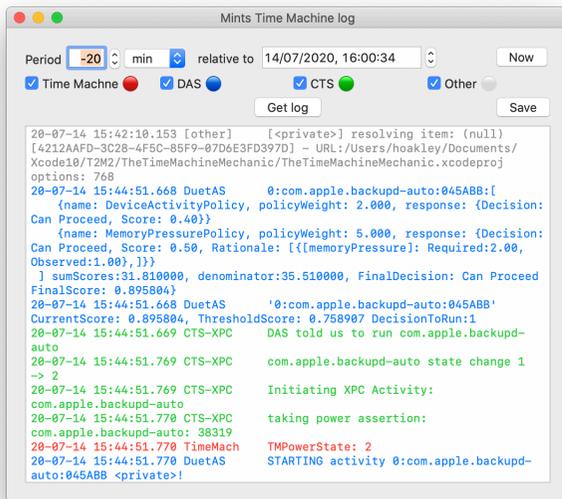


# Start

Mints is a growing collection of tools to provide deeper insight into macOS, to help you understand how its features work, and to help diagnose its problems. In this release, 24 tools are provided: these deliver log extracts covering iCloud, TCC privacy protection, Time Machine backups, the App Store, disk mounting, triald, Visual Look Up and task scheduling, test Spotlight search, list boot times, XProtect scans and Software Update information over the last 24 hours, look for Universal binaries, and show information about the Mach timebase, hardware, process environment, sudo, logs, SSDs, mounted volumes, sysctl and keychains. There's also a menu in the Window menu to explore different data types, including resolving inode numbers to regular paths, Doubles and Unicode normalization, a browser window for Visual Look Up, and a window to explore floating-point number formats.

Complex systems in macOS write dialogues to the log while they operate. Following these in a normal log extract can be difficult, because lines in each conversation are interspersed with other irrelevant entries. Mints' log browsers are different because they bring together entries from many different sub-systems and services, helping you to follow those dialogues. The use of colour to distinguish different sub-systems makes these conversations even more understandable.



# Contents

→ [Main window](#)

→ [Log Windows](#)

→ [Trial](#)

→ [Look Up](#)

→ [iCloud](#)

→ [Time Machine](#)

→ [DAS Scheduling](#)

→ [TCC](#)

→ [App Store](#)

→ [Boot](#)

→ [Disk Mount](#)

## Spotlight

→ [Create Test](#)

→ [Log Window](#)

→ [Check Search](#)

→ [Delete Test](#)

## Information

→ [Keychain](#)

→ [Logs](#)

→ [Sysctl Info](#)

→ [Mac](#)

→ [Environment](#)

→ [XProtect Scans](#)

→ [Universal Binary Checker](#)

→ [Disk Check](#)

→ [Mach Absolute Time](#)

→ [Software Update](#)

→ [Volume](#)

## Window menu

→ [Visual Look Up](#)

Data... sub-menu

→ [Floating Point Explorer](#)

→ [Inode](#)

→ [Double](#)

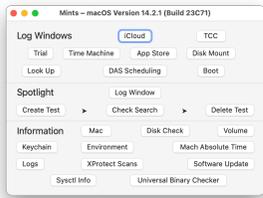
→ [Normalizer](#)

→ [Updates](#)

→ [Change list](#)

→ [Further information](#)

# Main window



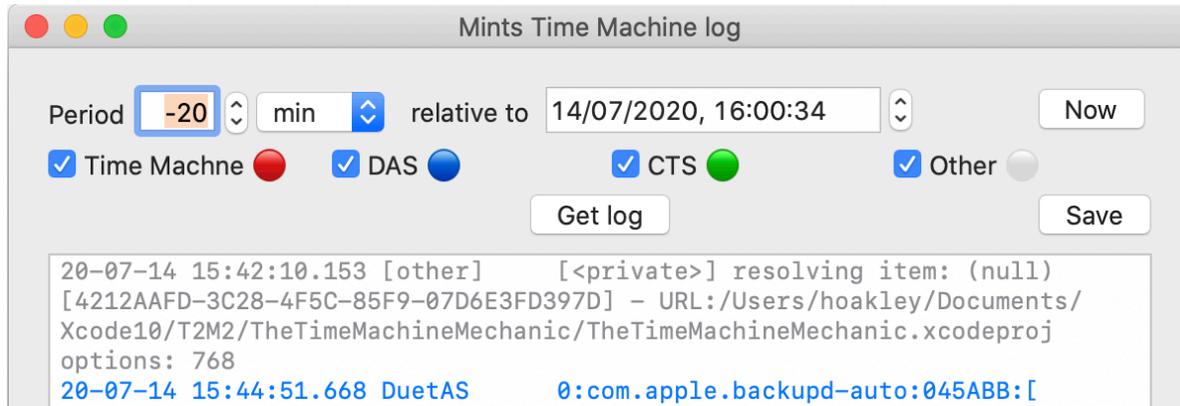
The main window currently offers 24 buttons to:

- open the → [iCloud Log Window](#), to explore iCloud messages in the log,
- open the → [TCC Log Window](#), to explore TCC and privacy system messages in the log,
- open the → [Trial Log Window](#), to explore the new trial service in the log,
- open the → [Time Machine Log Window](#), to explore Time Machine backup messages in the log,
- open the → [App Store Log Window](#), to explore App Store messages in the log,
- open the → [Disk Mount Log Window](#), to explore APFS and related subsystems in the log,
- open the → [Visual Look Up Window](#), to explore Visual Look Up messages in the log,
- open the → [DAS Scheduling Log Window](#), to explore task scheduling messages in the log,
- open the → [Spotlight Log Window](#), the explore Spotlight searches in the log,
- list the → [times of all boots](#) over the last 24 hours,
- → [create, run and delete](#) a test of Spotlight search,
- → [Get Mac Info](#),
- → run a [Disk Check](#),
- → [Get Volume Info](#),
- → [Get Keychain Info](#),
- → [Get Environment Info](#), about process execution environment,
- open → [Mach Absolute Time](#), to get information about clock rate and conversion factors,
- list → [Unified log](#) information
- list → [XProtect Scans](#) reported over the last 24 hours
- list → [Software Update](#) information over the last 24 hours
- open → [Sysctl Info](#) to get a wide range of information about that Mac and its system
- open the → [Universal Binary Checker](#), to discover which apps and other code runs native on Apple Silicon Macs (*Mojave and later only*).

When you close this window, Mints will quit.

→ [Log window controls](#)

# Log window controls



Each log window in Mints offers a simple method to specify the precise period over which log entries are to be extracted. This is based on a reference time, entered in the **relative to** box using its standard controls, and a **Period** offset from that reference, set using its stepper arrows or by editing the text directly. You can also copy and paste times in the **relative to** box: simply select an item in the box and use the normal commands.

