LOGS UNITE!
FORENSIC ANALYSIS OF APPLE UNIFIED LOGS

Sarah Edwards

@iamevltwin | oompa@csh.rit.edu | mac4n6.com

04/01/2017

WHERE WE CAME FROM

Apple System Logs (ASL, syslog)

- /var/log/asl/
- Binary Format
- MacOS, limited on iOS

Unix Logs (syslog)

- /var/log/
- ASCII/Compressed ASCII
- MacOS, limited on iOS

Basic Security Module (BSM) Audit Logs

- /var/audit/
- Binary Format
- MacOS

Check out my 'Analysis & Correlation of Mac Logs' Presentation!

- mac4n6.com/resources

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)

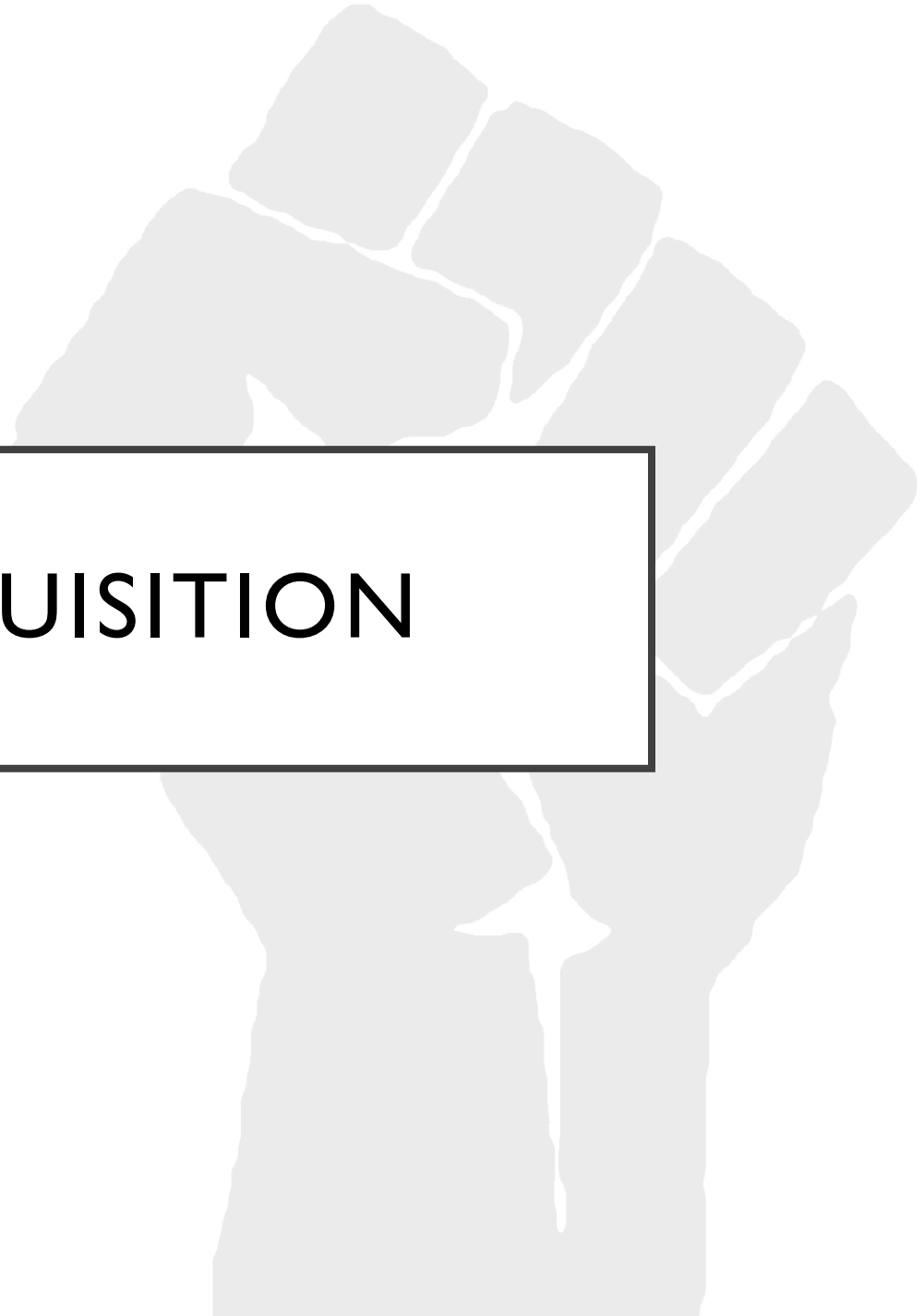
Similar Storage Locations

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.YYYYMMDDTHHMMSS.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-x---  24 root  wheel   816B Mar 25 09:14 .
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.20170320T141455.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.20170323T001645.tracev3
-rw-r-----   1 root  wheel    10M Mar 23 18:53 logdata.Persistent.20170323T005000.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:

```
bit:00 oompa$ strings BF8427967F3693A86FDA0F29B49BF3
%s:%i %s (on %s)
com.apple.
invalid NameSpace value
/BuildRoot/Library/Caches/com.apple.xbs/Sources/Gener
%@; status %d
invalid OnDuplicate value
invalid Name value
invalid options
PerUID
<GSAddition %p ns:"%@" n:"%@" o:%llx>
```

```
bit:uuidtext oompa$ pwd
/var/db/uuidtext
bit:uuidtext oompa$ tree -hu -L 4 .
.
├── [root      374]  00
│   ├── [root     3.6M]  35C17FEC2C33F48FB8DBCF8CA35C49
│   ├── [root     3.3K]  5166989E3833D289D243E6085C12F4
│   ├── [root      309]  5500A56B8937EE95AA79322B79C70D
│   ├── [root      15K]  922D3DA4C03273B50E989BAD3E00BD
│   ├── [root      16K]  9806B8B985304FB7CF636A50A2175B
│   ├── [root     7.8K]  BF8427967F3693A86FDA0F29B49BF3
│   ├── [root     9.2K]  D74B29F44B336CBC64480826B73EC4
│   ├── [root      65K]  F00E7E7EF4325486D3ADA4F67938CF
│   └── [root     2.9K]  F166FDCFFB399E968EC76D045D841C
├── [root      238]  01
│   ├── [root     8.2K]  0A0DA64D0C3B45B0456B0FD49E565C
│   ├── [root     2.4K]  105CC70858300FABC08FC53CAD7221
│   ├── [root      765]  62A103977B3D87A16192C63344A912
│   ├── [root      253]  9FAD844365304791B7BBF10541C371
│   └── [root      42K]  C3486071B536DDA9D04A6C272CE04B
├── [root      238]  02
│   ├── [root      15K]  072FC1649C3EC4BFE2B7D2E4095E95
│   ├── [root     10.0K]  2A136564A337959BAAB942733AF417
│   ├── [root       45]  9A79A0CF3032E9A5FA727F56E7722F
│   ├── [root     2.6K]  A952C23F26353997119996E6CE4A44
│   └── [root      42K]  CD62120A893BB5888C07B5E1F0A90A
├── [root      408]  03
│   ├── [root     3.2K]  1AE0424E5431468B95A3C0BE9477AA
│   ├── [root     2.8K]  5B708AB4933803B5D3FC83BECDC654
│   ├── [root      25K]  5F139864BB33C9A18CC15D60AB2D29
│   ├── [root     1.5K]  6702F4CA5636EA9720BF9E822C1A7F
│   ├── [root      15K]  7FC6FA6FB235849DD0145D468013C9
│   ├── [root     2.3K]  844A3AAB6E3370B92CCECE41347766
│   ├── [root      28K]  8612AE3813304AA5C786F1361F77CC
│   ├── [root     8.8K]  9984675D1E3C07AD4C16740C50DE92
│   ├── [root      141]  B1BDD0BD1B32AAB8100A1C77630942
│   └── [root     1.2K]  E0AA4694D63365B00FC693808F76EE
```

‘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.

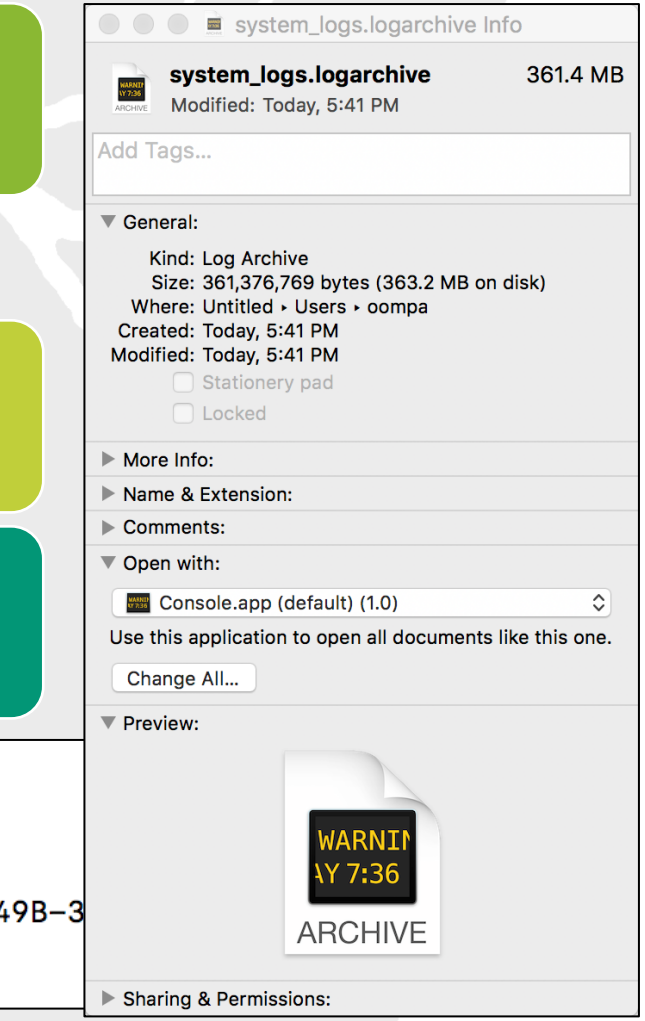
- Contains packaged *.tracev3 files and referenced data from /var/db/uuidtext/
- 'Package' File - shows a a single file in Finder, actually a directory.

