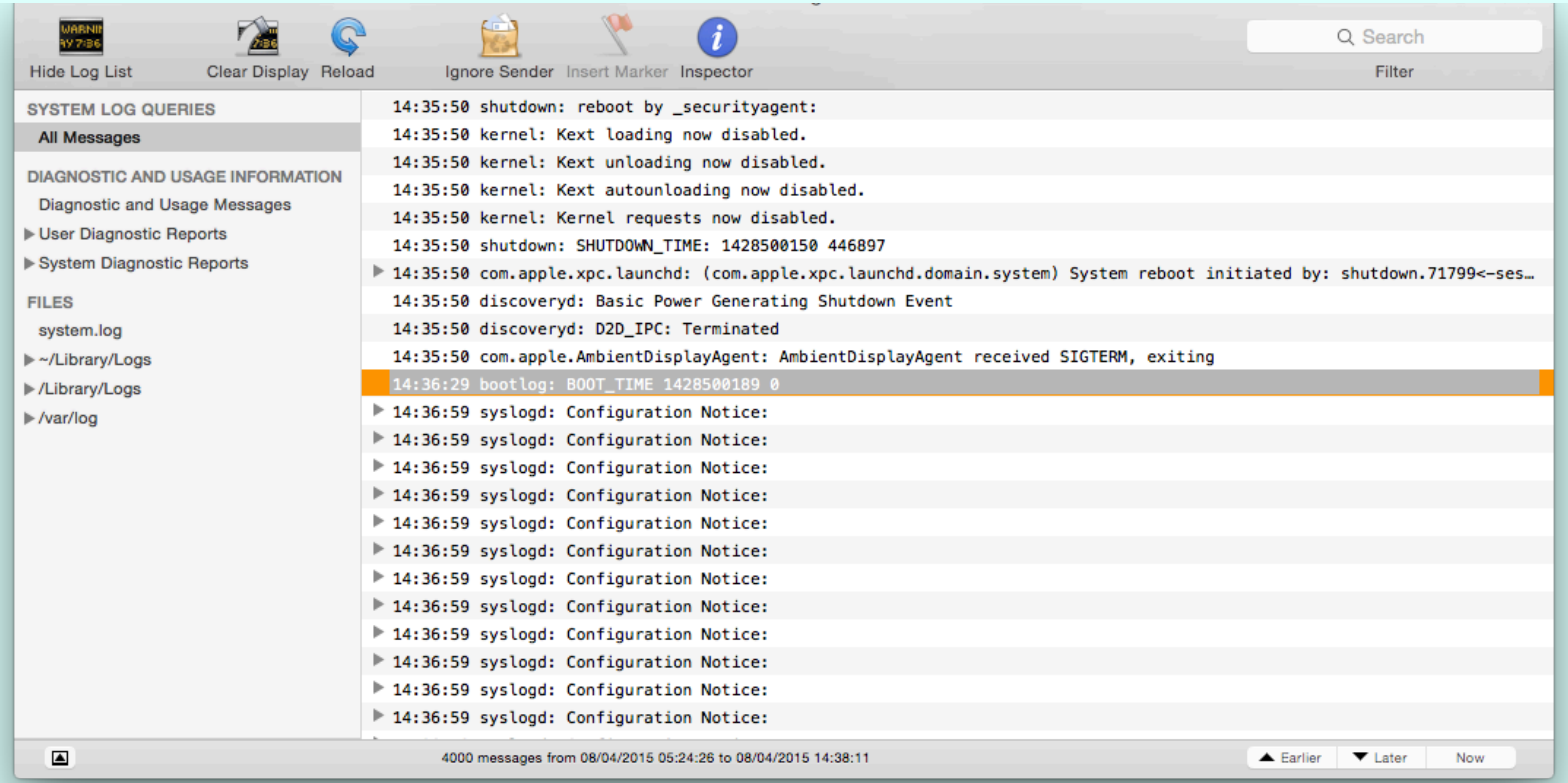
Apple Unified Log

Howard Oakley

https://eclecticlight.co



```
14:35:50 shutdown: reboot by _securityagent:
14:35:50 kernel: Kext loading now disabled.
14:35:50 kernel: Kext unloading now disabled.
14:35:50 kernel: Kext autounloading now disabled.
14:35:50 kernel: Kernel requests now disabled.
14:35:50 shutdown: SHUTDOWN_TIME: 1428500150 446897
14:35:50 com.apple.xpc.launchd: (com.apple.xpc.launchd.domain.system) System reboot initiated by: shutdown.71799<-ses…
14:35:50 discoveryd: Basic Power Generating Shutdown Event
14:35:50 discoveryd: D2D_IPC: Terminated
14:35:50 com.apple.AmbientDisplayAgent: AmbientDisplayAgent received SIGTERM, exiting
14:36:29 bootlog: BOOT_TIME 1428500189 0
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
14:36:59 syslogd: Configuration Notice:
```

4000 messages from 08/04/2015 05:24:26 to 08/04/2015 14:38:11

El Capitan

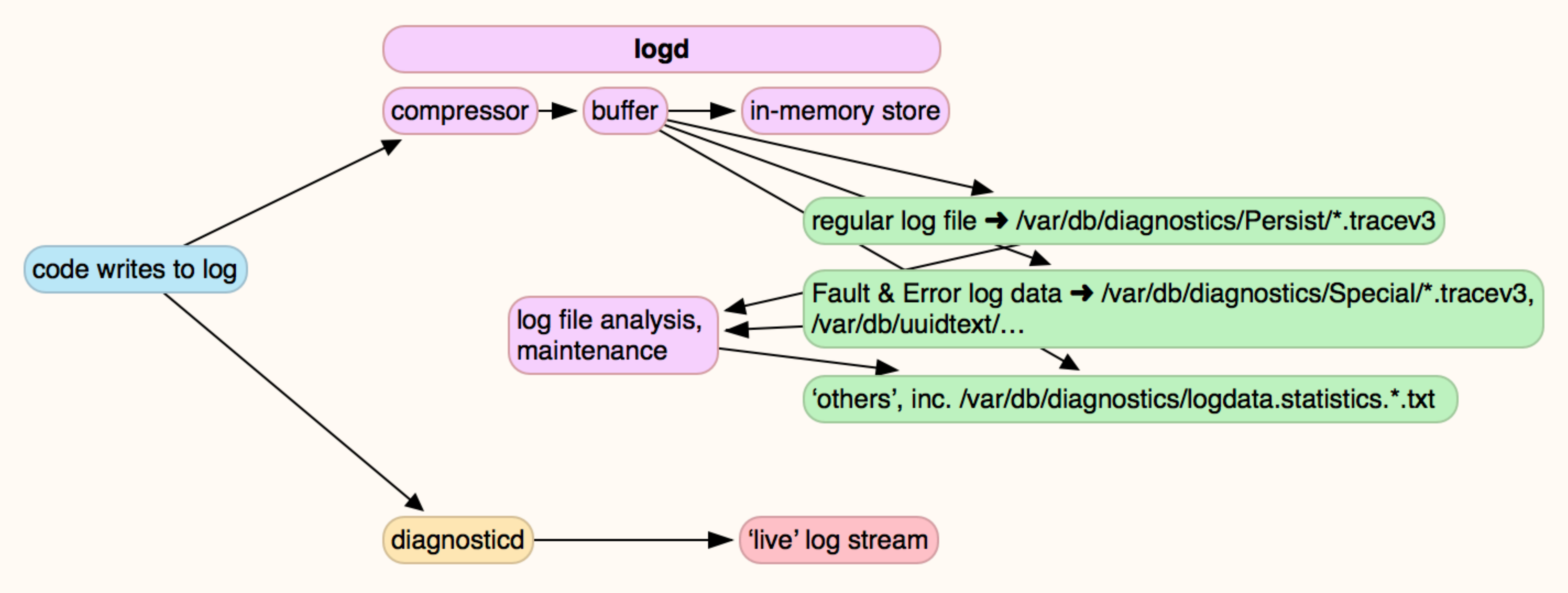
Up to 4000 log entries in 8-9 hours

Apple’s Goals 1

- a single efficient logging mechanism for user and kernel mode
- to maximise information collection with minimum observer effect
- the compression of log data
- a managed log message lifecycle
- as much logging on as much of the time as possible

Apple’s Goals 2

- for privacy to be designed into the logging system
- a common system across macOS, iOS, watchOS, tvOS
- all legacy APIs (NSLog, asl_log_message, syslog, etc.) to be redirected into the new unified log
- to emphasise debugging of macOS and apps, not providing any facilities for system administration or audit
- to link to the `sysdiagnose` tool for gathering information for bug reports etc.



logd

compressor

buffer

in-memory store

code writes to log

regular log file ➜ /var/db/diagnostics/Persist/*.tracev3

Fault & Error log data ➜ /var/db/diagnostics/Special/*.tracev3, /var/db/uuidtext/…

log file analysis, maintenance

'others', inc. /var/db/diagnostics/logdata.statistics.*.txt

diagnosticd

'live' log stream

Implementation of Unified log in Sierra, High Sierra

.tracev3 logs

- compressed binary format
- undocumented
- very efficient
- only accessible using `log` command and Console (closed source)
- Apple does not want us to access them direct

Log entry levels

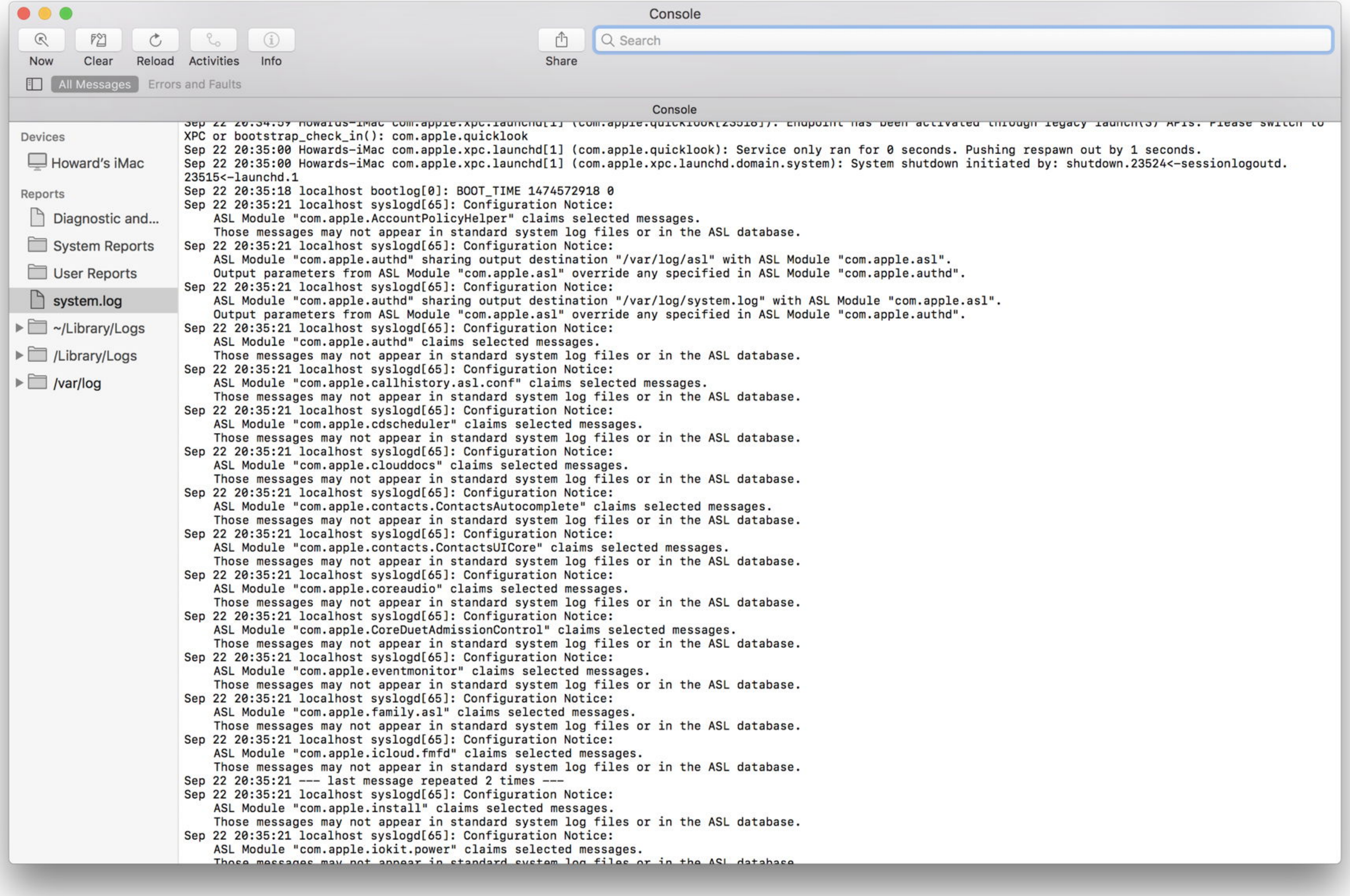
- Fault – saved to disk, often have additional info attached (large)
- Error – saved to disk, additional info
- Default – saved to disk, normally single entries
- Info – saved to memory, optionally to disk, single entries
- Debug – only when enabled by `log` command

