Woodpile (1.0b5) for macOS Sierra & High Sierra
Preliminary Documentation
Howard Oakley https://eclecticlight.co

This preliminary documentation describes the features and use of **Woodpile**, a tool for browsing the log and analysing its activity in macOS Sierra and High Sierra. Sierra introduced a new unified log system which is much more detailed and powerful that earlier log systems. Because of this, live logs on a Mac contain tens of millions of entries, spread across many different log files. The system daemon which maintains these log files also performs analyses of each log file that it handles, and keeps those records in its own log for periods of many months.

Woodpile is the first tool to bring a new type of log analysis to these logs, working from the top down. Traditional log browsers like **Consolation** are designed to help you locate problems and other issues by working from the bottom up: if you know what you're looking for, they are powerful tools. Woodpile looks at your logs the other way around, by showing you which processes made many log entries, and when. It then helps you zoom in and see what was going on at that time, in more detail, using frequency analysis of log entries.

Perhaps the best way to see this is to imagine that you're visiting a new place. If you know exactly where you're looking for, your best aid will be a set of directions to tell you how to get there. If you're not quite sure where you want to go, you are better off with a map, so that you can see what there is to visit, and where. You can then work out where to head next. Consolation is great if you know where you intend to go. If you need to browse a map, then you're better off starting with Woodpile. These two approaches are complementary, so most users who want to access their log will find it best to have both, and sometimes to use both side by side.

This beta-release of **Woodpile** provides a rich range of tools: it lets you identify which processes wrote most to the logs, and when, using the log file analysis already performed by `logd`, the log maintenance daemon. It then takes that analysis down inside individual log files, to identify narrow periods of interest, and within those periods showing you all log entries for each process of interest. You can add processes which don't appear in the standard analysis, view significant events such as startup and waking from sleep, and synchronise the time periods shown across many different windows. Most recent additions include proper support for preferences, log styles showing only the content you want and using colour, and instant search filters, including the use of regular expressions ('regex').

Woodpile can thus reach and view all the log entries contained within your logarchive – typically for the last twenty days or so.

What you need

- A Mac running macOS Sierra or High Sierra. This release has been built to be fully compatible with High Sierra.
- A copy of the latest release of Woodpile from https://eclecticlight.co/downloads/ If you want to use Consolation to access your logarchives, ensure that you have the latest version of Consolation 3 from there too. Earlier versions do not support all the features needed to get the best from logarchives.
  (These are delivered by secure HTTPS download.)

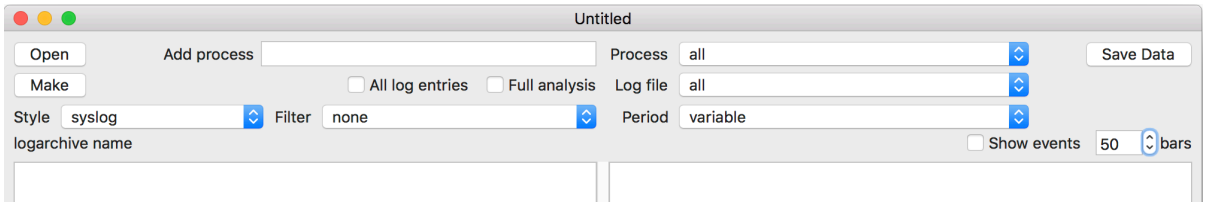
Woodpile (1.0b5) for macOS Sierra & High Sierra
Preliminary Documentation
Howard Oakley https://eclecticlight.co

Getting started

Woodpile comes compressed as a Zip file, which you should decompress, and move the app to your preferred folder, such as /Applications. It is not fussy where it is run from, though.

Woodpile uses my developer code signature, so should run normally first time after installation. If it does not, you should still be able to use it safely. Instead of double-clicking to run it the first time, select the app icon in a Finder window, and use the Finder's **Open** command to run it. You will be prompted to confirm that you want to open it: click on the button to say that you do. After that first use, on that Mac, you should be able to use it normally. If you are told that it is damaged or the signature is incorrect, please contact me.

Controls



Woodpile has the following controls in each of its windows:

- The **Open** button reads an existing logarchive, which can be one you have just created using this app, or one generated by another tool such as MakeLogarchive, Consolation or the `log` command, and extracts data from all the log files which are included in the `logd` log files.
- The **Make** button converts a folder containing log files into a logarchive bundle, using the same method as MakeLogarchive.
- The **Process** popup menu filters the frequency analyses of a logarchive which has already been opened, and shows only those rows for the selected process. The first menu item, **all**, shows data for all processes.
- The **Add process** text box lets you add processes, such as `com.apple.TimeMachine` or `co.eclecticlight.blowhole`, which are not included in the processes which are most frequent users of the log.
- The **Log file** popup menu hones in on one selected log file alone, even though it may not have been included in `logd`'s load analysis. The first menu item, **all**, shows data for the whole logarchive.
- The **Period** popup menu, which can set the period viewed in a window to the same as that of another window, to aid their comparison.
- The **All log entries** checkbox lets you review all log entries for the period being viewed, rather than those of the selected process alone.
- The **Full analysis** checkbox determines whether Woodpile performs full frequency or log load analysis on processes which you have added to the **Process** menu.
- The **Style** popup menu displays log excerpts using a custom style, which you define in the Preferences sheet.

- The **Filter** popup menu applies simple text filters to the messages shown in a log excerpt, when you are using a custom style.
- The **Show events** checkbox determines whether major systems events, startup and waking from sleep, will be shown in the bar chart.
- the **bars** control lets you set the maximum number of bars to display in the chart view.
- The **Save Data** button simply saves the current text in the text box below to a text file of your choice. This lets keep a record of the analysis.

The top section of the window also displays the path and name of the currently open logarchive, once you have opened one, just above the text view at the left. When you are browsing your log using Woodpile, your main control is your mouse or trackpad, which you use to zoom in time, and to reveal log extracts, by clicking/tapping.

There is one important menu command, other than the **New** command for opening a new window: **Preferences** opens Woodpile's Preferences sheet, in which you can customise processes, styles, and filters. You may also find the **Find** command in the **Edit** menu of value on occasion.

Make

To make a new logarchive bundle, you will need a folder, within which are two folders named diagnostics and uuidtext, containing the log files in the same layout as used in /var/db on a Mac. These should contain:

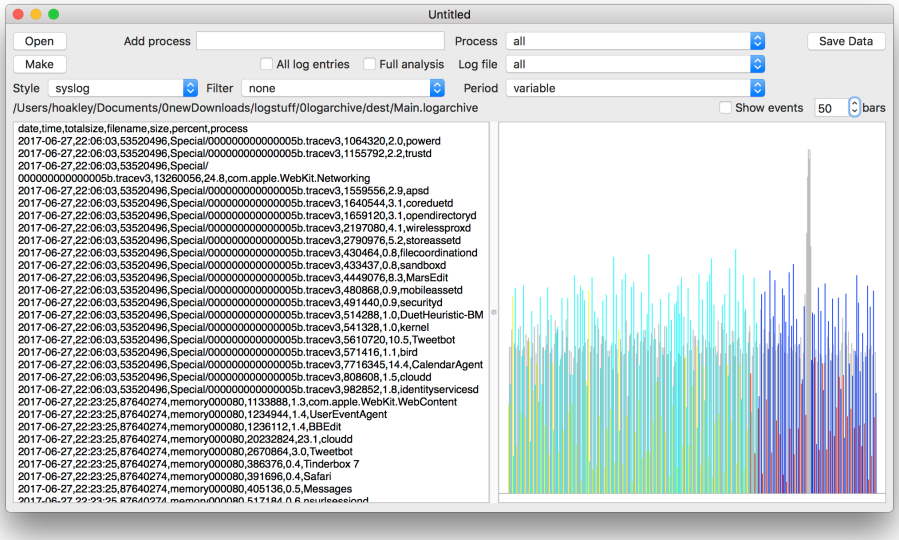
- in **diagnostics**:
  - one or more files named logdata.statistics.0.txt and similar, which are the `logd` log files
  - a folder named **Persist**, which contains one or more tracev3 log files
  - one file named shutdown.log
  - a folder named **Special**, which contains one or more tracev3 log files
  - a folder named **timesync**, which contains one or more .timesync files
  - one file named version.plist
- in **uuidtext**:
  - numbered folders named from **00** to **FF** containing various files named using UUIDs (hex characters)
  - a folder named **dsc** containing various files also named using UUIDs
  - possibly one or more tracev3 log files named logdata.LiveData.tracev3 or similar.

If you do not have all the files, or they are laid out in a different structure, you can try rearranging them as above, and using Woodpile in the hope that the resulting bundle will prove valid and usable.