The offset entered in the **Period** box has a popup menu to determine its units. There is also a button **Now** which will set the reference time to the immediate present. Use that with a period of  $-20$  sec to get log entries over the last 20 seconds.

To get a log extract for the 1 minute *before* a reference time, simply set **Period** to  $-1$  and the popup menu to **min**. To obtain an extract for 10 seconds each side of a time in the past, the total period wanted is 20 seconds. You can either specify that using the reference time at the start of that period and 20 sec, or the time at the end of the period and  $-20$  sec.

→ [Log window controls \(concluded\)](#)

## Log window controls *(concluded)*

The shortest period which can be used here depends on the version of macOS. In Sierra, periods less than about 30 seconds are unreliable, and entries can be missed. In Mojave and Catalina, shorter periods can be used, even below 10 seconds if you wish.

Times in the **relative to** box are in the current time zone for the set date. On days when clocks change, they use the second of the two zones. For example, when the change to summer time occurs on a day, times entered here for that day use summer time throughout.

The row of controls below the time settings set which sub-systems are shown in the log view in the main part of the window. Each uses an emoji to indicate the colour in which those log entries are displayed.

The last controls are two buttons: **Get log**, which runs the log show command to fetch a fresh log extract, parse and display it, and **Save**, which saves what's currently displayed of the log in Rich Text format, which you can also do through the **Save** command in the File menu.

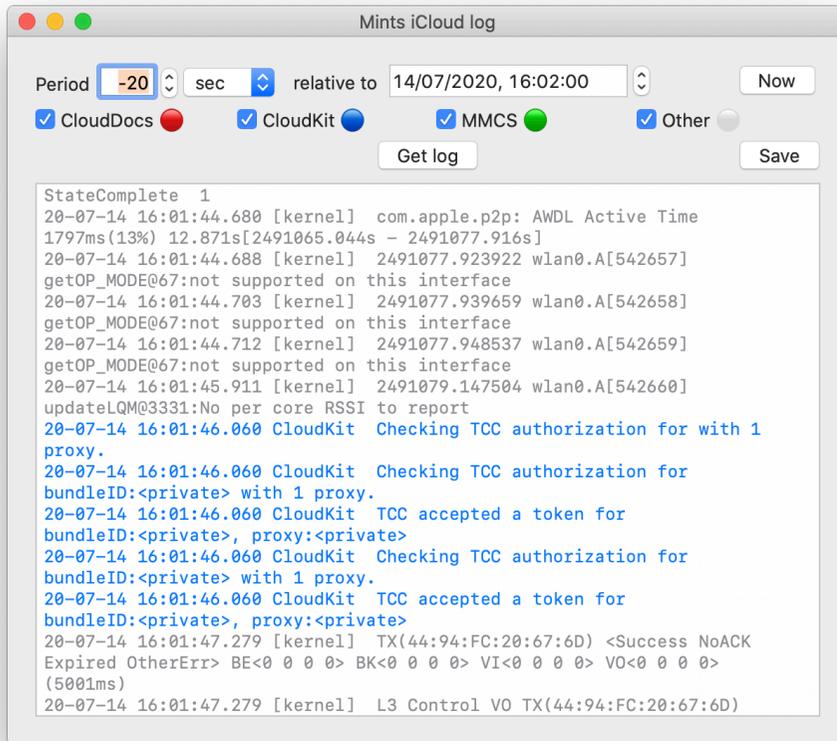
To enlarge the size of the text in any log extract, press ⌘+; to reduce the size, press ⌘- .

Each time you open Mints, it checks whether your log is in order and accessible. If it detects any problems, it will warn you about them, and suggest fixes when possible.

→ [iCloud log](#)

→ [Unified log information](#)

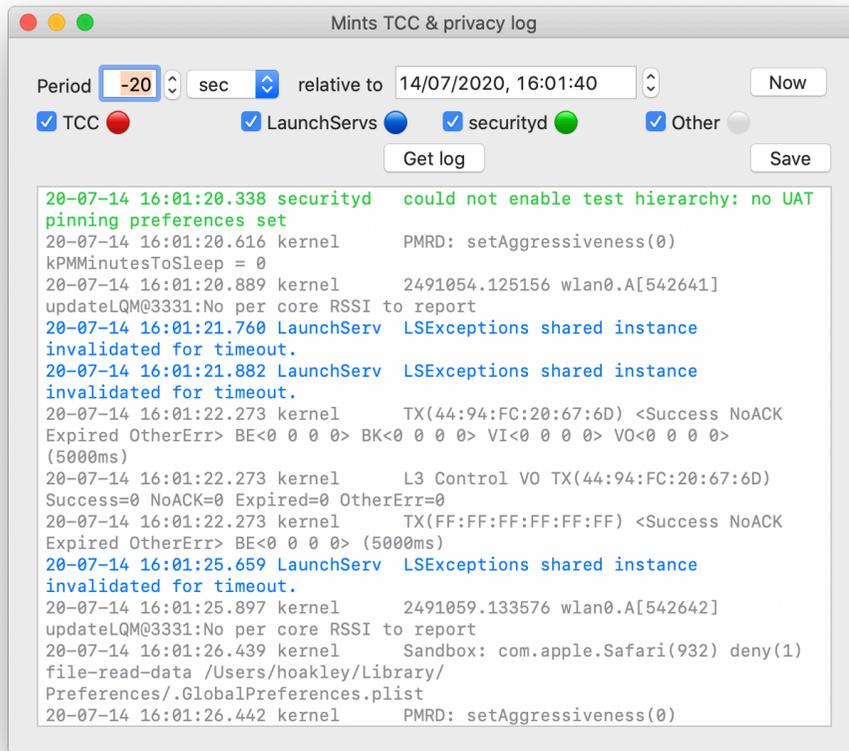
# iCloud log



The iCloud log extract shows entries from the three major sub-systems involved in iCloud transactions, and various related services and the kernel in the Other category. These are the same as shown in my free iCloud utility Cirrus.

