LOGS UNITE!
FORENSIC ANALYSIS OF APPLE UNIFIED LOGS

Sarah Edwards
@iamenvletwin | oompa@csh.rit.edu | mac4n6.com
04/01/2017
WHERE WE CAME FROM

<table>
<thead>
<tr>
<th>Apple System Logs (ASL, syslog)</th>
<th>Unix Logs (syslog)</th>
<th>Basic Security Module (BSM) Audit Logs</th>
<th>Check out my ‘Analysis &amp; Correlation of Mac Logs’ Presentation!</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/log/asl/</td>
<td>/var/log/</td>
<td>/var/audit/</td>
<td>mac4n6.com/resources</td>
</tr>
<tr>
<td>Binary Format</td>
<td>ASCII/Compressed ASCII</td>
<td>Binary Format</td>
<td></td>
</tr>
<tr>
<td>MacOS, limited on iOS</td>
<td>MacOS, limited on iOS</td>
<td>MacOS</td>
<td></td>
</tr>
</tbody>
</table>
WHERE WE ARE GOING

Unified logs across devices and operating systems!

Devices
- macOS 10.12 (Sierra) - Laptops/Desktops
- iOS 10 - iPhone, iPad, iPod
- watchOS 3.0 - Apple Watches
- tvOS 10 - Apple TV (Gen 4)

Similar Storage Locations

Volatile Logs

Binary Format

…and everything from the previous slide…for now.
UNIFIED LOG ACQUISITION
**LOG LEVELS & STORAGE [DEFAULT CONFIG]**
(ON DISK OR IN MEMORY)

**Default - “Things that might fail”**
- Storage: Memory -> Compressed -> On Disk
- Retention: Oldest Removed after storage exceeded

**Info – “Helpful, but non-essential”**
- Storage: Memory (default)
  - Retention: Removed when memory buffer full
- Storage: Disk (If faults/errors occur)
  - Retention: Oldest Removed after storage exceeded

**Debug – “Development troubleshooting”**
- Storage: Memory (Only if debug logs are enabled)
  - Retention: Removed per configuration

**Error – “Process level errors”**
- Storage: On Disk
- Retention: Oldest Removed after storage exceeded

**Fault – “System level/multi-process errors”**
- Storage: On Disk
- Retention: Oldest Removed after storage exceeded
ON DISK STORAGE [macOS]

- File Paths:
  - `/var/db/diagnostics/`
  - `/var/db/uuidtext`
    (Reference Data)
- Binary Format (*.tracev3)
- `logdata.Persistent.YYYYMMDD THHMMSS.tracev3`
- Tracev3 Files also in:
  - `/FaultsAndErrors/`
  - `/TTL/` (Includes TTL in filename)
- Statistics:
  - `logdata.statistics.0.txt`

```
bash-3.2# pwd
/var/db/diagnostics
bash-3.2# ls -lah
total 215112
drwxr-xr-x  74 root wheel  2.5K Mar  25 03:55 ..
drwxr-xr-x   2 root wheel  68B  Feb  5 23:15 Events
drwxr-xr-x  22 root wheel  748B Mar  25 09:14 FaultsAndErrors
drwxr-xr-x   2 root wheel  68B  Feb  5 23:15 Oversize
drwxr-xr-x   2 root wheel  68B  Feb  5 23:15 SpecialHandling
drwxr-xr-x   2 root wheel  68B  Feb  5 23:15 StateDumps
drwxr-xr-x  15 root wheel  510B Mar  25 09:14 TTL
-rw-r----  1 root wheel  4.8M Mar 16 21:33 logdata.Persistent.20170316T184112.tracev3
-rw-r----  1 root wheel 10M Mar 17 18:03 logdata.Persistent.20170317T013350.tracev3
-rw-r----  1 root wheel  1.4M Mar 17 21:16 logdata.Persistent.20170317T220414.tracev3
-rw-r----  1 root wheel  8.3M Mar 18 20:30 logdata.Persistent.20170318T011647.tracev3
-rw-r----  1 root wheel 10M Mar 19 03:25 logdata.Persistent.20170319T011032.tracev3
-rw-r----  1 root wheel  10M Mar 20 09:28 logdata.Persistent.20170319T074033.tracev3
-rw-r----  1 root wheel  3.5M Mar 20 22:26 logdata.Persistent.20170320T214455.tracev3
-rw-r----  1 root wheel 10M Mar 22 19:42 logdata.Persistent.20170322T222739.tracev3
-rw-r----  1 root wheel 10M Mar 22 20:16 logdata.Persistent.20170322T234321.tracev3
-rw-r----  1 root wheel  1.7M Mar 22 20:47 logdata.Persistent.20170322T232645.tracev3
-rw-r----  1 root wheel 10M Mar 23 18:53 logdata.Persistent.20170323T000500.tracev3
-rw-r----  1 root wheel  1.5M Mar 23 21:15 logdata.Persistent.20170323T225519.tracev3
-rw-r----  1 root wheel 10M Mar 24 18:51 logdata.Persistent.20170324T011606.tracev3
-rw-r----  1 root wheel  6.0M Mar 25 09:13 logdata.Persistent.20170324T225154.tracev3
-rw-r----  1 root wheel  5.7M Mar 25 15:52 logdata.Persistent.20170325T131407.tracev3
-rw-r----  1 root wheel  1.6M Mar 25 15:31 logdata.statistics.0.txt```
REFERENCE DATA

- `/var/db/uuidtext`
- Nested Directory Structure
- Proprietary Format
- Hex Header:
  - 9988 7766 0200 0000 0100 0000 0200 0000
- ASCII Strings:

```
<GSAddition %p ns:"%@" n:"%@" o:0x11>
```

'log' COMMAND OPTIONS

**collect** - Used for log acquisition, bundles into “logarchive” file
  - Filter on timeframe or size

**config** - Edit, review log configuration
  - Can configure mode, system, subsystem, process, category specifics.

**erase** - Remove log data
  - Remove by Time-To-Live (TTL), all, or by error/faults.

**show** - Review logs using file or log archive
  - Filter on predicates, source, timeframe.
  - Different view styles (JSON/Syslog)
  - By default does not show info and debug logs.

**stream** - Live view of log data
  - Filter on level, predicates, processes, source, type
  - Different view styles (JSON/Syslog)
macOS LOG ACQUISITION – ‘log collect’

log collect command will output system_logs.logarchive to current directory.

- Contains packaged *.tracev3 files and referenced data from /var/db/uuidtext/
- ‘Package’ File - shows a single file in Finder, actually a directory.

Can only run ‘log’ command as root.

Import into newer Console.app (10.12)

bit:~ oompa$ log collect
log: Must be root to run 'collect' command
bit:~ oompa$ sudo log collect
Password:
log: INFO: Failed to find 'missing main-exe uuidtext' information for pid 961 and uuid 1DCA009B-249B-3
Archive successfully written to ./system_logs.logarchive
CONSOLE.APP

Default GUI viewer for Mac Logs

• Different than macOS 10.11 and older

Useful for all sorts of forensic analysis

• Import other ASCII-based logs
• Filter/Find by various keywords.

Caution!: If reviewing on live system

• Will only show new new events since Console.app opened.
• Will show messages on disk & in memory (‘Volatile’ column).
macOS LOG ACQUISITION – ‘log show’

log show – On live system, output system logs to standard out, already in temporal order

Perform on *.logarchive, *.tracev3 (file or directory) extracted from image

• By File: *.tracev3 - Not in temporal order – may have to reorder. (See screenshot below)
• By Log Archive: *.logarchive – In temporal order

By default disregards Info and Debug messages

• Use --info and/or --debug for all log messages

Standard Output to Terminal

• --style = (JSON or Syslog Outputs)

<table>
<thead>
<tr>
<th>Time</th>
<th>File</th>
<th>Type</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-22</td>
<td>18:31:35</td>
<td>Activity</td>
<td>739276-0400 0x1486</td>
</tr>
<tr>
<td></td>
<td>18:31:37</td>
<td>Activity</td>
<td>315537-0400 0x3cf0</td>
</tr>
<tr>
<td></td>
<td>18:31:35.744803-0400 0x1486</td>
<td>Activity</td>
<td>0x80000000000039b3</td>
</tr>
<tr>
<td></td>
<td>18:31:37</td>
<td>Activity</td>
<td>321830-0400 0x3b63</td>
</tr>
<tr>
<td></td>
<td>18:31:35.750804-0400 0x17f0</td>
<td>Activity</td>
<td>0x8000000000002287</td>
</tr>
<tr>
<td></td>
<td>18:31:35.750844-0400 0x17c7</td>
<td>Activity</td>
<td>0x800000000002256</td>
</tr>
<tr>
<td></td>
<td>18:31:35.750984-0400 0x17e5</td>
<td>Activity</td>
<td>0x8000000000022d6</td>
</tr>
<tr>
<td></td>
<td>18:31:35.750982-0400 0x17cb</td>
<td>Activity</td>
<td>0x8000000000022a6</td>
</tr>
<tr>
<td></td>
<td>18:31:35.751004-0400 0x17f2</td>
<td>Activity</td>
<td>0x800000000002264</td>
</tr>
<tr>
<td></td>
<td>18:31:35.752327-0400 0x1486</td>
<td>Activity</td>
<td>0x8000000000040aa</td>
</tr>
<tr>
<td></td>
<td>18:31:42.346579-0400 0x3b63</td>
<td>Default</td>
<td>0x0</td>
</tr>
</tbody>
</table>

453
'log show' COMMAND

bash-3.2# log show logdata.Persistent.20170324T011606.tracev3
=========
/private/var/db/diagnostics/logdata.Persistent.20170324T011606.tracev3
=========

Skipping info and debug messages, pass --info and/or --debug to include.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Thread</th>
<th>Type</th>
<th>Activity</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-22 18:27:39</td>
<td>0x3b5</td>
<td>Default</td>
<td>0x0</td>
<td>119</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WindowServer: (SkyLight) [com.apple.SkyLight.default] Server is starting up</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x2a0</td>
<td>Activity</td>
<td>0x80000000000000130</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreFoundation) Loading Preferences From System CFPreferences ');</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x2a0</td>
<td>Activity</td>
<td>0x80000000000000130</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.AirPlayEndpointManagerFactory]</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x3c7</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.WiFiManagerCore] 2017-03-22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ParamErr</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x3c7</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APTTransportTrafficRegistrar] y traffic for AIDL at MAC 00:00:00:00:00:00 with target infra non critical PeerIndication=0 err=-3900</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x3c7</td>
<td>Error</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APSLogUtils] 2017-03-22 06:2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-3900/0xFFFFFF0C4 KA11ParamErr</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x3c7</td>
<td>Error</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APSLogUtils] 2017-03-22 06:2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0/0xFFFFFF0C4 KA11ParamErr</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x3c7</td>
<td>Error</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APSLogUtils] 2017-03-22 06:2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FFFF0C4 KA11ParamErr: APTTransportTrafficRegistrar: reset registration failed</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x2a0</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (libsystem_trace.dylib) subsystem: com.apple.bluetooth, call 0, debug_ttl: 0, generate_symptoms: 0, enable_oversize: 1, privacy_setting: 2, enable_private_data: 0</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x2a0</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (BluetoothAudio) [com.apple.bluetooth.BTFileE] Add Listeners</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x2a0</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (BluetoothAudio) [com.apple.bluetooth.BTFileE] Created Blue</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x2a0</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.AirPlayMain] 2017-03-22 06:2</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x3c5</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (BluetoothAudio) [com.apple.bluetooth.BTFileE] Starting LE</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x3c5</td>
<td>Activity</td>
<td>0x80000000000000131</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (CoreFoundation) Loading Preferences From System CFPreferencesE</td>
</tr>
<tr>
<td>2017-03-22 18:27:40</td>
<td>0x2a0</td>
<td>Default</td>
<td>0x0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AirPlayXPCHelper: (libsystem_trace.dylib) subsystem: com.apple.coreaudio, call 0, debug_ttl: 0, generate_symptoms: 0, enable_oversize: 1, privacy_setting: 2, enable_private_data: 0</td>
</tr>
</tbody>
</table>
iDEVICE - LOG ACQUISITION

- Devices:
  - iOS
  - watchOS
  - tvOS
- ‘sysdiagnosis’ utility – key-chords for each devices
- Console.app
- More researched needed to see if useful for forensic analysis
ON DISK STORAGE [iOS]
/private/var/db/ [diagnostics & uuidtext]