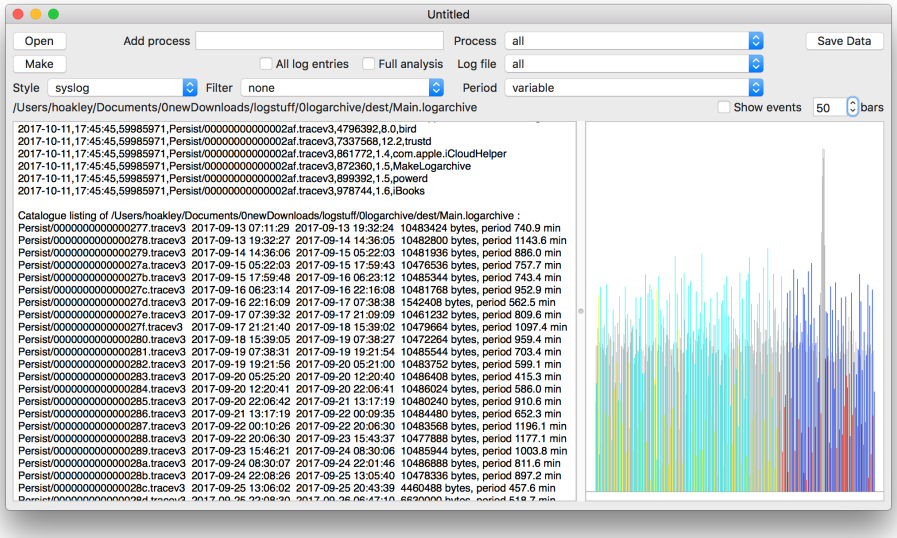
Click on the **Make** button, and you will first be prompted for the folder which contains the diagnostics and uuidtext folders. This could be /var/db on the host Mac: Woodpile is quite happy to make a logarchive from the live logs if you wish.

You will then be prompted to enter the details of the logarchive to be saved. This should, of course, be well away from folders such as /var/db, preferably in your Documents folder, and you must preserve its .logarchive extension, as it is in fact a bundle and not a file.
Woodpile copies the files into the logarchive once you have clicked the **Save** button, and completes that work *before* the save dialog is dismissed. Be patient, and once the save dialog has cleared, it should be ready.

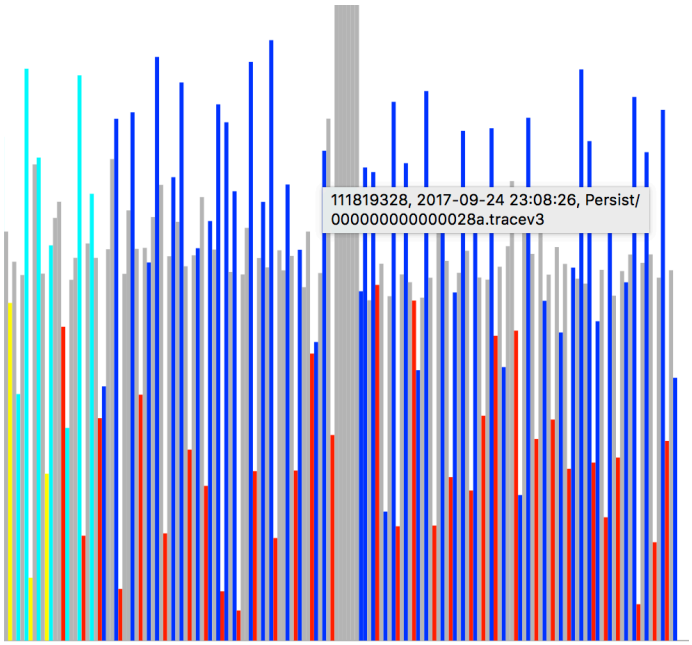
Open



Click on the **Open** button, and select the logarchive you want to analyse. The `logd` log files found there will then be analysed. This takes a few seconds, following which all the frequencies found will be displayed in CSV format in the text box below, and in bar chart form in the pane at the right of the window. The name and path of the logarchive which you opened is displayed in a text box between the **Open** button and the popup menu.



On this ***first*** occasion when opening a logarchive, a catalogue of the log files found within the logarchive is appended after that. You can then save that as a text file using the **Save** button. In the catalogue, each file is listed by its path within the logarchive, the date and time of its creation, the date and time of the last change to its content, its size in bytes, and the period (in minutes) which its entries cover.



When you let the pointer 'hover' over any of the bars in the chart view, a ToolTip will pop up, giving the size, date, time, and log file name of the underlying bar. This helps you identify which individual log file to examine in more detail, should you wish.

Selecting Processes

Once you have opened a logarchive and it has been analysed by Woodpile, the popup menu contains a sorted list of all the processes which feature in the frequency analyses performed by the `logd` daemon. Select **all** to view the whole analysis, or select an individual process to list just those frequency analyses for that given process.

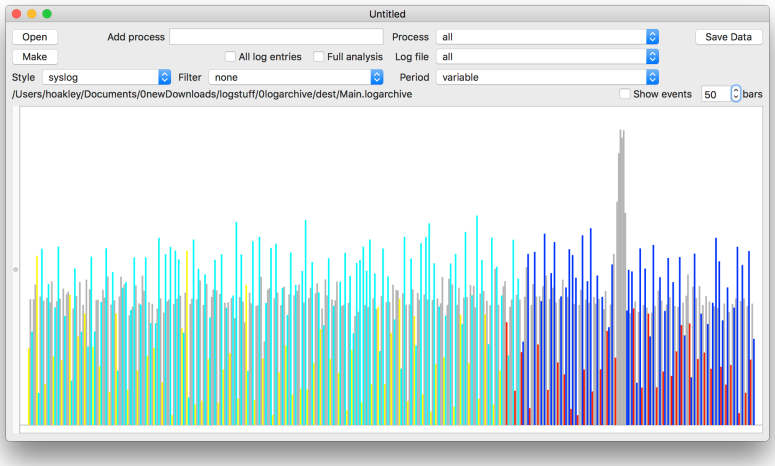
The first line in the CSV file gives the column headers, and each subsequent line lists the 'log load' of that process in the given log file. As these analyses typically go back more than 3 months, but log files are usually only kept for the last 20 days or so, most of these log files will have long since gone. You may still be able to obtain them from your Time Machine backups, if you wish.

The total size and size figures appear to be the uncompressed space occupied in that log file. The values appear far to high to be the number of messages written to the log, and too high to be the size of the messages within the tracev3 compressed format.

These sizes appear to be indicative of both the activity of the process, and the frequency with which it writes to the log. They are also valuable for anyone wishing to browse individual log

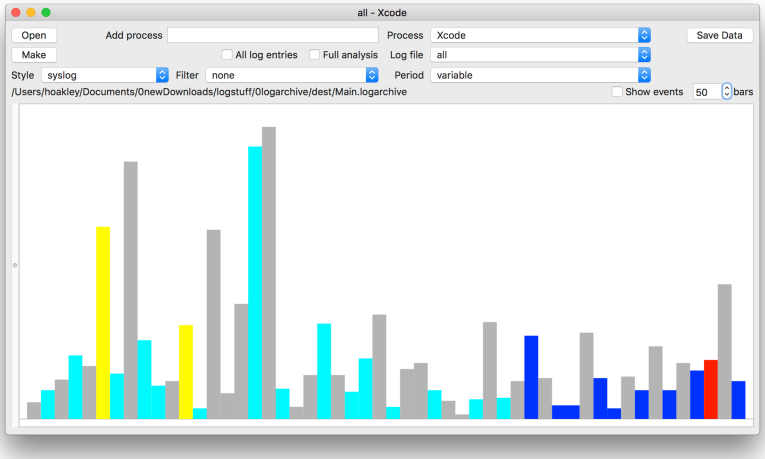
files within the logarchive, and particularly for developers wanting to get an overview of use and performance of their apps.

Note that `logd` doesn't always record in these logs when it rotates log files: it is impossible to know whether this is a bug, as `logd` is undocumented. However, it does mean that some time periods will not have been analysed. However, you can still access those individual log files which have been included in the logarchive, using the **Log file** popup menu, which lists all the .tracev3 format log files found.



When the popup menu is set to **all**, the data shown in the chart is the **total log load** given for that log file:

- bars shown in **grey** represent analyses from memory rollovers, which have never been saved to disk, and you cannot access in any further detail;
- those shown in **dark blue** are regular log files which are currently accessible in the **Persist** folder; when they have been purged and lost from storage, they are shown in **cyan** (light blue);
- those shown in **red** are additional log files which are currently accessible in the **Special** folder; when they have been purged and lost from storage, they are shown in **yellow**.



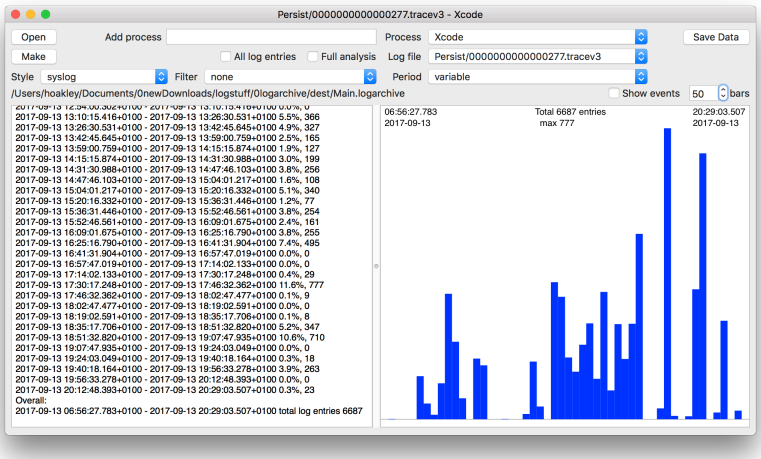
When the popup menu is set to a process name, rather than **all**, the height of the bars represents the percentage for that process in that individual log file (or memory rollover). The same colour coding applies. Note that when the popup menu is set to a custom process rather than one listed in the standard analysis, and **Full analysis** is enabled, only red and dark blue bars are shown, as Woodpile only has the data which is has been able to obtain from the log files themselves.