→ [TCC log](#)

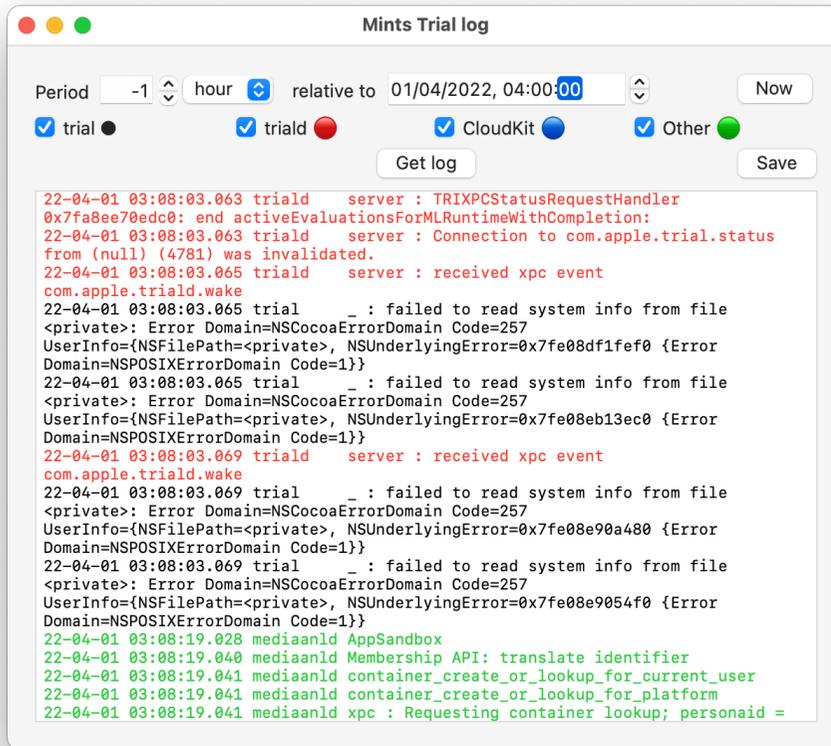
# TCC log



The TCC log extract shows entries from the three major sub-systems involved in controlling privacy and controlled access in Mojave and later. The Other category here includes additional services and the kernel. These are the same as shown in my free utility Taccy.

→ [Trial log](#)

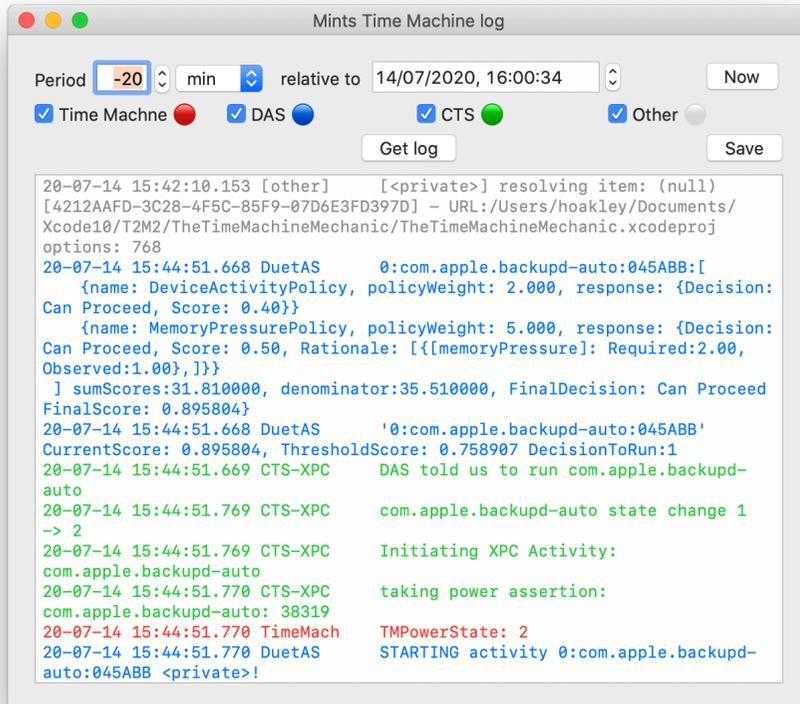
# Trial log



The Trial log extract shows entries from the major sub-systems involved in the new trial service in macOS Big Sur and Monterey. These include Signposts, and where given each entry starts with the category, in the form [category] : [entry body].

→ [Time Machine log](#)

# Time Machine log



The Time Machine log extract shows entries from the three major sub-systems involved in scheduling, despatching and making Time Machine backups. The Other category here shows related services, but doesn't include the kernel. Although based on the extracts analysed by my free utility The Time Machine Mechanic, these extracts are new for Mints.

[→ App Store log](#)

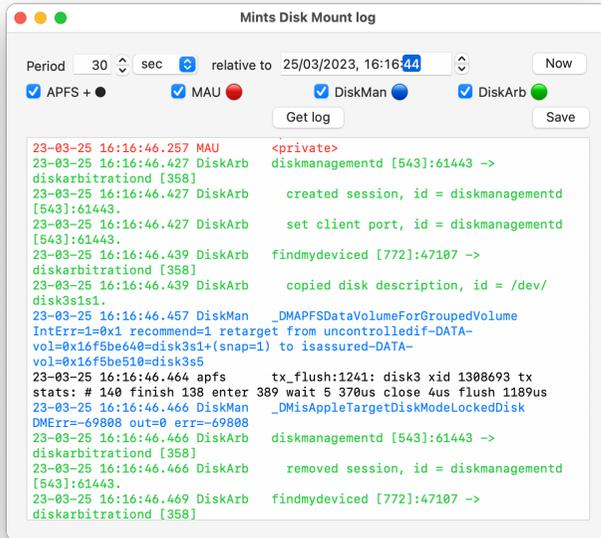
# App Store log

```
21-05-05 12:19:26.513 AppStore App Store bootstrap completed
21-05-05 12:19:26.515 AMS AMSAcknowledgePrivacyTask: [AC15E192] Determining if privacy acknowl
21-05-05 12:19:26.519 AMS AMSAcknowledgePrivacyTask: [AC15E192] Privacy acknowledgement is not
21-05-05 12:19:26.520 AMS AMSAcknowledgePrivacyTask: [AC15E192] Determining if privacy acknowl
21-05-05 12:19:26.523 AMS AMSAcknowledgePrivacyTask: [AC15E192] Privacy acknowledgement is not
21-05-05 12:19:26.523 AppStore Onboarding finished.
21-05-05 12:19:26.524 AMS AMSAcknowledgePrivacyTask: [AC15E192] Determining if privacy acknowl
21-05-05 12:19:26.525 AMS AMSAcknowledgePrivacyTask: [AC15E192] Privacy acknowledgement is not
21-05-05 12:19:26.526 AMS AMSAcknowledgePrivacyTask: [AC15E192] Determining if privacy acknowl
21-05-05 12:19:26.526 AMS AMSAcknowledgePrivacyTask: [AC15E192] Privacy acknowledgement is not
21-05-05 12:19:26.561 appstored [AppStoreKit.UpdateStore]: getUpdatesWithCompletionBlock
21-05-05 12:19:26.561 appstored [C56AD324] getUpdates requested for client: com.apple.AppStore
21-05-05 12:19:26.563 appstored [C56AD324] Returning 0 available and 14 recent update(s)
21-05-05 12:19:26.563 appstored [C56AD324] getUpdates completed successfully
21-05-05 12:19:26.565 appstored [AppStoreKit.UpdateStore]: refreshUpdateCountWithCompletionBlock
21-05-05 12:19:26.565 appstored [4DA2F90E] refreshUpdateCount requested for client: com.apple.AppSto
21-05-05 12:19:26.566 appstored [4DA2F90E] Current update count: 0 elapsedTime: 0.000146
21-05-05 12:19:26.566 appstored Leaving badge count at: 0 badgeValue: 0 reason: Client Refresh Count
21-05-05 12:19:26.566 appstored [4DA2F90E] Refresh update count returning count: 0
21-05-05 12:19:26.566 appstored [4DA2F90E] refreshUpdateCount completed successfully
21-05-05 12:19:26.580 appstored [1C178923] Completed with 179 result(s)
21-05-05 12:19:26.600 kernel Sandbox: 1 duplicate report for App Store deny(1) mach-lookup com.ap
21-05-05 12:19:26.600 kernel Sandbox: App Store(24415) deny(1) mach-lookup com.apple.remoted
21-05-05 12:19:26.603 kernel PMRD: setAggressiveness(0) kPMMinutesToSleep = 0
21-05-05 12:19:26.624 kernel Sandbox: App Store(24415) deny(1) mach-lookup com.apple.AddressBook.
21-05-05 12:19:26.630 kernel Sandbox: App Store(24415) deny(1) file-read-data /private/var/folder
21-05-05 12:19:26.631 AMS AMSURLSession: [3BDA5CF9] Task received response
```