```
miPhone7:/private/var/db root# ls
FIPS UpdateMetrics dhcpclient fud roldd timezone
MobileIdentityData astras dhcpdleases icutz spindump uuidtext
PanicReporter com.apple.xpc.launchd diagnostics lsd stash
PlugInKit-Annotations datadetectors findmydevice ondemand systemstats
miPhone7:/private/var/db root# ls -l diagnostics/
total 103812
drwxr-xr-x 2 root wheel 68 Sep  5 2016 Events
drwxr-xr-x 2 root wheel 544 Mar 30 21:34 FaultsAndErrors
drwxr-xr-x 2 root wheel 68 Sep  5 2016 Oversize
drwxr-xr-x 2 root wheel 68 Sep  5 2016 SpecialHandling
drwxr-xr-x 2 root wheel 68 Sep  5 2016 StateDumps
drwxr-xr-x 2 root wheel 340 Mar 30 20:06 TTL
-rw-r----- 1 root wheel 10518228 Mar 30 09:36 logdata.Persistent.20170330T122803.tracev3
-rw-r----- 1 root wheel 10491888 Mar 30 12:02 logdata.Persistent.20170330T133622.tracev3
-rw-r----- 1 root wheel 10494920 Mar 30 14:18 logdata.Persistent.20170330T160253.tracev3
-rw-r----- 1 root wheel 10555944 Mar 30 17:17 logdata.Persistent.20170330T181909.tracev3
-rw-r----- 1 root wheel 10522152 Mar 30 18:15 logdata.Persistent.20170330T211755.tracev3
-rw-r----- 1 root wheel 10612312 Mar 30 19:36 logdata.Persistent.20170330T221544.tracev3
-rw-r----- 1 root wheel 5936984 Mar 30 20:04 logdata.Persistent.20170330T233632.tracev3
-rw-r----- 1 root wheel 10501704 Mar 30 21:19 logdata.Persistent.20170331T000604.tracev3
-rw-r----- 1 root wheel 8750692 Mar 30 21:28 logdata.Persistent.20170331T011926.tracev3
-rw-r----- 1 root wheel 3616984 Mar 30 21:29 logdata.Persistent.20170331T012906.tracev3
-rw-r----- 1 root wheel 6783728 Mar 30 21:33 logdata.Persistent.20170331T013013.tracev3
-rw-r----- 1 root wheel 4971560 Mar 30 21:37 logdata.Persistent.20170331T013343.tracev3
-rw-r----- 1 root wheel 407434 Mar 30 21:36 logdata.statistics.0.txt
-rw-r----- 1 root wheel 2097523 Mar 29 18:48 logdata.statistics.1.txt
-rw-r-r-- 1 root wheel 7503 Mar 29 14:05 shutdown.log
```
UNIFIED LOG ANALYSIS
LOG FORMAT
DEFAULT 'log' COMMAND' OUTPUT

Timestamp [YYYY-MM-DD HH:MM:SS.ssssss-TZ]
Thread ID 0x26b2c3
Log Level Type (Default, Info, Debug, Error, Fault)
Activity ID 0x8000000000097d26
Activity Info TimeMachine
PID 14929
Process Name [com.apple.TimeMachine.TMLogInfo]
Starting manual backup
Library
Subsystem
Category
Message
Predicate Filtering

Filter log events using logical statements (AND/OR/NOT/<>/=/CONTAINS/BEGINSWITH/TRUE/FALSE, etc)

- **eventType** – Filters on Event Types (Log, Trace, Activity)
- **eventMessage** – Filters on message text or Activity Name (if log/trace event)
- **messageType** – Filters on Log Level (Default, Info, Debug, Error, Fault)
- **processImagePath** – Filters on the process name of the event originator
- **senderImagePath** – Filters on sender name of the event originator (Library, framework, kext, mach-o binary)
- **subsystem** – Filters on subsystem (reverse DNS ID)
- **category** – Filters on subsystem category

Skipping debug messages, pass --debug to include.

Filling the log data using "processImagePath CONTAINS[cd] "backupd" and category CONTAINS[cd] "TLogInfo" and eventMessage CONTAINS "Starting" --start "2017-03-25 15:00:00"

[cd] = Ignore case/diacritics
CONSOLATION - 3rd PARTY GUI ANALYSIS TOOL
ECLECTICLIGHT.CO/DOWNLOADS/
### NON-VOLATILE VS. VOLATILE MESSAGES

The table below illustrates the differences between non-volatile and volatile messages in the context of DNS queries and responses:

<table>
<thead>
<tr>
<th>Message</th>
<th>Volatile</th>
<th>Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>-- Sent UDP DNS Query (flags 0100) RCODE: NoErr (0) RD ID: 6517 19 bytes from port 56026 to 2601:01...</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>1 Questions</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>0 d.dropbox.com. AAAA</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>0 Answers</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>0 Authorities</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>0 Additions</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>-----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 11920 69 bytes from 2601:0141...</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>1 Questions</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>0 d.dropbox.com. Addr</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>3 Answers</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
<tr>
<td>0 TTL 76 17 d.dropbox.com. CNAME d.v.dropbox.com.</td>
<td>1</td>
<td>com.apple.mDNS_</td>
</tr>
</tbody>
</table>

The table highlights the number of messages and their corresponding subsystems, showing the differences between volatile and non-volatile messages in terms of their movement and the context in which they are exchanged.
POTENTIAL FOR MEMORY ANALYSIS

- Look in the ‘diagnostic’d process

<table>
<thead>
<tr>
<th>Message</th>
<th>Volatile</th>
<th>Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Received UDP DNS Response</strong> (flags 8180) RCODE: NoErr (0) RD RA ID: 11920 69 bytes from 2601:0141:0302:1F30:0200:9FF:FE34:1C00:53</td>
<td>1</td>
<td>com.apple.mDNS..</td>
</tr>
</tbody>
</table>

1 Questions
0 d.dropbox.com. Addr
3 Answers
0 TTL 76 17 d.dropbox.com. CNAME d.v.dropbox.com.
ANALYSIS CAVEATS
USER LOGINS
OLD METHOD - SYSTEM.LOG

Local Terminal
- May 28 15:07:29 byte login[812]: USER_PROCESS: 812 ttys002
- May 28 15:07:51 byte login[812]: DEAD_PROCESS: 812 ttys002

Login Window
- May 28 12:42:23 byte loginwindow[66]: DEAD_PROCESS: 74 console
- May 28 14:28:04 byte loginwindow[66]: USER_PROCESS: 60 console

SSH
- May 28 15:15:38 byte sshd[831]: USER_PROCESS: 842 ttys002
- May 28 15:15:52 byte sshd[831]: DEAD_PROCESS: 842 ttys002
USER LOGINS
UNIFIED LOGS

- All “logout” events in unified logs - where are the user “login” events?