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

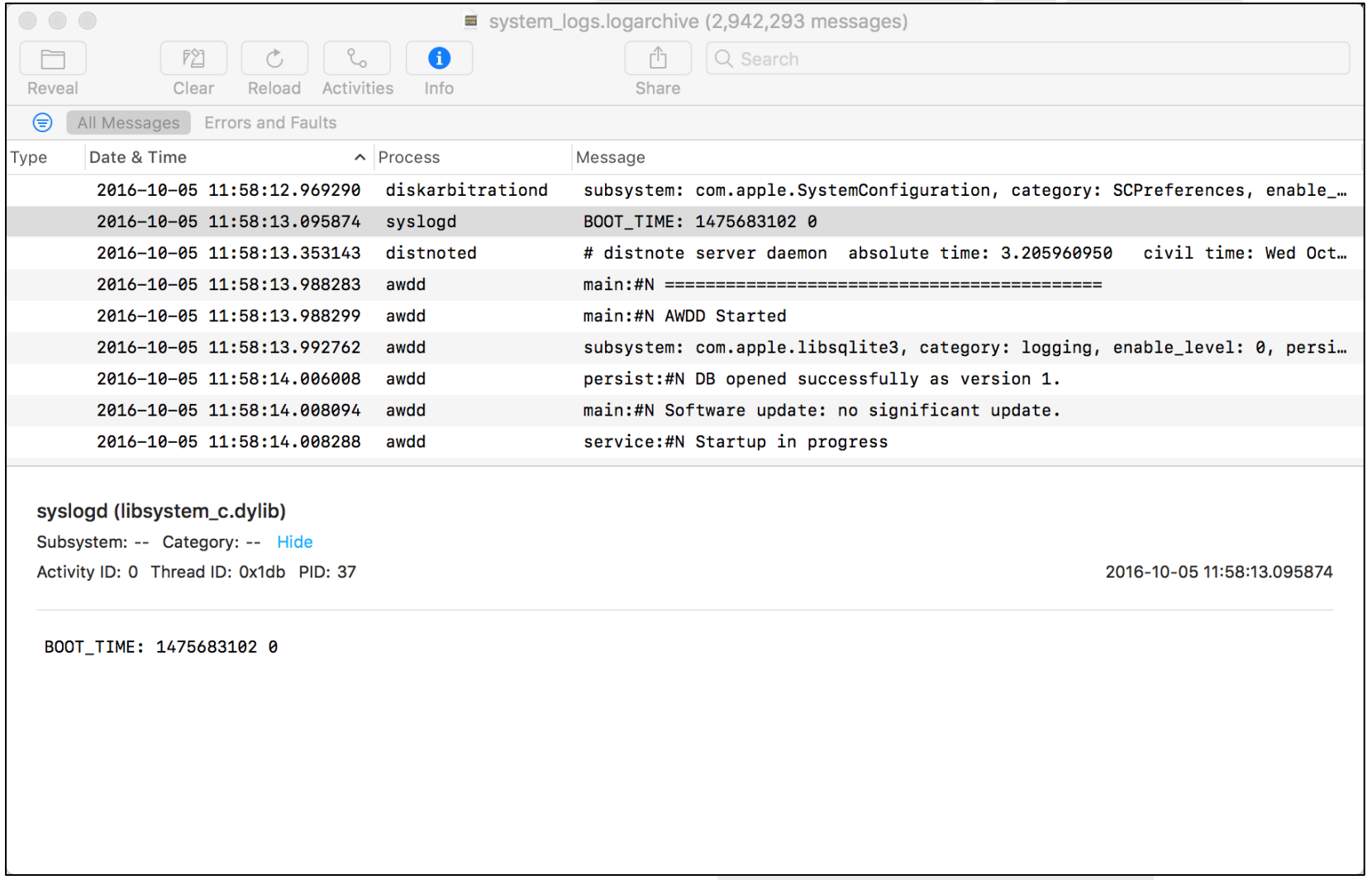
- Different than macOS 10.11 and older

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)

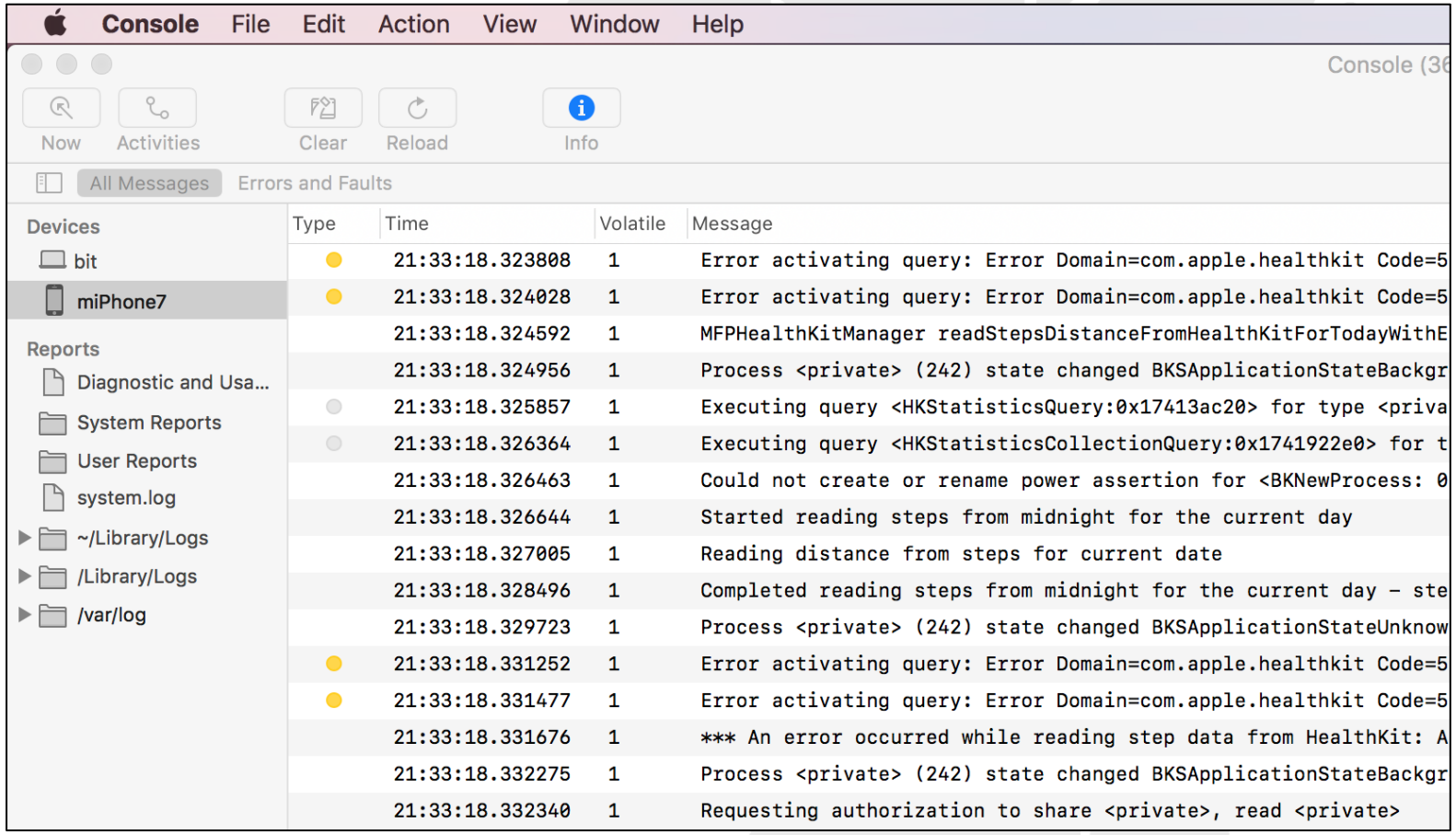
```
2017-03-22 18:31:35.739276-0400 0x1486     Activity    0x80000000000040a8  443
2017-03-22 18:31:37.315537-0400 0x3cf0     Activity    0x80000000000039b3  453
2017-03-22 18:31:35.744803-0400 0x1486     Activity    0x80000000000040a9  443
2017-03-22 18:31:37.321830-0400 0x3b63     Activity    0x80000000000039b4  453
2017-03-22 18:31:35.750804-0400 0x17f0     Activity    0x8000000000002287  499
2017-03-22 18:31:35.750844-0400 0x17c7     Activity    0x8000000000002256  488
2017-03-22 18:31:35.750984-0400 0x17e5     Activity    0x80000000000022d6  498
2017-03-22 18:31:35.750982-0400 0x17cb     Activity    0x80000000000022a6  490
2017-03-22 18:31:35.751004-0400 0x17f2     Activity    0x80000000000022e6  500
2017-03-22 18:31:35.752327-0400 0x1486     Activity    0x80000000000040aa  443
2017-03-22 18:31:42.346579-0400 0x3b63     Default     0x0                 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.
Timestamp                       Thread     Type        Activity            PID
2017-03-22 18:27:39.822799-0400 0x3b5      Default     0x0                 119    WindowServer: (SkyLight) [com.apple.SkyLight.default] Server is starting up
2017-03-22 18:27:40.227810-0400 0x2a0      Activity    0x8000000000000130  100    AirPlayXPCHelper: (CoreFoundation) Loading Preferences From System CFPrefsD
2017-03-22 18:27:40.251386-0400 0x2a0      Default     0x0                 100    AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.AirPlayEndpointManagerFactor
2017-03-22 18:27:40.447857-0400 0x3c7      Default     0x0                 100    AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.WiFiManagerCore] 2017-03-22
ParamErr
2017-03-22 18:27:40.448019-0400 0x3c7      Default     0x0                 100    AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APTransportTrafficRegistrar]
y traffic for AWDL at MAC 00:00:00:00:00:00 with target infra non critical PeerIndication=0 err=-3900
2017-03-22 18:27:40.448103-0400 0x3c7      Error       0x0                 100    AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APSLogUtils] 2017-03-22 06:2
-3900/0xFFFFF0C4 kA11ParamErr
2017-03-22 18:27:40.448110-0400 0x3c7      Error       0x0                 100    AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APSLogUtils] 2017-03-22 06:2
0/0xFFFFF0C4 kA11ParamErr
2017-03-22 18:27:40.448116-0400 0x3c7      Error       0x0                 100    AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.APSLogUtils] 2017-03-22 06:2
FFFF0C4 kA11ParamErr: APTransportTrafficRegistrar: reset registration failed
2017-03-22 18:27:40.467646-0400 0x2a0      Default     0x0                 100    AirPlayXPCHelper: (libsystem_trace.dylib) subsystem: com.apple.bluetooth, ca
0, debug_ttl: 0, generate_symptoms: 0, enable_oversize: 1, privacy_setting: 2, enable_private_data: 0
2017-03-22 18:27:40.467849-0400 0x2a0      Default     0x0                 100    AirPlayXPCHelper: (BluetoothAudio) [com.apple.bluetooth.BTFigE] Add Listener
2017-03-22 18:27:40.468397-0400 0x2a0      Default     0x0                 100    AirPlayXPCHelper: (BluetoothAudio) [com.apple.bluetooth.BTFigE] Created Blue
2017-03-22 18:27:40.468472-0400 0x2a0      Default     0x0                 100    AirPlayXPCHelper: (CoreUtils) [AirPlayXPCHelper.AirPlayMain] 2017-03-22 06:2
2017-03-22 18:27:40.468562-0400 0x3c5      Default     0x0                 100    AirPlayXPCHelper: (BluetoothAudio) [com.apple.bluetooth.BTFigE] Starting LE
2017-03-22 18:27:40.469458-0400 0x3c5      Activity    0x8000000000000131  100    AirPlayXPCHelper: (CoreFoundation) Loading Preferences From System CFPrefsD
2017-03-22 18:27:40.473533-0400 0x2a0      Default     0x0                 100    AirPlayXPCHelper: (libsystem_trace.dylib) subsystem: com.apple.coreaudio, ca
```