The App Store log extract shows entries from the three major sub-systems involved in obtaining, downloading, installing and updating App Store apps. **AMS** is Apple Media Services, and the **Other** category here shows the kernel and other related services.

→ [Disk Mount log](#)

# Disk Mount log

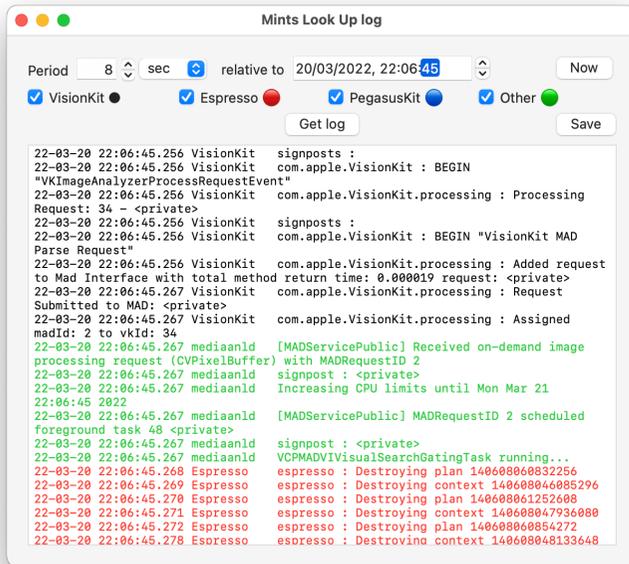


The Disk Mount log extract shows entries from processes involved in mounting APFS disks. **APFS +** shows entries from IOAccessoryManager (IOAccMan) and APFS, which bear the brunt of the work. Because they're seldom active at the same time, both processes are shown in the same category. **MAU** is MobileAccessoryUpdater, whose messages are normally given as `<private>` unless you remove privacy from the log. **DiskMan** is DiskManagement, and **DiskArb** is DiskArbitration and `diskarbitrationd`, which contain some important milestones.

This log extract is also valuable for studying APFS entries in the log more generally. As they usually come direct from the `apfs` process, they won't normally be found using a subsystem in a predicate.

→ [Visual Look Up log](#)

# Visual Look Up log



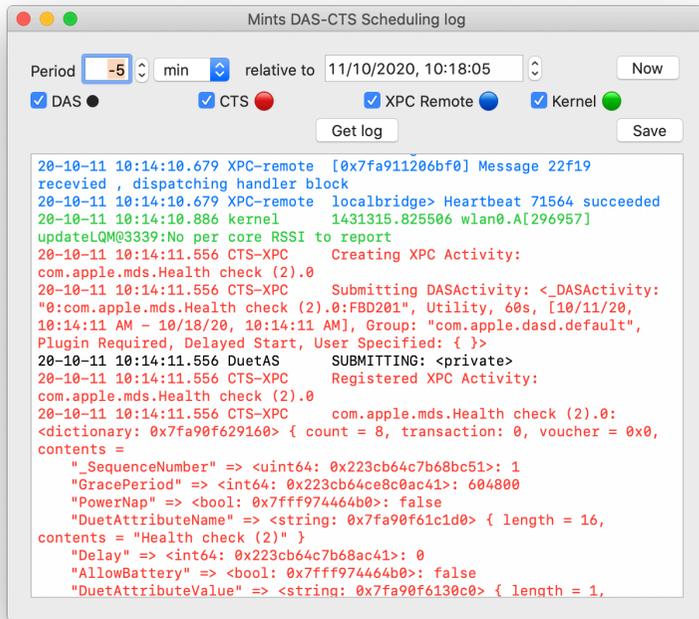
The Visual Look Up log extract shows entries from the major sub-systems involved in performing Visual Look Up for images in macOS Monterey. These include Signposts, and where given each entry starts with the category, in the form [category] : [entry body].

To save you from having to open another app to perform Visual Look Up, use that command in the Window menu to open a browser window within Mints.

→ [Visual Look Up window](#)

→ [DAS Scheduling log](#)