```
bite:LogsUnite compa$ log show --info --predicate 'eventMessage contains "_PROCESS"' --last 3d
Skipping debug messages, pass --debug to include.
Filtering the log data using "eventMessage CONTAINS "_PROCESS""

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Thread</th>
<th>Type</th>
<th>Activity</th>
<th>PID</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-29 21:53:31.760265-0400 0x2b86682 Default 0x0</td>
<td>16267</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 16267 ttys003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-29 21:53:45.153336-0400 0x2bae70 Default 0x0</td>
<td>18093</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 18093 ttys004</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-29 21:53:50.122238-0400 0x2bd35 Default 0x0</td>
<td>18199</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 18199 ttys005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-29 21:53:53.366367-0400 0x2c82e2 Default 0x0</td>
<td>18439</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 18439 ttys006</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-30 22:23:01.973781-0400 0x3827e9 Default 0x0</td>
<td>25435</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 25435 ttys004</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-30 22:23:03.093753-0400 0x3b2a1d Default 0x0</td>
<td>25449</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 25449 ttys005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:01:18.641809-0400 0x3b9190 Default 0x0</td>
<td>27046</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 27046 ttys005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:01:59.652285-0400 0x3b9351 Default 0x0</td>
<td>27076</td>
<td>sshd: (libsystem_c.dylib) DEAD_PROCESS: 27076 ttys005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:08:01.182684-0400 0x136a47 Default 0x0</td>
<td>10018</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 10018 ttys000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:08:01.301243-0400 0x136d3d Default 0x0</td>
<td>10021</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 10021 ttys001</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:08:01.377587-0400 0x14a9e9 Default 0x0</td>
<td>10076</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 10076 ttys002</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:08:01.479821-0400 0x33f3f9 Default 0x0</td>
<td>23375</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 23375 ttys003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:08:01.573287-0400 0x386e88 Default 0x0</td>
<td>25613</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 25613 ttys006</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:08:01.677944-0400 0x3b8d8a Default 0x0</td>
<td>27029</td>
<td>login: (libsystem_c.dylib) DEAD_PROCESS: 27029 ttys004</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-03-31 12:08:55.123852-0400 0x3ba6d9 Default 0x0</td>
<td>27221</td>
<td>sessionlogoud: (libsystem_c.dylib) DEAD_PROCESS: 94 console</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
USER LOGINS
GOING OLD SKOOL - SYSTEM.LOG