Bars are scaled so that the highest on any display is 100%, reaching to 10 points short of the top of the view. They are shown in time order according to the timestamp recorded by `logd` when it added the analysis to its log. This is normally shortly after that log file was closed. Note that time is not linear along the X axis: all values given by `logd` are shown in order, and no gaps are added to represent periods when that process is not represented in `logd`'s analysis of the top twenty log loads for that period.

Examining a process in a specific log file

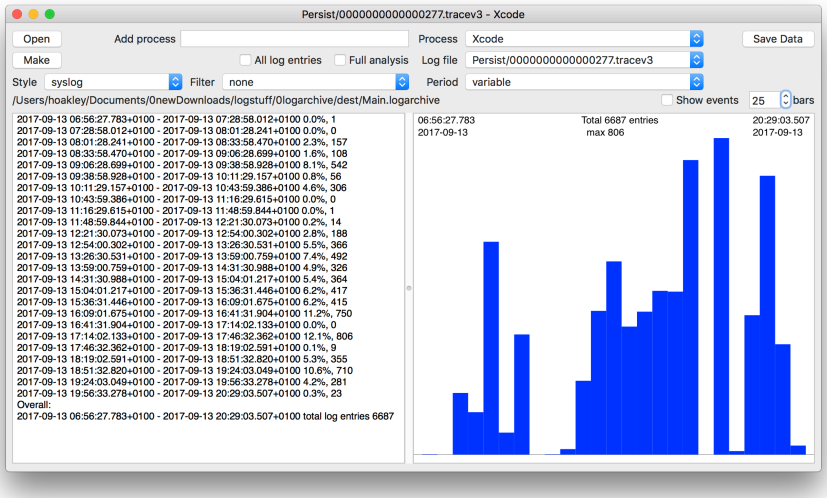
To look in more detail at a process in any given log file, click on one of the bars. Typically, you will be most interested in the taller bars, where that process has made many entries in the log. You can only obtain more detailed information from bars which are coloured dark blue or red, as those are the only datasets held in the log files within your logarchive. As `logd` progressively weeds the contents of Special log files (shown in red), older Special log files contain fewer and fewer log entries, and may not contain any for the process which you are interested in. Alternatively, if you already know which log file you want to examine, you can select that in the **Log file** popup menu.

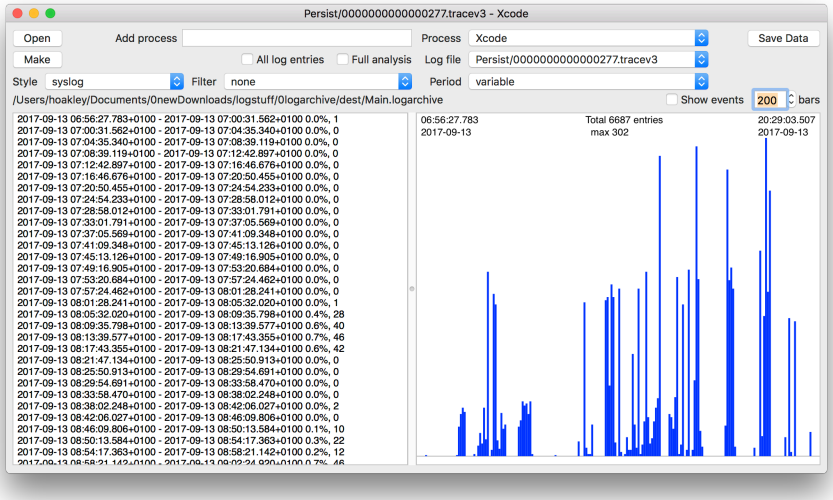
When you click on a bar in this top-level process view, please be patient. Woodpile pauses while it first obtains a log extract from the file which contains all relevant log entries; that may take several seconds. Woodpile next extracts the frequency information from those log entries. If there are many entries, this can take several seconds, during which you will see the spinning beachball cursor. This does not mean that Woodpile has frozen or crashed: an individual log file often contains several million log entries, and it takes time to analyse them fully. Once that analysis is complete, both the views in the window will change.



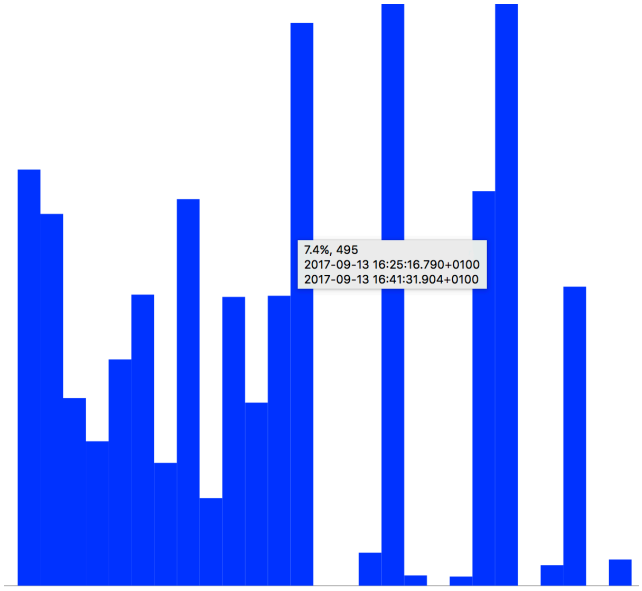
The text view on the left gives frequency, both in percentage and the actual number of log entries, for fifty time intervals spanning the period over which the log file was collected. At the end of those figures, overall information is given for that log file, including the date and time of the first log entry by the selected process, those of the last entry, and the total number of log entries for that process between those two moments.

You can change the number of bars displayed in the chart view using the **bars** control. Type a number between 5 and 200 (inclusive, default 50) into the text box and press **Tab** or **Enter**, or use the stepper control to the right of the text box to increment or decrement the number. When you are happy with the setting, **Shift-click**/tap or **Shift-right-click**/2-finger-tap on the chart view to set the new value and redraw the chart. Shift-click/tap also refreshes the text view, whilst Shift-right-click/2-finger-tap only refreshes the chart.





This provides a simple way to control the time period for each bar on the chart, and is particularly valuable for setting the duration of log excerpts obtained. This setting is not applied globally to all open windows: it only applies to the window in which it is set, allowing you to scale different windows separately.



The bar chart at the right displays the same frequencies over time. Now when you hover the pointer over any of the bars, a different ToolTip is shown, giving the percentage frequency and number of log entries for that time period, and the dates and times which define the start and end of that period.

At the top of the bar chart, there are three areas of text information. Those on the left and right give the start and end times and dates for the data shown in that view. They match the dates given at the end of the text in the text view. In the centre, the total number of log entries for the selected process is given for the period shown in the chart, and the maximum number in the bars.

You can of course open two or more windows on the same logarchive, and compare analyses on different processes within the same log file. Note that the period over which frequency analysis is performed runs from the first log entry by that process to its last. Those can differ considerably between different processes, something which you can synchronise using the **Period** popup menu, described later.

If you click on one of the bars when **all** processes are shown, or if the bar that you click on doesn't have a corresponding log file within the logarchive, nothing changes. When you change process in the popup menu, Woodpile will respect any Log file setting, and display data for the newly-selected process and the selected Log file. If Woodpile fails to find any log entries in a given log file for the specified process – even though the `logd` log claimed that there had been entries – the text view displays a message to explain that.

Zooming in time

The initial view of a process's activity in a single log file may cover a period of several hours, and tens or hundreds of thousands of individual log entries. In most cases, you will want to zoom in to view just one section within that whole period: just **click** (left-click, single-finger

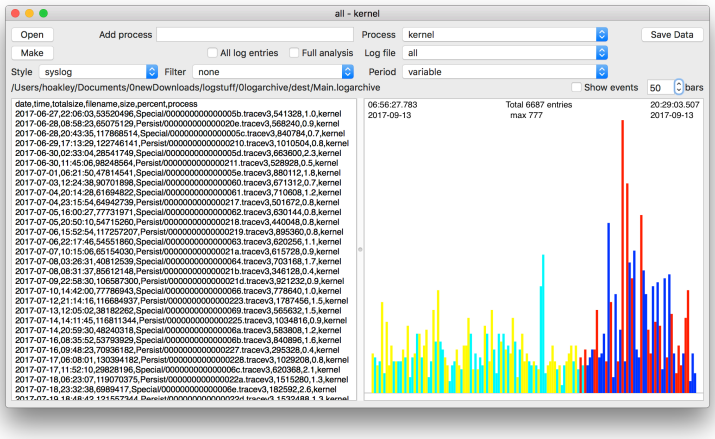
tap) on the bar of interest, and Woodpile will display a frequency analysis for the time period of that bar alone.