# DAS Scheduling log

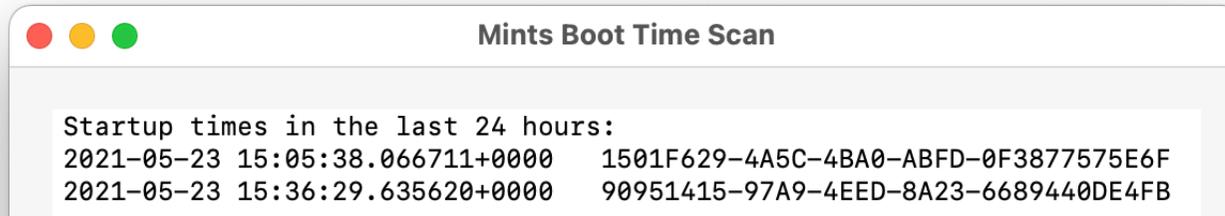


```
20-10-11 10:14:10.679 XPC-remote [0x7fa911206bf0] Message 22f19
received , dispatching handler block
20-10-11 10:14:10.679 XPC-remote localbridge> Heartbeat 71564 succeeded
20-10-11 10:14:10.886 kernel 1431315.825506 wlan0.A[296957]
updateLQM@3339:No per core RSSI to report
20-10-11 10:14:11.556 CTS-XPC Creating XPC Activity:
com.apple.mds.Health check (2).0
20-10-11 10:14:11.556 CTS-XPC Submitting DASActivity: <_DASActivity:
"0:com.apple.mds.Health check (2).0:FBD201", Utility, 60s, [10/11/20,
10:14:11 AM - 10/18/20, 10:14:11 AM], Group: "com.apple.das.default",
Plugin Required, Delayed Start, User Specified: { }>
20-10-11 10:14:11.556 DuetAS SUBMITTING: <private>
20-10-11 10:14:11.556 CTS-XPC Registered XPC Activity:
com.apple.mds.Health check (2).0
20-10-11 10:14:11.556 CTS-XPC com.apple.mds.Health check (2).0:
<dictionary: 0x7fa90f629160> { count = 8, transaction: 0, voucher = 0x0,
contents =
  "_SequenceNumber" => <uint64: 0x223cb64c7b68bc51>: 1
  "GracePeriod" => <int64: 0x223cb64ce8c0ac41>: 604800
  "PowerNap" => <bool: 0x7fff974464b0>: false
  "DuetAttributeName" => <string: 0x7fa90f61c1d0> { length = 16,
contents = "Health check (2)" }
  "Delay" => <int64: 0x223cb64c7b68ac41>: 0
  "AllowBattery" => <bool: 0x7fff974464b0>: false
  "DuetAttributeValue" => <string: 0x7fa90f6130c0> { length = 1,
```

The DAS scheduling log extract shows entries from the two major sub-systems involved in macOS background scheduling, which dispatch and execute tasks, **DAS** (Duet Activity Scheduler) and **CTS** (XPC, Centralized Task Scheduling). The **XPC Remote** category here shows entries for XPC External, and **Kernel** shows messages from the kernel.

Routine background tasks in macOS often use this system for their scheduling. DAS determines when they can be run, according to priorities and load, then calls on CTS to call them using XPC. This log extract lets you watch the dialog between DAS and CTS, supplemented by information about external XPC activity, and that of the kernel.

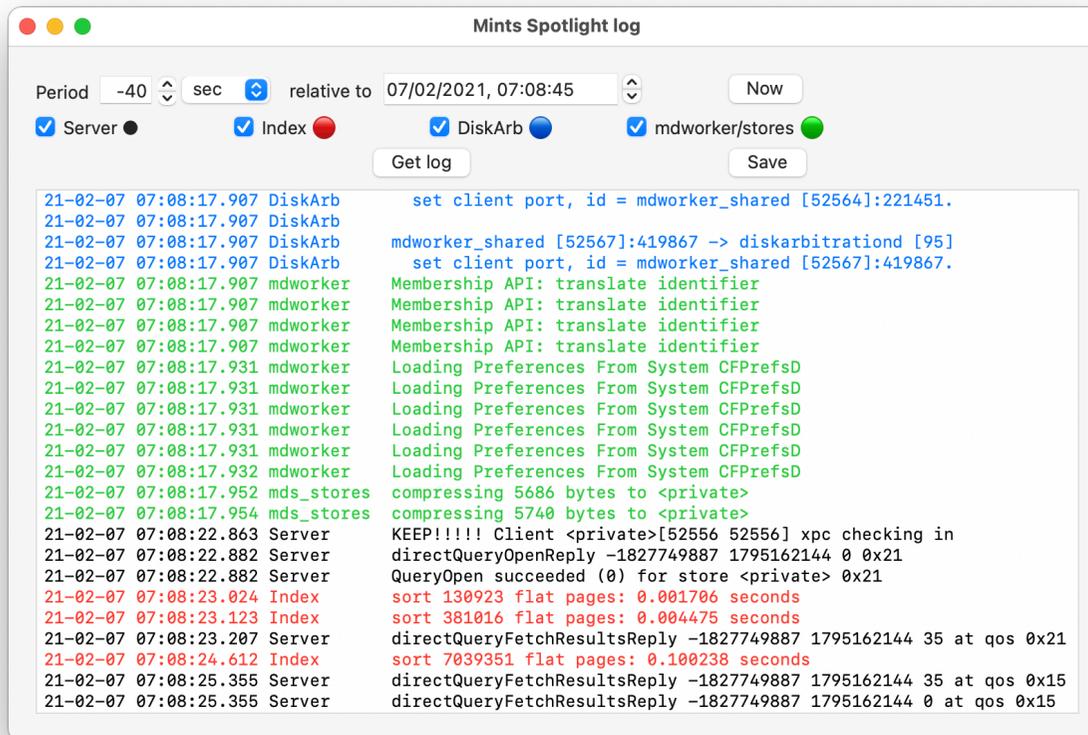
# Boot times



When you open the Boot window, Mints searches the last 24 hours of your Mac's unified log to identify each occasion on which it started up. This takes some time - typically at least a couple of minutes - during which a progress indicator spins. Once it has found all those times, it displays them in this window, giving the log time at which that boot started (note carefully the time zone correction provided), and the UUID for that boot. You can then use those in log browsers like Ulbow to discover the cause of any preceding kernel panic, etc.

→ [Unified log information](#)

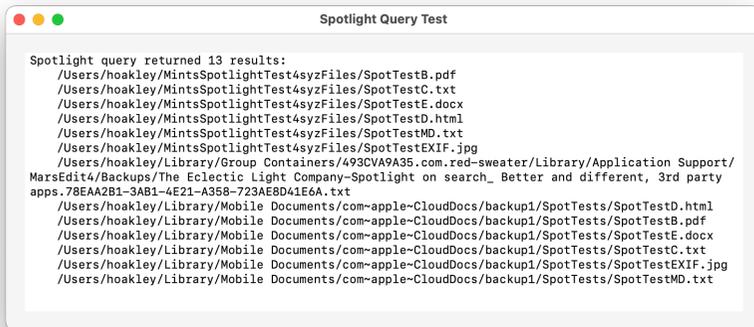
# Spotlight log



The Spotlight log extract shows entries from the three sub-systems involved in maintaining and accessing the Spotlight indexes: Spotlight Server, Index, and Disk Arbitration. The **mdworkers/stores** category here shows entries for `mdworker_shared` and `mds_stores`.