Mar 31 12:00:37 bit login[27029]: USER_PROCESS: 27029 ttys004
Mar 31 12:01:16 bit login[27046]: USER_PROCESS: 27046 ttys005
Mar 31 12:01:50 bit sshd: oompa [priv][27076]: USER_PROCESS: 27079 ttys005
Mar 31 12:09:05 bit loginwindow[27228]: USER_PROCESS: 27228 console
Mar 31 12:09:43 bit login[27456]: USER_PROCESS: 27456 ttys000
Mar 31 12:09:43 bit login[27466]: USER_PROCESS: 27466 ttys001
Mar 31 12:09:43 bit login[27476]: USER_PROCESS: 27476 ttys002
Mar 31 12:09:43 bit login[27486]: USER_PROCESS: 27486 ttys003
Mar 31 12:09:43 bit login[27496]: USER_PROCESS: 27496 ttys004
Mar 31 12:09:44 bit login[27506]: USER_PROCESS: 27506 ttys005
log show system_logs.logarchive/ --predicate 'senderImagePath contains[cd]' "TimeMachine" --info --start "2017-03-31 06:58:42"

bit:logunite compa log show system_logs.logarchive/ --predicate 'senderImagePath contains[cd]' "TimeMachine" --info --start "2017-03-31 06:58:42"

Skipping debug messages, pass --debug to include.

Filtering the log data using "senderImagePath CONTAINS[cd]" "TimeMachine"

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Thread</th>
<th>Type</th>
<th>Activity</th>
<th>PID</th>
<th>Pid</th>
<th>Pid</th>
<th>Pid</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-31 06:58:42</td>
<td>29956</td>
<td>backup:</td>
<td>(TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting automatic backup</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
</tr>
<tr>
<td>2017-03-31 06:58:42</td>
<td>29956</td>
<td>info</td>
<td>(TimeMachine) [com.apple.TimeMachine.TMLogInfo] Attempting to mount network destination URL: afp://SarahMG2Edwards/AUTH=SPRPPDoleane_.afpovertcp _.tcp.local./Data</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
</tr>
<tr>
<td>2017-03-31 06:58:42</td>
<td>29956</td>
<td>info</td>
<td>(TimeMachine) [com.apple.TimeMachine.TMLogInfo] Mounted network destination at mount point: /Volumes/Data using URL: afp://SarahMG2Edwards/AUTH=SPRPPDoleane_.afpovertcp _.tcp.local./Data</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
</tr>
<tr>
<td>2017-03-31 06:58:42</td>
<td>29956</td>
<td>error</td>
<td>(TimeMachine) [com.apple.TimeMachine.TMLogError] - [FileAttr.setAttributesToDeleteAtPath: ] setattrlist failed for path '/MobileBackups/Computer/2017-03-31-065844/Volume/Library/Preferences' (errno 1)</td>
<td>188</td>
<td>188</td>
<td>188</td>
<td>188</td>
</tr>
<tr>
<td>2017-03-31 06:58:42</td>
<td>29956</td>
<td>error</td>
<td>(TimeMachine) [com.apple.TimeMachine.TMLogError] - [FileAttr.setAttributesToDeleteAtPath: ] setattrlist failed for path '/MobileBackups/Computer/2017-03-31-065844/Volume/Library/Preferences/SystemConfiguration' (errno 1)</td>
<td>188</td>
<td>188</td>
<td>188</td>
<td>188</td>
</tr>
<tr>
<td>2017-03-31 06:58:42</td>
<td>29956</td>
<td>info</td>
<td>(TimeMachine) [com.apple.TimeMachine.TMLogInfo] Checking for runtime corruption on /dev/disk2s2</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
</tr>
<tr>
<td>2017-03-31 06:58:42</td>
<td>29956</td>
<td>info</td>
<td>(TimeMachine) [com.apple.TimeMachine.TMLogInfo] Can't trash_MobileBackups while MDM Snapshot Handler is running!</td>
<td>188</td>
<td>188</td>
<td>188</td>
<td>188</td>
</tr>
</tbody>
</table>
TIME MACHINE BACKUPS
A CASE FOR ‘--info’
TIME MACHINE BACKUPS
START & END TIMES

• Start/End Filter

log show system_logs.logarchive/ -- predicate 'senderImagePath contains[cd] "TimeMachine"' --info --start "2017-03-31 06:58:42"

• What if I want to slice it?

log show system_logs.logarchive/ -- predicate 'senderImagePath contains[cd] "TimeMachine"' --info --start "2017-03-31 06:58:42" --end "2017-03-31 07:04:24"
log show system_logs.logarchive/ --predicate 'senderImagePath contains[cd] "TimeMachine"' --info --start "2017-03-31 06:58:42" --end "2017-03-31 07:04:24"
TIME MACHINE BACKUPS