iDEVICE - LOG ACQUISITION

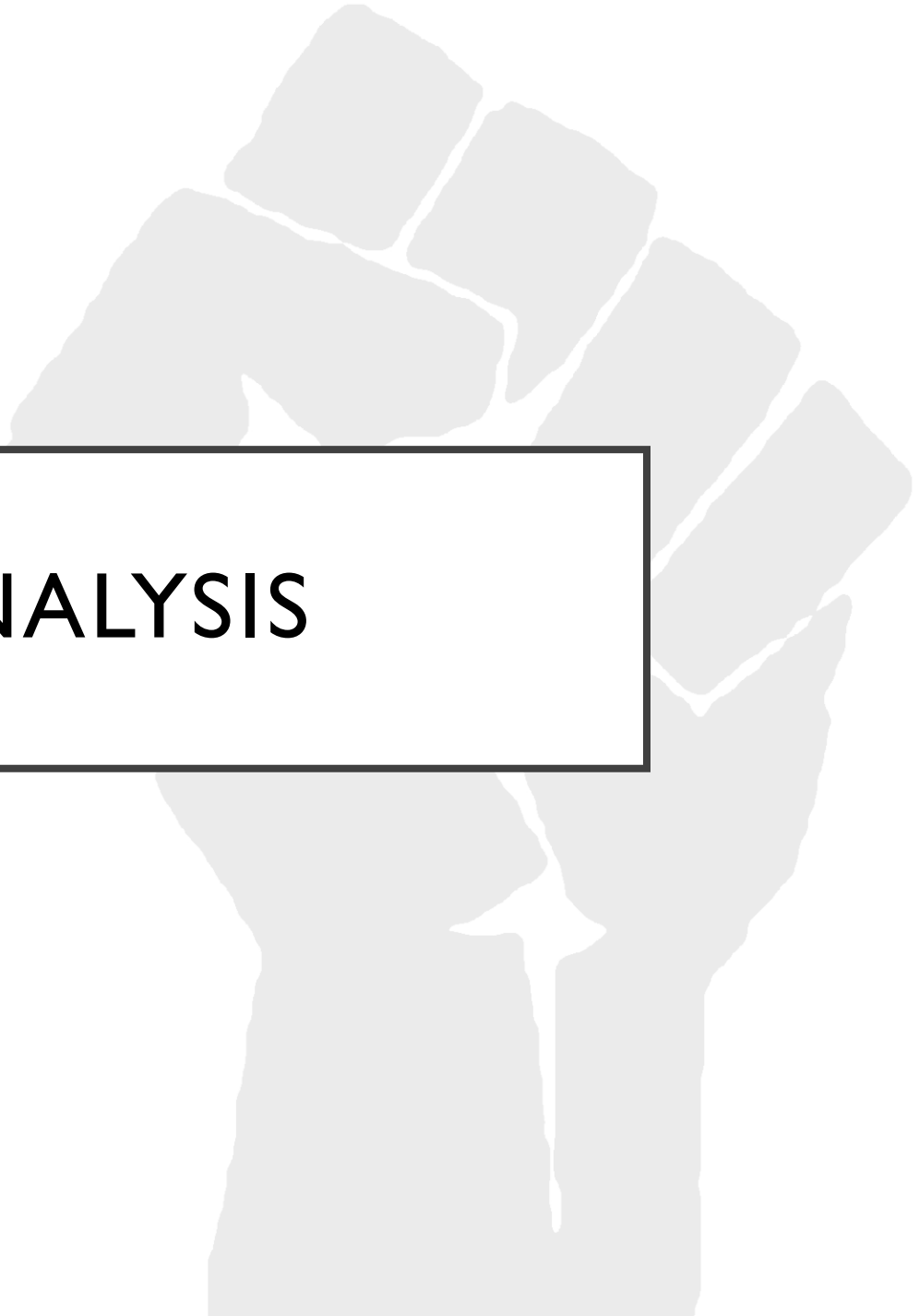
- Devices:
  - iOS
  - watchOS
  - tvOS
- ‘sysdiagnosis’ utility – key-chords for each devices
- Console.app
- More researched needed to see if useful for forensic analysis



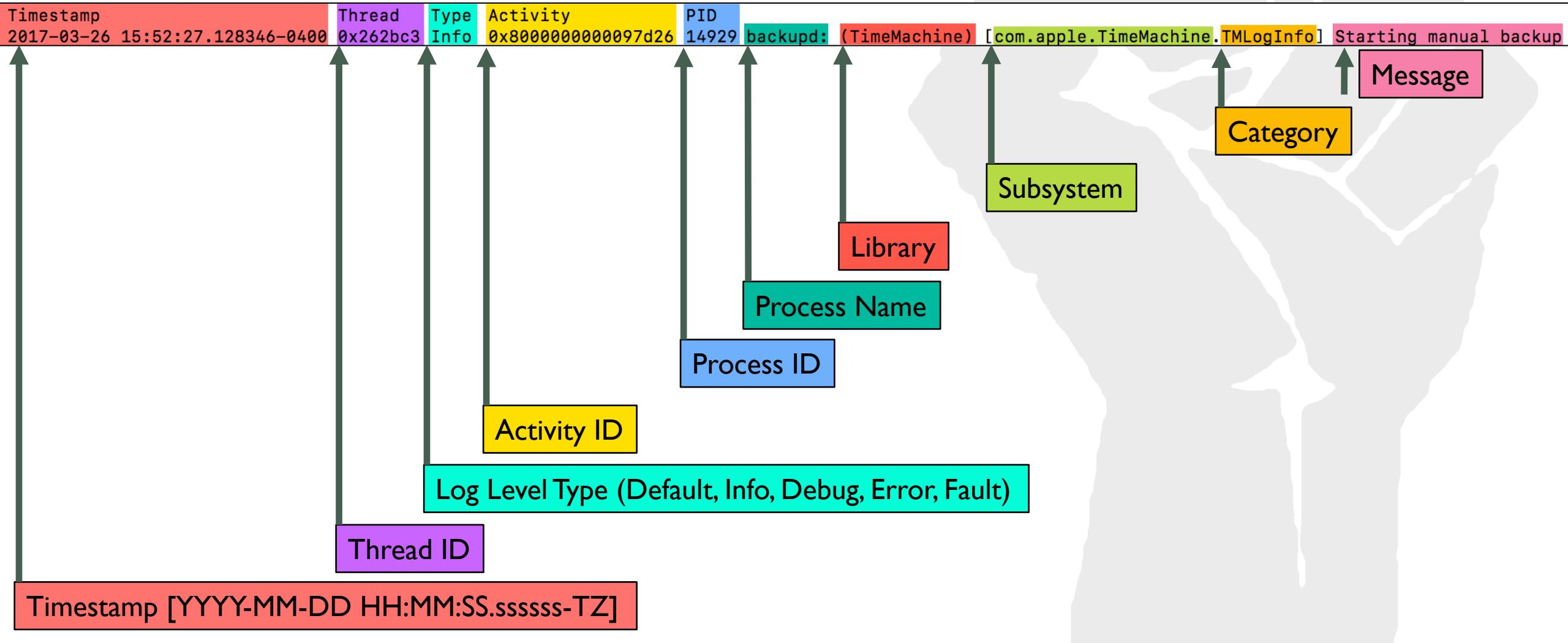
ON DISK STORAGE [iOS]
/private/var/db/ [diagnostics & uuidtext]

```
miPhone7:/private/var/db root# ls
FIPS                  UpdateMetrics          dhcpclient    fud       rolld        timezone
MobileIdentityData    astris                 dhcpd_leases  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 10518928 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  8750592 Mar 30 21:28 logdata.Persistent.20170331T011926.tracev3
-rw-r----- 1 root wheel  3616904 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



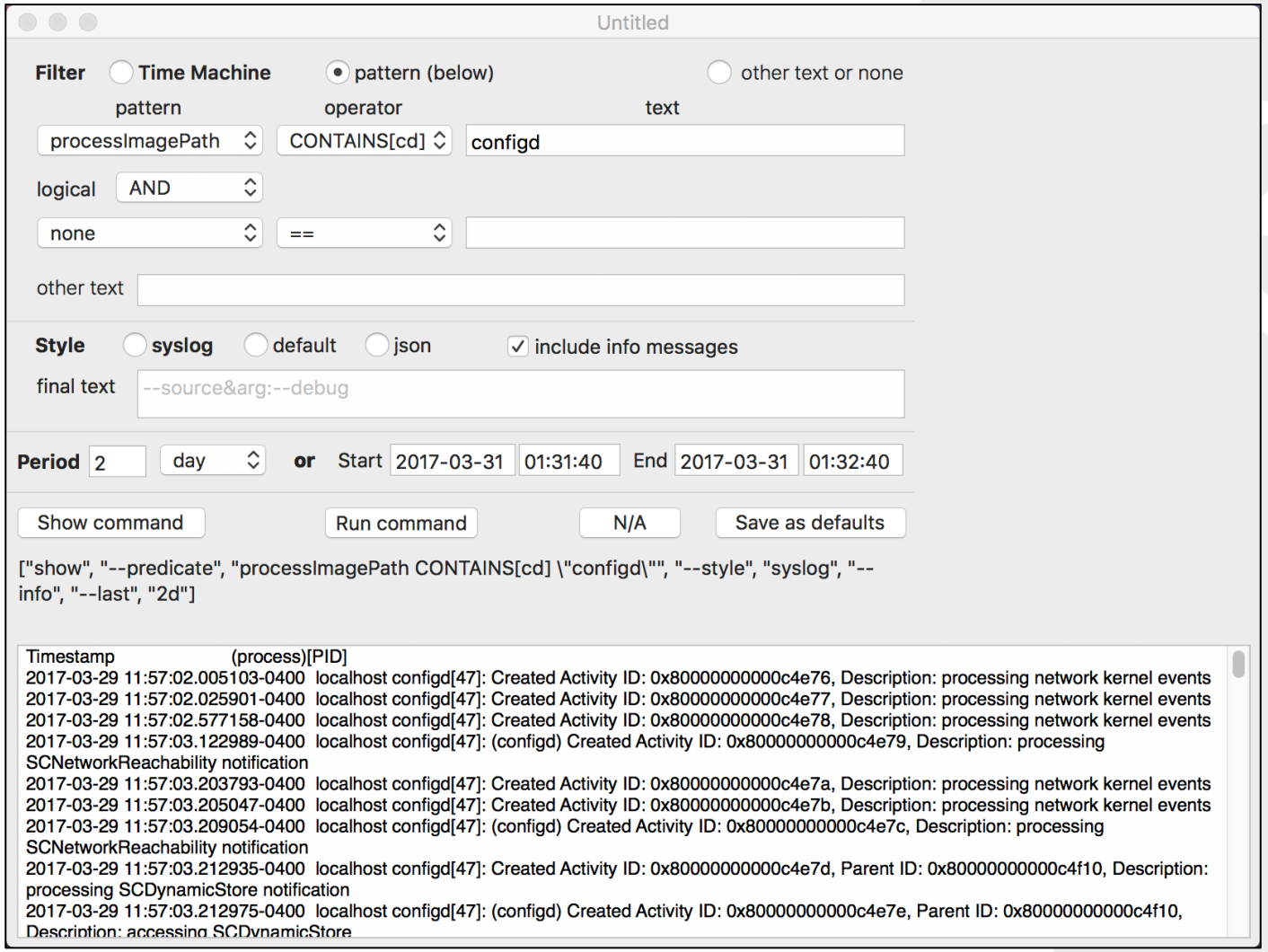
PREDICATE FILTERING
`--predicate`

- 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

[cd] = Ignore case/diacritics

