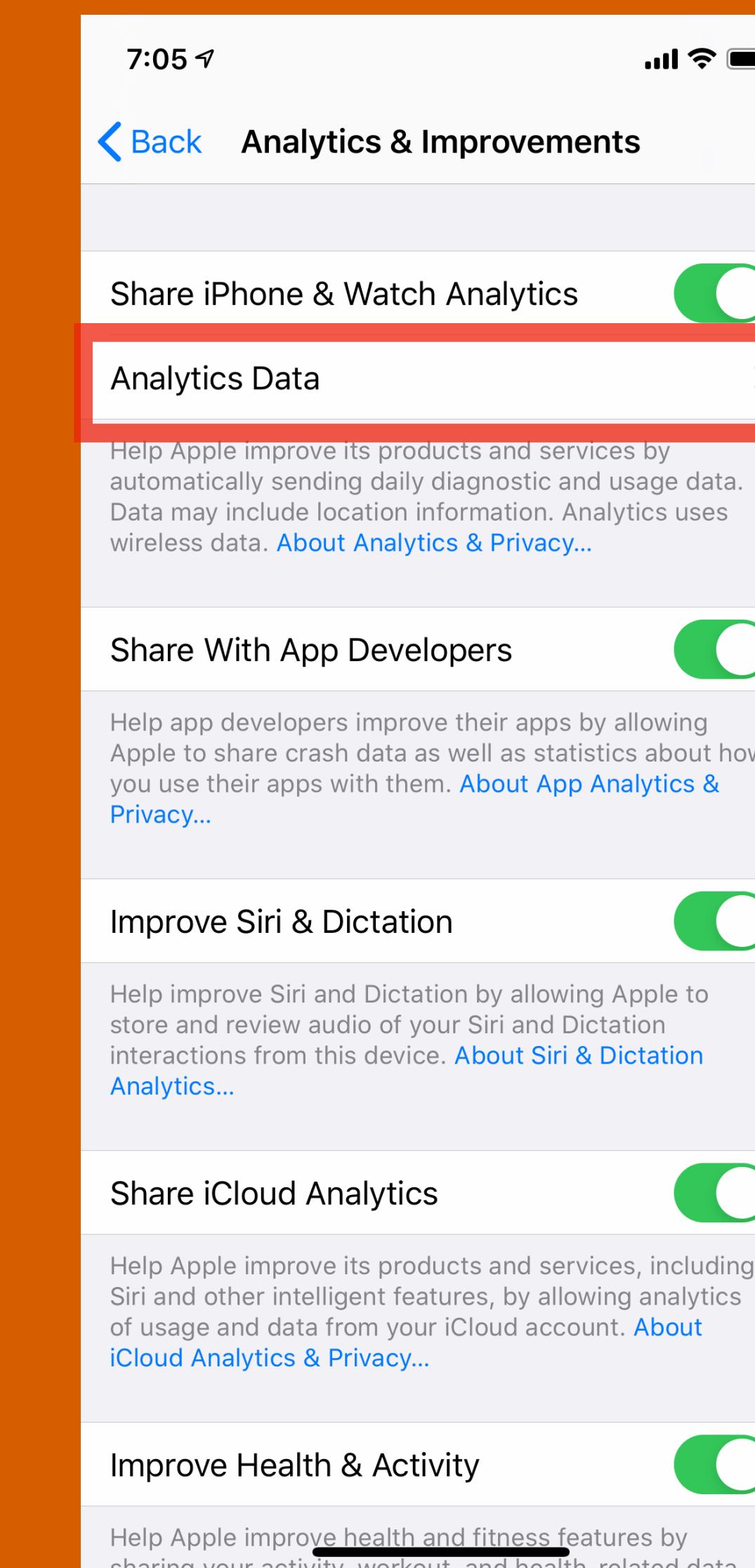
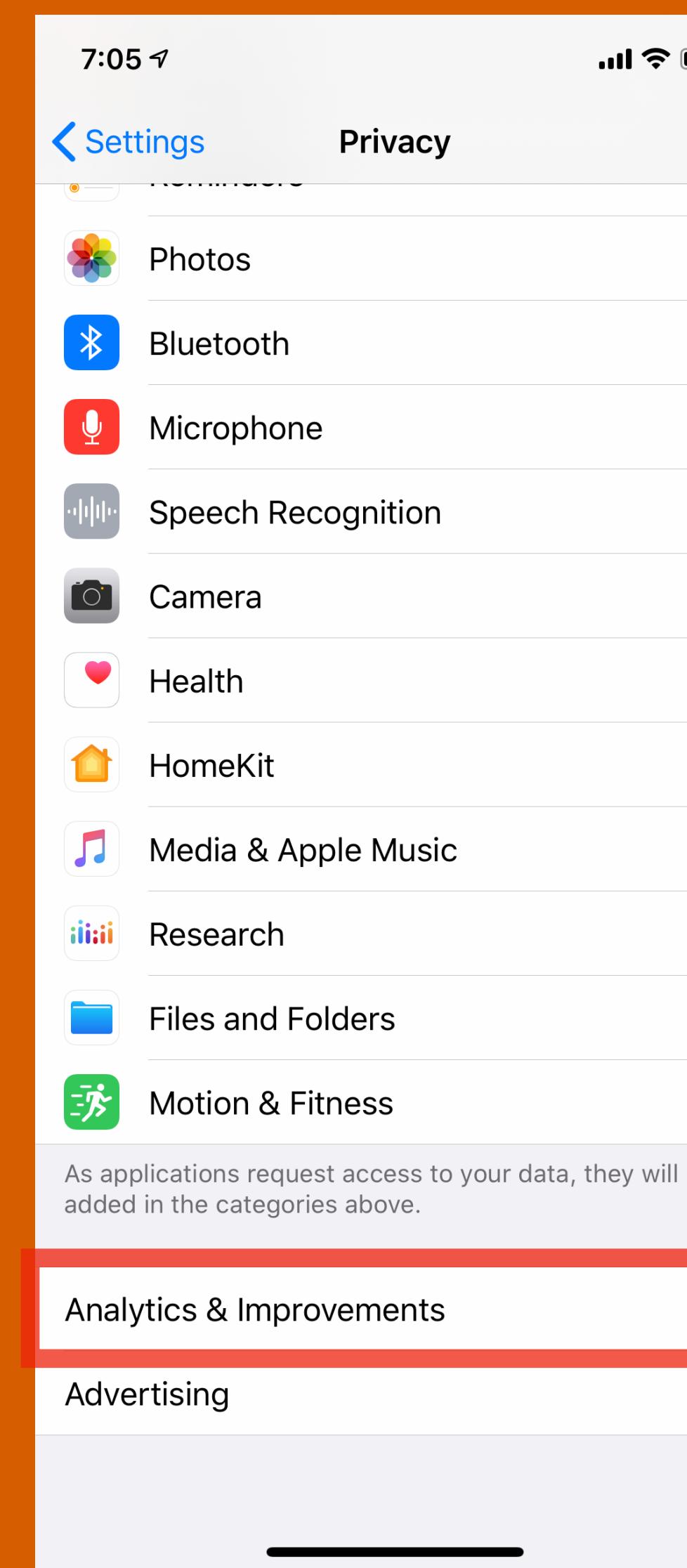
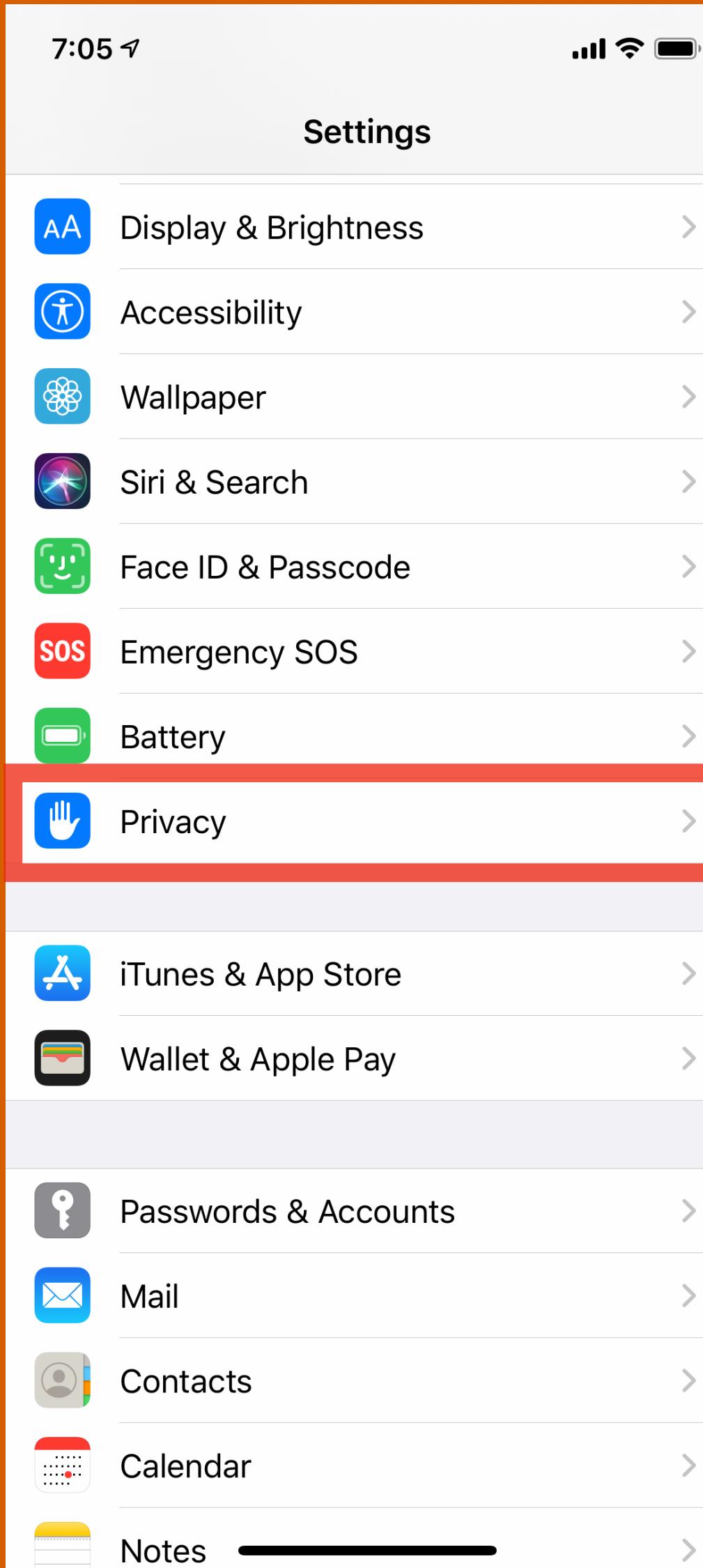
- Press and hold *both* volume buttons *and* side or top button for 1.0 to 1.5 seconds, then release.
- Press too long and iPhone will restart. Oops!