BUG/FEATURE?

log show system_logs.logarchive/ --predicate 'senderImagePath contains[cd] "TimeMachine"' --info --start "2017-03-31 06:58:42" --end "2017-03-31 07:05:00"

```
LOG show system_logs.logarchive/ --predicate 'senderImagePath contains[cd] "TimeMachine"' --info --start "2017-03-31 06:58:42" --end "2017-03-31 07:05:00"

Skipping debug messages, pass --debug to include.
```

Filtering the log data using "senderImagePath CONTAINS[cd] "TimeMachine""

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Thread</th>
<th>Type</th>
<th>Activity</th>
<th>PID</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-31 06:58:42.361177-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 06:58:42.394647-0000</td>
<td>0x65d</td>
<td>Info 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 06:58:42.459650-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 06:58:42.463767-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 06:58:42.463812-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 06:58:42.471348-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 06:58:42.894362-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:00:06.982232-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:00:06.986335-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:00:06.989509-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:01:29.222868-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:02:25.909215-0000</td>
<td>0x3e9e5a</td>
<td>Error 0x0</td>
<td>mntd: (TimeMachine)</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:02:26.976615-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:02:26.810709-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:02:42.570843-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:02:42.581648-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:02:42.594372-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:04:02.795615-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:04:08.837333-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:04:08.354206-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:04:24.769984-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:04:24.770117-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
<tr>
<td>2017-03-31 07:04:24.977374-0000</td>
<td>0x3e9e5a</td>
<td>Info 0x0</td>
<td>backup: (TimeMachine)</td>
<td>25956</td>
<td></td>
</tr>
</tbody>
</table>

End of log show output.
TIMEZONE CHANGE VIA LOCATIOND
HINTS OF TIME CHANGES
• …many hundreds of entries later…

• Really only ~17 seconds

• Always look within context, even before/after hundreds of entries!
OTHER INTERESTING EXAMPLES
log show --info --predicate 'senderImagePath contains[cd] "IPConfiguration" and (eventMessage contains[cd] "SSID" or eventMessage contains[cd] "Lease" or eventMessage contains[cd] "network changed")'

Removing stale Lease 172.19.131.167 Router 172.19.131.17

DHCP en0: status = 'network changed'
DHCP bridge0: status = 'network changed'
en0: no SSID
DHCP en0: status = 'network changed'
en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
DHCP en0: status = 'network changed'
en0: SSID is now hhonors (was United_Wi-Fi)
en0: No lease for hhonors
DHCP en0: status = 'network changed'
en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
DHCP en0: status = 'network changed'
en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
DHCP en0: status = 'network changed'
en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
DHCP en0: status = 'network changed'
en0: Automatic-Vo en0: status = 'network changed'
en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
DHCP en0: status = 'network changed'
en0: No lease for hhonors
ignoring lease with SSID station
DHCP en0: ARP router: No leases to query for
ignoring lease with SSID station
DHCP en0: ARP router: No leases to query for
ignoring lease with SSID station
DHCP en0: ARP router: No leases to query for
ignoring lease with SSID station
DHCP en0: ARP router: No leases to query for
ignoring lease with SSID station
DHCP en0: ARP router: No leases to query for
ignoring lease with SSID station
DHCP en0: ARP router: No leases to query for
ignoring lease with SSID station
DHCP en0: ARP router: No leases to query for
ignoring lease with SSID station
DHCP en0: INIT lease = { start 0xe8f0a9a, t1, 0xe8f0aa, t2, 0xe8f0aa, expiration 0xe8f0aa }
FIND USER DEVICES WITH SECD

log show --info --predicate 'subsystem contains[cd] "com.apple.securityd" and category contains[cd] "log"'

Default secd: [com.apple.securityd.accountLogState] Start
Default secd: [com.apple.securityd.accountLogState] Peers In Circle:
Default secd: [com.apple.securityd.accountLogState] PI: [name: Sarah's Macbook Air] [mASrKv] [type: MacBook Air] [spid: ] [os: 1501044] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: byte] [mASrKv] [type: Mac mini] [spid: ] [os: 1501045] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: word] [mASrKv] [type: MacBook Pro] [spid: ] [os: 1501046] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: Mini miPad4] [mASrKv] [type: iPad] [spid: ] [os: 14A485] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: bit] [mASrKv] [type: MacBook Pro] [spid: ] [os: 166279] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: word] [mASrKv] [type: MacBook Pro] [spid: ] [os: Unknown] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: bit] [mASrKv] [type: MacBook Pro] [spid: ] [os: 160308] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: Mini miPad] [mASrKv] [type: iPad] [spid: ] [os: 14C92] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: nibble] [mASrKv] [type: MacBook Air] [spid: ] [os: Unknown] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: iPhone] [mASrKv] [type: iPhone] [spid: ] [os: 13034] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: iPhone] [mASrKv] [type: iPhone] [spid: ] [os: Unknown] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: Sarah's Macbook Pro] [mASrKv] [type: MacBook Pro] [spid: ] [os: 16B2657] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: word] [mASrKv] [type: MacBook Pro] [spid: ] [os: 16B2556] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: nibble (2)] [mASrKv] [type: MacBook Air] [spid: ] [os: Unknown] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: iPhon3] [mASrKv] [type: iPhone] [spid: ] [os: 14B100] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: word] [mASrKv] [type: MacBook Pro] [spid: ] [os: 15842] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] PI: [name: Sarah's Macbook Air] [mASrKv] [type: MacBook Air] [spid: ] [os: 16A323] [devid: ] [serial: ]
Default secd: [com.apple.securityd.accountLogState] Rejected Applicants To Circle: None
Default secd: [com.apple.securityd.accountLogState] Sync: IB PeerViews: (AccessoryPairing, AppleTV, BackupBagV0, ContinuityUnlock, CreditCards, HomeKit, OtherSyncable, PCS-Backup, PCS-CloudKit, PCS-Encrow, interkeyring, PCS-iCloudDrive, PCS-iMessage, Passwords, WiFi, iCloudIdentity)
Default secd: [com.apple.securityd.accountLogState] outstanding views: null
Default secd: [com.apple.securityd.accountLogState] Finish
FIND USER DEVICES WITH SECD