```
bit:LogsUnite oompa$ log show system_logs.logarchive/ --info  --predicate 'processImagePath contains[cd] "backupd" and category contains[cd] "TMLogInfo" and eventMessage
 contains "Starting"' --start "2017-03-25 15:00:00"
==========
/Users/oompa/Dropbox (Personal)/LogsUnite/system_logs.logarchive
==========
Skipping debug messages, pass --debug to include.
Filtering the log data using "processImagePath CONTAINS[cd] "backupd" AND category CONTAINS[cd] "TMLogInfo" AND eventMessage CONTAINS "Starting""
Timestamp                       Thread     Type        Activity             PID
2017-03-25 15:09:52.159122-0400 0xbb011    Info        0x0                  9802   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting automatic backup
2017-03-25 15:12:37.464005-0400 0xbb011    Info        0x0                  9802   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting post-backup thinning
2017-03-25 16:21:36.193812-0400 0x187e14   Info        0x0                  12334  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting automatic backup
2017-03-25 16:26:59.910274-0400 0x187e14   Info        0x0                  12334  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting post-backup thinning
2017-03-25 17:21:32.309421-0400 0x21ab5c   Info        0x0                  12566  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting automatic backup
2017-03-25 17:26:55.642558-0400 0x21ab5c   Info        0x0                  12566  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting post-backup thinning
 ---------------------------------------------------------------------------------------------------------------
Log      - Default:          0, Info:               6, Debug:            0, Error:         0, Fault:         0
Activity - Create:           0, Transition:         0, Actions:          0
```

CONSOLATION - 3RD PARTY GUI ANALYSIS TOOL ECLECTICLIGHT.CO/DOWNLOADS/



NON-VOLATILE VS. VOLATILE MESSAGES

```
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_RegisterInterface: Frequent transitions for interface en0 (FE80:0000:0000:0000:18D4:735E:45E9:9803)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_RegisterInterface: Frequent transitions for interface en0 (10.11.12.214)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_RegisterInterface: Frequent transitions for interface en0 (FE80:0000:0000:0000:18D4:735E:45E9:9803)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_RegisterInterface: Frequent transitions for interface en0 (10.11.12.214)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_DeregisterInterface: Frequent transitions for interface en0 (10.11.12.214)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_RegisterInterface: Frequent transitions for interface en0 (FE80:0000:0000:0000:18D4:735E:45E9:9803)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_RegisterInterface: Frequent transitions for interface en0 (10.11.12.214)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_RegisterInterface: Frequent transitions for interface en0 (10.11.12.214)
mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNS_DeregisterInterface: Frequent transitions for interface en0 (10.11.12.214)
```

Message	Volatile	Subsystem
-- Sent UDP DNS Query (flags 0100) RCODE: NoErr (0) RD ID: 6517 19 bytes from port 56026 to 2601:01…	1	com.apple.mDNS…
1 Questions	1	com.apple.mDNS…
0 d.dropbox.com. AAAA	1	com.apple.mDNS…
0 Answers	1	com.apple.mDNS…
0 Authorities	1	com.apple.mDNS…
0 Additionals	1	com.apple.mDNS…
--------------	1	com.apple.mDNS…
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 11920 69 bytes from 2601:0141:…	1	com.apple.mDNS…
1 Questions	1	com.apple.mDNS…
0 d.dropbox.com. Addr	1	com.apple.mDNS…
3 Answers	1	com.apple.mDNS…
0 TTL 76 17 d.dropbox.com. CNAME d.v.dropbox.com.	1	com.apple.mDNS…
1 TTL 39 4 d.v.dropbox.com. Addr 108.160.172.193	1	com.apple.mDNS…
2 TTL 39 4 d.v.dropbox.com. Addr 108.160.172.225	1	com.apple.mDNS…

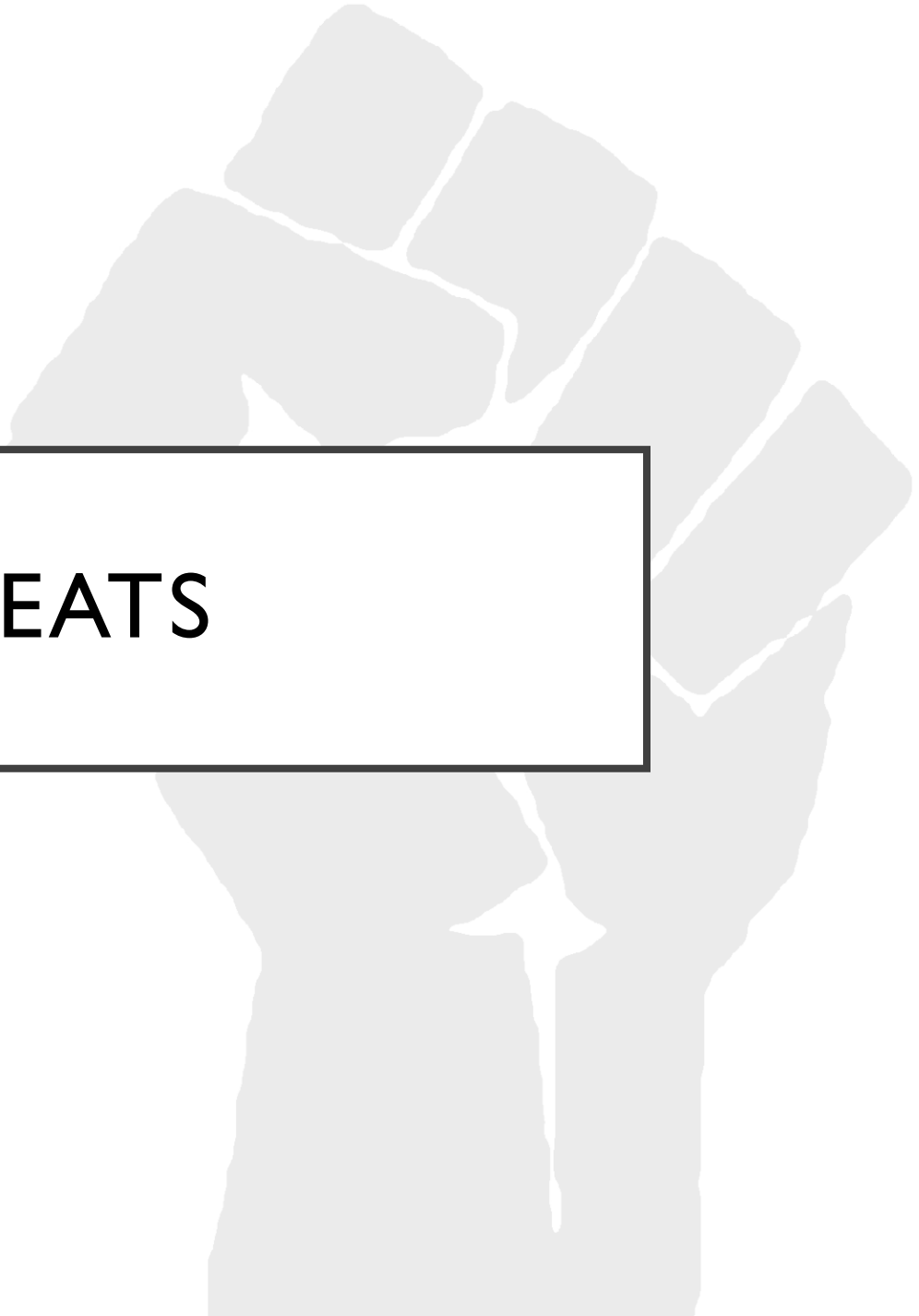
POTENTIAL FOR MEMORY ANALYSIS

- Look in the 'diagnosticd' process