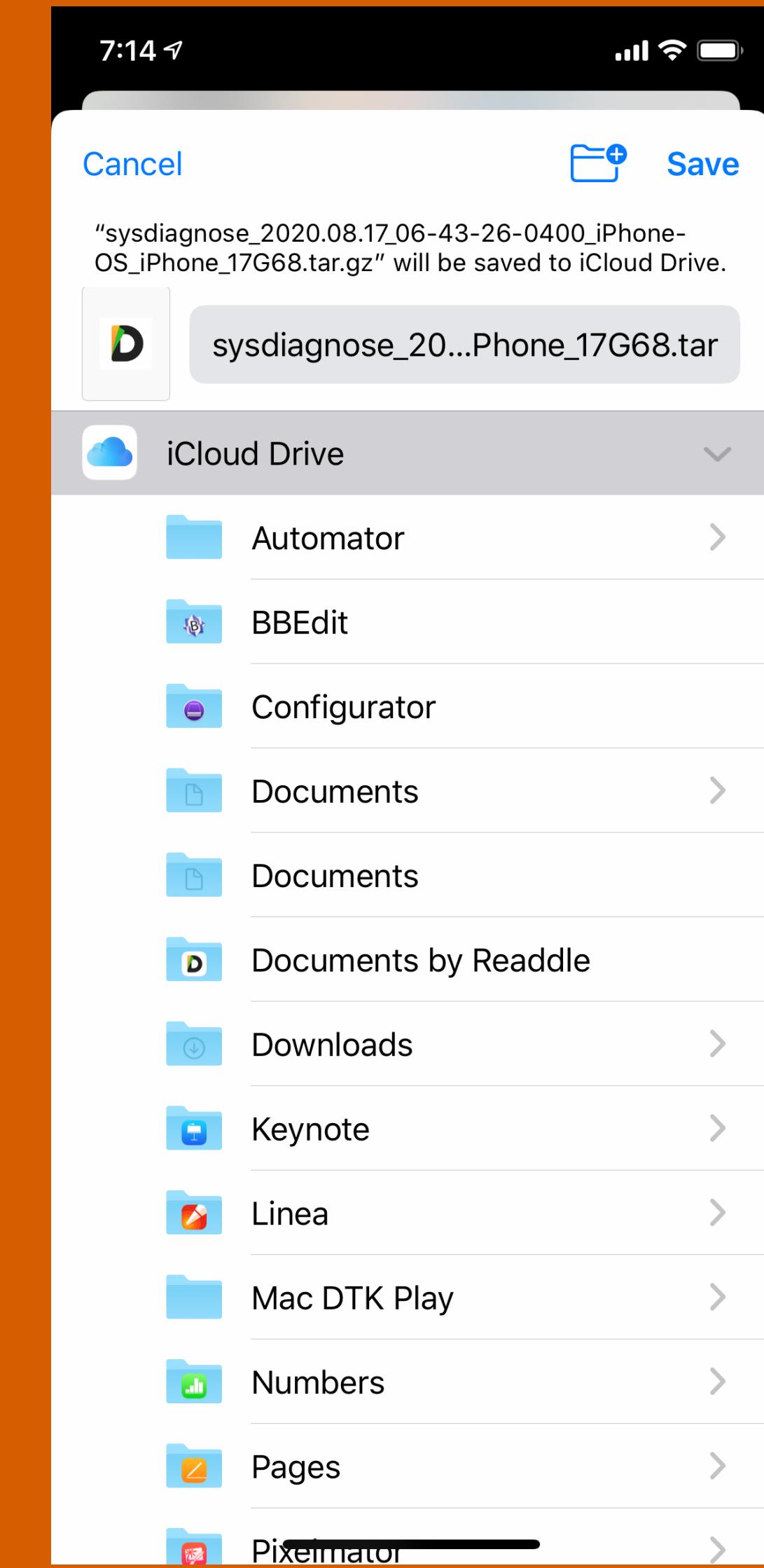
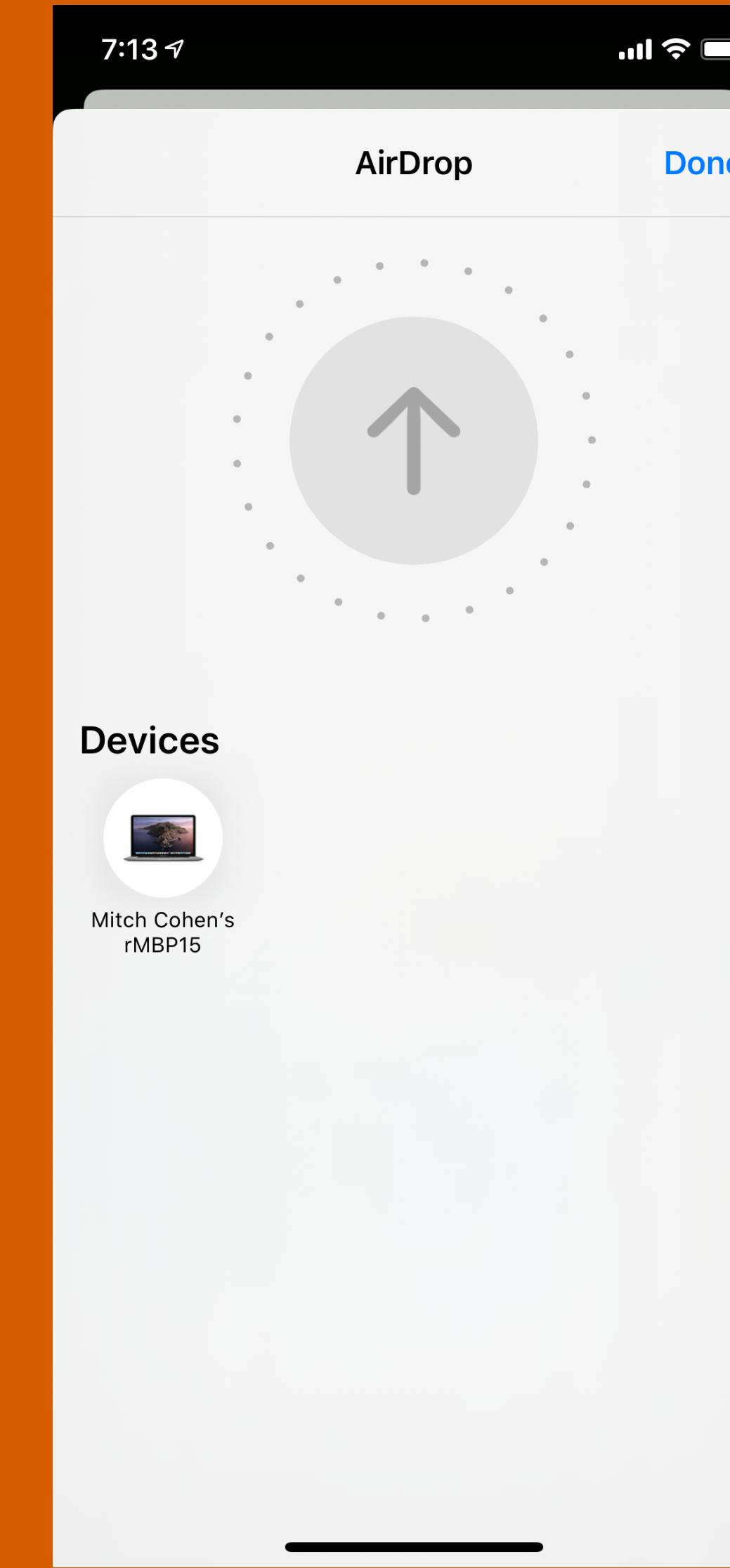