log show --info --predicate 'subsystem contains[cd] "com.apple.securityd" and category contains[cd] "log"'

Start
ACCOUNT: [keyStatus: [SOSCCStatus: kSOSCCInCircle]
Peers In Circle:
PI: [name: Sarah's MacBook Air] [mASrbKv] [type: MacBook Air ] [spid: ] [os: 15G1004] [devid: ] [serial: ]
PI: [name: byte ] [mASrbKv] [type: Mac mini ] [spid: ] [os: 15E665] [devid: ] [serial: ]
PI: [name: word ] [mASrbKv] [type: MacBook Pro ] [spid: ] [os: 15G1004] [devid: ] [serial: ]
PI: [name: Mini miPad4] [mASrbKv] [type: iPad ] [spid: ] [os: 14A463] [devid: ] [serial: ]
PI: [name: bit ] [mASrbKv] [type: MacBook Pro ] [spid: ] [os: 16C67] [devid: ] [serial: ]
PI: [name: word ] [mASrbKv] [type: MacBook Pro ] [spid: ] [os: Unknown ] [devid: ] [serial: ]
PI: [name: mPHONE6] [mASrbKv] [type: iPhone ] [spid: ] [os: 13A452] [devid: ] [serial: ]
PI: [name: bit ] [mASrbKv] [type: MacBook Pro ] [spid: ] [os: 16D30] [devid: ] [serial: ]
PI: [name: nibble ] [mASrbKv] [type: iPad ] [spid: ] [os: 14C92] [devid: ] [serial: ]
PI: [name: iPhone ] [mASrbKv] [type: MacBook Air ] [spid: ] [os: Unknown ] [devid: ] [serial: ]
PI: [name: mPHONE65a] [mASrbKv] [type: iPhone ] [spid: ] [os: 13G34 ] [devid: ] [serial: ]
PI: [name: Sarah's MacBook Pro ] [mASrbKv] [type: MacBook Pro ] [spid: ] [os: 16B2657] [devid: ] [serial: ]
PI: [name: word ] [mASrbKv] [type: MacBook Pro ] [spid: ] [os: 16B2555] [devid: ] [serial: ]
PI: [name: nibble (2) ] [mASrbKv] [type: MacBook Air ] [spid: ] [os: Unknown ] [devid: ] [serial: ]
PI: [name: mPHONE7] [mASrbKv] [type: iPhone ] [spid: ] [os: 14B100 ] [devid: ] [serial: ]
PI: [name: word ] [mASrbKv] [type: MacBook Pro ] [spid: ] [os: 15B42 ] [devid: ] [serial: ]
PI: [name: Sarah's MacBook Air] [mASrbKv] [type: MacBook Air ] [spid: ] [os: 16A323] [devid: ] [serial: ]
Applicants To Circle: None
Rejected Applicants To Circle: None
Sync: IB PeerViews: {(AccessoryPairing, AppleTV, BackupBagV0, ContinuityUnlock, CreditCards, HomeKit, OtherSyncable, PCS-Backup, PCS-CloudKit, PCS-Escrow, s, WiFi, iCloudIdentity)}
outstanding views: null
Finish
LOOK UP ‘os’ & ‘serial’ FIELDS

14A403

is build 14A403 the final release? | Official Apple Support ...
https://discussions.apple.com/thread/7665841?start=0&tstart=0 ▼
Sep 14, 2016 - iPhone. Sep 14, 2016 1:38 PM in response to spartucus49. I have never installed a beta and upgraded from 9.3.5 and have 10.0.1(14A403).

airdrop wont work : iphone6s+ 10.0.1 (14A403) - Apple Support ...
Oct 13, 2016
iOS 10 iPhone SS
Sep 13, 2016

iOS 10.0.1 Information - IPSW Downloads
https://ipsw.me/10.0.1 ▼
iPad 4 (WiFi) (iPad3r3), iOS 10.0.1 (14A403), 09/13/2016, iPad_32bit_10.0.1_14A403_Restore.ipsw, 1.9 GB, MD5: 08a53aead4f51755656f062358b324

Your Service and Support Coverage

iPad mini 4 Wi-Fi, Cellular

Valid Purchase Date
A validated purchase date lets Apple quickly find your product and provide the help you need.