```
bit:unzip_mem oompa$ strings mem | grep "Received UDP DNS Response"
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 64943 100 bytesXTUM
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 50357 253 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:0000:0000:0000:17B8:54424 --
-- Received UDP DNS Response (flags 8183) RCODE: NXDomain (3) RD RA ID: 49294 119 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:0000:0000:0000:17B8:50683 --
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 54986 188 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:0000:0000:0000:17B8:59691 --
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 35998 216 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:042C:7360:EB74:D3E5:57952 -qA
Received UDP DNS Response (flags 8180) RCODE: NoErr (0) A ID: 35998 91 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:042C:7360:EB74:D3E5:57952 --qA
Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 41363 121 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:042C:7360:EB74:D3E5:60173 -qA
Received UDP DNS Response (flags 8180) RCODE: NoErr (0) A ID: 37510 103 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:042C:7360:EB74:D3E5:59930 -qA
Received UDP DNS Response (flags 8180) RCODE: NoErr (0) A ID: 63978 138 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:042C:7360:EB74:D3E5:61959 -qA
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 29870 141 bytes from 2A
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 52261 138 bytes from 10.11.12.254:53 to 10.11.12.214:51175 --
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 1141 124 bytes from 2601:0141:0302:1F30:020D:B9FF:FE34:1C00:53 to 2601:0141:0302:1F30:0000:0000:0000:17B8:63995 --
```

Message	Volatile	Subsystem
-- Received UDP DNS Response (flags 8180) RCODE: NoErr (0) RD RA ID: 11920 69 bytes from 2601:0141:…	1	com.apple.mDNS…
1 Questions	1	com.apple.mDNS…
0 d.dropbox.com. Addr	1	com.apple.mDNS…
3 Answers	1	com.apple.mDNS…
0 TTL 76 17 d.dropbox.com. CNAME d.v.dropbox.com.	1	com.apple.mDNS…
1 TTL 39 4 d.v.dropbox.com. Addr 108.160.172.193	1	com.apple.mDNS…
2 TTL 39 4 d.v.dropbox.com. Addr 108.160.172.225	1	com.apple.mDNS…

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

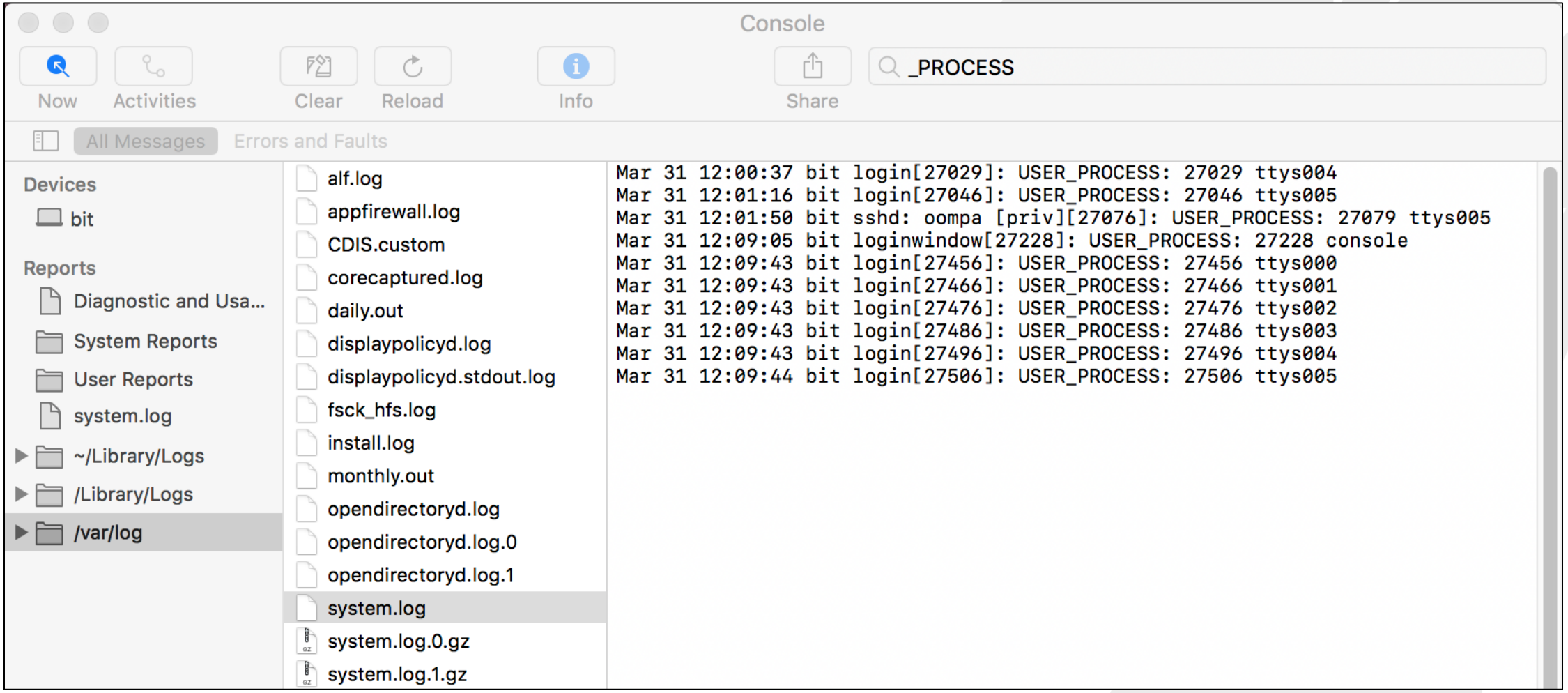
- `May 28 15:15:38 byte sshd[831]: USER_PROCESS: 842 ttys002`
- `May 28 15:15:52 byte sshd[831]: DEAD_PROCESS: 842 ttys002`

USER LOGINS
UNIFIED LOGS

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

```
bit:LogsUnite oompa$ log show --info --predicate ' eventMessage contains "_PROCESS"' --last 3d
Skipping debug messages, pass --debug to include.
Filtering the log data using "eventMessage CONTAINS "_PROCESS""
Timestamp                       Thread     Type        Activity             PID
2017-03-29 21:53:31.760265-0400 0x286682   Default     0x0                  16267  login: (libsystem_c.dylib) DEAD_PROCESS: 16267 ttys003
2017-03-29 21:53:45.153336-0400 0x2bae70   Default     0x0                  18093  login: (libsystem_c.dylib) DEAD_PROCESS: 18093 ttys004
2017-03-29 21:53:50.122238-0400 0x2bd357   Default     0x0                  18199  login: (libsystem_c.dylib) DEAD_PROCESS: 18199 ttys005
2017-03-29 21:53:53.366307-0400 0x2c82e2   Default     0x0                  18439  login: (libsystem_c.dylib) DEAD_PROCESS: 18439 ttys006
2017-03-30 22:23:01.973781-0400 0x3827e9   Default     0x0                  25435  login: (libsystem_c.dylib) DEAD_PROCESS: 25435 ttys004
2017-03-30 22:23:03.093753-0400 0x382a1d   Default     0x0                  25449  login: (libsystem_c.dylib) DEAD_PROCESS: 25449 ttys005
2017-03-31 12:01:18.641809-0400 0x3b9190   Default     0x0                  27046  login: (libsystem_c.dylib) DEAD_PROCESS: 27046 ttys005
2017-03-31 12:01:59.652285-0400 0x3b9351   Default     0x0                  27076  sshd: (libsystem_c.dylib) DEAD_PROCESS: 27079 ttys005
2017-03-31 12:08:01.182684-0400 0x136a47   Default     0x0                  10010  login: (libsystem_c.dylib) DEAD_PROCESS: 10010 ttys000
2017-03-31 12:08:01.301243-0400 0x136dd3   Default     0x0                  10021  login: (libsystem_c.dylib) DEAD_PROCESS: 10021 ttys001
2017-03-31 12:08:01.377587-0400 0x14ab9e   Default     0x0                  10076  login: (libsystem_c.dylib) DEAD_PROCESS: 10076 ttys002
2017-03-31 12:08:01.479821-0400 0x33f3f9   Default     0x0                  23375  login: (libsystem_c.dylib) DEAD_PROCESS: 23375 ttys003
2017-03-31 12:08:01.573287-0400 0x386e08   Default     0x0                  25613  login: (libsystem_c.dylib) DEAD_PROCESS: 25613 ttys006
2017-03-31 12:08:01.677944-0400 0x3b8d8a   Default     0x0                  27029  login: (libsystem_c.dylib) DEAD_PROCESS: 27029 ttys004
2017-03-31 12:08:55.123852-0400 0x3ba6d9   Default     0x0                  27221  sessionlogoutd: (libsystem_c.dylib) DEAD_PROCESS: 94 console
 ------------------------------------------------------------------------------------------------------------------------------
Log      - Default:          15, Info:                0, Debug:            0, Error:          0, Fault:          0
Activity - Create:           0, Transition:           0, Actions:          0
```

USER LOGINS
GOING OLD SKOOL - SYSTEM.LOG



TIME MACHINE BACKUPS

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

```
bit:LogsUnite oompa$ log show system_logs.logarchive/ --predicate 'senderImagePath contains[cd] "TimeMachine"' --info --start "2017-03-31 06:58:42"
==========
/Users/oompa/Dropbox (Personal)/LogsUnite/system_logs.logarchive
==========
Skipping debug messages, pass --debug to include.
Filtering the log data using "senderImagePath CONTAINS[cd] "TimeMachine""
Timestamp                       Thread     Type        Activity             PID
2017-03-31 06:58:42.361177-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting automatic backup
2017-03-31 06:58:42.394547-0400 0x65d      Info        0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Set snapshot time: 2017-03-31 06:58:44 -0400 (current time: 2017-03-31 06:58:42 -0400)
2017-03-31 06:58:42.459050-0400 0x39e562   Error       0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Computer/2017-03-31-065844/Volume/private' (errno 1)
2017-03-31 06:58:42.463767-0400 0x39e562   Error       0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Computer/2017-03-31-065844/Volume/private/var' (errno 1)
2017-03-31 06:58:42.468315-0400 0x39e562   Error       0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Computer/2017-03-31-065844/Volume/private/var/db' (errno 1)
2017-03-31 06:58:42.471348-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Attempting to mount network destination URL: afp://Sarah%20Edwards;AUTH=SRP@Delorean._afpovertcp._tcp.local./Data
2017-03-31 06:58:42.894362-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Mounted network destination at mount point: /Volumes/Data using URL: afp://Sarah%20Edwards;AUTH=SRP@Delorean._afpovertcp._tcp.local./Data
2017-03-31 07:00:06.982232-0400 0x39eb02   Error       0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Computer/2017-03-31-065844/Volume/Library' (errno 1)
2017-03-31 07:00:06.986335-0400 0x39eb02   Error       0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Computer/2017-03-31-065844/Volume/Library/Preferences' (errno 1)
2017-03-31 07:00:06.989509-0400 0x39eb02   Error       0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Computer/2017-03-31-065844/Volume/Library/Preferences/SystemConfiguration' (errno 1)
2017-03-31 07:01:29.222060-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Checking for runtime corruption on /dev/disk2s2
2017-03-31 07:02:25.908928-0400 0x65d      Error       0x0                  180     mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] Can't trash .MobileBackups while MTM Snapshot Handler is running!
2017-03-31 07:02:26.976615-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Disk image /Volumes/Data/bit.sparsebundle mounted at: /Volumes/Time Machine Backups
2017-03-31 07:02:28.610709-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Backing up to /dev/disk2s2: /Volumes/Time Machine Backups/Backups.backupdb
2017-03-31 07:02:42.570843-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Will copy (46.4 MB) from Untitled
2017-03-31 07:02:42.581048-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Found 527 files (46.4 MB) needing backup
2017-03-31 07:02:42.594372-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] 104.9 MB required (including padding), 926.27 GB available
2017-03-31 07:04:02.795015-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Copied 639 items (46.4 MB) from volume Untitled. Linked 3002.
2017-03-31 07:04:05.837633-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Created new backup: 2017-03-31-070403
2017-03-31 07:04:07.354206-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting post-backup thinning
2017-03-31 07:04:24.769984-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/2017-03-30-061857 (38.7 MB)
2017-03-31 07:04:24.770117-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Post-backup thinning complete: 1 expired backups removed
2017-03-31 07:04:24.977374-0400 0x39e55a   Info        0x0                  25956   backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Backup completed successfully.
```

TIME MACHINE BACKUPS
A CASE FOR '`--info`'

```
Type        Activity             PID
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting automatic backup
Info        0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Set snapshot time: 2017-03-31 06:58:44 -0400 (current time: 2017-03-31 06:58:42 -0400)
Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Com

Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Com
 1)
Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Com
rno 1)
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Attempting to mount network destination URL: afp://Sarah%20Edwards;AUTH=SRP@Delorean._af

Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Mounted network destination at mount point: /Volumes/Data using URL: afp://Sarah%20Edwar

Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Com

Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Com
' (errno 1)
Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPath:] setattrlist failed for path '/.MobileBackups/Com
s/SystemConfiguration' (errno 1)
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Checking for runtime corruption on /dev/disk2s2
Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] Can't trash .MobileBackups while MTM Snapshot Handler is running!
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Disk image /Volumes/Data/bit.sparsebundle mounted at: /Volumes/Time Machine Backups
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Backing up to /dev/disk2s2: /Volumes/Time Machine Backups/Backups.backupdb
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Will copy (46.4 MB) from Untitled
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Found 527 files (46.4 MB) needing backup
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] 104.9 MB required (including padding), 926.27 GB available
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Copied 639 items (46.4 MB) from volume Untitled. Linked 3002.
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Created new backup: 2017-03-31-070403
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting post-backup thinning
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/2017-03-30-061857 (38.7 MB)
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Post-backup thinning complete: 1 expired backups removed
Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Backup completed successfully.
```

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?

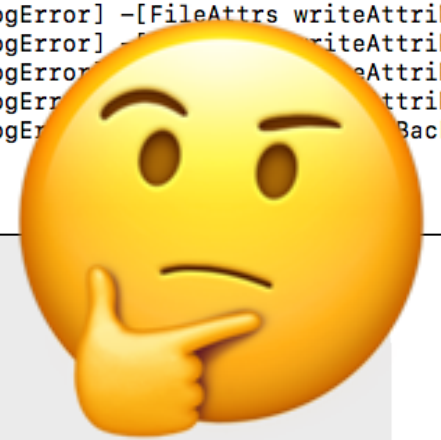
```
log show system_logs.logarchive/ --
predicate 'senderImagePath contains[cd]
"TimeMachine"' --info --start "2017-03-31
06:58:42" --end "2017-03-31 07:04:24"
```

```
Timestamp
2017-03-31 06:58:42.361177-0400
2017-03-31 06:58:42.394547-0400
2017-03-31 06:58:42.459050-0400
17-03-31-065844/Volume/private'
2017-03-31 06:58:42.463767-0400
17-03-31-065844/Volume/private/v
2017-03-31 06:58:42.468315-0400
17-03-31-065844/Volume/private/v
2017-03-31 06:58:42.471348-0400
._tcp.local./Data
2017-03-31 06:58:42.894362-0400
SRP@Delorean._afpovertcp._tcp.lo
2017-03-31 07:00:06.982232-0400
17-03-31-065844/Volume/Library'
2017-03-31 07:00:06.986335-0400
17-03-31-065844/Volume/Library/P
2017-03-31 07:00:06.989509-0400
17-03-31-065844/Volume/Library/P
2017-03-31 07:01:29.222060-0400
2017-03-31 07:02:25.908928-0400
2017-03-31 07:02:26.976615-0400
2017-03-31 07:02:28.610709-0400
2017-03-31 07:02:42.570843-0400
2017-03-31 07:02:42.581048-0400
2017-03-31 07:02:42.594372-0400
2017-03-31 07:04:02.795015-0400
2017-03-31 07:04:05.837633-0400
2017-03-31 07:04:07.354206-0400
2017-03-31 07:04:24.769984-0400
2017-03-31 07:04:24.770117-0400
2017-03-31 07:04:24.977374-0400
```

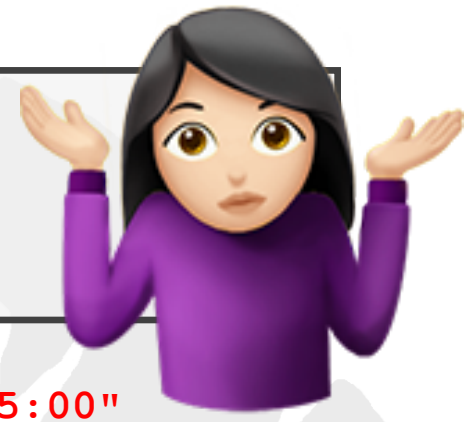
TIME MACHINE BACKUPS
TIME SLICING

```
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"
```

```
[bit:LogsUnite oompa$ 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"
==========
/Users/oompa/Dropbox (Personal)/LogsUnite/system_logs.logarchive
==========
Skipping debug messages, pass --debug to include.
Filtering the log data using "senderImagePath CONTAINS[cd] "TimeMachine""
Timestamp                       Thread     Type        Activity            PID
2017-03-31 06:58:42.394547-0400 0x65d      Info        0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Set snapshot time: 2017-03-31 06:58:44
2017-03-31 06:58:42.459050-0400 0x39e562   Error       0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPat
2017-03-31 06:58:42.463767-0400 0x39e562   Error       0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPat
2017-03-31 06:58:42.468315-0400 0x39e562   Error       0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPat
2017-03-31 07:00:06.982232-0400 0x39eb02   Error       0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPat
2017-03-31 07:00:06.986335-0400 0x39eb02   Error       0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPat
2017-03-31 07:00:06.989509-0400 0x39eb02   Error       0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPat
2017-03-31 07:02:25.908928-0400 0x65d      Error       0x0                 180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] Backups while MTM S
---------------------------------------------------------------------------------------------------------------------------
Log      - Default:          0, Info:               1, Debug:            0, Error:          7, Fault:          0
Activity - Create:           0, Transition:         0, Actions:          0
```



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"
```

```
[bit:LogsUnite oompa$ 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"
==========
/Users/oompa/Dropbox (Personal)/LogsUnite/system_logs.logarchive
==========
Skipping debug messages, pass --debug to include.
Filtering the log data using "senderImagePath CONTAINS[cd] "TimeMachine""
Timestamp                       Thread     Type        Activity             PID
2017-03-31 06:58:42.361177-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting automatic backup
2017-03-31 06:58:42.394547-0400 0x65d      Info        0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Set snapshot time: 2017-03-31 06:58:44
2017-03-31 06:58:42.459050-0400 0x39e562   Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPa
2017-03-31 06:58:42.463767-0400 0x39e562   Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPa
2017-03-31 06:58:42.468315-0400 0x39e562   Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPa
2017-03-31 06:58:42.471348-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Attempting to mount network destina
2017-03-31 06:58:42.894362-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Mounted network destination at moun
2017-03-31 07:00:06.982232-0400 0x39eb02   Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPa
2017-03-31 07:00:06.986335-0400 0x39eb02   Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPa
2017-03-31 07:00:06.989509-0400 0x39eb02   Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] -[FileAttrs writeAttributesToItemAtPa
2017-03-31 07:01:29.222060-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Checking for runtime corruption on
2017-03-31 07:02:25.908928-0400 0x65d      Error       0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogError] Can't trash .MobileBackups while MTM
2017-03-31 07:02:26.976615-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Disk image /Volumes/Data/bit.sparse
2017-03-31 07:02:28.610709-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Backing up to /dev/disk2s2: /Volume
2017-03-31 07:02:42.570843-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Will copy (46.4 MB) from Untitled
2017-03-31 07:02:42.581048-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Found 527 files (46.4 MB) needing b
2017-03-31 07:02:42.594372-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] 104.9 MB required (including paddin
2017-03-31 07:04:02.795015-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Copied 639 items (46.4 MB) from vol
2017-03-31 07:04:05.837633-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Created new backup: 2017-03-31-0704
2017-03-31 07:04:07.354206-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting post-backup thinning
2017-03-31 07:04:24.769984-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Deleted /Volumes/Time Machine Backu
2017-03-31 07:04:24.770117-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Post-backup thinning complete: 1 ex
2017-03-31 07:04:24.977374-0400 0x39e55a   Info        0x0                  25956  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Backup completed successfully.
 ---------------------------------------------------------------------------------------------------------------
Log      - Default:          0, Info:              16, Debug:            0, Error:          7, Fault:          0
Activity - Create:           0, Transition:         0, Actions:          0
```

TIMEZONE CHANGE VIA LOCATIOND HINTS OF TIME CHANGES

```
2017-03-31 17:20:25.957164-0400 0x19b      Default     0x0                  0      kernel: (AirPortBrcm4360) [0]    1 Valid
2017-03-31 17:20:25.957172-0400 0x19b      Default     0x0                  0      kernel: (AirPortBrcm4360) ARPT: 220996.776091: [2]    0 IM
2017-03-31 17:20:25.957180-0400 0x19b      Default     0x0                  0      kernel: (AirPortBrcm4360) ARPT: 220996.776099: [3]    0 PM
2017-03-31 17:20:25.957189-0400 0x19b      Default     0x0                  0      kernel: (AirPortBrcm4360) ARPT: 220996.776108: [7-4]  0 Suppr
2017-03-31 17:20:25.957198-0400 0x19b      Default     0x0                  0      kernel: (AirPortBrcm4360) ARPT: 220996.776116: [14:8] 1 Ncons
2017-03-31 17:20:25.957207-0400 0x19b      Default     0x0                  0      kernel: (AirPortBrcm4360) ARPT: 220996.776125: [15]   0 Acked
2017-03-31 17:20:25.957220-0400 0x19b      Default     0x0                  0      kernel: (AirPortBrcm4360) ARPT: 220996.776137: txpktpend AC_BK 0 AC_BE
2017-03-31 16:20:26.227814-0500 0x735      Info        0x0                  193    thermald: [thermald.log] 39/0/0 SFI:0/0/0/0/0/0 GPU:0/0/0/0 IO:0/0/0/0
2017-03-31 17:20:26.351193-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNSPlatformSendUDP -
42.239.1:53 skt 37 error -1 errno 51 (Network is unreachable) 1121464237
2017-03-31 17:20:26.351346-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO] -- ERROR -65562 Sendi
7 to 10.42.239.1:53 --
2017-03-31 17:20:26.351455-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  1 Questions
2017-03-31 17:20:26.351536-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 lb._dns-sd._udp.0.
2017-03-31 17:20:26.351602-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 Answers
2017-03-31 17:20:26.351681-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 Authorities
2017-03-31 17:20:26.351747-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 Additionals
2017-03-31 17:20:26.351798-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO] --------------
2017-03-31 17:20:26.351932-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNSPlatformSendUDP -
42.239.1:53 skt 48 error -1 errno 51 (Network is unreachable) 1121464237
2017-03-31 17:20:26.352240-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO] -- ERROR -65562 Sendi
1 to 10.42.239.1:53 --
2017-03-31 17:20:26.352297-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  1 Questions
2017-03-31 17:20:26.352560-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 lb._dns-sd._udp.34
2017-03-31 17:20:26.352603-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 Answers
2017-03-31 17:20:26.352638-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 Authorities
2017-03-31 17:20:26.352691-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO]  0 Additionals
2017-03-31 17:20:26.352744-0400 0x63e      Info        0x0                  121    mDNSResponder: [com.apple.mDNSResponder.AllINFO] --------------
2017-03-31 16:20:26.476271-0500 0x3ccafa   Info        0x0                  28392  backupd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Starting auto
2017-03-31 17:20:26.425314-0400 0x65d      Default     0x0                  0      kernel: nspace-handler-set-snapshot-time: 1490995228
2017-03-31 17:20:26.425576-0400 0x65d      Info        0x0                  180    mtmd: (TimeMachine) [com.apple.TimeMachine.TMLogInfo] Set snapshot tim
```