→ [Spotlight check and test](#)

# Spotlight check and test



```
Spotlight Query Test

Spotlight query returned 13 results:
/Users/hoakley/MintsSpotlightTest4syzFiles/SpotTestB.pdf
/Users/hoakley/MintsSpotlightTest4syzFiles/SpotTestC.txt
/Users/hoakley/MintsSpotlightTest4syzFiles/SpotTestE.docx
/Users/hoakley/MintsSpotlightTest4syzFiles/SpotTestD.html
/Users/hoakley/MintsSpotlightTest4syzFiles/SpotTestMD.txt
/Users/hoakley/MintsSpotlightTest4syzFiles/SpotTestEXIF.jpg
/Users/hoakley/Library/Group Containers/493CVA9A35.com.red-sweater/Library/Application Support/
MarsEdit4/Backups/The Eclectic Light Company-Spotlight on search_ Better and different, 3rd party
apps.78EAA2B1-3AB1-4E21-A358-723AE8D41E6A.txt
/Users/hoakley/Library/Mobile Documents/com-apple-CloudDocs/backup1/SpotTests/SpotTestD.html
/Users/hoakley/Library/Mobile Documents/com-apple-CloudDocs/backup1/SpotTests/SpotTestB.pdf
/Users/hoakley/Library/Mobile Documents/com-apple-CloudDocs/backup1/SpotTests/SpotTestE.docx
/Users/hoakley/Library/Mobile Documents/com-apple-CloudDocs/backup1/SpotTests/SpotTestC.txt
/Users/hoakley/Library/Mobile Documents/com-apple-CloudDocs/backup1/SpotTests/SpotTestEXIF.jpg
/Users/hoakley/Library/Mobile Documents/com-apple-CloudDocs/backup1/SpotTests/SpotTestMD.txt
```

Three buttons let you perform tests on Spotlight indexing and search, which are conveniently linked with inspecting its entries in the log.

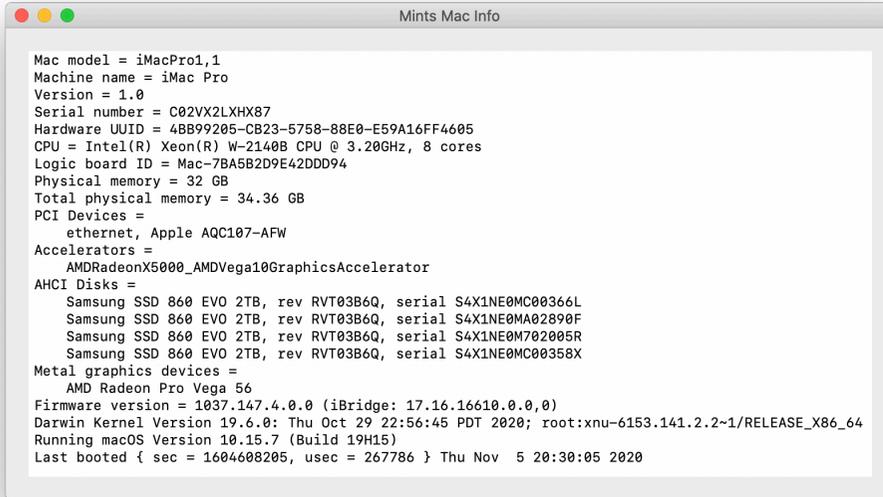
**Create Test** creates a new folder in your Home folder named `MintsSpotlightTest4syzFiles` to contain the test files. Mints then copies 9 files there for testing purposes. To delete that folder and its contents, use the **Delete Test** button.

**Check Search** performs a Spotlight search for the text `syzygy999` in files in the whole of your Home folder, including iCloud. It then opens a new window and displays the results, which should include the test files `SpotTestA.rtf` (Rich Text), `SpotTestB.pdf` (PDF), `SpotTestC.txt` (plain text), `SpotTestD.html` (HTML), `SpotTestE.docx` (Microsoft Word), `SpotTestF.numbers` (Numbers), `SpotTestG.pages` (Pages), `SpotTestEXIF.jpg` (EXIF metadata in JPEG), and `SpotTestMD.txt` (Keywords extended attribute). You can also add your own containing the search text to the folder. In addition to reporting which files were found, Mints also reports UTI and Spotlight Importer information for each test file in that folder, and gives the time taken to perform the search.

A standard check might start with **Create Test** at a clock time of, say, 01:00:00, followed by **Check Search** at 01:00:10. At 01:00:30 open the Spotlight log and set the period to -30 seconds to capture all entries since 01:00:00. When finished, clean up using **Delete Test** to delete the test folder and its entire contents, *including any custom files* you may have put there.

[→ Spotlight log](#)

# Get Mac Info

A screenshot of a macOS window titled "Mints Mac Info". The window contains a list of system information including Mac model, machine name, version, serial number, hardware UUID, CPU details, logic board ID, physical memory, PCI devices, accelerators, AHCI disks, metal graphics devices, firmware version, Darwin kernel version, macOS version, and the last boot time.

```
Mac model = iMacPro1,1
Machine name = iMac Pro
Version = 1.0
Serial number = C02VX2LXH87
Hardware UUID = 4BB99205-CB23-5758-88E0-E59A16FF4605
CPU = Intel(R) Xeon(R) W-2140B CPU @ 3.20GHz, 8 cores
Logic board ID = Mac-7BA5B2D9E42DDD94
Physical memory = 32 GB
Total physical memory = 34.36 GB
PCI Devices =
  ethernet, Apple AQC107-AFW
Accelerators =
  AMDRadeonX5000_AMDVega10GraphicsAccelerator
AHCI Disks =
  Samsung SSD 860 EVO 2TB, rev RVT03B6Q, serial S4X1NE0MC00366L
  Samsung SSD 860 EVO 2TB, rev RVT03B6Q, serial S4X1NE0MA02890F
  Samsung SSD 860 EVO 2TB, rev RVT03B6Q, serial S4X1NE0M702005R
  Samsung SSD 860 EVO 2TB, rev RVT03B6Q, serial S4X1NE0MC00358X
Metal graphics devices =
  AMD Radeon Pro Vega 56
Firmware version = 1037.147.4.0.0 (iBridge: 17.16.16610.0.0.0)
Darwin Kernel Version 19.6.0: Thu Oct 29 22:56:45 PDT 2020; root:xnu-6153.141.2.2~1/RELEASE_X86_64
Running macOS Version 10.15.7 (Build 19H15)
Last booted { sec = 1604608205, usec = 267786 } Thu Nov  5 20:30:05 2020
```

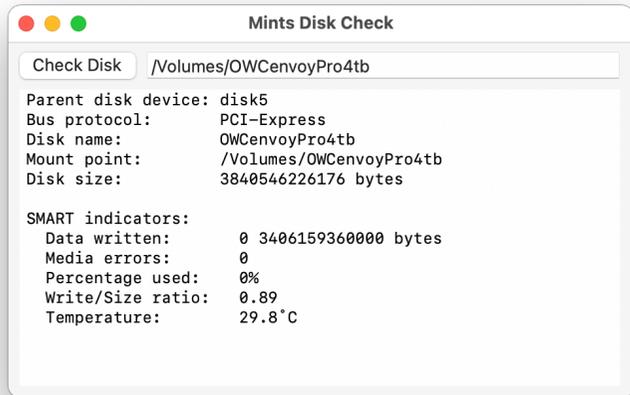
This window lists information about your Mac's hardware. This includes:

- the model designator, e.g. iMac17,1, machine name and version
- the serial number of that specific Mac, its hardware UUID
- the CPU type and details, and the ID for its logic board
- physical memory installed (two units), PCI devices (Ethernet card)
- graphics accelerators, AHCI disks, Metal graphics devices
- firmware version, kernel version, macOS version, and time of last boot.