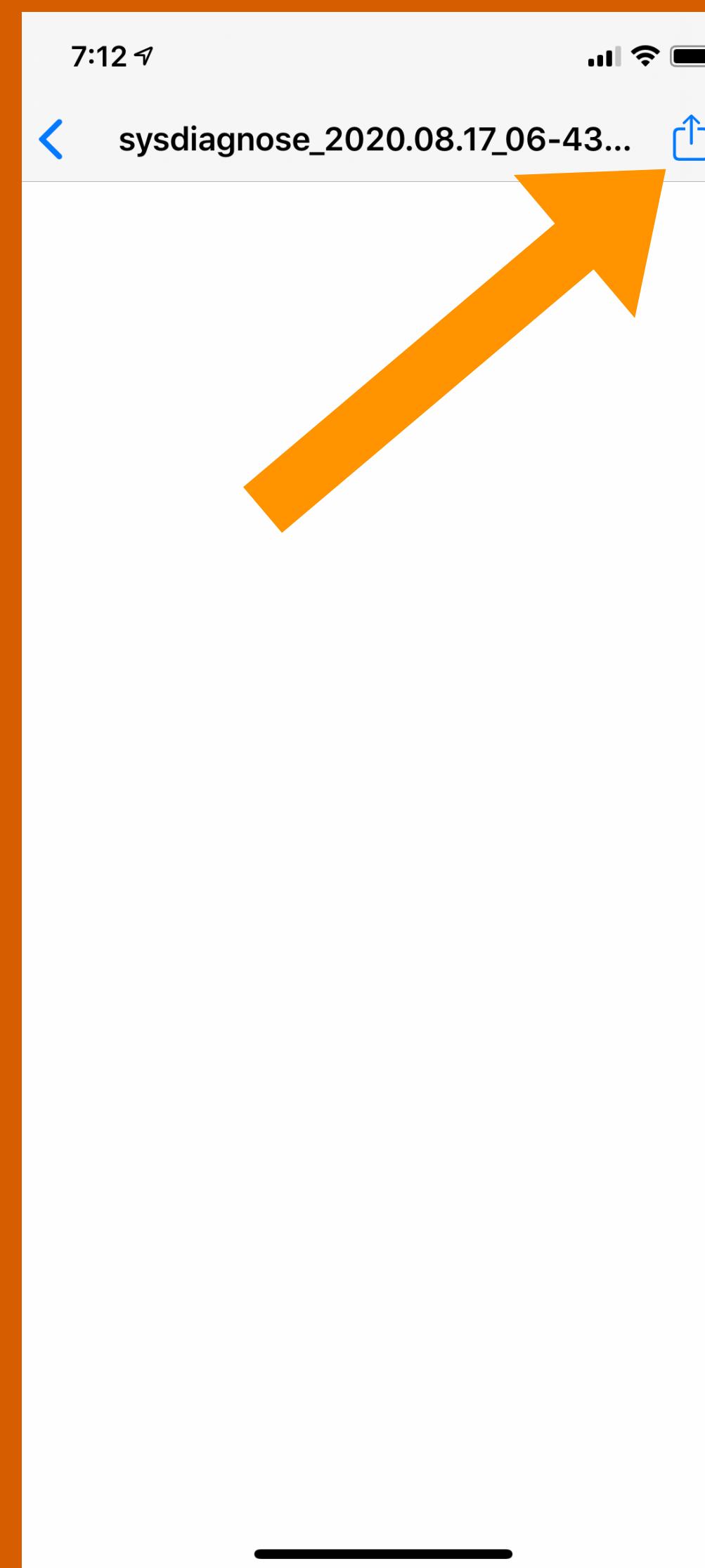
- Upon releasing buttons, iPhone will vibrate briefly.
- Same steps for iPad, but no vibrating.