Telephone Technical Support: Expired
You are eligible to purchase telephone technical support from an Apple Advisor.
Contact Apple Support >

Repairs and Service Coverage: Expired
Our records indicate that your product is not covered under Apple’s Limited warranty or an AppleCare product (hardware repairs and service based on the terms and conditions of your warranty or service plan).
EXTERNAL MEDIA

...OR PRINTERS AND PHONES!
EMAIL
ACCOUNTS & SYNCING

log show --info system_logs.logarchive/ --predicate 'subsystem = "com.apple.mail" and (category = "AccountFetch" or category = "IMAPSyncActivity")'

Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs] Removing handler (0x6000008f6b00)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs] Removing handler (0x6000008f6b00)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs - Archive] Reset mailbox in sync state
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs - Archive] Reset mailbox in sync state
Mail: (Mail) [com.apple.mail.AccountFetch] <stedefx@gmail.com>imap.gmail.com> Background fetch completed
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs - Archive] <Sync> Created mailbox sync task
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs - Archive] <Sync> Recalculated priorities - network: 22, persistence: 0
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs] Creating account sync task, 7 mailboxes needing status
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [Google] Removing handler (0x6000008e7200)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [Google] Removing handler (0x6000008e7200)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [Google - Archive] Reset mailbox in sync state
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [Google - Archive] Reset mailbox in sync state
Mail: (Mail) [com.apple.mail.AccountFetch] <stedefx@gmail.com>imap.gmail.com> Background fetch completed
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [Google - Archive] <Sync> Created mailbox sync task
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [Google - Archive] <Sync> Recalculated priorities - network: 22, persistence: 0
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing account sync task, 15 mailboxes needing status
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing handler (0x600000ef9280)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing handler (0x600000af6080)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing handler (0x600000ef9280)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud - Inbox] Reset mailbox in sync state
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud - Inbox] Remove mailbox in sync state
Mail: (Mail) [com.apple.mail.AccountFetch] <compa@csch.rit.edu>imap.me.com> Background fetch completed
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud - Inbox] <Sync> Created mailbox sync task
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud - Inbox] <Sync> Recalculated priorities - network: 22, persistence: 0
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Creating account sync task, 7 mailboxes needing status
USER LOGINS
via APPLE WATCH

log show --info system_logs.logarchive/ --predicate 'subsystem = "com.apple.sharing" and category = "AutoUnlock"'

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>PID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-31 18:28:00.674247-0400</td>
<td>27228</td>
<td>loginwindow: (Sharing) [com.apple.sharing.AutoUnlock] Dynamic store enabled state { 581 = 1; }</td>
</tr>
<tr>
<td>2017-03-31 18:28:00.764337-0400</td>
<td>27339</td>
<td>sharingd: [com.apple.sharing.AutoUnlock] Invalidating hint provider</td>
</tr>
<tr>
<td>2017-03-31 18:28:00.764805-0400</td>
<td>27339</td>
<td>sharingd: [com.apple.sharing.AutoUnlock] Received screen lock unlocked notification</td>
</tr>
<tr>
<td>2017-03-31 18:28:00.764912-0400</td>
<td>27339</td>
<td>sharingd: [com.apple.sharing.AutoUnlock] Invalidating hint provider</td>
</tr>
<tr>
<td>2017-03-31 18:28:01.017959-0400</td>
<td>27339</td>
<td>sharingd: [com.apple.sharing.AutoUnlock] Enabled dictionary exists { 581 = 1; }</td>
</tr>
</tbody>
</table>
### USER LOGINS VIA APPLE WATCH

**DEVICE INFORMATION**

```
log show --info system_logs.logarchive/ --predicate 'subsystem = "com.apple.sharing" and category = "AutoUnlock" and eventMessage contains[cd] "Found Peer"
```

```

/Users/oomps/Dropbox (Personal)/LogsUnite/system_logs.logarchive

Skipping debug messages, pass --debug to include.

Filtering the log data using "subsystem == "com.apple.sharing" AND category == "AutoUnlock" AND eventMessage CONTAINS[cd] "Found Peer"

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Device Model</th>
<th>Unique ID</th>
<th>Bluetooth ID</th>
<th>Model Identifier</th>
<th>Device Name</th>
<th>RSSI</th>
<th>Paired</th>
<th>Proxy Unlock Enabled</th>
<th>Locked on Wrist</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-23 21:15:58.940782-0400 0x5e716</td>
<td>iPhone 7</td>
<td>F9B65FFC-2BC6-4E80-93DA-67508472C8F</td>
<td>F768D25B-1EC8-476B-B4A3-D757890CD2EB</td>
<td>iPhone9,3</td>
<td>miPhone7</td>
<td>-47</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>2017-03-23 21:16:00.086856-0400 0x5e716</td>
<td>Watch Series 1</td>
<td>47B476E2-6876-4D3D-B678-A24305AF1A21</td>
<td>C905A733-BEA0-4680-A41F-4DCDF577A899</td>
<td>Watch2,3</td>
<td>miWatch</td>
<td>-38</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>
```

```
• man log on macOS
• https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/Predicates/AdditionalChapters/Introduction.html
• https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/Predicates/Articles/pBNF.html
• https://eclecticlight.co/2016/10/17/log-a-primer-on-predicates/
• https://eclecticlight.co/2016/10/01/using-the-logs-in-sierra-some-practical-tips/
• https://eclecticlight.co/downloads/
• https://www.objc.io/issues/19-debugging/activity-tracing/