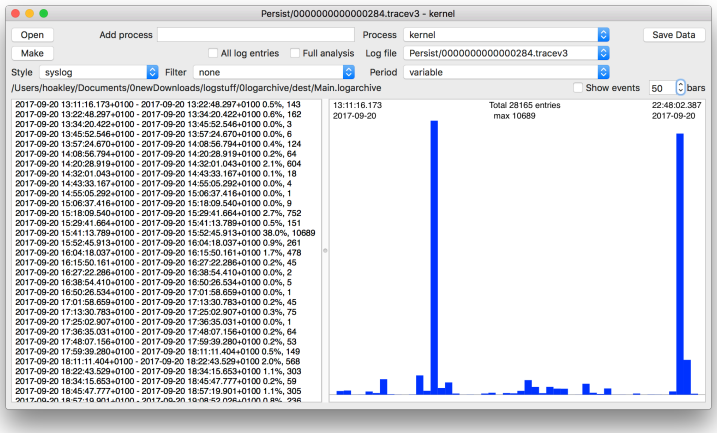
You can continue to zoom in by clicking on bars until you have identified a short enough period for which to browse log entries. Normally, this is best when the bar has less than 1000 entries in the period. If you then **Command-click** instead of just clicking, the bar chart will zoom in as usual, but the text view will show a log extract for the current process over that period.

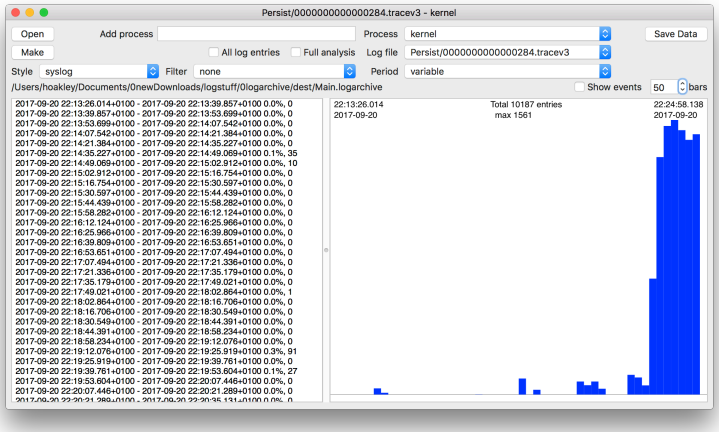
To zoom back out, and view longer time periods, simply **right-click** (two-finger tap) anywhere on the bar chart, and it will return to the previous zoom level.

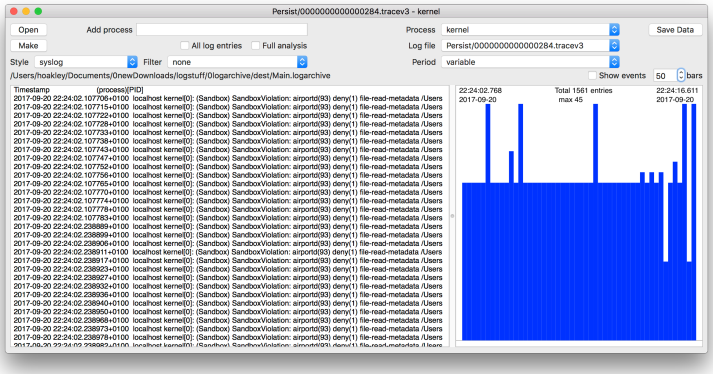
Sometimes, zooming in or out may involve considerable computation, and there may be a slight delay before the views are updated. It is normally much quicker to zoom in or out than when first viewing a single log file for an individual process – the first step after you have chosen which process to examine.

The screenshots which follow show the process of zooming in progressively on shorter periods of log entries for the kernel, until in the last its log entries are browsed for a time period of just 13 seconds.







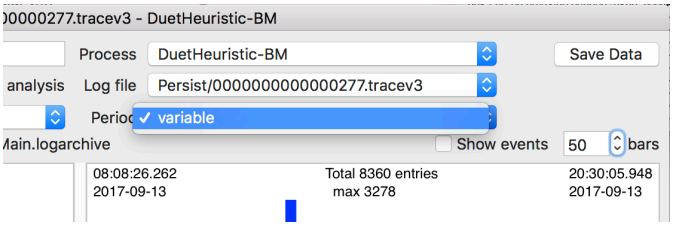


For your own numeric safety, there is a limit imposed on zooming into periods shorter than 0.001 seconds.

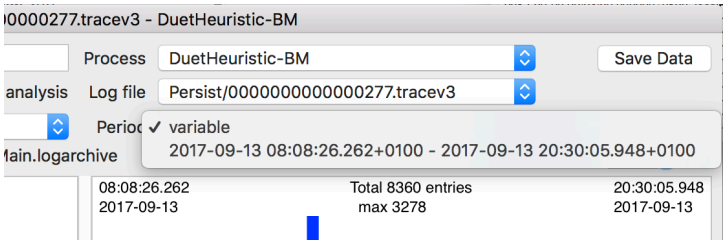
Sometimes, the chart view may not appear to have updated correctly for the set combination of **Process**, **Log file**, and **Period**. To force the chart view to refresh, simply Shift-right-click anywhere on that view, to refresh the text view too use Shift-click. If that doesn't help, click to zoom in, and Right-click to zoom back out again.

Synchronising windows

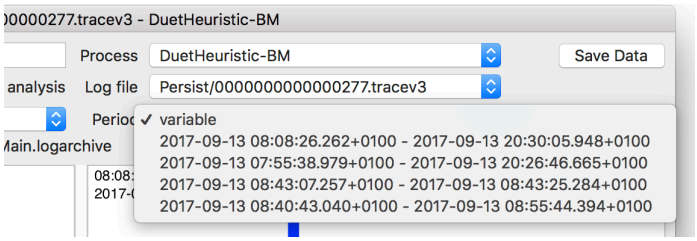
When you want to examine two or more processes in the same log file, Woodpile's standard automatic scaling of charts makes life harder, as they may have quite different periods. This isn't an easy problem to solve, because there is no reliable way to get the precise time interval covered by each log file. The best solution is to set two or more windows to a common time period, using the **Period** popup menu.



When you open your first window and set it to show a **Process** and one **Log file**, at first the **Period** menu shows a single entry, **variable**. To add that window's time period to the menu, Shift-click (or Shift-right-click) anywhere on the chart view.



You will then see the time period for that setting added to the **Period** menu. As you open additional windows on the same log file, repeat this process with each, and you will see their menus fill up with each of the periods. If you want to zoom into one window and use a shorter time period, do so in the normal manner, and you should see that period listed in the menu too.



When you have decided on the period that you want displayed in each, simply select it in the **Period** menu for each window, and the data will be rescaled to show that period.

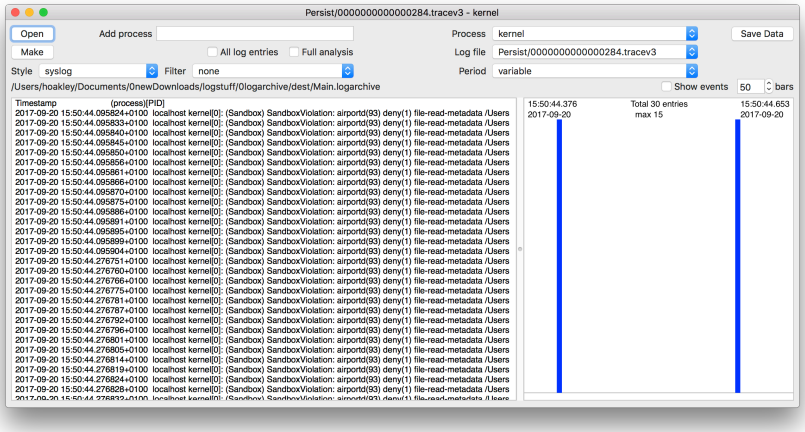
You can keep windows open on several different log files if you wish: Woodpile will only offer appropriate periods in the menu of each, depending on which log file that window is currently inspecting.

Although the **Period** menu normally updates automatically, it does sometimes appear to get stuck, and may not show the period set in a window (particularly when that is set to **variable**). Simply Shift-click to fix this.

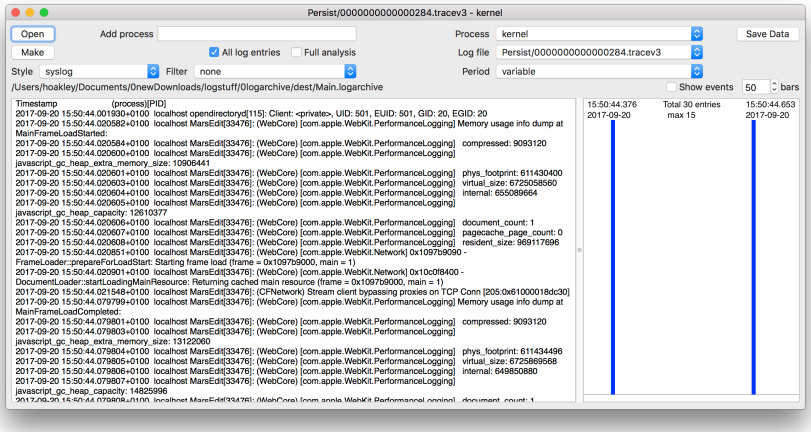
When you set a window to the same period as another, its previous period is removed from the menu, as that only offers those periods which are currently in use in windows examining that individual log file. To return a window to its full-scale zoom and scaling, use the **variable** menu command in the **Period** popup menu. If this doesn't appear to work properly the first time, Shift-click on the chart view.