Wait 5-10 minutes
(hopefully, if you pressed it right)

Dive into Settings



AirDrop, save to Files, DropBox...





sysdiagnose_2020.08.17_06-43-26-040... 254.3 MB

Modified: Today, 6:45 AM

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

system_logs.logarchive (3,542,874 messages)

system_logs.logarchive (116,717 messages)

The screenshot shows the macOS System Log window titled "system_logs.logarchive (116,717 messages)". The window has a toolbar with icons for Reveal, Activities, Clear, Reload, Info, Share, and a Search field. Below the toolbar is a navigation bar with tabs: "All Messages" (selected) and "Errors and Faults". The main area is a table with columns: Type, Date & Time, Process, and Message. The table lists numerous log entries from various processes like syncdefaultsd, awdd, and kernel, detailing system events such as configuration changes, trigger activations, and network activity. The last entry in the table is highlighted in blue.

| Type | Date & Time | Process | Message |
|------|---------------------------------|-----------------------|---|
| | 2020-08-17 06:44:20.699573-0400 | syncdefaultsd | core:#I DeviceConfigurationId changing from 0 to 6110; marking clients as needing config |
| | 2020-08-17 06:44:20.699577-0400 | syncdefaultsd | client.trigger:#N CCFG for cid 0x35 has # of profiles: 4 |
| | 2020-08-17 06:44:20.699578-0400 | syncdefaultsd | client:#I In switch branch for pii/location message msg. cid=0x35 collectPII is 0, collectL... |
| | 2020-08-17 06:44:20.699785-0400 | syncdefaultsd | core:#I Got trigger metric 0x350000; Metric: 86 bytes [<private>] |
| | 2020-08-17 06:44:20.699892-0400 | awdd | conn:#I Got AWD Register Trigger Message from component 0x35 for trigger 0x350004 and longe... |
| | 2020-08-17 06:44:20.699899-0400 | syncdefaultsd | client.trigger:#I Random sample for 0x350000 is skip |
| | 2020-08-17 06:44:20.700009-0400 | awdd | conn:#I Got AWD Register Trigger Message from component 0x35 for trigger 0x350005 and longe... |
| | 2020-08-17 06:44:20.700045-0400 | awdd | persist:#I Inserting into triggers table (trid=0x350004, cid=0x35, 0 sec) |
| | 2020-08-17 06:44:20.700073-0400 | awdd | persist:#I Executing DB command. |
| | 2020-08-17 06:44:20.700165-0400 | awdd | conn:#I Got AWD Register Trigger Message from component 0x35 for trigger 0x350002 and longe... |
| | 2020-08-17 06:44:20.700265-0400 | awdd | conn:#I Got AWD Register Trigger Message from component 0x35 for trigger 0x350000 and longe... |
| | 2020-08-17 06:44:20.701306-0400 | awdd | persist:#I Inserting into triggers table (trid=0x350005, cid=0x35, 0 sec) |
| | 2020-08-17 06:44:20.701324-0400 | awdd | persist:#I Executing DB command. |
| | 2020-08-17 06:44:20.701510-0400 | awdd | persist:#I Inserting into triggers table (trid=0x350002, cid=0x35, 0 sec) |
| | 2020-08-17 06:44:20.701524-0400 | awdd | persist:#I Executing DB command. |
| | 2020-08-17 06:44:20.701704-0400 | awdd | persist:#I Inserting into triggers table (trid=0x350000, cid=0x35, 0 sec) |
| | 2020-08-17 06:44:20.701714-0400 | awdd | persist:#I Executing DB command. |
| | 2020-08-17 06:44:20.723439-0400 | syncdefaultsd | Synchronization with server succeeded for app:com.apple.security.cloudkeychainproxy3/0x104e... |
| | 2020-08-17 06:44:20.737277-0400 | bluetoothd | Sending MagnetStats to WCM |
| | 2020-08-17 06:44:20.737672-0400 | WirelessRadioManagerd | <private> |
| | 2020-08-17 06:44:20.872999-0400 | kernel | 710846.754051 usb-drdr-port-hs@00100000: AppleUSBHostPort::portMonitorTimeout: |
| | 2020-08-17 06:44:20.873043-0400 | kernel | 710846.754113 usb-drdr-port-hs@00100000: AppleUSBHostPort::portMonitorTimeout: unable to rai... |
| | 2020-08-17 06:44:20.904448-0400 | CloudKeychainProxy | <CKDKVSSStore: 0x1011062e0> KVS Remote changed notification: NSConcreteNotification 0x101211... |
| | 2020-08-17 06:44:20.905679-0400 | CloudKeychainProxy | <LBK-----> keysChangedInCloud: ak q5KdbYRQ1jDGaACpwswzU+dHS:DRqOgEvnS0fpBuBrgmeoJoPld7p a... |