Privacy

- by default, static strings are saved in full
- by default, dynamic strings, collections, objects are censored
- programmer can override, but often left to the default
- have been bugs as well
- many log entries are made information-free by **`<private>`**

Logs not yet unified

- daily.out, monthly.out, wifi.log
- /var/log/install.log, a valuable log of `softwareupdate` etc. installations
- CUPS in /var/log/cups
- third-party apps, e.g. Adobe CS/CC
- system.log, now a wasteland for legacy apps



```
Sep 22 20:34:59 Howards-iMac com.apple.xpc.launchd[1] (com.apple.quicklook[23518]): Endpoint has been activated through legacy launch(3) APIs. Please switch to
XPC or bootstrap_check_in(): com.apple.quicklook
Sep 22 20:35:00 Howards-iMac com.apple.xpc.launchd[1] (com.apple.quicklook): Service only ran for 0 seconds. Pushing respawn out by 1 seconds.
Sep 22 20:35:00 Howards-iMac com.apple.xpc.launchd[1] (com.apple.xpc.launchd.domain.system): System shutdown initiated by: shutdown.23524<-sessionlogoutd.
23515<-launchd.1
Sep 22 20:35:18 localhost bootlog[0]: BOOT_TIME 1474572918 0
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.AccountPolicyHelper" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.authd" sharing output destination "/var/log/asl" with ASL Module "com.apple.asl".
    Output parameters from ASL Module "com.apple.asl" override any specified in ASL Module "com.apple.authd".
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.authd" sharing output destination "/var/log/system.log" with ASL Module "com.apple.asl".
    Output parameters from ASL Module "com.apple.asl" override any specified in ASL Module "com.apple.authd".
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.authd" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.callhistory.asl.conf" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.cdscheduler" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.clouddocs" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.contacts.ContactsAutocomplete" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.contacts.ContactsUICore" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.coreaudio" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.CoreDuetAdmissionControl" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.eventmonitor" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.family.asl" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.icloud.fmfd" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 --- last message repeated 2 times ---
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.install" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
Sep 22 20:35:21 localhost syslogd[65]: Configuration Notice:
    ASL Module "com.apple.iokit.power" claims selected messages.
    Those messages may not appear in standard system log files or in the ASL database.
```

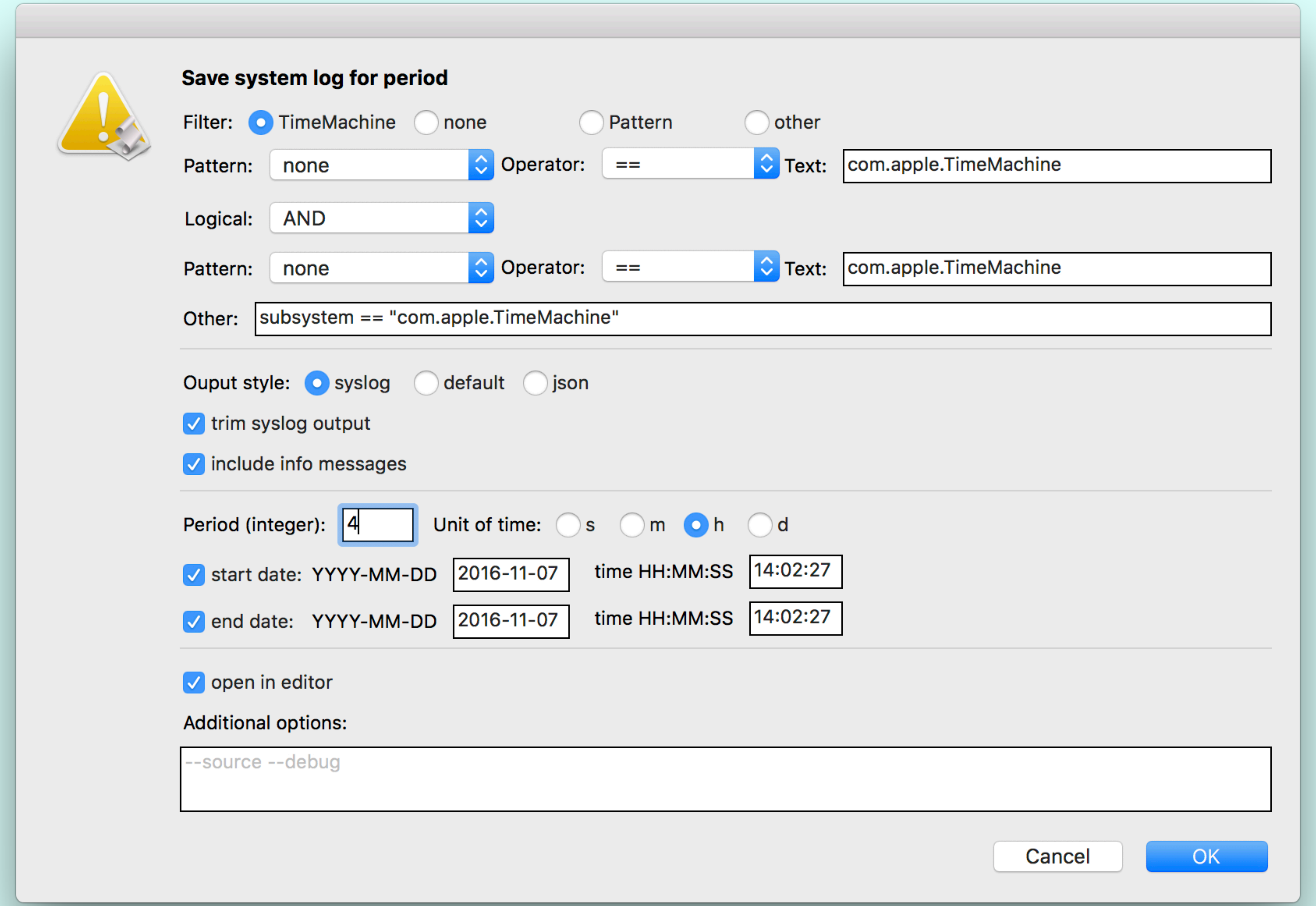
Console (Sierra)

Console

- works with live log stream from `diagnosticd`, current entries only
- works with logarchive packages, but easily overwhelmed
- predicate editing sucks (Sierra)
- trying to examine a past event such as a startup too difficult

`log` command

- very powerful
- complex to use
- `man log`
- live streaming with `log stream`, but constrained by firehose
- most useful is `log show`
- at the heart of all my tools



Save system log for period

Filter: ● TimeMachine ○ none ○ Pattern ○ other

Pattern: none Operator: == Text: com.apple.TimeMachine

Logical: AND

Pattern: none Operator: == Text: com.apple.TimeMachine

Other: subsystem == "com.apple.TimeMachine"

Ouput style: ● syslog ○ default ○ json

☑ trim syslog output

☑ include info messages

Period (integer): 4 Unit of time: ○ s ○ m ● h ○ d

☑ start date: YYYY-MM-DD 2016-11-07 time HH:MM:SS 14:02:27

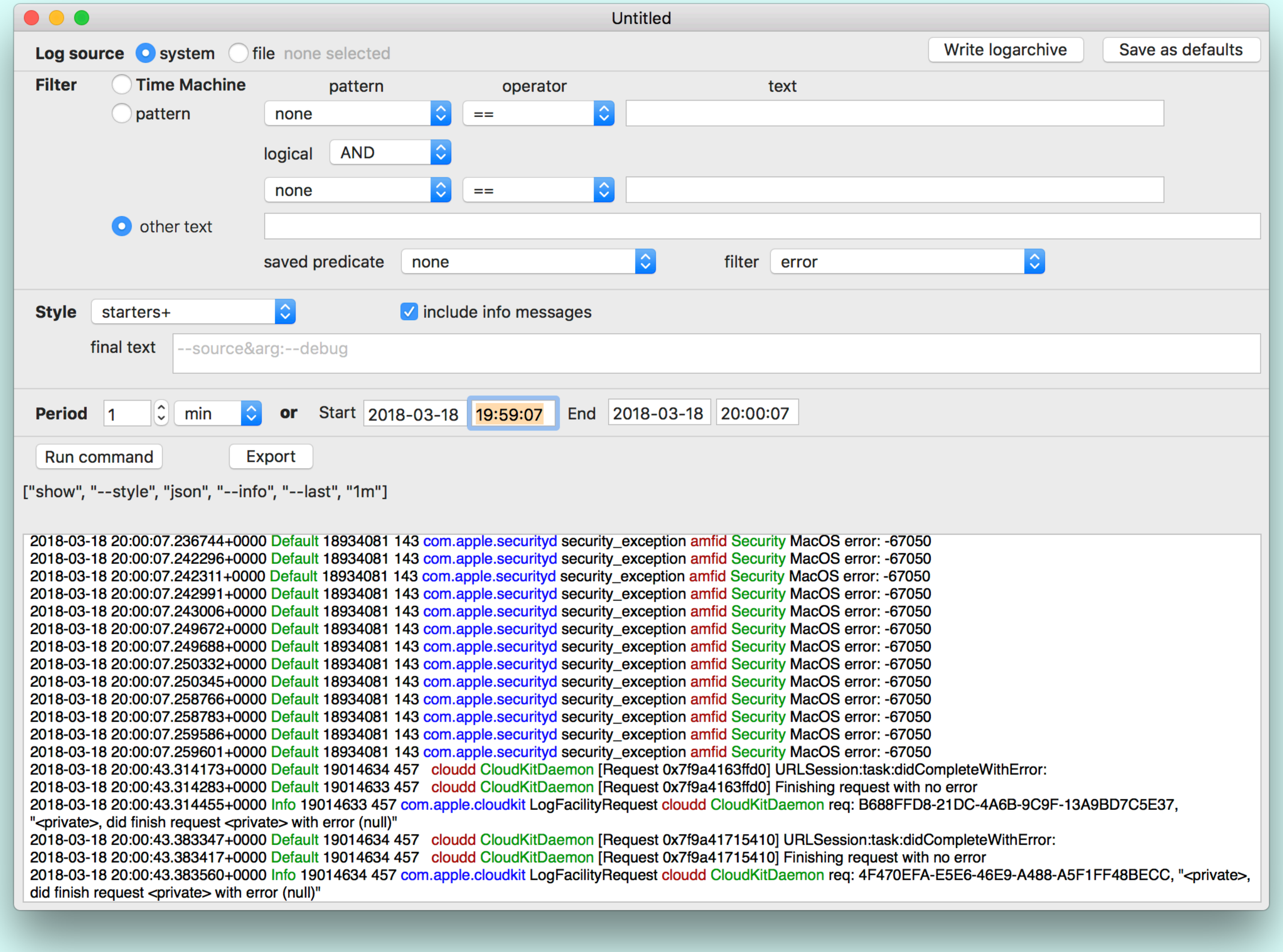
☑ end date: YYYY-MM-DD 2016-11-07 time HH:MM:SS 14:02:27

☑ open in editor

Additional options:

--source --debug

LogLogger (AppleScript, Oct 2016 - Jan 2017)



Log source ● system ○ file none selected

Filter ○ Time Machine

○ pattern — pattern: none, operator: ==, text:

logical: AND

pattern: none, operator: ==, text:

● other text

saved predicate: none   filter: error

Style: starters+   ☑ include info messages

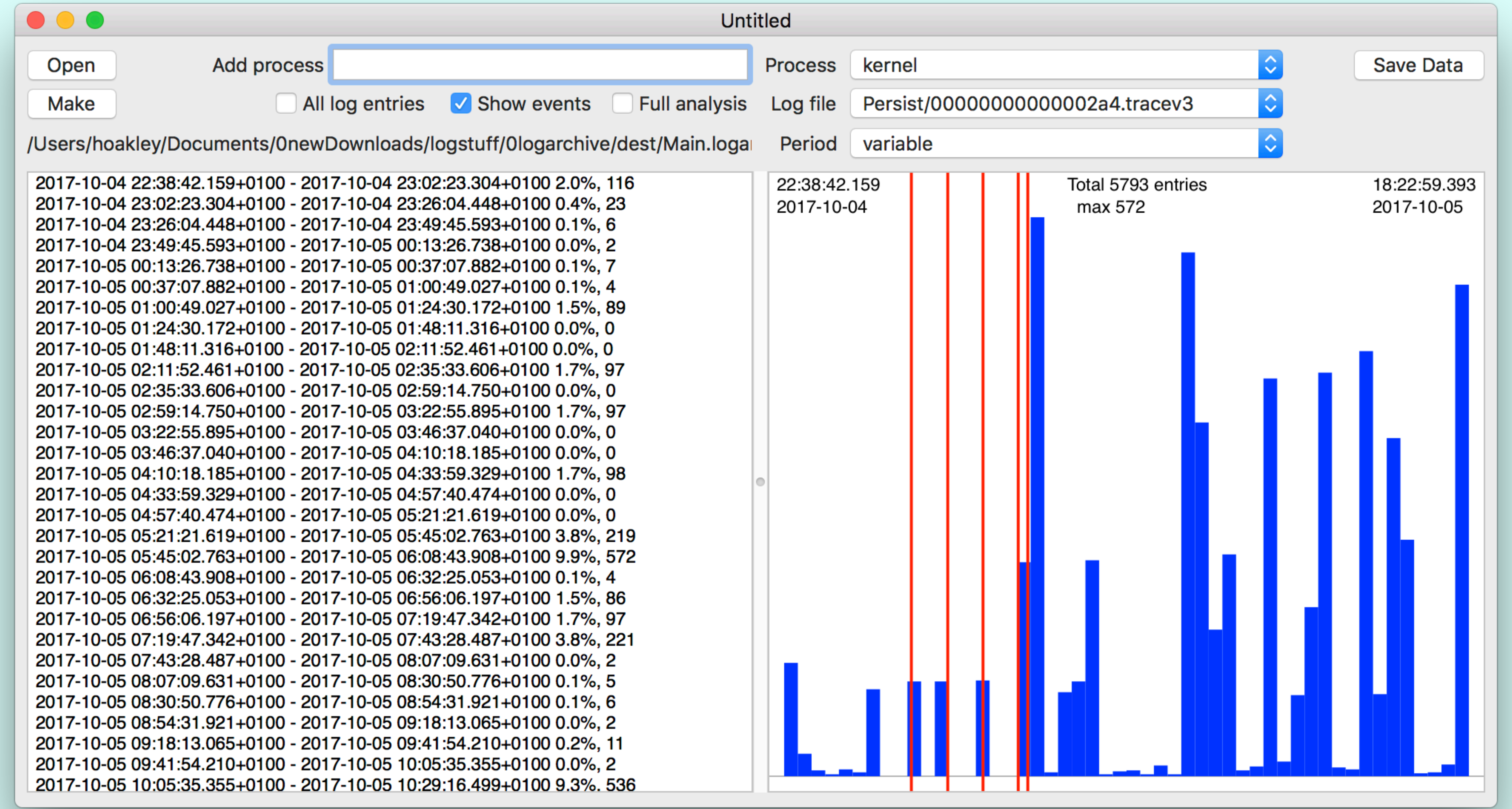
final text: --source&arg:--debug

Period 1 min or Start 2018-03-18 19:59:07 End 2018-03-18 20:00:07

```
["show", "--style", "json", "--info", "--last", "1m"]
```

```
2018-03-18 20:00:07.236744+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.242296+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.242311+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.242991+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.243006+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.249672+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.249688+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.250332+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.250345+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.258766+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.258783+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259586+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259601+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:43.314173+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.314283+0000 Default 19014633 457   cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] Finishing request with no error
2018-03-18 20:00:43.314455+0000 Info 19014633 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: B688FFD8-21DC-4A6B-9C9F-13A9BD7C5E37,
"<private>, did finish request <private> with error (null)"
2018-03-18 20:00:43.383347+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a41715410] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.383417+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a41715410] Finishing request with no error
2018-03-18 20:00:43.383560+0000 Info 19014634 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: 4F470EFA-E5E6-46E9-A488-A5F1FF48BECC, "<private>,
did finish request <private> with error (null)"
```

Consolation 3



Add process

☐ All log entries ☑ Show events ☐ Full analysis

Process: kernel

Log file: Persist/00000000000002a4.tracev3

Period: variable

/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logai

```
2017-10-04 22:38:42.159+0100 - 2017-10-04 23:02:23.304+0100 2.0%, 116
2017-10-04 23:02:23.304+0100 - 2017-10-04 23:26:04.448+0100 0.4%, 23
2017-10-04 23:26:04.448+0100 - 2017-10-04 23:49:45.593+0100 0.1%, 6
2017-10-04 23:49:45.593+0100 - 2017-10-05 00:13:26.738+0100 0.0%, 2
2017-10-05 00:13:26.738+0100 - 2017-10-05 00:37:07.882+0100 0.1%, 7
2017-10-05 00:37:07.882+0100 - 2017-10-05 01:00:49.027+0100 0.1%, 4
2017-10-05 01:00:49.027+0100 - 2017-10-05 01:24:30.172+0100 1.5%, 89
2017-10-05 01:24:30.172+0100 - 2017-10-05 01:48:11.316+0100 0.0%, 0
2017-10-05 01:48:11.316+0100 - 2017-10-05 02:11:52.461+0100 0.0%, 0
2017-10-05 02:11:52.461+0100 - 2017-10-05 02:35:33.606+0100 1.7%, 97
2017-10-05 02:35:33.606+0100 - 2017-10-05 02:59:14.750+0100 0.0%, 0
2017-10-05 02:59:14.750+0100 - 2017-10-05 03:22:55.895+0100 1.7%, 97
2017-10-05 03:22:55.895+0100 - 2017-10-05 03:46:37.040+0100 0.0%, 0
2017-10-05 03:46:37.040+0100 - 2017-10-05 04:10:18.185+0100 0.0%, 0
2017-10-05 04:10:18.185+0100 - 2017-10-05 04:33:59.329+0100 1.7%, 98
2017-10-05 04:33:59.329+0100 - 2017-10-05 04:57:40.474+0100 0.0%, 0
2017-10-05 04:57:40.474+0100 - 2017-10-05 05:21:21.619+0100 0.0%, 0
2017-10-05 05:21:21.619+0100 - 2017-10-05 05:45:02.763+0100 3.8%, 219
2017-10-05 05:45:02.763+0100 - 2017-10-05 06:08:43.908+0100 9.9%, 572
2017-10-05 06:08:43.908+0100 - 2017-10-05 06:32:25.053+0100 0.1%, 4
2017-10-05 06:32:25.053+0100 - 2017-10-05 06:56:06.197+0100 1.5%, 86
2017-10-05 06:56:06.197+0100 - 2017-10-05 07:19:47.342+0100 1.7%, 97
2017-10-05 07:19:47.342+0100 - 2017-10-05 07:43:28.487+0100 3.8%, 221
2017-10-05 07:43:28.487+0100 - 2017-10-05 08:07:09.631+0100 0.0%, 2
2017-10-05 08:07:09.631+0100 - 2017-10-05 08:30:50.776+0100 0.1%, 5
2017-10-05 08:30:50.776+0100 - 2017-10-05 08:54:31.921+0100 0.1%, 6
2017-10-05 08:54:31.921+0100 - 2017-10-05 09:18:13.065+0100 0.0%, 2
2017-10-05 09:18:13.065+0100 - 2017-10-05 09:41:54.210+0100 0.2%, 11
2017-10-05 09:41:54.210+0100 - 2017-10-05 10:05:35.355+0100 0.0%, 2
2017-10-05 10:05:35.355+0100 - 2017-10-05 10:29:16.499+0100 9.3%, 536
```

Woodpile

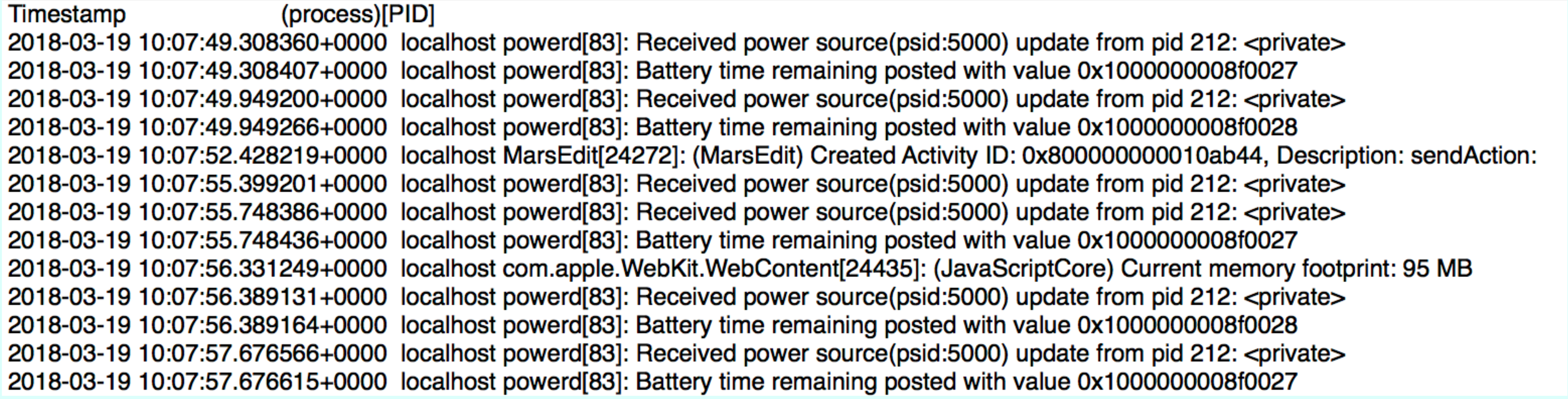
Free tools

- Consolation 2, RunConsolation (2), Consolation 3
- Blowhole – command tool to write to the log, e.g. for shell scripts
- Woodpile
- DispatchView – specialised look at DAS and CTS dispatching
- T2M2, RunT2M2 – Time Machine log analysis and diagnosis

Content & formats

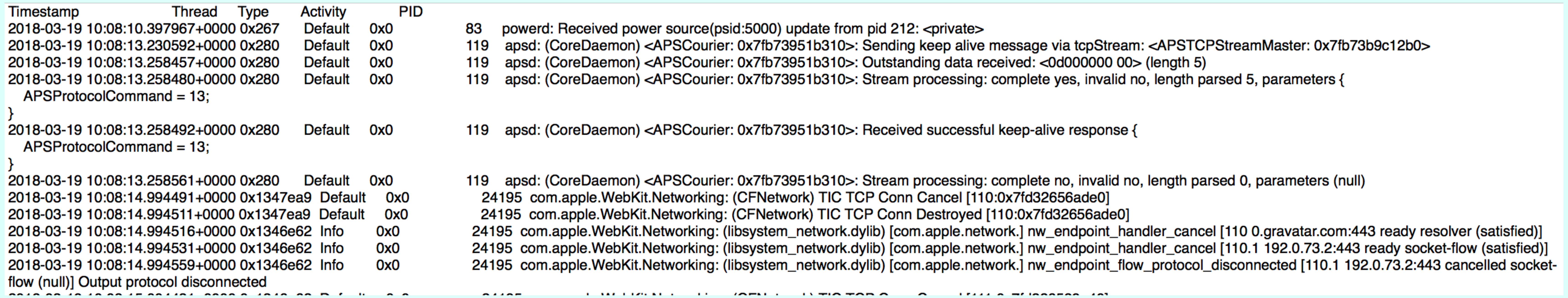
Each log entry is structured into data fields

syslog



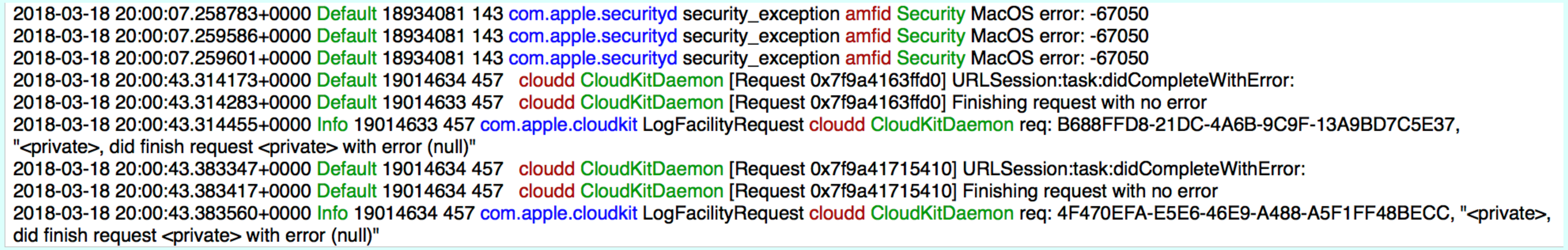
```
Timestamp                    (process)[PID]
2018-03-19 10:07:49.308360+0000  localhost powerd[83]: Received power source(psid:5000) update from pid 212: <private>
2018-03-19 10:07:49.308407+0000  localhost powerd[83]: Battery time remaining posted with value 0x1000000008f0027
2018-03-19 10:07:49.949200+0000  localhost powerd[83]: Received power source(psid:5000) update from pid 212: <private>
2018-03-19 10:07:49.949266+0000  localhost powerd[83]: Battery time remaining posted with value 0x1000000008f0028
2018-03-19 10:07:52.428219+0000  localhost MarsEdit[24272]: (MarsEdit) Created Activity ID: 0x80000000010ab44, Description: sendAction:
2018-03-19 10:07:55.399201+0000  localhost powerd[83]: Received power source(psid:5000) update from pid 212: <private>
2018-03-19 10:07:55.748386+0000  localhost powerd[83]: Received power source(psid:5000) update from pid 212: <private>
2018-03-19 10:07:55.748436+0000  localhost powerd[83]: Battery time remaining posted with value 0x1000000008f0027
2018-03-19 10:07:56.331249+0000  localhost com.apple.WebKit.WebContent[24435]: (JavaScriptCore) Current memory footprint: 95 MB
2018-03-19 10:07:56.389131+0000  localhost powerd[83]: Received power source(psid:5000) update from pid 212: <private>
2018-03-19 10:07:56.389164+0000  localhost powerd[83]: Battery time remaining posted with value 0x1000000008f0028
2018-03-19 10:07:57.676566+0000  localhost powerd[83]: Received power source(psid:5000) update from pid 212: <private>
2018-03-19 10:07:57.676615+0000  localhost powerd[83]: Battery time remaining posted with value 0x1000000008f0027
```