Showing log entries

Most of the time, when you want to inspect log entries in the text view, you will only want to see those for the selected process. Sometimes it is important to be able to see these in the context of other log entries. To help you do that, you can now choose whether to see **All log entries** when you Command-click, or just those of the selected process: set that in the checkbox.



With the checkbox unticked (the default setting), only log entries from the selected process will be shown.

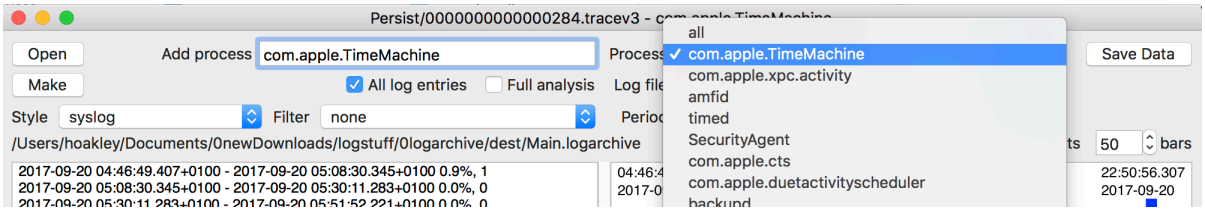


With the checkbox ticked, all log entries for the current period will be displayed. If you try this with a longer period, more than a minute or so, or during a period of intense log activity, you may find yourself scrolling through tens of thousands of log entries.

Adding your own processes

When Woodpile has analysed your logarchive, it lists only those processes which have written to the log most heavily, in the **Process** popup menu. If you want to analyse and browse the log entries made by a process which is not included in that list, you can add it using the **Add process** text box, or in the **Preferences** sheet.

To do this, simply type the name of the process which you want to be used as the search string in the log, into the **Add process** text box, and press the **Tab** or **Return** key. Inspect the **Process** popup menu and you should now see your process added to it. If it does not appear, this is likely to be because it is already included.



Processes which you have added in this way have not been included in `logd`'s statistical analysis of the log files, so they normally only analysed in individual log files. When the **Log file** popup menu is set to **all**, you will see an explanatory message in the text view, reading:

```
The selected process is not included in the statistics available for this
logarchive. Please select an individual log file for statistics covering that
period, or turn on Full analysis using the Checkbox above.
```

You can change that by enabling a **Full analysis**, detailed below.

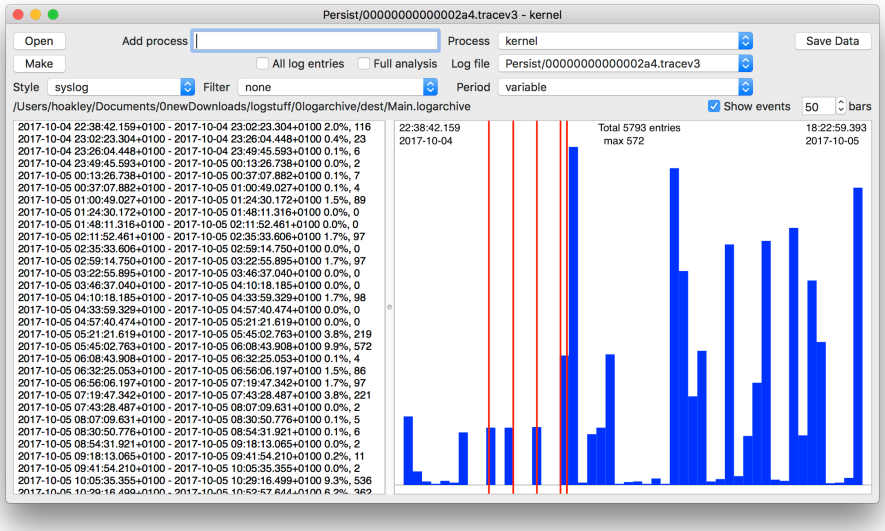
The bar chart display is left unchanged, and its Tooltips still work, but you cannot use it to zoom in on another process unless you re-select the all item in the **Process** popup menu.

To examine your custom process, select one of the entries in the **Log file** popup menu, and Woodpile will fetch and analyse that log file for entries made by your chosen process. They will then be displayed as normal in the text and bar chart views, and you can zoom in and use the other mouse/trackpad actions to examine entries by that process in the selected log file.

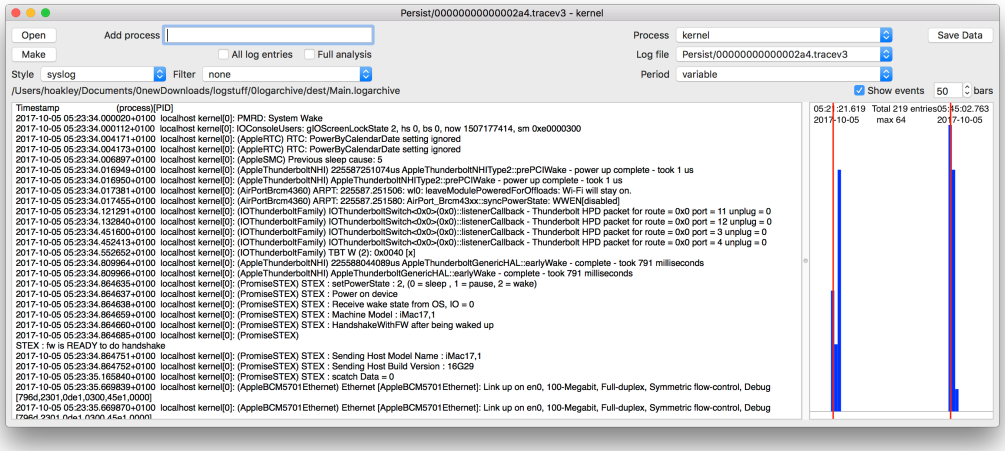
When you add a custom process, it is made available in the **Process** menus of all open and new windows. It is also saved to Woodpile's preference file when you quit the app. You can always edit the list of custom processes in the **Preferences** sheet, detailed later.

Showing significant events

The most significant events – startup, and transition between sleep and being awake – are recorded in the log, but can be very difficult to spot in log load charts. They are also not identified by `logd`. Startup invariably results in `logd` opening a new Persistent log file, which makes identification from patterns even more difficult. This version of Woodpile has a new option, **Show events**. When that box is ticked, each time that you open a log file in the **Log file** menu, additional analysis is performed on that file to determine any startup or event events. The times of any found are then marked using a full-height red line in the bar chart.



The example above shows five separate events in which the Mac woke from sleep. Startup and wake events are not distinguished in the chart view: both are marked using the same red lines. Those lines do not support any additional ToolTips either.

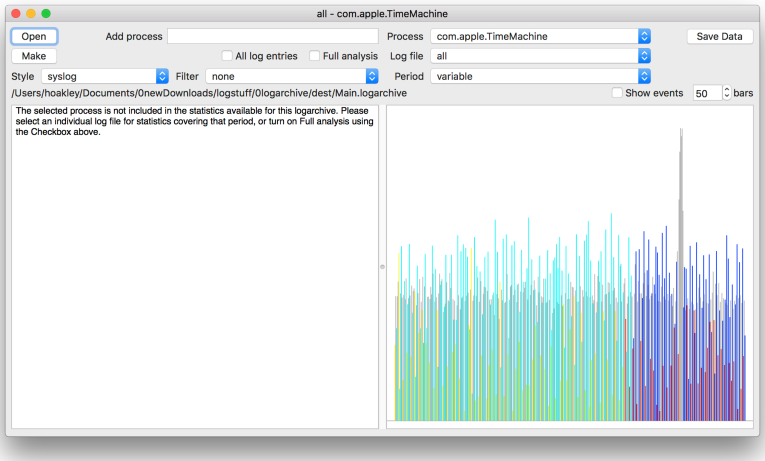


One good way to ascertain the precise time and details of these events is to select the kernel process for the log file which you are examining. Zoom in on a blue bar containing a red event line until there are a modest number of log entries, and Command-click to browse them, as shown above.

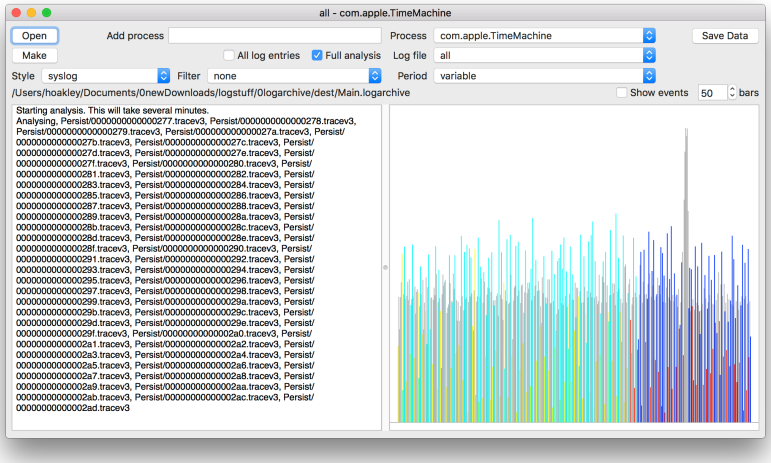
Show events does not alter the charts shown when **all** is selected in the **Log file** menu, because the data used for that display are drawn from `logd`'s summary figures. As **Show events** requires an additional examination of the log for the selected log file, it does add significantly to the time required to load and display the data.