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!

```
2017-03-31 16:20:43.849218-0500 0x720      Activity    0x80000000000f366a 188    socketfilterfw: (Security) SecTrustEvaluateIfNecessary
2017-03-31 16:20:43.850671-0500 0x3cd14a   Default     0x80000000000f366a 131    trustd: [com.apple.securityd.policy] cert[2]: AnchorTrusted =(leaf)[force]> 0
2017-03-31 16:20:43.853911-0500 0x3cd2c6   Activity    0x80000000000f36c0 28476  timezoned: (CoreFoundation) Loading Preferences From System CFPrefsD
2017-03-31 16:20:43.855151-0500 0x3cd1e4   Activity    0x80000000000f0e9c 85     locationd: (Security) SecTrustEvaluateIfNecessary
2017-03-31 16:20:43.856425-0500 0x3cd14a   Default     0x80000000000f0e9c 131    trustd: [com.apple.securityd.policy] cert[2]: AnchorTrusted =(leaf)[force]> 0
2017-03-31 16:20:43.858671-0500 0x3cd1e4   Activity    0x80000000000f0e9d 85     locationd: (Security) SecTrustEvaluateIfNecessary
2017-03-31 16:20:43.859765-0500 0x3cd14a   Default     0x80000000000f0e9d 131    trustd: [com.apple.securityd.policy] cert[2]: AnchorTrusted =(leaf)[force]> 0
2017-03-31 16:20:43.862060-0500 0x3cd2c6   Info        0x0                28476  timezoned: (CoreLocation) [com.apple.locationd.Core.Client] New location is identical to c
2017-03-31 17:20:43.861773-0400 0x3cd2cf   Info        0x0                85     locationd: [com.apple.locationd.Position.WifiPosition] TlurState, End, <private>
2017-03-31 17:20:43.901803-0400 0x63e      Info        0x0                121    mDNSResponder: [com.apple.mDNSResponder.AllINFO] mDNSPlatformSendUDP -> sendto(37) failed
```

OTHER INTERESTING EXAMPLES

NETWORK USAGE
CONFIGD

```
log show --info --predicate 'senderImagePath contains[cd]
"IPConfiguration" and (eventMessage contains[cd] "SSID" or
eventMessage contains[cd] "Lease" or eventMessage contains[cd]
"network changed")'
```

```
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] Removing Stale Lease 172.19.131.157 Router 172.19.131.2
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: no SSID
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: status = 'network changed'
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP bridge0: status = 'network changed'
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: status = 'network changed'
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: SSID is now hhonors (was United_Wi-Fi)
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: No lease for hhonors
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] AUTOMATIC-V6 en0: status = 'network changed'
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: SSID hhonors BSSID 0:23:ea:7f:4d:91
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] ignoring lease with SSID stationx
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: ARP router: No leases to query for
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] ignoring lease with SSID stationx
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: ARP router: No leases to query for
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] ignoring lease with SSID stationx
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: ARP router: No leases to query for
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] en0: SSID hhonors BSSID 0:24:13:8:7f:e1
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] ignoring lease with SSID stationx
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: ARP router: No leases to query for
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] ignoring lease with SSID stationx
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: ARP router: No leases to query for
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: INIT lease = { start 0x1e8efa9a, t1 0x1e8f01a2, t2 0x1e8f06e8, expiration 0x1e8f08aa }
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] DHCP en0: SELECT lease = { start 0x1e8efa9c, t1 0x1e8f01a4, t2 0x1e8f06ea, expiration 0x1e8f08ac }
configd: (IPConfiguration) [com.apple.IPConfiguration.Server] Saved lease for 107.16.207.185
```

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] ACCOUNT: [keyStatus: ] [SOSCCStatus: kSOSCCInCircle]
Default   secd: [com.apple.securityd.accountLogState] CIRCLE:    [[2014-12-15 19:58 23]] UserSigned: V
Default   secd: [com.apple.securityd.accountLogState] Peers In Circle:
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: Sarah's MacBook Air] [mASrbKv] [type: MacBook Air        ] [spid:  [os:    15G1004] [devid:  [serial:
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: byte               ] [mASrbKv] [type: Mac mini          ] [spid:  ] [os:     15E65] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: word               ] [mASrbKv] [type: MacBook Pro       ] [spid:  ] [os:   15G1004] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: Mini miPad4        ] [mASrbIV] [type: iPad              ] [spid:  ] [os:    14A403] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: bit                ] [mASrBIv] [type: MacBook Pro       ] [spid:  ] [os:    16C67] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: word               ] [mASrbKv] [type: MacBook Pro       ] [spid:  ] [os:  Unknown ] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: miPhone6           ] [mASrbKv] [type: iPhone            ] [spid:  ] [os:    13A452] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: bit                ] [MASrBIV] [type: MacBook Pro       ] [spid:  ] [os:    16D30] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: Mini miPad         ] [mASrBIV] [type: iPad              ] [spid:  ] [os:    14C92] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: nibble             ] [mASrbKv] [type: MacBook Air       ] [spid:  ] [os:  Unknown ] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: iPhone             ] [mASrBKv] [type: iPhone            ] [spid:  ] [os:    13G34] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: miPhone5s          ] [mASrbKv] [type: iPhone            ] [spid:  ] [os:  Unknown ] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: Sarah's MacBook Pro] [mASrBIv] [type: MacBook Pro       ] [spid:  [os:    16B2657] [devid:  [serial:
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: word               ] [mASrBIV] [type: MacBook Pro       ] [spid:  ] [os:    16B2555] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: nibble (2)         ] [mASrbKv] [type: MacBook Air       ] [spid:  ] [os:  Unknown ] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: miPhone7           ] [mASrBIV] [type: iPhone            ] [spid:  ] [os:    14B100] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: word               ] [mASrbKv] [type: MacBook Pro       ] [spid:  ] [os:    15B42] [devid:  ] [serial:  ]
Default   secd: [com.apple.securityd.accountLogState] PI:    [name: Sarah's MacBook Air] [mASrbIv] [type: MacBook Air        ] [spid:  [os:    16A323] [devid:  [serial:
Default   secd: [com.apple.securityd.accountLogState] Applicants To Circle: None
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-Escrow,
asterKey aring, 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]
CIRCLE:    [[2014-12-15 19:58 23]] UserSigned: V
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:      15E65] [devid:                ] [serial:                ]
PI:    [name: word                ] [mASrbKv] [type: MacBook Pro       ] [spid:                ] [os:    15G1004] [devid:                ] [serial:                ]
PI:    [name: Mini miPad4         ] [mASrbIV] [type: iPad              ] [spid:                ] [os:     14A403] [devid:                ] [serial:                ]
PI:    [name: bit                 ] [mASrBIv] [type: MacBook Pro       ] [spid:                ] [os:      16C67] [devid:                ] [serial:                ]
PI:    [name: word                ] [mASrbKv] [type: MacBook Pro       ] [spid:                ] [os:   Unknown ] [devid:                ] [serial:                ]
PI:    [name: miPhone6            ] [mASrbKv] [type: iPhone            ] [spid:                ] [os:     13A452] [devid:                ] [serial:                ]
PI:    [name: bit                 ] [MASrBIV] [type: MacBook Pro       ] [spid:                ] [os:      16D30] [devid:                ] [serial:                ]
PI:    [name: Mini miPad          ] [mASrBIV] [type: iPad              ] [spid:                ] [os:      14C92] [devid:                ] [serial:                ]
PI:    [name: nibble              ] [mASrbKv] [type: MacBook Air       ] [spid:                ] [os:   Unknown ] [devid:                ] [serial:                ]
PI:    [name: iPhone              ] [mASrBKv] [type: iPhone            ] [spid:                ] [os:      13G34] [devid:                ] [serial:                ]
PI:    [name: miPhone5s           ] [mASrbKv] [type: iPhone            ] [spid:                ] [os:   Unknown ] [devid:                ] [serial:                ]
PI:    [name: Sarah's MacBook Pro] [mASrBIv] [type: MacBook Pro       ] [spid:                 [os:    16B2657] [devid:                 [serial:
PI:    [name: word                ] [mASrBIV] [type: MacBook Pro       ] [spid:                ] [os:    16B2555] [devid:                ] [serial:                ]
PI:    [name: nibble (2)          ] [mASrbKv] [type: MacBook Air       ] [spid:                ] [os:   Unknown ] [devid:                ] [serial:                ]
PI:    [name: miPhone7            ] [mASrBIV] [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] [mASrbIv] [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

All | Maps | Videos | Shopping | News | More | Settings | Tools

About 57,000 results (0.56 seconds)

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 5S Sep 13, 2016
More results from discussions.apple.com

iOS 10.0.1 Information - IPSW Downloads
https://ipsw.me/10.0.1
iPad 4 (WiFi) (iPad3,4), iOS 10.0.1 (**14A403**), 09/13/2016, iPad_32bit_10.0.1_14A403_Restore.ipsw, 1.9 GB, MD5: 08a539eaed4f51755656f062358bd324

Service and Support Coverage

Apple Inc. [US] https://checkcoverage.apple.com/us/en/?sn=

Mac iPad iPhone Watch TV Music Support

Check Coverage Sign in

Your Service and Support Coverage

iPad mini 4 Wi-Fi, Cellular

Serial Number:

Check another serial number ›

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

EXTERNAL MEDIA MOUNT & UNMOUNT

```
log show --info --predicate 'subsystem = "com.apple.imagecapture" or
processImagePath contains[cd] "fseventsd"'
```

```
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 23:{ICWiredBrowser.m} (USB Device first match)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 23:{ICWiredBrowser.m} (USB Device first match)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 388:{ICWiredBrowser.m} (10 USB Descriptions Managed)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 460:{ICDDMessageCenter.m} (+Add FlashBlu 30 - 0x0/0x0/0x0 - 0x100000 - ICDeviceDescriptionSUQuery)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 213:{ICResourceManager.m} (30373038-3433-3739-3232-363544383633|FlashBlu 30|MANUFACTURER:Kanguru;MODEL:FlashBlu 30|SW=FALSE|)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 460:{ICDDMessageCenter.m} (+Add FlashBlu 30 - 0x0/0x0/0x0 - 0x100000 - ICDeviceDescriptionAdded)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 37:{ICWiredBrowser.m} (USB Interface first match)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 388:{ICWiredBrowser.m} (11 USB Descriptions Managed)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 460:{ICDDMessageCenter.m} (+Add FlashBlu 30 - 0x8/0x6/0x50 - 0x100000 - ICDeviceDescriptionSUQuery)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 213:{ICResourceManager.m} (00000000-0000-0000-0000-00001E1D1104|FlashBlu 30|(null)|SW=FALSE|)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 460:{ICDDMessageCenter.m} (+Add FlashBlu 30 - 0x8/0x6/0x50 - 0x100000 - ICDeviceDescriptionUndefined)
fseventsd: could not open <</Volumes/EXFATUSB/.fseventsd/fseventsd-uuid>> (No such file or directory)
fseventsd: Failed to load UUID.  Removing all old log files in /Volumes/EXFATUSB/.fseventsd
fseventsd: log dir: /Volumes/EXFATUSB/.fseventsd getting new uuid: 72A0E2E9-3726-4703-81DC-343B300A2387
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 51:{ICWiredBrowser.m} (USB terminate)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 344:{ICWiredBrowser.m} (--> USB Terminate)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 363:{ICWiredBrowser.m} (Reclaiming Resource: FlashBlu 30)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 363:{ICWiredBrowser.m} (Reclaiming Resource: FlashBlu 30)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 371:{ICWiredBrowser.m} (9 USB Descriptions Managed)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 373:{ICWiredBrowser.m} (<-- USB Terminate)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 509:{ICDDMessageCenter.m} (-Rem FlashBlu 30 - 0x0/0x0/0x0 - 0x100000 - ICDeviceDescriptionUpdated)
icdd: (ICALogging) [com.apple.imagecapture.icdd] #ICDebug - 509:{ICDDMessageCenter.m} (-Rem FlashBlu 30 - 0x8/0x6/0x50 - 0x100000 - ICDeviceDescriptionEmpty)
fseventsd: disk logger: failed to open output file /Volumes/EXFATUSB/.fseventsd/0000000001cd2cef (No such file or directory). mount point /Volumes/EXFATUSB/.fseventsd
fseventsd: disk logger: failed to open output file /Volumes/EXFATUSB/.fseventsd/0000000001cd2cef (No such file or directory). mount point /Volumes/EXFATUSB/.fseventsd
```

```
2017-03-31 17:53:18.873976-0500 0x6de
2017-03-31 17:53:18.874195-0500 0x6de
2017-03-31 18:02:59.225804-0500 0x3cd356
2017-03-31 18:02:59.225919-0500 0x3cd356
```

EXTERNAL MEDIA
…OR PRINTERS AND PHONES!

```
460:{ICDDMessageCenter.m} (+Add Brother HL-2170W series - _printer._tcp. - ICDeviceDescriptionUnsupported)
460:{ICDDMessageCenter.m} (+Add Brother HL-2170W series - _pdl-datastream._tcp. - ICDeviceDescriptionUnsupported)
460:{ICDDMessageCenter.m} (+Add Brother HL-2170W series - _ipp._tcp. - ICDeviceDescriptionUnsupported)
```

```
23:{ICWiredBrowser.m} (USB Device first match)
388:{ICWiredBrowser.m} (10 USB Descriptions Managed)
460:{ICDDMessageCenter.m} (+Add iPhone - 0x0/0x0/0x0 - 0x14300000 - ICDeviceDescriptionSUQuery)
37:{ICWiredBrowser.m} (USB Interface first match)
388:{ICWiredBrowser.m} (11 USB Descriptions Managed)
37:{ICWiredBrowser.m} (USB Interface first match)
388:{ICWiredBrowser.m} (12 USB Descriptions Managed)
213:{ICResourceManager.m} (30316264-6334-3638-6565-316531663062|iPhone|MANUFACTURER:Apple Inc.;MODEL:iPhone|SW=FALSE|)
460:{ICDDMessageCenter.m} (+Add iPhone - 0x0/0x0/0x0 - 0x14300000 - ICDeviceDescriptionAdded)
460:{ICDDMessageCenter.m} (+Add iPhone - 0x6/0x1/0x1 - 0x14300000 - ICDeviceDescriptionUpdated)
460:{ICDDMessageCenter.m} (+Add iPhone - 0xff/0xfe/0x2 - 0x14300000 - ICDeviceDescriptionSUQuery)
213:{ICResourceManager.m} (00000000-0000-0000-0000-000005AC12A8|iPhone|(null)|SW=FALSE|)
460:{ICDDMessageCenter.m} (+Add iPhone - 0xff/0xfe/0x2 - 0x14300000 - ICDeviceDescriptionUndefined)
51:{ICWiredBrowser.m} (USB terminate)
344:{ICWiredBrowser.m} (--> USB Terminate)
363:{ICWiredBrowser.m} (Reclaiming Resource: iPhone)
363:{ICWiredBrowser.m} (Reclaiming Resource: iPhone)
363:{ICWiredBrowser.m} (Reclaiming Resource: iPhone)
371:{ICWiredBrowser.m} (9 USB Descriptions Managed)
373:{ICWiredBrowser.m} (<-- USB Terminate)
509:{ICDDMessageCenter.m} (-Rem iPhone - 0x0/0x0/0x0 - 0x14300000 - ICDeviceDescriptionUpdated)
509:{ICDDMessageCenter.m} (-Rem iPhone - 0x6/0x1/0x1 - 0x14300000 - ICDeviceDescriptionUpdated)
509:{ICDDMessageCenter.m} (-Rem iPhone - 0xff/0xfe/0x2 - 0x14300000 - ICDeviceDescriptionEmpty)
```

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 (0x6080008fb600)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [StationXLabs] Removing handler (0x6080008fb600)
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] <stationxlabs@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 (0x608000ee7200)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [Google] Removing handler (0x608000ee7200)
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] <sledwards@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] [Google] Creating account sync task, 15 mailboxes needing status
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing handler (0x608000ef9280)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing handler (0x608000af6080)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing handler (0x608000ef9280)
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud - Inbox] Reset mailbox in sync state
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud] Removing handler (0x608000af6080)
Mail: (Mail) [com.apple.mail.AccountFetch] <oompa@csh.rit.edu@p02-imap.mail.me.com> Background fetch completed
Mail: (IMAP) [com.apple.mail.IMAPSyncActivity] [iCloud - Inbox] Reset mailbox in sync state
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"'
```

```
Timestamp                       PID
2017-03-31 18:28:00.674247-0400  27228  loginwindow: (Sharing) [com.apple.sharing.AutoUnlock] Dynamic store enabled state {
    501 = 1;
}
2017-03-31 18:28:00.764293-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Hints provider deactivated
2017-03-31 18:28:00.764337-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Invalidating hint provider
2017-03-31 18:28:00.764464-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Updating in progress state in dynamic store: NO
2017-03-31 18:28:00.764805-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Received screen lock unlocked notification
2017-03-31 18:28:00.764863-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Clearing Auto Unlock device cache
2017-03-31 18:28:00.764876-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Hints provider deactivated
2017-03-31 18:28:00.764912-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Invalidating hint provider
2017-03-31 18:28:00.765707-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Updating in progress state in dynamic store: NO
2017-03-31 18:28:00.813506-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Client bundle ID: (null)
2017-03-31 18:28:00.826964-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Client bundle ID: (null)
2017-03-31 18:28:00.984235-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Auth session -- create (session id: 278149119)
2017-03-31 18:28:00.984273-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Auth session -- reset (session id: 278149119)
2017-03-31 18:28:00.986155-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Device version: 3
2017-03-31 18:28:01.015652-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Auth session -- create (session id: 1034777402)
2017-03-31 18:28:01.015693-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Auth session -- reset (session id: 1034777402)
2017-03-31 18:28:01.017560-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Updating enable state in dynamic store: YES
2017-03-31 18:28:01.017959-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Enabled dictionary exists {
    501 = 1;
}
2017-03-31 18:28:01.018020-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Local LTK Exists
2017-03-31 18:28:01.038807-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Keychain devices: ("01F1072E-9084-4A6D-81C0-573252
2017-03-31 18:28:01.058765-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Updated remote LTKs: ("47B476E2-6B76-4D3D-B078-A24
305AF1A21")
2017-03-31 18:28:01.058853-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Remote LTK data: <private>
2017-03-31 18:28:01.065266-0400  27339  sharingd: [com.apple.sharing.AutoUnlock] Checking remote LTKs
```

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"'
```

```
[bit:LogsUnite oompa$ log show --info system_logs.logarchive/ --predicate 'subsystem = "com.apple.sharing" and category = "AutoUnlock" and eventMessage contai]
ns[cd] "Found Peer"'
==========
/Users/oompa/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""
Timestamp                       Thread     Type        Activity             PID
2017-03-23 21:15:58.940782-0400 0x5e716    Default     0x0                  406    sharingd: [com.apple.sharing.AutoUnlock] Found peer callback
2017-03-23 21:15:58.940935-0400 0x5e716    Default     0x0                  406    sharingd: [com.apple.sharing.AutoUnlock] Found Peer:
        Device <name:miPhone7, uniqueID:F9B85FFC-2BC6-4E80-93DA-67508472C8F8, bluetooth ID:F768D25B-1EC8-476B-B4A3-D757890CD2E8, modelIdentifier:iPhone9,3>,
        Peer <SFBLEDevice ID f768d25b-1ec8-476b-b4a3-d757890cd2e8, AdvData '0a40', RSSI -47, 0, [-47], Name '?', Paired no>,
        Unlock Enabled: NO,
        Proxy Unlock Enabled: YES,
        Locked on Wrist: NO
2017-03-23 21:16:00.086856-0400 0x5e716    Default     0x0                  406    sharingd: [com.apple.sharing.AutoUnlock] Found peer callback
2017-03-23 21:16:00.087012-0400 0x5e716    Default     0x0                  406    sharingd: [com.apple.sharing.AutoUnlock] Found Peer:
        Device <name:miWatch, uniqueID:47B476E2-6B76-4D3D-B078-A24305AF1A21, bluetooth ID:C905A733-BEA0-4680-A41F-4DCDF577A099, modelIdentifier:Watch2,3>,
        Peer <SFBLEDevice ID c905a733-bea0-4680-a41f-4dcdf577a099, AdvData '0180', RSSI -38, 0, [-38], Name '?', Paired no>,
        Unlock Enabled: YES,
        Proxy Unlock Enabled: NO,
        Locked on Wrist: NO
```

REFERENCE MATERIALS

- man log on macOS
- https://developer.apple.com/videos/play/wwdc2016/721/
- https://developer.apple.com/reference/os/logging
- http://devstreaming.apple.com/videos/wwdc/2016/721wh2etddp4ghxhpcg/721/721_unified_logging_and_activity_tracing.pdf
- http://devstreaming.apple.com/videos/wwdc/2014/714xx1h4szxdnyz/714/714_fix_bugs_faster_using_activity_tracing.pdf
- 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/
- https://github.com/mac4n6/Presentations/blob/master/Analysis%20and%20Correlation%20of%20Mac%20Logs/Analysis_and_Correlation_of_Mac_Logs_2016.pdf