default

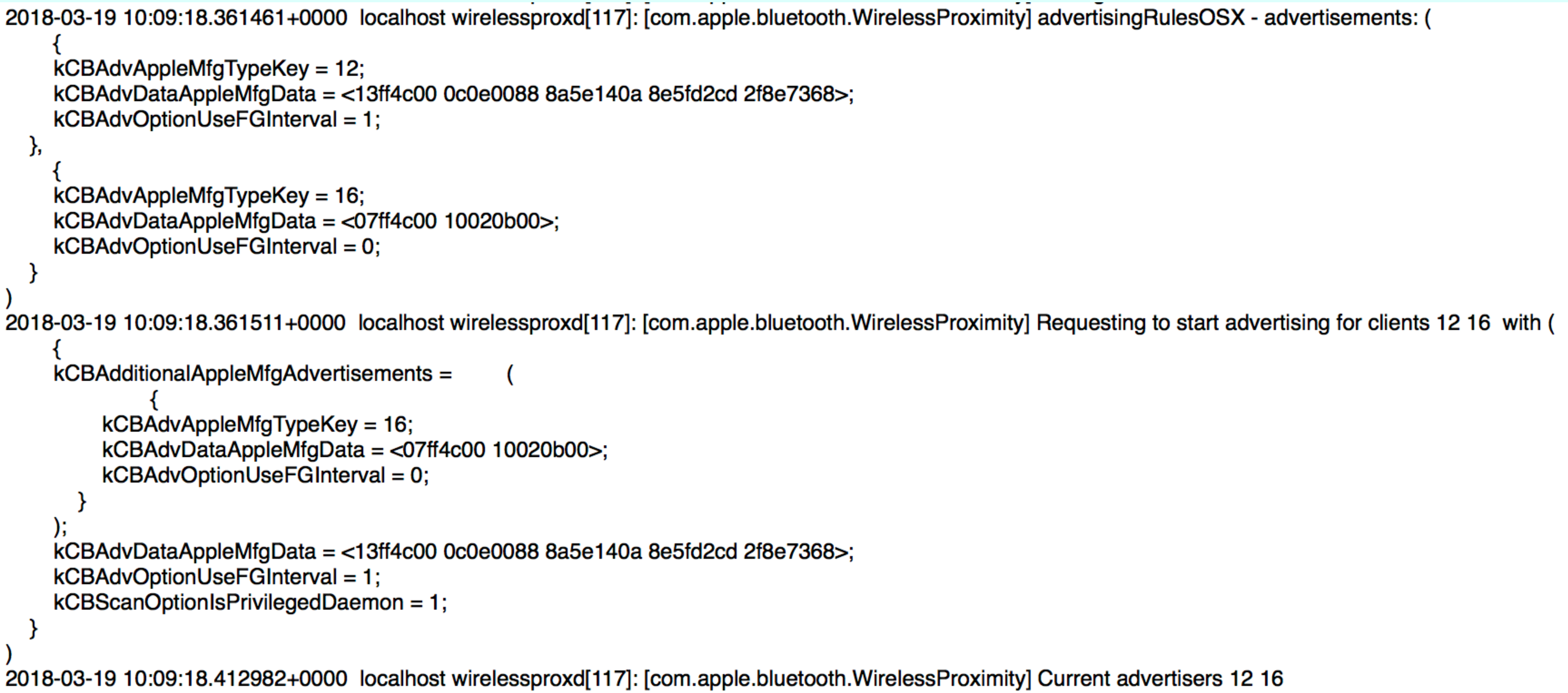


```
Timestamp                     Thread    Type      Activity          PID
2018-03-19 10:08:10.397967+0000 0x267     Default    0x0              83    powerd: Received power source(psid:5000) update from pid 212: <private>
2018-03-19 10:08:13.230592+0000 0x280     Default    0x0              119   apsd: (CoreDaemon) <APSCourier: 0x7fb73951b310>: Sending keep alive message via tcpStream: <APSTCPStreamMaster: 0x7fb73b9c12b0>
2018-03-19 10:08:13.258457+0000 0x280     Default    0x0              119   apsd: (CoreDaemon) <APSCourier: 0x7fb73951b310>: Outstanding data received: <0d000000 00> (length 5)
2018-03-19 10:08:13.258480+0000 0x280     Default    0x0              119   apsd: (CoreDaemon) <APSCourier: 0x7fb73951b310>: Stream processing: complete yes, invalid no, length parsed 5, parameters {
   APSProtocolCommand = 13;
}
2018-03-19 10:08:13.258492+0000 0x280     Default    0x0              119   apsd: (CoreDaemon) <APSCourier: 0x7fb73951b310>: Received successful keep-alive response {
   APSProtocolCommand = 13;
}
2018-03-19 10:08:13.258561+0000 0x280     Default    0x0              119   apsd: (CoreDaemon) <APSCourier: 0x7fb73951b310>: Stream processing: complete no, invalid no, length parsed 0, parameters (null)
2018-03-19 10:08:14.994491+0000 0x1347ea9  Default    0x0              24195  com.apple.WebKit.Networking: (CFNetwork) TIC TCP Conn Cancel [110:0x7fd32656ade0]
2018-03-19 10:08:14.994511+0000 0x1347ea9  Default    0x0              24195  com.apple.WebKit.Networking: (CFNetwork) TIC TCP Conn Destroyed [110:0x7fd32656ade0]
2018-03-19 10:08:14.994516+0000 0x1346e62  Info      0x0             24195  com.apple.WebKit.Networking: (libsystem_network.dylib) [com.apple.network.] nw_endpoint_handler_cancel [110 0.gravatar.com:443 ready resolver (satisfied)]
2018-03-19 10:08:14.994531+0000 0x1346e62  Info      0x0             24195  com.apple.WebKit.Networking: (libsystem_network.dylib) [com.apple.network.] nw_endpoint_handler_cancel [110.1 192.0.73.2:443 ready socket-flow (satisfied)]
2018-03-19 10:08:14.994559+0000 0x1346e62  Info      0x0             24195  com.apple.WebKit.Networking: (libsystem_network.dylib) [com.apple.network.] nw_endpoint_flow_protocol_disconnected [110.1 192.0.73.2:443 cancelled socket-
flow (null)] Output protocol disconnected
```

Consolation



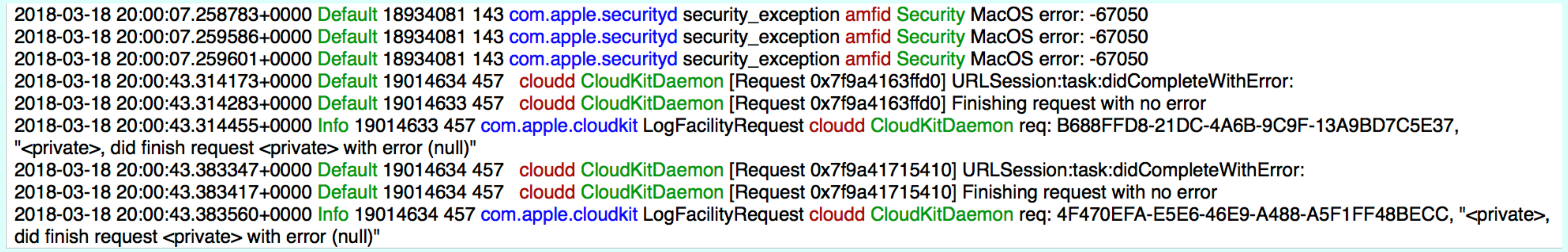
```
2018-03-18 20:00:07.258783+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259586+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259601+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:43.314173+0000 Default 19014634 457  cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.314283+0000 Default 19014633 457  cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] Finishing request with no error
2018-03-18 20:00:43.314455+0000 Info 19014633 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: B688FFD8-21DC-4A6B-9C9F-13A9BD7C5E37,
"<private>, did finish request <private> with error (null)"
2018-03-18 20:00:43.383347+0000 Default 19014634 457  cloudd CloudKitDaemon [Request 0x7f9a41715410] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.383417+0000 Default 19014634 457  cloudd CloudKitDaemon [Request 0x7f9a41715410] Finishing request with no error
2018-03-18 20:00:43.383560+0000 Info 19014634 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: 4F470EFA-E5E6-46E9-A488-A5F1FF48BECC, "<private>,
did finish request <private> with error (null)"
```



```
2018-03-19 10:09:18.361461+0000  localhost wirelessproxd[117]: [com.apple.bluetooth.WirelessProximity] advertisingRulesOSX - advertisements: (
        {
        kCBAdvAppleMfgTypeKey = 12;
        kCBAdvDataAppleMfgData = <13ff4c00 0c0e0088 8a5e140a 8e5fd2cd 2f8e7368>;
        kCBAdvOptionUseFGInterval = 1;
    },
        {
        kCBAdvAppleMfgTypeKey = 16;
        kCBAdvDataAppleMfgData = <07ff4c00 10020b00>;
        kCBAdvOptionUseFGInterval = 0;
    }
)
2018-03-19 10:09:18.361511+0000  localhost wirelessproxd[117]: [com.apple.bluetooth.WirelessProximity] Requesting to start advertising for clients 12 16  with (
        {
        kCBAdditionalAppleMfgAdvertisements =         (
                        {
                kCBAdvAppleMfgTypeKey = 16;
                kCBAdvDataAppleMfgData = <07ff4c00 10020b00>;
                kCBAdvOptionUseFGInterval = 0;
            }
        );
        kCBAdvDataAppleMfgData = <13ff4c00 0c0e0088 8a5e140a 8e5fd2cd 2f8e7368>;
        kCBAdvOptionUseFGInterval = 1;
        kCBScanOptionIsPrivilegedDaemon = 1;
    }
)
2018-03-19 10:09:18.412982+0000  localhost wirelessproxd[117]: [com.apple.bluetooth.WirelessProximity] Current advertisers 12 16
```

multi-line entries

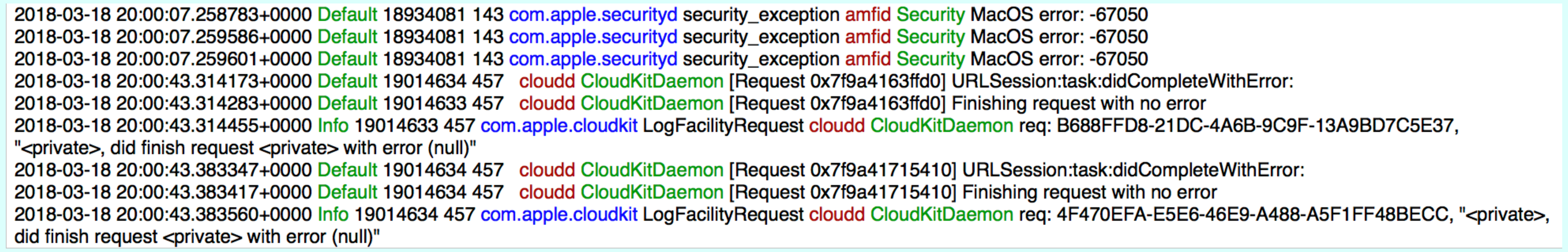
Log fields 1



```
2018-03-18 20:00:07.258783+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259586+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259601+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:43.314173+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.314283+0000 Default 19014633 457   cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] Finishing request with no error
2018-03-18 20:00:43.314455+0000 Info 19014633 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: B688FFD8-21DC-4A6B-9C9F-13A9BD7C5E37,
"<private>, did finish request <private> with error (null)"
2018-03-18 20:00:43.383347+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a41715410] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.383417+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a41715410] Finishing request with no error
2018-03-18 20:00:43.383560+0000 Info 19014634 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: 4F470EFA-E5E6-46E9-A488-A5F1FF48BECC, "<private>,
did finish request <private> with error (null)"
```

- **timestamp**, in full, 2017-07-26 20:24:59.326229+0100
- machTimestamp, in system ticks, 608403543041193
- messageType, Default
- category, security_exception
- **subsystem**, com.apple.securityd
- processUniqueID, 156
- threadID, 868
- traceID, 833721519476834308

Log fields 2



```
2018-03-18 20:00:07.258783+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259586+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:07.259601+0000 Default 18934081 143 com.apple.securityd security_exception amfid Security MacOS error: -67050
2018-03-18 20:00:43.314173+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.314283+0000 Default 19014633 457   cloudd CloudKitDaemon [Request 0x7f9a4163ffd0] Finishing request with no error
2018-03-18 20:00:43.314455+0000 Info 19014633 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: B688FFD8-21DC-4A6B-9C9F-13A9BD7C5E37,
"<private>, did finish request <private> with error (null)"
2018-03-18 20:00:43.383347+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a41715410] URLSession:task:didCompleteWithError:
2018-03-18 20:00:43.383417+0000 Default 19014634 457   cloudd CloudKitDaemon [Request 0x7f9a41715410] Finishing request with no error
2018-03-18 20:00:43.383560+0000 Info 19014634 457 com.apple.cloudkit LogFacilityRequest cloudd CloudKitDaemon req: 4F470EFA-E5E6-46E9-A488-A5F1FF48BECC, "<private>,
did finish request <private> with error (null)"
```

- senderProgramCounter, 193733726
- processID, 156
- **eventMessage**, MacOS error: -67062
- **processImagePath**, /usr/libexec/taskgated
- processImageUUID, 4F6F0B24-7A18-3AF9-853F-8F72F6C7D7C7
- **senderImagePath**, /System/Library/Frameworks/Security.framework/Versions/A/Security
- senderImageUUID, 005E8C96-40B6-35E3-B58B-888A5F5957C2
- timezoneName, may be blank.