Showing a full analysis of a custom process

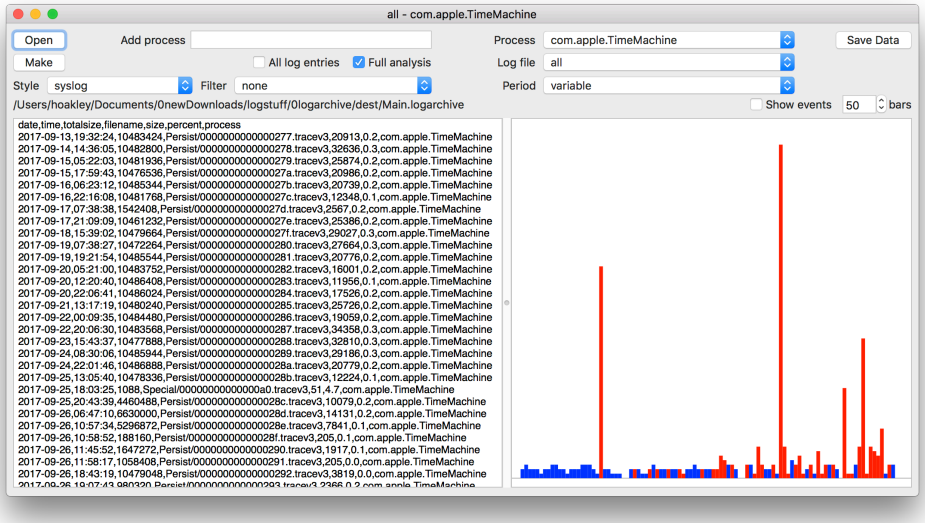
Normally, if you select a custom process when all is selected in the **Log file** menu, the text output view will display a message informing you that the data are not available.



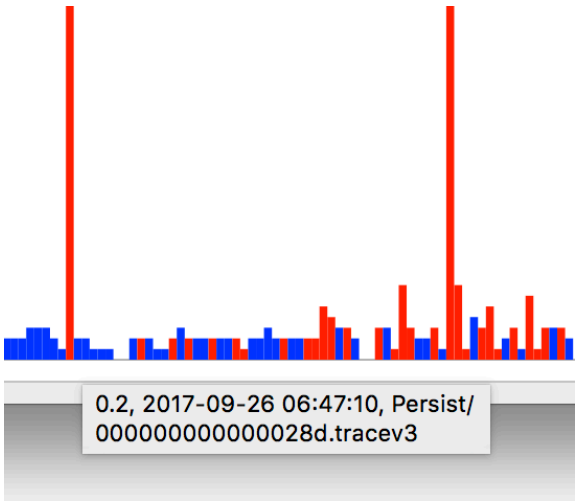
If you wish, you can opt to have Woodpile perform a **Full analysis** on custom processes. When that option is selected, if you set the **Process** menu to a custom process (which you have added) and set the **Log file** menu to **all**, Woodpile starts to analyse all the log files within the logarchive to estimate the log loads of your custom process. This will take several minutes, during which the text view on the left will give indication of progress, by detailing the log files which have been analysed so far.



When that is finally complete, a full analysis across all the available log files will be displayed in both the text and chart views. Because Woodpile can only perform this on the log files which are left, all the bars will be red or dark blue in colour. The load figures given are also different from those normally displayed, as they are the absolute size of all log entries for the custom process, and the percentage of the total log file size. However, these do appear to approximate to a log load similar those those used by `logd`'s analyses.



You can then view ToolTips information about each bar, and click or tap on a bar to zoom into that time period.



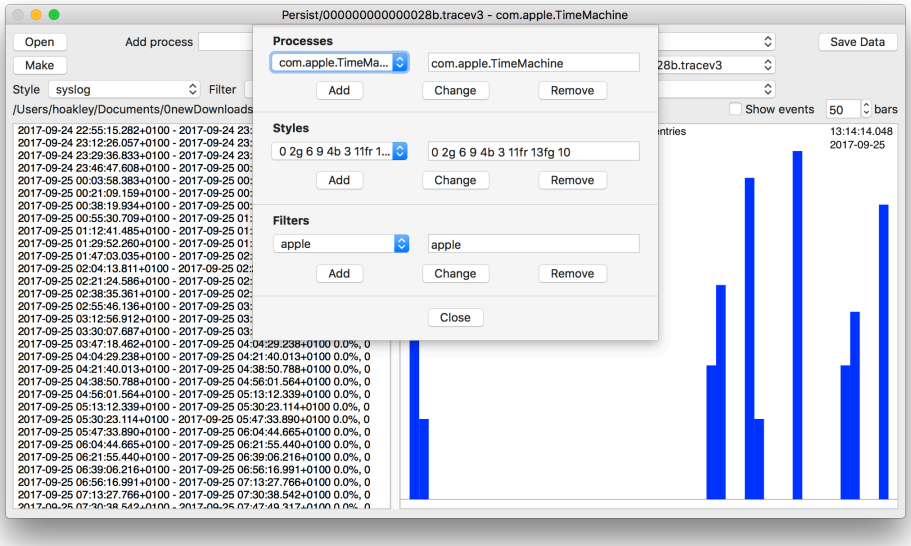
You should only leave the **Full analysis** checkbox ticked when you want this performed. If you inadvertently leave it ticked and set the menus to show a custom process across all log files, then Woodpile will launch the lengthy process of analysing all the log files again. A future version will cache data from analyses, so that they can be reused: the current version doesn't do that.

Because of the complex view hierarchy, you will find it best to perform full analyses in a newly opened window. Currently, if you use a window which has already been browsing other processes at different levels, you may find that the text and chart views fall out of sync. This will be fixed in a future update.

Woodpile (1.0b5) for macOS Sierra & High Sierra
Preliminary Documentation
Howard Oakley https://eclecticlight.co

Preferences: Your library of custom processes

Use the app menu **Preferences** command, when any window is open in Woodpile, to edit the list of custom processes. These are added to the Process popup menu to appear between the top item, **all**, and those processes added from the `logd` analysis. You can add any other processes which you wish, to make them instantly accessible.



To add a new process, open the popup menu in Preferences and select the **New…** item at the end. In the adjacent text box, enter the name of the process, such as `com.apple.TimeMachine`.

When ready, click on the **Add** button to add it to the popup menu, and continue to add the process names which you want to store. To change a process already in the menu, select that menu item and its name will be loaded ready to edit. When you have finished editing it, click on the **Change** button. If you do not click on the button, your changes will be ignored. To remove a predicate from the menu, select it in the menu, then click on the **Remove** button.

Once you have finished editing your preferences, click on **Close** and those changes will be saved to Consolation's preferences, and immediately available in all windows.

Preferences: Defining your styles

The controls used to define your own library of styles are in the Preferences sheet shown previously. They operate the same as those for processes, and are added to the **Style** popup menu after the default of syslog. You cannot edit or remove that default.

A style, at its most basic, simply lists the different fields to be shown in the log excerpt, in the order in which they are to be shown. A popular minimal style might consist simply of three integers separated by single space characters:

```
0 2 10
```

This will result in the display, in sequence, of the timestamp (field 0), messageType (2), and eventMessage (10). You can display fields in any order that you wish.

The timestamp field can be displayed in 3 variants: as it comes, e.g.
`2017-07-26 19:47:54.951146+0100`
or you can add a formatting character of `h` or `d` for just the time part of the timestamp, or the timestamp without the UTC shift. So using `0h` would produce
`19:47:54.951146`
and `0d` would produce
`2017-07-26 19:47:54.951146`

Other fields have two groups of formatting options:

- **content options** determine how much of the field is shown:
  - the default is to show the whole field
  - `t` shows only the first 20 characters in the field
  - `T` shows the last 20 characters
  - `f` shows all characters after the last slash / in the field. This specifically intended to eliminate very long pathnames in the processImagePath and sendImagePath fields.
- **colour options** set the colour of the text to be used:
  - the default is standard black text
  - `r` displays red
  - `g` displays green
  - `b` displays blue.

These can be used in any order and combination, provided that no more than *one* of the content options is used, and no more than *one* of the colour options, for any given field. So
`0h 2g 6 9 4b 3 11fr 13fg 10`
will display the timestamp without the date in black, the messageType in green, threadID and processID in black, the subsystem in blue, the category in black, the processImagePath truncated to just the file name in red, the senderImagePath truncated to just the file name in green, and the eventMessage in black. You cannot use `11tfr` or `10trg`, for example.