Further items will be added to this list in the future.

Increase the size of the text used with `⌘+`; to reduce the size, press `⌘-`. Save the text to a text file using the **Save...** command in the **File** menu.

# Run a Disk Check



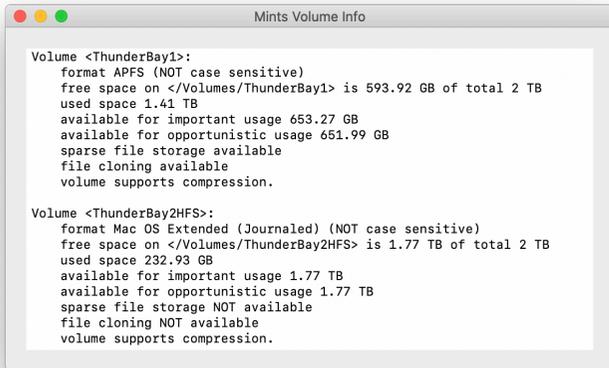
To run a check on any mounted SSD, click the **Check Disk** button and select the disk you want to check. Mints then calls `diskutil` for the information it can provide about that disk or container. The size given is normally for the whole disk, but may sometimes be the selected container size.

SSDs using Apple Fabric or PCI-Express (PCIe) buses over internal connections or Thunderbolt will normally provide SMART indicators, but those aren't available over USB, or through SATA interfaces. Those shown are:

- **Data written** gives the two standard byte counts, but only one is used to calculate the Write/Size ratio;
- **Media errors** are given as -1 when no value is returned;
- **Percentage used** is that of the manufacturer's expected life for the SSD; -1 is given when no value is returned;
- **Write/Size ratio** is the data written divided by the disk size; this rises with age, and typically should be able to exceed 600 before there's any danger of the SSD failing through an excess of erase cycles, and in some cases that may be significantly higher.
- **Temperature** given may not be reliable, as many need correction according to manufacturers' data.

For more reliable and extensive information, use a commercial product such as DriveDx.

# Get Volume Info



```
Mints Volume Info

Volume <ThunderBay1>:
format APFS (NOT case sensitive)
free space on </Volumes/ThunderBay1> is 593.92 GB of total 2 TB
used space 1.41 TB
available for important usage 653.27 GB
available for opportunistic usage 651.99 GB
sparse file storage available
file cloning available
volume supports compression.

Volume <ThunderBay2HFS>:
format Mac OS Extended (Journaled) (NOT case sensitive)
free space on </Volumes/ThunderBay2HFS> is 1.77 TB of total 2 TB
used space 232.93 GB
available for important usage 1.77 TB
available for opportunistic usage 1.77 TB
sparse file storage NOT available
file cloning NOT available
volume supports compression.
```

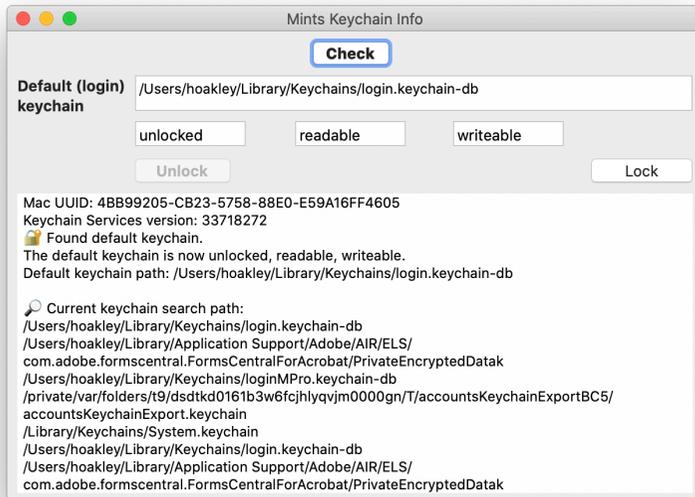
This window lists capacity information for all volumes currently mounted in the path `/Volumes`. This includes:

- volume name, format and case sensitivity
- total free space and total capacity
- the derived used space
- the amount of space available for ‘important’ and ‘opportunistic’ use
- whether sparse files, file cloning, and compression are supported.

On APFS volumes, this should include mounted snapshots, but doesn’t include the current Data volume in the startup Volume Group (as that isn’t mounted in `/Volumes`).

Increase the size of the text used with `⌘+`; to reduce the size, press `⌘-`. Save the text to a text file using the **Save...** command in the **File** menu.

# Get Keychain Info



This window has three simple button controls:

- **Check**, which runs its checks and updates the information in its text boxes;
- **Unlock**, which unlocks your default (login) keychain;
- **Lock**, which locks your default (login) keychain.

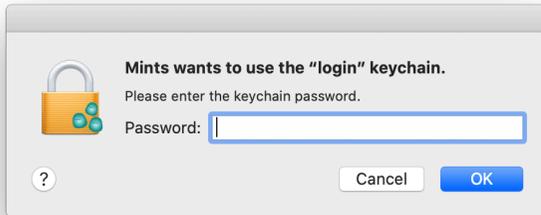
When you click on the **Check** button, Mints runs its full battery of tests, and completes the text boxes as shown below.

Displayed in the **Default (login) keychain** box is the full path to the keychain which macOS is using as your main user keychain at present. Even if you are using iCloud Keychain, this should be a path to the file named login.keychain-db in the Library/Keychains folder of your Home folder. If it isn't, then you need to establish why.

→ [Get Keychain Info](#) (concluded)

## Get Keychain Info (*concluded*)

Below that box are three smaller boxes, which tell you whether that default keychain is **locked**, **readable**, and **writable**. You can change two of those by clicking on the **Unlock** or **Lock** buttons nearby. When you click on **Unlock**, a dialog will appear requiring you to enter the password for your default keychain (which should be the same as your normal user login password) in order to unlock that keychain, although in Catalina that may only appear when you click on **Lock**.



The bottom scrolling box contains the hardware UUID number of your Mac, its version number of Keychain Services, all the information from the other boxes, and a lot more too.

You can save that to a text file using the **Save...** command in the **File** menu. You can also select, copy and paste any of the text, but cannot modify it within this app.