Extraction

- live in /var/db, or logarchive?
- you can’t analyse isolated tracev3 files
- time period – last *X* s/m/h/d or defined start – end
- filter predicate(s)

Filter predicates

```
subsystem == “com.apple.duetactivityscheduler”
```

```
subsystem == "com.apple.duetactivityscheduler" ||
subsystem == "com.apple.xpc.activity" ||
(subsystem == "com.apple.TimeMachine" &&
eventMessage CONTAINS[c] “start")
```

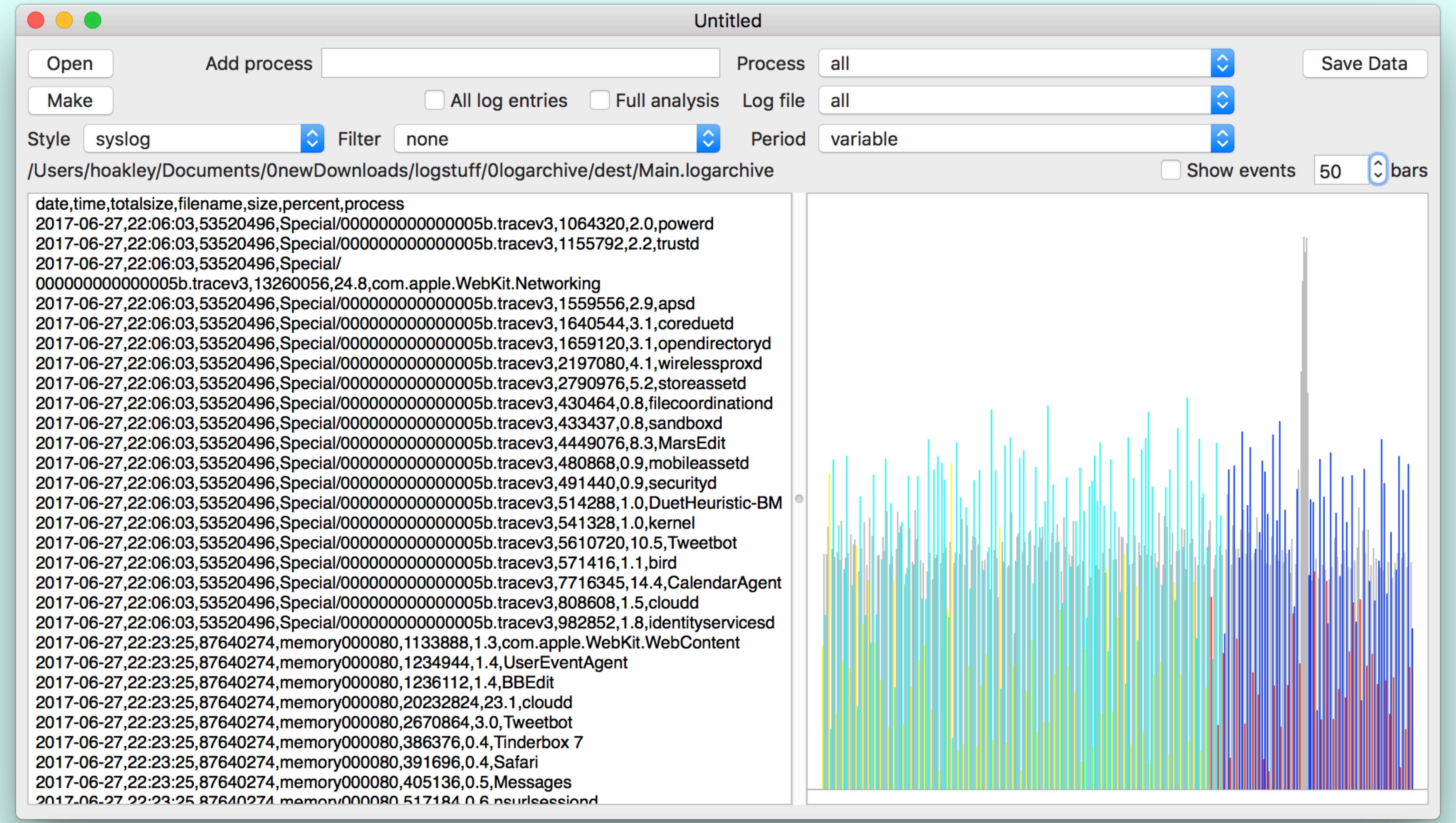
```
log show --predicate ‘subsystem ==
"com.apple.duetactivityscheduler" || subsystem ==
"com.apple.xpc.activity" || (subsystem ==
"com.apple.TimeMachine" && eventMessage CONTAINS[c]
“start”)' --style syslog --info --start "2018-03-19
19:30:20 --end  "2018-03-19 20:31:20"
```

Tip: Consolation 3 shows the command it submits.
Use that to learn how to get the best from `log`.

Additional filtering

- string search in eventMessage – Consolation 3 (plain & regex), Woodpile
- `log` ➜ your own filters/search, but the log messages are slabs of text
- export as CSV – Consolation 3
- export as JSON – `log`, Consolation 3
- top-down search – Woodpile

All



Add process

Process all

□ All log entries □ Full analysis

Log file all

Style syslog

Filter none

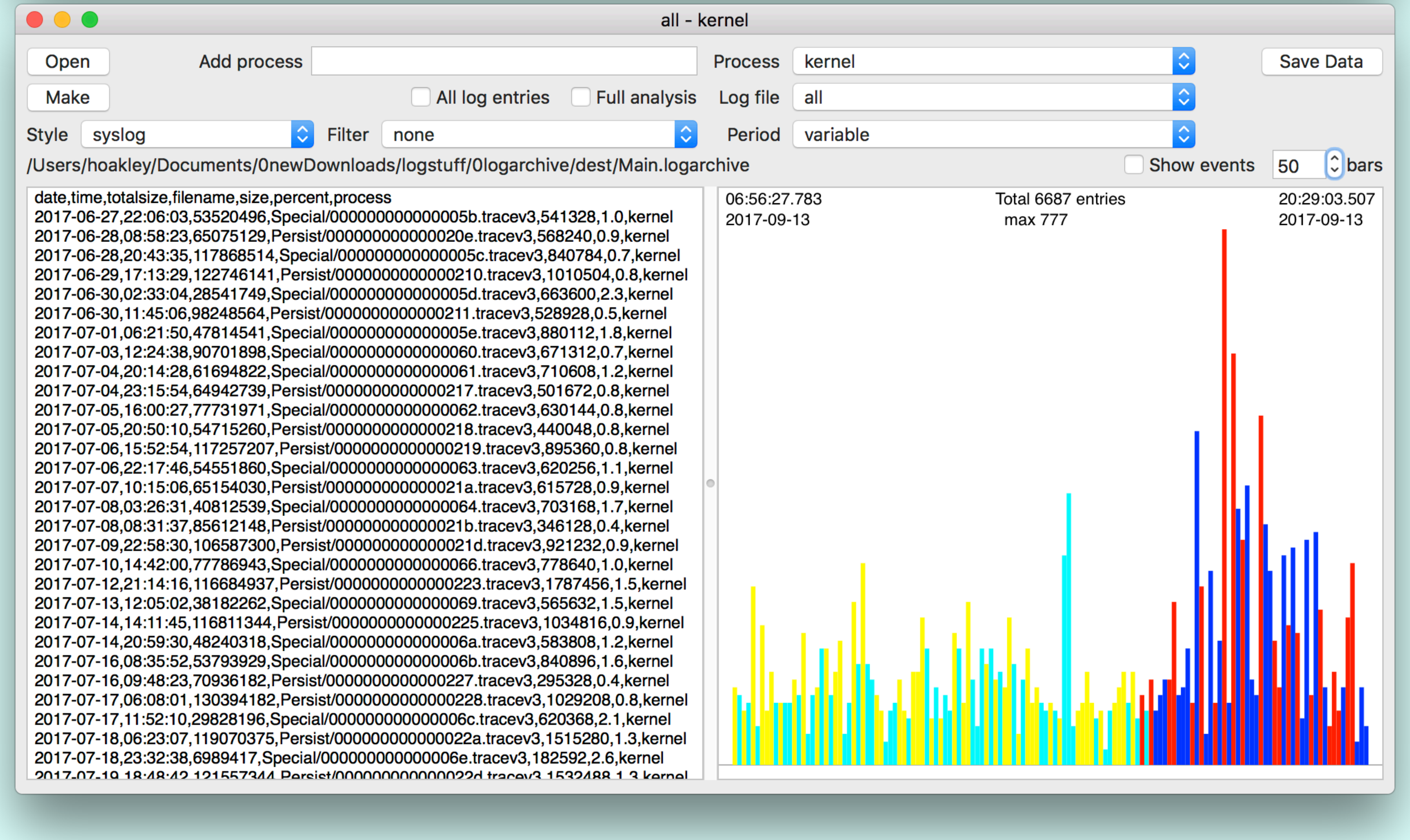
Period variable

/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logarchive

□ Show events 50 bars

```
date,time,totalsize,filename,size,percent,process
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,1064320,2.0,powerd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,1155792,2.2,trustd
2017-06-27,22:06:03,53520496,Special/
000000000000005b.tracev3,13260056,24.8,com.apple.WebKit.Networking
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,1559556,2.9,apsd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,1640544,3.1,coreduetd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,1659120,3.1,opendirectoryd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,2197080,4.1,wirelessproxd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,2790976,5.2,storeassetd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,430464,0.8,filecoordinationd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,433437,0.8,sandboxd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,4449076,8.3,MarsEdit
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,480868,0.9,mobileassetd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,491440,0.9,securityd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,514288,1.0,DuetHeuristic-BM
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,541328,1.0,kernel
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,5610720,10.5,Tweetbot
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,571416,1.1,bird
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,7716345,14.4,CalendarAgent
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,808608,1.5,cloudd
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,982852,1.8,identityservicesd
2017-06-27,22:23:25,87640274,memory000080,1133888,1.3,com.apple.WebKit.WebContent
2017-06-27,22:23:25,87640274,memory000080,1234944,1.4,UserEventAgent
2017-06-27,22:23:25,87640274,memory000080,1236112,1.4,BBEdit
2017-06-27,22:23:25,87640274,memory000080,20232824,23.1,cloudd
2017-06-27,22:23:25,87640274,memory000080,2670864,3.0,Tweetbot
2017-06-27,22:23:25,87640274,memory000080,386376,0.4,Tinderbox 7
2017-06-27,22:23:25,87640274,memory000080,391696,0.4,Safari
2017-06-27,22:23:25,87640274,memory000080,405136,0.5,Messages
2017-06-27,22:23:25,87640274,memory000080,517184,0.6,nsurlsessiond
```