The full list of available fields and their numbers is:

0. timestamp, in full e.g. 2017-07-26 20:24:59.326229+0100, or with `h` or `d` format
1. machTimestamp, in system ticks, e.g. 608403543041193
2. messageType, e.g. Default
3. category, e.g. security_exception
4. subsystem, e.g. com.apple.securityd
5. processUniqueID, e.g. 156
6. threadID, e.g. 868
7. traceID, e.g. 833721519476834308
8. senderProgramCounter, e.g. 193733726
9. processID, e.g. 156
10. eventMessage, e.g. MacOS error: -67062, can usefully be truncated with `t/T` format
11. processImagePath, e.g. /usr/libexec/taskgated, can be truncated with `t/T` or `f` format
12. processImageUUID, e.g. 4F6F0B24-7A18-3AF9-853F-8F72F6C7D7C7
13. senderImagePath, e.g. /System/Library/Frameworks/Security.framework/Versions/A/Security, can be truncated with `t/T` or `f` format
14. senderImageUUID, e.g. 005E8C96-40B6-35E3-B58B-888A5F5957C2
15. timezoneName, may be blank.

The way that Woodpile achieves this is to obtain a full JSON log extract, then compiles the field content according to your selected style. This takes a little longer, particularly on very large log extracts, but shows only the information that you want to see.

Message filters

Unlike Consolation, Woodpile doesn't give you access to complex predicate-based filtering of log extracts, as it already uses that to filter by process. You can use the **Find** command in the **Edit** menu to search log extracts in the text view, which works in the normal way. However, there are times when it is very helpful to filter log extracts to show only those entries which contain certain characters in their message fields (eventMessage in the list of fields above).

Woodpile lets you specify a search string to be applied as a **filter** to an existing log extract which uses a custom style (these do not work with the default syslog style, as its contents are unstructured). This is usually very quick, and often almost instantaneous, because Woodpile doesn't have to obtain a fresh log extract. Woodpile now supports not only simple text search, but also the use of regular expressions (regex).

To add a new search string to the filter menu, open **Preferences**, and use the **New…** command in the **Filters** popup menu.

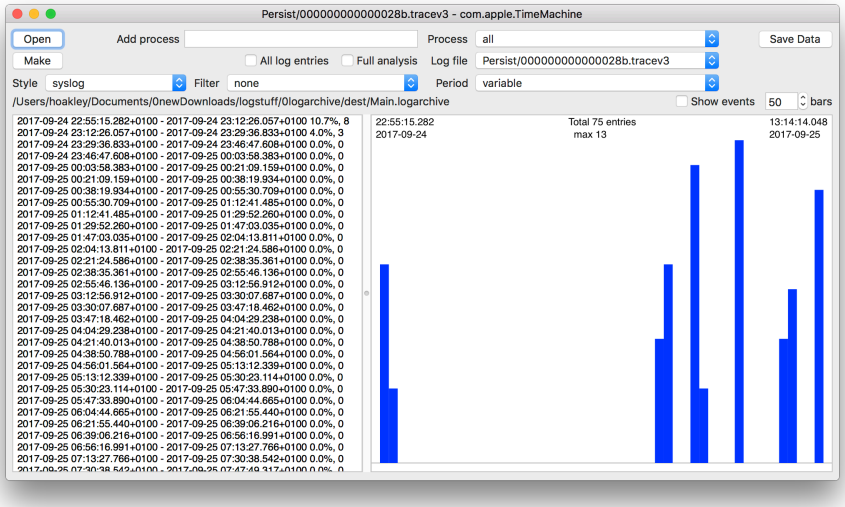
To add a simple search filter, which will be used for localised case-insensitive search, type the search string into the adjacent text box. To add a regex filter, type the ® character first (Option-r) followed immediately by the regular expression you want to use.

When you have finished defining your new filter, click on the **Add** button to add it to the filter menu. The **Change** and **Remove** controls work as for the other sections, and you must click on the **Close** button to close the preferences dialog.

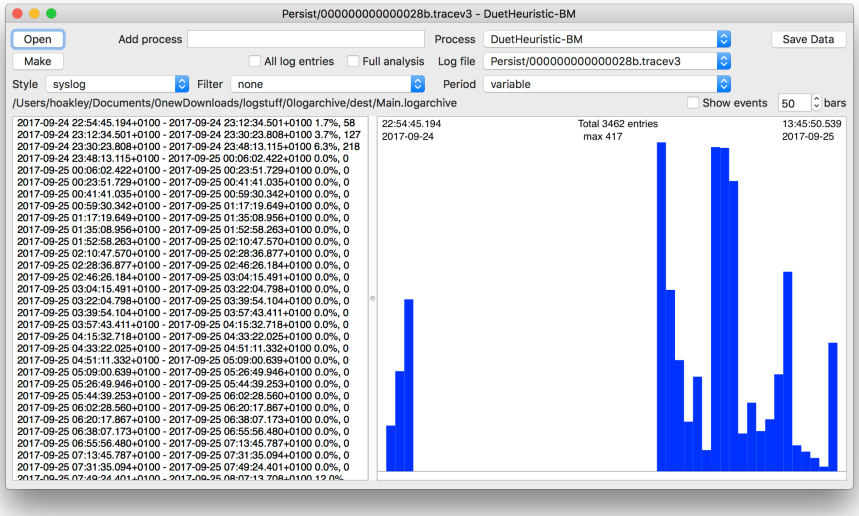
Custom process and log file example

You can investigate breakdown in regular hourly Time Machine backups very easily using Woodpile's new features. Unless something goes serious wrong with it, Time Machine writes very few messages to the log, so will not appear in routine analyses of log load.

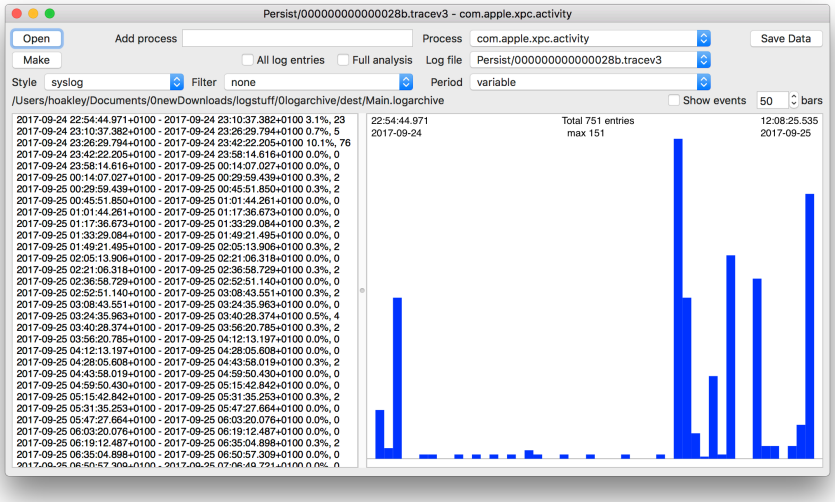
I started by adding `com.apple.TimeMachine` as a new process, then turned on **Full analysis**, which generated the results shown previously. These revealed a tell-tale gap, which occurred in the small hours of 25 September 2017, and is recorded in the log file Persist/0…028b.tracev3.



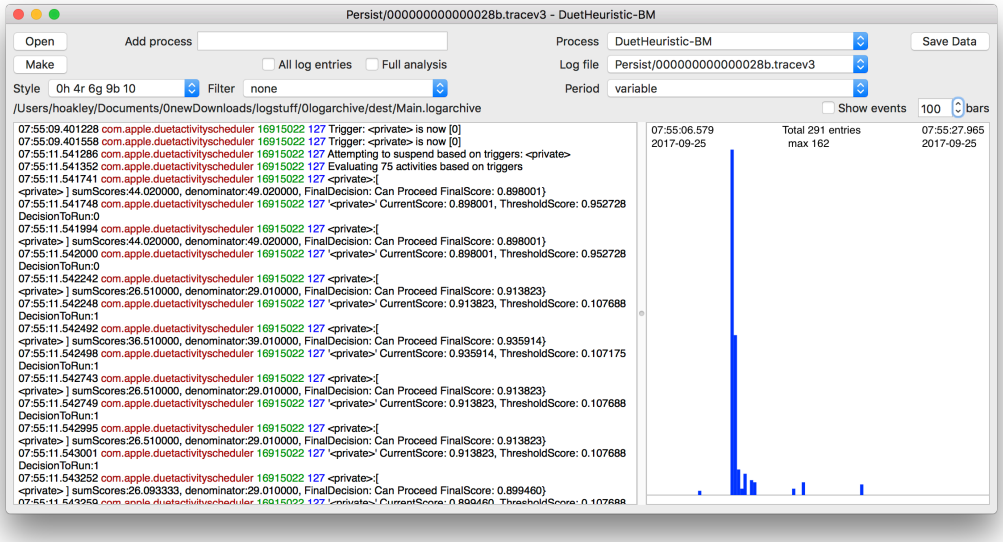
I viewed that same log file with one of the processes already listed, `DuetHeuristic-BM`, which shows a matching gap. This process shows activity in one of the undocumented macOS scheduling and dispatching systems, DuetActivityScheduler or DAS.



I then added a custom process to another window, for `com.apple.xpc.activity`, which looks at the other scheduling and dispatching system, CTS. I set that for the same log file, and saw that its gap is not as total as that in DAS, and reflects some continuing XPC dispatching, but not driven from DAS.