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



system_logs.logarchive (3,542,874 messages)

```
magicNumerator: 100
```

```
magicDenominator: 0
```

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

User shows you their iPhone:



Device Configuration

| File Path |
|---|
| logs |
| Accessibility |
| AccessibilityPrefs |
| com.apple.Accessibility.GuidedAccess.plist |
| com.apple.Accessibility.Magnifier.plist |
| com.apple.Accessibility.plist |
| com.apple.Accessibility.SwitchControl.plist |
| com.apple.AssistiveTouch.plist |
| com.apple.HearingAids.plist |
| com.apple.SpeakSelection.plist |
| com.apple.VoiceOverTouch.plist |
| com.apple.ZoomTouch.plist |

| | | |
|---|---------|-----|
| HearingAidCompliance | Boolean | NO |
| DarkenSystemColors | Number | 0 |
| SoftwareTTYPreference | Number | 0 |
| ReduceMotionEnabled | Number | 0 |
| AXSClassicInvertColorsPreference | Number | 1 |
| MasterStereoBalance | Number | 0 |
| Volume | Number | 1 |
| InvertColorsEnabled | Number | 0 |
| kVOTOriginalKBAttachedKey | 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

The screenshot shows the macOS System Log window. The title bar reads "system_logs.logarchive (96 messages)". The toolbar includes icons for Reveal, Activities, Clear, Reload, Info, Share, and a search field set to "PROCESS" with the value "swcd". Below the toolbar are buttons for "All Messages" and "Errors and Faults", with "All Messages" being selected. A "Save" button is also present. The main table has columns for Type, Date & Time, Process, and Message. A single log entry is highlighted in blue:

| Type | Date & Time | Process | Message |
|------|---------------------------------|---------|--------------------------|
| ● | 2020-08-17 06:44:18.988914-0400 | swcd | nextCheckDate for '{...' |
| | 2020-08-17 06:44:18.988914-0400 | swcd | nextCheckDate for '{...' |

At the bottom, a dropdown menu shows "Showing: All Messages".

swcd
Subsystem: com.apple.swc Category: entry [Details](#) Volatile INFO
2020-08-17 06:44:18.988914-0400

nextCheckDate for '{ s = applinks, a = <app id>, d = www.ce...com, ua = unspecified, sa = unspecified }' will be distant future because it is at its retry limit (8 of 8)

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