kernel



Add process

Process kernel

□ All log entries □ Full analysis

Log file all

Style syslog

Filter none

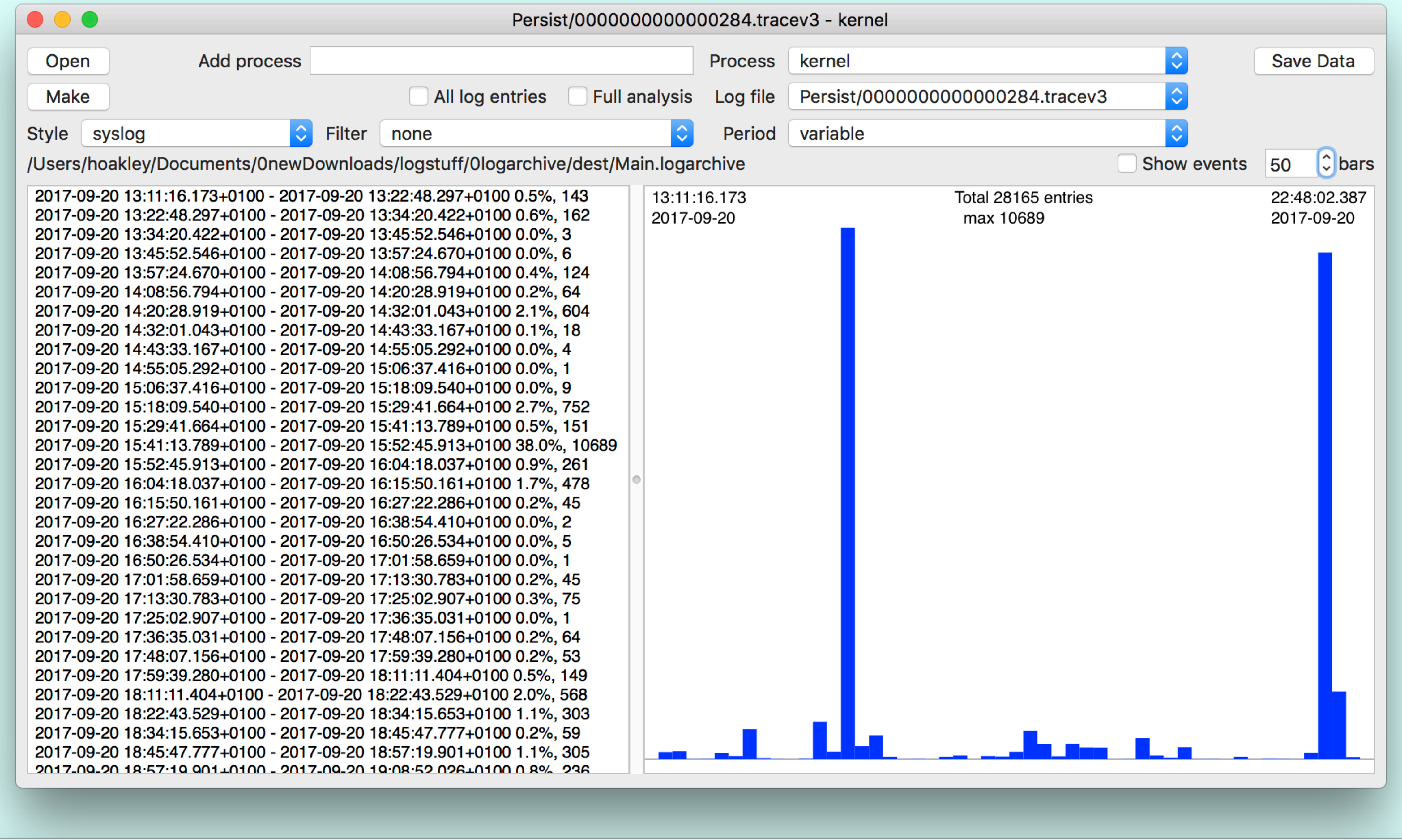
Period variable

/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logarchive

□ Show events 50 bars

```
date,time,totalsize,filename,size,percent,process
2017-06-27,22:06:03,53520496,Special/000000000000005b.tracev3,541328,1.0,kernel
2017-06-28,08:58:23,65075129,Persist/000000000000020e.tracev3,568240,0.9,kernel
2017-06-28,20:43:35,117868514,Special/000000000000005c.tracev3,840784,0.7,kernel
2017-06-29,17:13:29,122746141,Persist/0000000000000210.tracev3,1010504,0.8,kernel
2017-06-30,02:33:04,28541749,Special/000000000000005d.tracev3,663600,2.3,kernel
2017-06-30,11:45:06,98248564,Persist/0000000000000211.tracev3,528928,0.5,kernel
2017-07-01,06:21:50,47814541,Special/000000000000005e.tracev3,880112,1.8,kernel
2017-07-03,12:24:38,90701898,Special/0000000000000060.tracev3,671312,0.7,kernel
2017-07-04,20:14:28,61694822,Special/0000000000000061.tracev3,710608,1.2,kernel
2017-07-04,23:15:54,64942739,Persist/0000000000000217.tracev3,501672,0.8,kernel
2017-07-05,16:00:27,77731971,Special/0000000000000062.tracev3,630144,0.8,kernel
2017-07-05,20:50:10,54715260,Persist/0000000000000218.tracev3,440048,0.8,kernel
2017-07-06,15:52:54,117257207,Persist/0000000000000219.tracev3,895360,0.8,kernel
2017-07-06,22:17:46,54551860,Special/0000000000000063.tracev3,620256,1.1,kernel
2017-07-07,10:15:06,65154030,Persist/000000000000021a.tracev3,615728,0.9,kernel
2017-07-08,03:26:31,40812539,Special/0000000000000064.tracev3,703168,1.7,kernel
2017-07-08,08:31:37,85612148,Persist/000000000000021b.tracev3,346128,0.4,kernel
2017-07-09,22:58:30,106587300,Persist/000000000000021d.tracev3,921232,0.9,kernel
2017-07-10,14:42:00,77786943,Special/0000000000000066.tracev3,778640,1.0,kernel
2017-07-12,21:14:16,116684937,Persist/0000000000000223.tracev3,1787456,1.5,kernel
2017-07-13,12:05:02,38182262,Special/0000000000000069.tracev3,565632,1.5,kernel
2017-07-14,14:11:45,116811344,Persist/0000000000000225.tracev3,1034816,0.9,kernel
2017-07-14,20:59:30,48240318,Special/000000000000006a.tracev3,583808,1.2,kernel
2017-07-16,08:35:52,53793929,Special/000000000000006b.tracev3,840896,1.6,kernel
2017-07-16,09:48:23,70936182,Persist/0000000000000227.tracev3,295328,0.4,kernel
2017-07-17,06:08:01,130394182,Persist/0000000000000228.tracev3,1029208,0.8,kernel
2017-07-17,11:52:10,29828196,Special/000000000000006c.tracev3,620368,2.1,kernel
2017-07-18,06:23:07,119070375,Persist/000000000000022a.tracev3,1515280,1.3,kernel
2017-07-18,23:32:38,6989417,Special/000000000000006e.tracev3,182592,2.6,kernel
2017-07-19,18:48:42,121557344,Persist/000000000000022d.tracev3,1532488,1.3,kernel
```

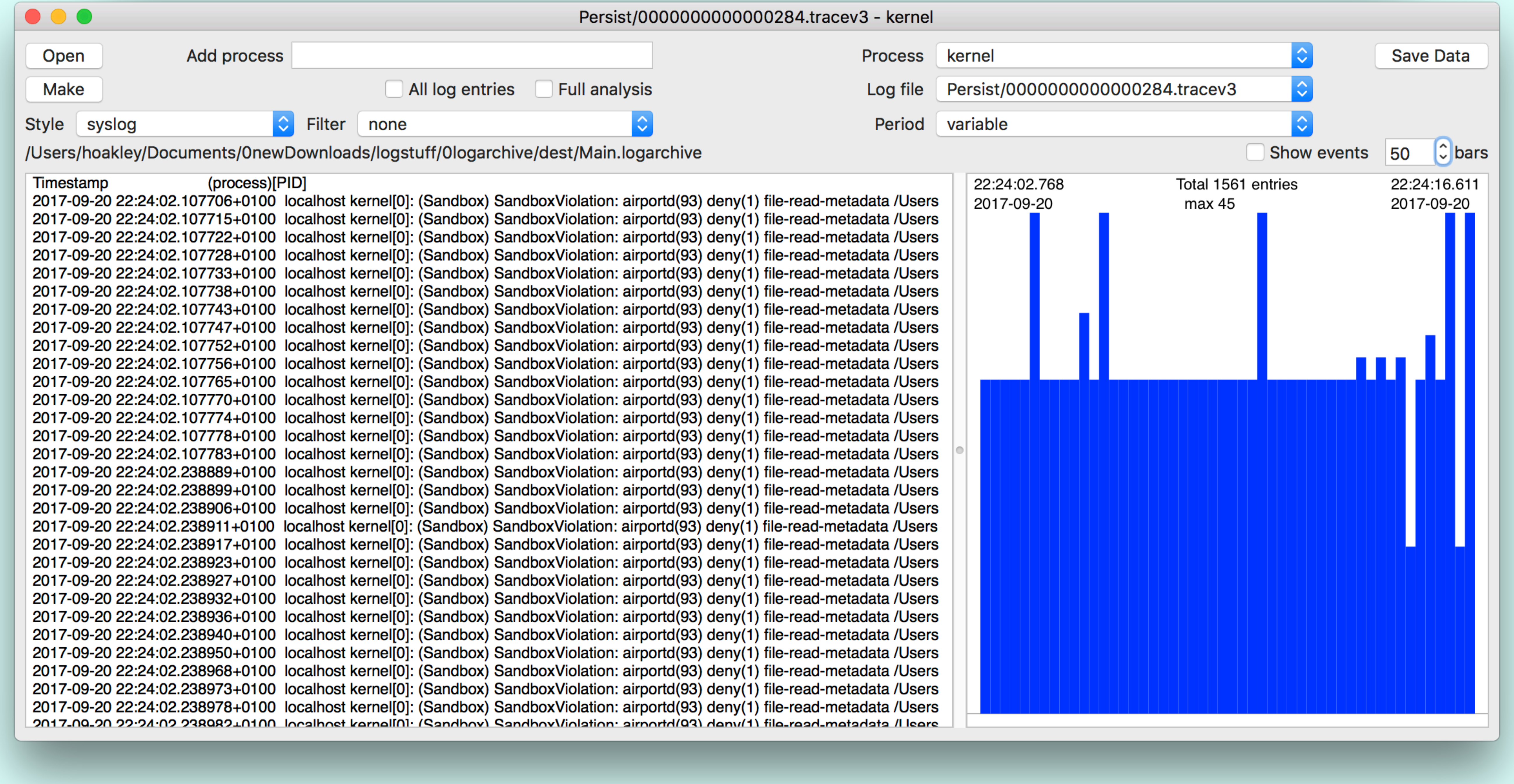
kernel



Add process
□ All log entries □ Full analysis
Process: kernel
Log file: Persist/0000000000000284.tracev3
Style: syslog
Filter: none
Period: variable
/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logarchive
□ Show events 50 bars