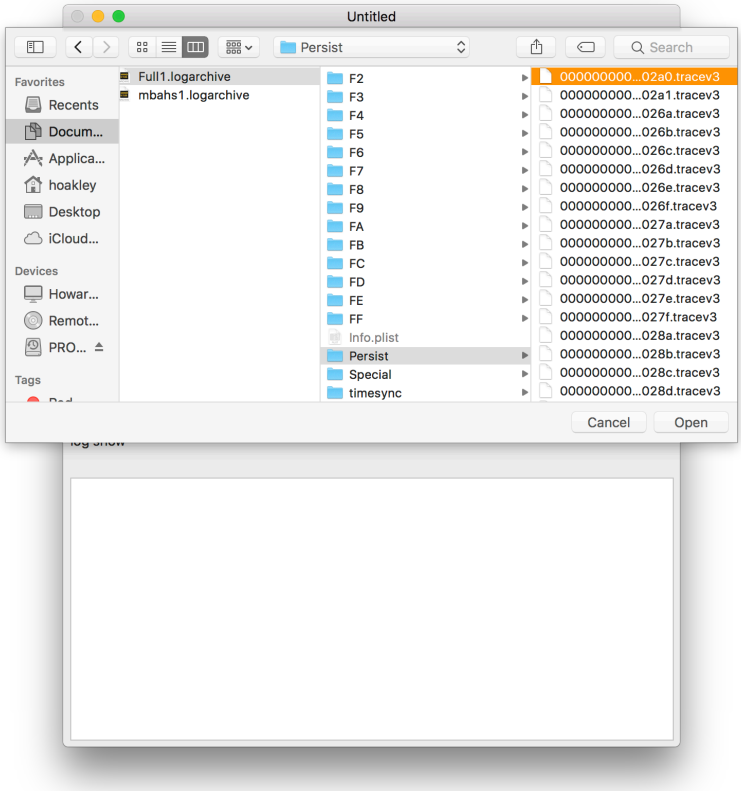
Finally, back in the DuetHeuristic-BM view, I zoomed in on the return of activity after the gap, with the Command key held, so that I could browse the log entries made by DAS when it was trying to get going again. Here, I'm using a custom style which displays much more information from each log entry than the default syslog, and uses colour for different fields to make them significantly easier to read. I have also increased the bars setting to 100, and Shift-clicked on the chart view, to see finer resolution in that chart.



Using any other log browser, you would never find this needle in the haystack of a huge logarchive, but with Woodpile you can go on and identify further failures in Time Machine backups at other times, and compare patterns across different processes.

Browsing logs in Consolation

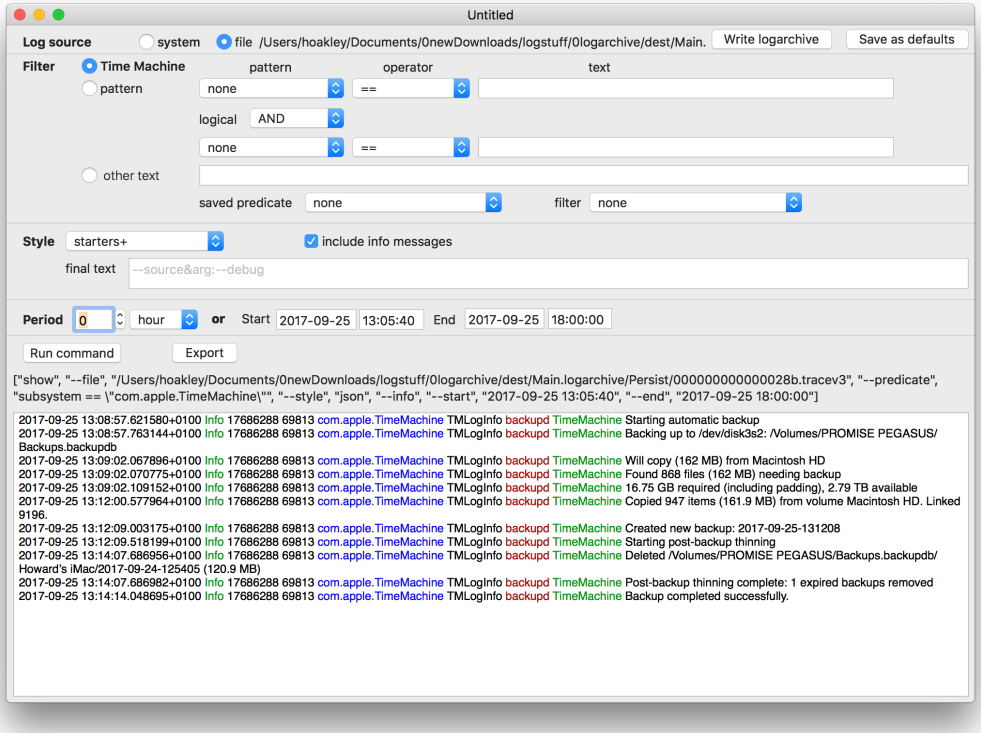
Unlike Apple's Console, which can only browse complete logarchives, Consolation can browse either logarchives as a whole, or individual tracev3 log files within a properly-formed logarchive. Currently no tool is able to browse an isolated tracev3 log file.
To open a logarchive or tracev3 file in Consolation 3, click on the **file** radio button in the **Log source** section at the top of its window. You will then be prompted to select the logarchive or log file within it.



Consolation lets you select either the logarchive, or an individual log file, as its Open File dialog sees inside the logarchive bundle. Remember that you should only find tracev3 log files at the top level of the bundle, or within its **Persist** or **Special** folders.

Ensure that you have the logarchive's catalogue open, either in Woodpile or a text editor, or the frequency analysis of an individual process in a single log file. Depending on which tracev3 log file you have selected, you can then copy and paste the start and end dates and times into Consolation's **Start** and **End** text boxes. Set the **Period** to **0** (with any time unit), so that the app uses the **Start** and **End** times rather than the period.

Set the rest of the controls up, and then make a final check that the **Start** and **End** dates and times are within the period for your selected log file. Then click on **Run command** to view that log excerpt.



You can use the same technique to view selected periods from within the whole logarchive, if you prefer to do that rather than home in on an individual log file.

When you want to change log files, instead of clicking on the **system** radio button at the top and then the **file** button, simply click on the **file** button, and you should be prompted to select the new log file to be browsed. Remember to change the **Start** and **End** dates and times to those appropriate to that log file, or you may not see any log entries.

Technical note

When examining frequencies of entries within a specific .tracev3 log file for a given process name, the predicate submitted to the `log show` command is
`subsystem ==[c] processname OR processImagePath CONTAINS[c] processname OR senderImagePath CONTAINS[c] processname`
where `processname` is the name of the process as listed in the popup menu. The same predicate is used when obtaining log extracts using Command-click, but with set start and end times.

Significant events are obtained using the following predicate for the `log show` command:
`eventMessage CONTAINS[c] "system boot:" OR eventMessage CONTAINS[c] "BOOT_TIME" OR eventMessage CONTAINS[c] "PMRD: System Wake""`
This should elicit startup events and wake events on all current versions of Sierra and High Sierra.

Change list

1.0b5:

- addresses an 'unexpected quit' or crash when opening.

1.0b4:

- added regex option to filters
- fixed bug constraining column widths in chart view, leading to mismatch with events, etc.
- worked around Xcode 9 generic window bug by creating custom window class
- changed Shift-click/tap to refresh text as well as chart view.

1.0b3:

- fixed the Process textbox, stopping it from adding empty strings
- fixed a crashing bug which occurred rarely when using a custom Period
- inserted log file and process name as window title
- added bars control, and moved Show events
- fixed Process menu selection to stay with same Log file, when not set to all
- further improvements in synchronisation of controls and views
- added Shift-click (left or right, single or two-finger tap) to refresh chart view.

1.0b2:

- added Preferences sheet, with custom process editing
- added Styles, with editing in Preferences
- added Filters, with editing in Preferences
- rearranged controls to accommodate two additional popup menus.

1.0b1:

- added option to show all log entries on Command-click
- added text info to chart view
- made custom processes global settings, and saved to preference file.

0.8a1:

- fixed two occasional divide-by-zero errors
- imposed a limit on zooming to prevent other numeric errors
- handled empty datasets better, preventing infrequent crashes
- added functionality to the Period popup menu
- started adding support for preference settings; not functional yet
- added within-app notifications to support period synchronisation.

0.7a1:

- fixed bug in changing the open logarchive, which prevented new logarchive from being accessed properly, and concatenated their log file lists
- added Show events
- added Full analysis
- added (currently functionless) Period popup menu and rearranged controls
- added code to handle long processes better.

0.6a1:

- changed window controls and layout
- removed old log file text box
- added Log file popup menu to select log file to be used
- added Add process and extended Process popup menu to allow custom additions.

0.5a1:

- added zooming in and out within a tracev3 file
- added log extract with Command-click
- fixed crash which occurred if log failed to return any dated log entries.

0.4a1:

- added support for opening tracev3 log files and examining entry frequencies by process.

0.3a2:

- fixed a drawing bug which didn't update the bounds and rescale correctly.

0.3a1:

- added ToolTips
- optimised ChartView drawing.

0.2a1:

- split the window, and added the chart view.

0.1a1:

- first version.

28 November 2017.