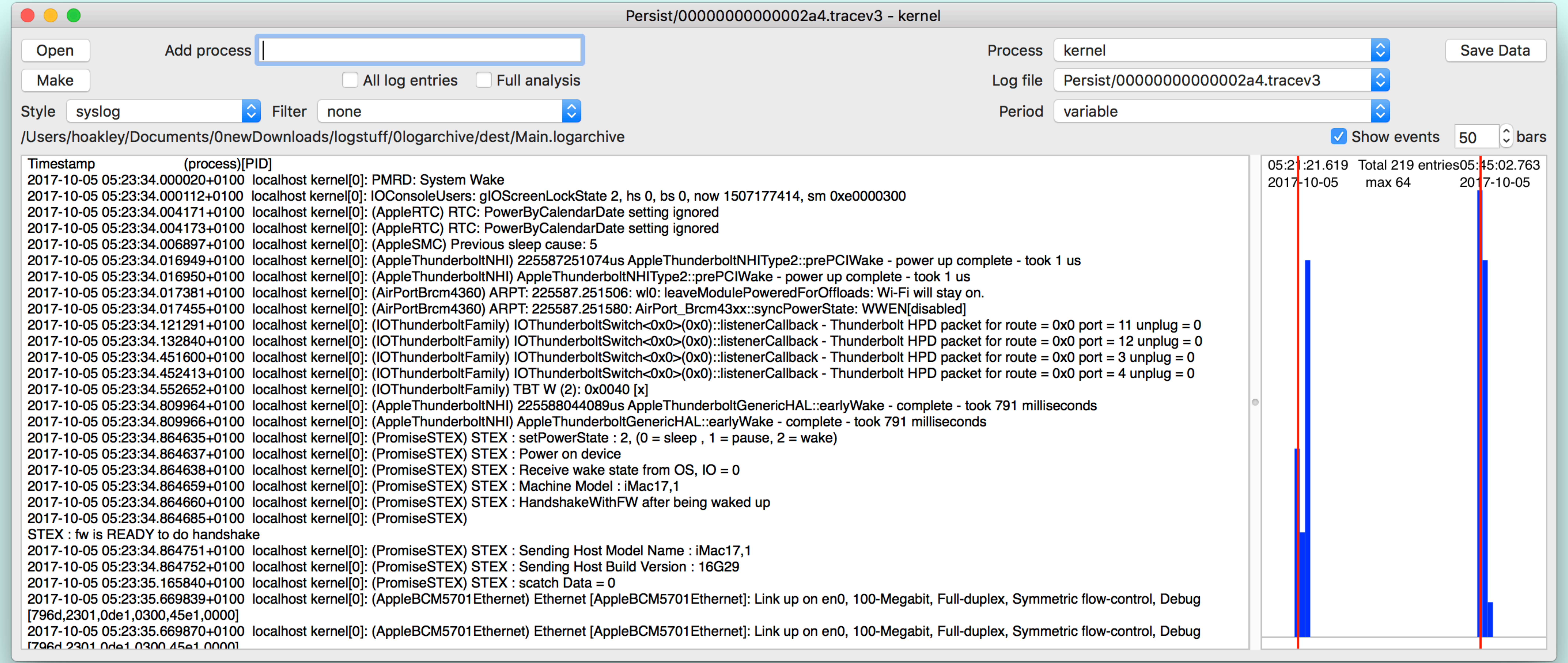
```
2017-09-20 13:11:16.173+0100 - 2017-09-20 13:22:48.297+0100 0.5%, 143
2017-09-20 13:22:48.297+0100 - 2017-09-20 13:34:20.422+0100 0.6%, 162
2017-09-20 13:34:20.422+0100 - 2017-09-20 13:45:52.546+0100 0.0%, 3
2017-09-20 13:45:52.546+0100 - 2017-09-20 13:57:24.670+0100 0.0%, 6
2017-09-20 13:57:24.670+0100 - 2017-09-20 14:08:56.794+0100 0.4%, 124
2017-09-20 14:08:56.794+0100 - 2017-09-20 14:20:28.919+0100 0.2%, 64
2017-09-20 14:20:28.919+0100 - 2017-09-20 14:32:01.043+0100 2.1%, 604
2017-09-20 14:32:01.043+0100 - 2017-09-20 14:43:33.167+0100 0.1%, 18
2017-09-20 14:43:33.167+0100 - 2017-09-20 14:55:05.292+0100 0.0%, 4
2017-09-20 14:55:05.292+0100 - 2017-09-20 15:06:37.416+0100 0.0%, 1
2017-09-20 15:06:37.416+0100 - 2017-09-20 15:18:09.540+0100 0.0%, 9
2017-09-20 15:18:09.540+0100 - 2017-09-20 15:29:41.664+0100 2.7%, 752
2017-09-20 15:29:41.664+0100 - 2017-09-20 15:41:13.789+0100 0.5%, 151
2017-09-20 15:41:13.789+0100 - 2017-09-20 15:52:45.913+0100 38.0%, 10689
2017-09-20 15:52:45.913+0100 - 2017-09-20 16:04:18.037+0100 0.9%, 261
2017-09-20 16:04:18.037+0100 - 2017-09-20 16:15:50.161+0100 1.7%, 478
2017-09-20 16:15:50.161+0100 - 2017-09-20 16:27:22.286+0100 0.2%, 45
2017-09-20 16:27:22.286+0100 - 2017-09-20 16:38:54.410+0100 0.0%, 2
2017-09-20 16:38:54.410+0100 - 2017-09-20 16:50:26.534+0100 0.0%, 5
2017-09-20 16:50:26.534+0100 - 2017-09-20 17:01:58.659+0100 0.0%, 1
2017-09-20 17:01:58.659+0100 - 2017-09-20 17:13:30.783+0100 0.2%, 45
2017-09-20 17:13:30.783+0100 - 2017-09-20 17:25:02.907+0100 0.3%, 75
2017-09-20 17:25:02.907+0100 - 2017-09-20 17:36:35.031+0100 0.0%, 1
2017-09-20 17:36:35.031+0100 - 2017-09-20 17:48:07.156+0100 0.2%, 64
2017-09-20 17:48:07.156+0100 - 2017-09-20 17:59:39.280+0100 0.2%, 53
2017-09-20 17:59:39.280+0100 - 2017-09-20 18:11:11.404+0100 0.5%, 149
2017-09-20 18:11:11.404+0100 - 2017-09-20 18:22:43.529+0100 2.0%, 568
2017-09-20 18:22:43.529+0100 - 2017-09-20 18:34:15.653+0100 1.1%, 303
2017-09-20 18:34:15.653+0100 - 2017-09-20 18:45:47.777+0100 0.2%, 59
2017-09-20 18:45:47.777+0100 - 2017-09-20 18:57:19.901+0100 1.1%, 305
2017-09-20 18:57:19.901+0100 - 2017-09-20 19:08:52.026+0100 0.8%, 236
```

kernel



Add process
□ All log entries □ Full analysis
Process: kernel
Log file: Persist/0000000000000284.tracev3
Style: syslog
Filter: none
Period: variable
/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logarchive
□ Show events 50 bars

```
Timestamp                    (process)[PID]
2017-09-20 22:24:02.107706+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107715+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107722+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107728+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107733+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107738+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107743+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107747+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107752+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107756+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107765+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107770+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107774+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107778+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.107783+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238889+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238899+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238906+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238911+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238917+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238923+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238927+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238932+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238936+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238940+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238950+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238968+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238973+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238978+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
2017-09-20 22:24:02.238982+0100  localhost kernel[0]: (Sandbox) SandboxViolation: airportd(93) deny(1) file-read-metadata /Users
```



Persist/00000000000002a4.tracev3 - kernel

Add process

☐ All log entries ☐ Full analysis

Style: syslog
Filter: none

Process: kernel
Log file: Persist/00000000000002a4.tracev3
Period: variable

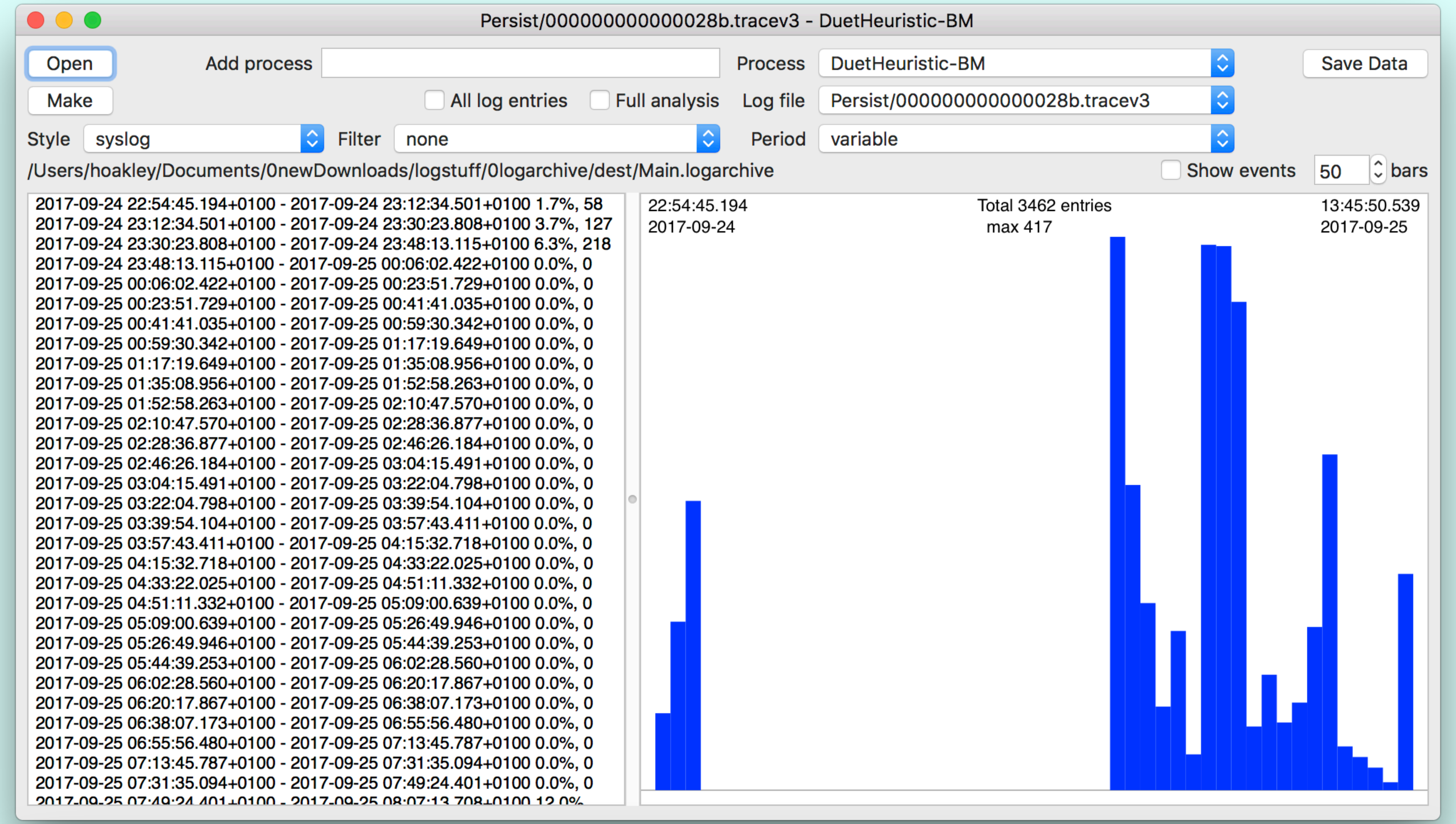
/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logarchive

☑ Show events 50 bars

```
Timestamp                  (process)[PID]
2017-10-05 05:23:34.000020+0100  localhost kernel[0]: PMRD: System Wake
2017-10-05 05:23:34.000112+0100  localhost kernel[0]: IOConsoleUsers: gIOScreenLockState 2, hs 0, bs 0, now 1507177414, sm 0xe0000300
2017-10-05 05:23:34.004171+0100  localhost kernel[0]: (AppleRTC) RTC: PowerByCalendarDate setting ignored
2017-10-05 05:23:34.004173+0100  localhost kernel[0]: (AppleRTC) RTC: PowerByCalendarDate setting ignored
2017-10-05 05:23:34.006897+0100  localhost kernel[0]: (AppleSMC) Previous sleep cause: 5
2017-10-05 05:23:34.016949+0100  localhost kernel[0]: (AppleThunderboltNHI) 225587251074us AppleThunderboltNHIType2::prePCIWake - power up complete - took 1 us
2017-10-05 05:23:34.016950+0100  localhost kernel[0]: (AppleThunderboltNHI) AppleThunderboltNHIType2::prePCIWake - power up complete - took 1 us
2017-10-05 05:23:34.017381+0100  localhost kernel[0]: (AirPortBrcm4360) ARPT: 225587.251506: wl0: leaveModulePoweredForOffloads: Wi-Fi will stay on.
2017-10-05 05:23:34.017455+0100  localhost kernel[0]: (AirPortBrcm4360) ARPT: 225587.251580: AirPort_Brcm43xx::syncPowerState: WWEN[disabled]
2017-10-05 05:23:34.121291+0100  localhost kernel[0]: (IOThunderboltFamily) IOThunderboltSwitch<0x0>(0x0)::listenerCallback - Thunderbolt HPD packet for route = 0x0 port = 11 unplug = 0
2017-10-05 05:23:34.132840+0100  localhost kernel[0]: (IOThunderboltFamily) IOThunderboltSwitch<0x0>(0x0)::listenerCallback - Thunderbolt HPD packet for route = 0x0 port = 12 unplug = 0
2017-10-05 05:23:34.451600+0100  localhost kernel[0]: (IOThunderboltFamily) IOThunderboltSwitch<0x0>(0x0)::listenerCallback - Thunderbolt HPD packet for route = 0x0 port = 3 unplug = 0
2017-10-05 05:23:34.452413+0100  localhost kernel[0]: (IOThunderboltFamily) IOThunderboltSwitch<0x0>(0x0)::listenerCallback - Thunderbolt HPD packet for route = 0x0 port = 4 unplug = 0
2017-10-05 05:23:34.552652+0100  localhost kernel[0]: (IOThunderboltFamily) TBT W (2): 0x0040 [x]
2017-10-05 05:23:34.809964+0100  localhost kernel[0]: (AppleThunderboltNHI) 225588044089us AppleThunderboltGenericHAL::earlyWake - complete - took 791 milliseconds
2017-10-05 05:23:34.809966+0100  localhost kernel[0]: (AppleThunderboltNHI) AppleThunderboltGenericHAL::earlyWake - complete - took 791 milliseconds
2017-10-05 05:23:34.864635+0100  localhost kernel[0]: (PromiseSTEX) STEX : setPowerState : 2, (0 = sleep , 1 = pause, 2 = wake)
2017-10-05 05:23:34.864637+0100  localhost kernel[0]: (PromiseSTEX) STEX : Power on device
2017-10-05 05:23:34.864638+0100  localhost kernel[0]: (PromiseSTEX) STEX : Receive wake state from OS, IO = 0
2017-10-05 05:23:34.864659+0100  localhost kernel[0]: (PromiseSTEX) STEX : Machine Model : iMac17,1
2017-10-05 05:23:34.864660+0100  localhost kernel[0]: (PromiseSTEX) STEX : HandshakeWithFW after being waked up
2017-10-05 05:23:34.864685+0100  localhost kernel[0]: (PromiseSTEX)
STEX : fw is READY to do handshake
2017-10-05 05:23:34.864751+0100  localhost kernel[0]: (PromiseSTEX) STEX : Sending Host Model Name : iMac17,1
2017-10-05 05:23:34.864752+0100  localhost kernel[0]: (PromiseSTEX) STEX : Sending Host Build Version : 16G29
2017-10-05 05:23:35.165840+0100  localhost kernel[0]: (PromiseSTEX) STEX : scatch Data = 0
2017-10-05 05:23:35.669839+0100  localhost kernel[0]: (AppleBCM5701Ethernet) Ethernet [AppleBCM5701Ethernet]: Link up on en0, 100-Megabit, Full-duplex, Symmetric flow-control, Debug
[796d,2301,0de1,0300,45e1,0000]
2017-10-05 05:23:35.669870+0100  localhost kernel[0]: (AppleBCM5701Ethernet) Ethernet [AppleBCM5701Ethernet]: Link up on en0, 100-Megabit, Full-duplex, Symmetric flow-control, Debug
[796d,2301,0de1,0300,45e1,0000]
```

kernel – wake from sleep

DAS



Persist/000000000000028b.tracev3 - DuetHeuristic-BM

Add process

Process DuetHeuristic-BM

□ All log entries □ Full analysis

Log file Persist/000000000000028b.tracev3

Style syslog

Filter none

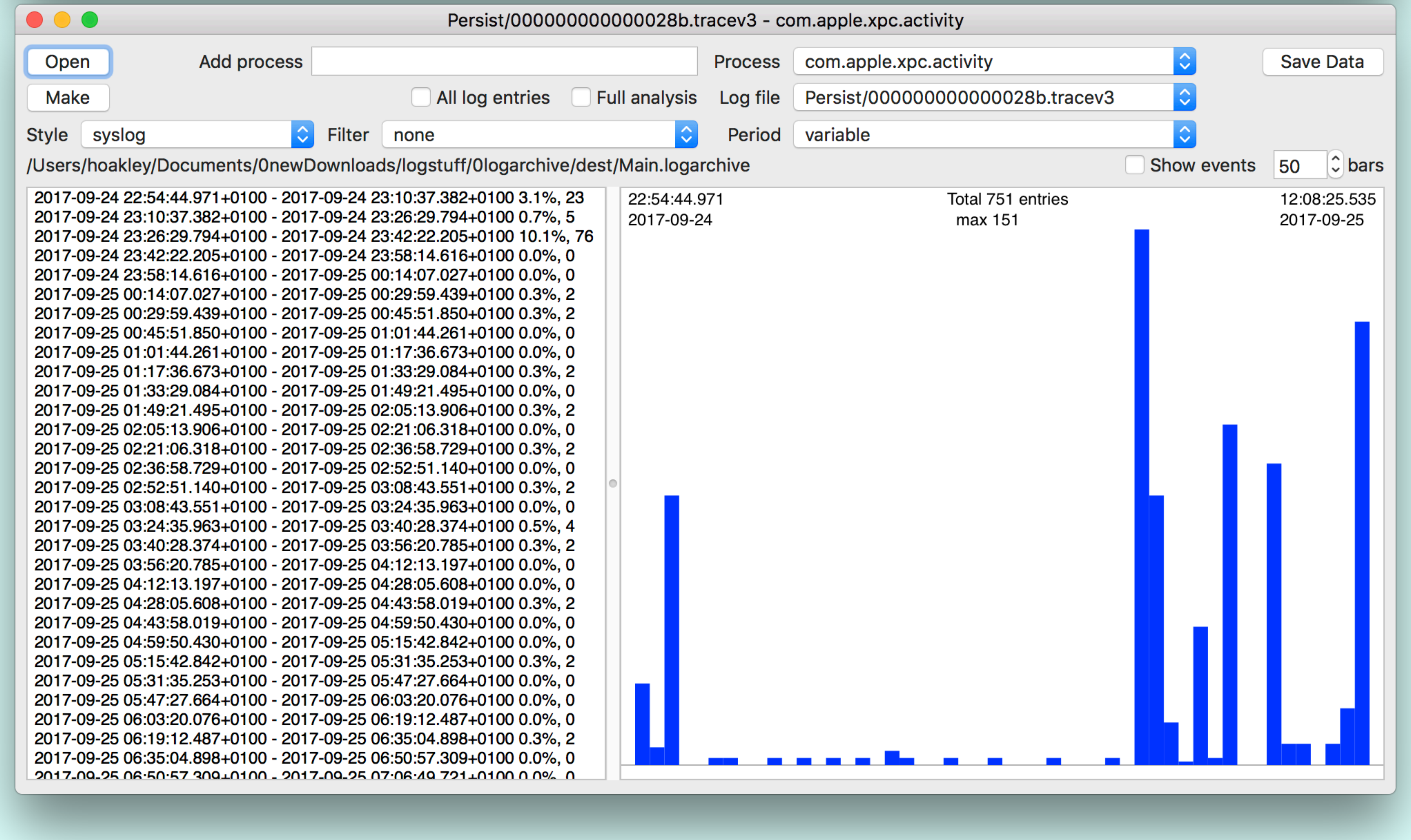
Period variable

/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logarchive

□ Show events 50 bars

```
2017-09-24 22:54:45.194+0100 - 2017-09-24 23:12:34.501+0100 1.7%, 58
2017-09-24 23:12:34.501+0100 - 2017-09-24 23:30:23.808+0100 3.7%, 127
2017-09-24 23:30:23.808+0100 - 2017-09-24 23:48:13.115+0100 6.3%, 218
2017-09-24 23:48:13.115+0100 - 2017-09-25 00:06:02.422+0100 0.0%, 0
2017-09-25 00:06:02.422+0100 - 2017-09-25 00:23:51.729+0100 0.0%, 0
2017-09-25 00:23:51.729+0100 - 2017-09-25 00:41:41.035+0100 0.0%, 0
2017-09-25 00:41:41.035+0100 - 2017-09-25 00:59:30.342+0100 0.0%, 0
2017-09-25 00:59:30.342+0100 - 2017-09-25 01:17:19.649+0100 0.0%, 0
2017-09-25 01:17:19.649+0100 - 2017-09-25 01:35:08.956+0100 0.0%, 0
2017-09-25 01:35:08.956+0100 - 2017-09-25 01:52:58.263+0100 0.0%, 0
2017-09-25 01:52:58.263+0100 - 2017-09-25 02:10:47.570+0100 0.0%, 0
2017-09-25 02:10:47.570+0100 - 2017-09-25 02:28:36.877+0100 0.0%, 0
2017-09-25 02:28:36.877+0100 - 2017-09-25 02:46:26.184+0100 0.0%, 0
2017-09-25 02:46:26.184+0100 - 2017-09-25 03:04:15.491+0100 0.0%, 0
2017-09-25 03:04:15.491+0100 - 2017-09-25 03:22:04.798+0100 0.0%, 0
2017-09-25 03:22:04.798+0100 - 2017-09-25 03:39:54.104+0100 0.0%, 0
2017-09-25 03:39:54.104+0100 - 2017-09-25 03:57:43.411+0100 0.0%, 0
2017-09-25 03:57:43.411+0100 - 2017-09-25 04:15:32.718+0100 0.0%, 0
2017-09-25 04:15:32.718+0100 - 2017-09-25 04:33:22.025+0100 0.0%, 0
2017-09-25 04:33:22.025+0100 - 2017-09-25 04:51:11.332+0100 0.0%, 0
2017-09-25 04:51:11.332+0100 - 2017-09-25 05:09:00.639+0100 0.0%, 0
2017-09-25 05:09:00.639+0100 - 2017-09-25 05:26:49.946+0100 0.0%, 0
2017-09-25 05:26:49.946+0100 - 2017-09-25 05:44:39.253+0100 0.0%, 0
2017-09-25 05:44:39.253+0100 - 2017-09-25 06:02:28.560+0100 0.0%, 0
2017-09-25 06:02:28.560+0100 - 2017-09-25 06:20:17.867+0100 0.0%, 0
2017-09-25 06:20:17.867+0100 - 2017-09-25 06:38:07.173+0100 0.0%, 0
2017-09-25 06:38:07.173+0100 - 2017-09-25 06:55:56.480+0100 0.0%, 0
2017-09-25 06:55:56.480+0100 - 2017-09-25 07:13:45.787+0100 0.0%, 0
2017-09-25 07:13:45.787+0100 - 2017-09-25 07:31:35.094+0100 0.0%, 0
2017-09-25 07:31:35.094+0100 - 2017-09-25 07:49:24.401+0100 0.0%, 0
2017-09-25 07:49:24.401+0100 - 2017-09-25 08:07:13.708+0100 12.0%
```

CTS



Persist/000000000000028b.tracev3 - com.apple.xpc.activity

Add process

Process com.apple.xpc.activity

□ All log entries □ Full analysis

Log file Persist/000000000000028b.tracev3

Style syslog

Filter none

Period variable

/Users/hoakley/Documents/0newDownloads/logstuff/0logarchive/dest/Main.logarchive

□ Show events 50 bars

```
2017-09-24 22:54:44.971+0100 - 2017-09-24 23:10:37.382+0100 3.1%, 23
2017-09-24 23:10:37.382+0100 - 2017-09-24 23:26:29.794+0100 0.7%, 5
2017-09-24 23:26:29.794+0100 - 2017-09-24 23:42:22.205+0100 10.1%, 76
2017-09-24 23:42:22.205+0100 - 2017-09-24 23:58:14.616+0100 0.0%, 0
2017-09-24 23:58:14.616+0100 - 2017-09-25 00:14:07.027+0100 0.0%, 0
2017-09-25 00:14:07.027+0100 - 2017-09-25 00:29:59.439+0100 0.3%, 2
2017-09-25 00:29:59.439+0100 - 2017-09-25 00:45:51.850+0100 0.3%, 2
2017-09-25 00:45:51.850+0100 - 2017-09-25 01:01:44.261+0100 0.0%, 0
2017-09-25 01:01:44.261+0100 - 2017-09-25 01:17:36.673+0100 0.0%, 0
2017-09-25 01:17:36.673+0100 - 2017-09-25 01:33:29.084+0100 0.3%, 2
2017-09-25 01:33:29.084+0100 - 2017-09-25 01:49:21.495+0100 0.0%, 0
2017-09-25 01:49:21.495+0100 - 2017-09-25 02:05:13.906+0100 0.3%, 2
2017-09-25 02:05:13.906+0100 - 2017-09-25 02:21:06.318+0100 0.0%, 0
2017-09-25 02:21:06.318+0100 - 2017-09-25 02:36:58.729+0100 0.3%, 2
2017-09-25 02:36:58.729+0100 - 2017-09-25 02:52:51.140+0100 0.0%, 0
2017-09-25 02:52:51.140+0100 - 2017-09-25 03:08:43.551+0100 0.3%, 2
2017-09-25 03:08:43.551+0100 - 2017-09-25 03:24:35.963+0100 0.0%, 0
2017-09-25 03:24:35.963+0100 - 2017-09-25 03:40:28.374+0100 0.5%, 4
2017-09-25 03:40:28.374+0100 - 2017-09-25 03:56:20.785+0100 0.3%, 2
2017-09-25 03:56:20.785+0100 - 2017-09-25 04:12:13.197+0100 0.0%, 0
2017-09-25 04:12:13.197+0100 - 2017-09-25 04:28:05.608+0100 0.0%, 0
2017-09-25 04:28:05.608+0100 - 2017-09-25 04:43:58.019+0100 0.3%, 2
2017-09-25 04:43:58.019+0100 - 2017-09-25 04:59:50.430+0100 0.0%, 0
2017-09-25 04:59:50.430+0100 - 2017-09-25 05:15:42.842+0100 0.0%, 0
2017-09-25 05:15:42.842+0100 - 2017-09-25 05:31:35.253+0100 0.3%, 2
2017-09-25 05:31:35.253+0100 - 2017-09-25 05:47:27.664+0100 0.0%, 0
2017-09-25 05:47:27.664+0100 - 2017-09-25 06:03:20.076+0100 0.0%, 0
2017-09-25 06:03:20.076+0100 - 2017-09-25 06:19:12.487+0100 0.0%, 0
2017-09-25 06:19:12.487+0100 - 2017-09-25 06:35:04.898+0100 0.3%, 2
2017-09-25 06:35:04.898+0100 - 2017-09-25 06:50:57.309+0100 0.0%, 0
2017-09-25 06:50:57.309+0100 - 2017-09-25 07:06:49.721+0100 0.0%, 0
```

Waypoints 1

- `BOOT_TIME`, `SHUTDOWN_TIME` up to Sierra 10.12.4/5
- `=== system boot:`, `=== system wallclock time adjusted` in later Sierra
- `Previous shutdown cause: 5`
- `Login Window Application Started`

Waypoints 2

- `gIOLastWakeAbsTime:` before sleep
- `PMRD: System Wake`, `User Active` (twice), `Wake reason:` on wake
- `AuthenticationAllowed`, `result: Success`, `login proceeding` on login
- `point of no return` on logout

Tips

- `logger` now writes to the unified log, but try Blowhole:
  - `blowhole -s "Script failed, error -2”`
- installation log at /var/log/install.log still works; browse with Console

Security & Audit

- given the goals of the unified log, quite unsuitable – use BSM

- better to instrument macOS specifically, for separate logs

Image: Michael Barrera,
via Wikimedia Commons

Commonality

- all tools – `log`, Consolation, Woodpile – should work fine with macOS, iOS, watchOS, tvOS logarchives

- all tools using `log` – Consolation, Woodpile – should analyse High Sierra logs on Sierra hosts https://eclecticlight.co