You can resize text in the lower scrolling window between 4 and 24 points using ⌘+ to enlarge and ⌘– to reduce the size.

→ [Keychain Details](#)

# Keychain Details

**Mac UUID:** this should correspond with the Hardware UUID given in System Information.

**Keychain Services version:** this should be 33718272 for all versions of macOS from 10.12 to 10.15.

**Default keychain path:** should be `/Users/[username]/Library/Keychains/login.keychain-db` where [username] is the short user name of the current user.

**Current keychain search path:** should include the default keychain and `/Library/Keychains/System.keychain`.

**Keychain system search path:** should include `/Library/Keychains/System.keychain`.

**Keychain common search path:** should include `/Library/Keychains/System.keychain`.

**Keychain dynamic search path:** most probably empty.

**Keychain user search path:** should include the default keychain.

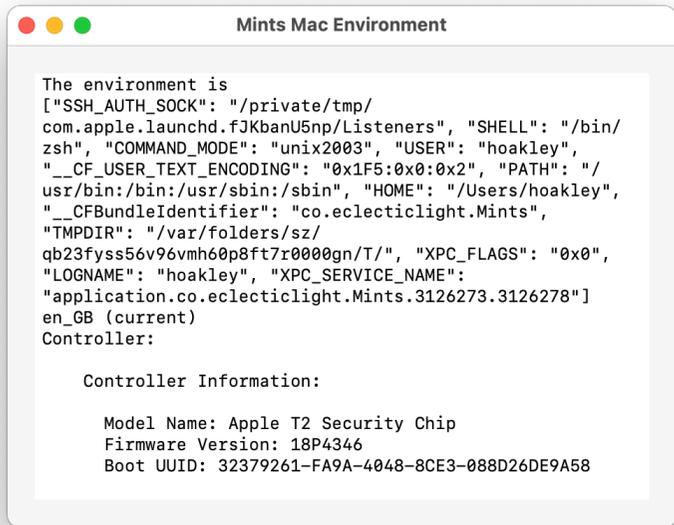
**Contents of `~/Library/Keychains`:** should include `login.keychain-db`, and is likely to include `metadata.keychain-db` too. For each file found, the date and time of last modification is given first, then that of the file's creation, then the size in bytes. The default keychain should not be empty.

**Contents of `~/Library/Keychains/[UUID]`:** this is the folder used for iCloud Keychain, or for the Local Items listed in Keychain Access. It may not exist, but if it does it should include `keychain-2.db` at least, and sometimes much more.

**Contents of `/Library/Keychains`:** should include `System.keychain`, and may well also include the Apple Push Services keychain `apsd.keychain`

**Contents of `/System/Library/Keychains`:** should include `SystemRootCertificates.keychain` and is likely to contain `EVRoots.plist`, `X509Anchors`, and `SystemTrustSettings.plist`.

# Get Environment Info



```
The environment is
["SSH_AUTH_SOCK": "/private/tmp/
com.apple.launchd.fJKbanU5np/Listeners", "SHELL": "/bin/
zsh", "COMMAND_MODE": "unix2003", "USER": "hoakley",
"__CF_USER_TEXT_ENCODING": "0x1F5:0x0:0x2", "PATH": "/
usr/bin:/bin:/usr/sbin:/sbin", "HOME": "/Users/hoakley",
"__CFBundleIdentifier": "co.electiclight.Mints",
"TMPDIR": "/var/folders/sz/
qb23fyss56v96vmh60p8ft7r0000gn/T/", "XPC_FLAGS": "0x0",
"LOGNAME": "hoakley", "XPC_SERVICE_NAME":
"application.co.electiclight.Mints.3126273.3126278"]
en_GB (current)
Controller:

Controller Information:

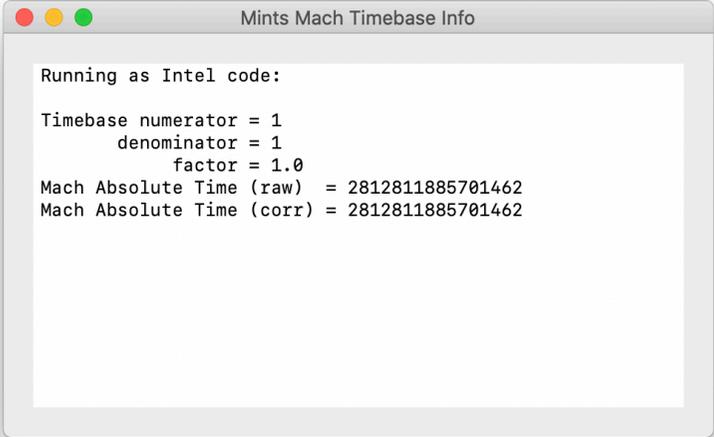
Model Name: Apple T2 Security Chip
Firmware Version: 18P4346
Boot UUID: 32379261-FA9A-4048-8CE3-088D26DE9A58
```

This window shows the process execution environment which processes launched by Mints would inherit. This is of particular interest to anyone experiencing problems which may be attributable to environment variables. Although the environment shown is that for Mints, it should be typical of most apps run. Of particular interest are the shell, text encoding and any localisation, and TMPDIR variables.

Following that, an assessment is made as to whether the current version of macOS has been patched to fix the serious vulnerability in the sudo command. This is omitted for more recent versions of macOS.

The Controller information given at the end is specific to the type of Mac, differing between non-T2 and T2 Intel systems, and M1 Macs.

# Mach Absolute Time

A screenshot of a macOS window titled "Mints Mach Timebase Info". The window has a standard macOS title bar with red, yellow, and green window control buttons. The content of the window is as follows:

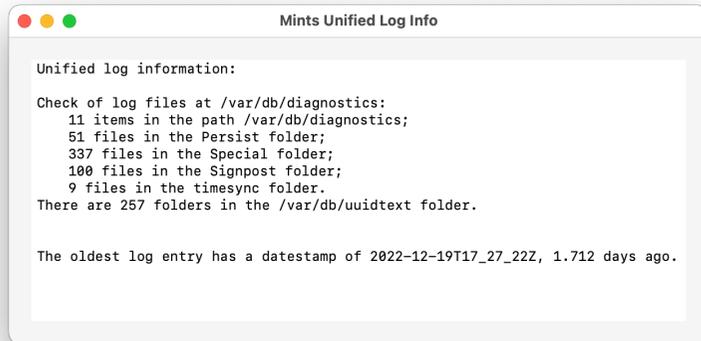
```
Running as Intel code:
Timebase numerator = 1
    denominator = 1
        factor = 1.0
Mach Absolute Time (raw) = 2812811885701462
Mach Absolute Time (corr) = 2812811885701462
```

This window displays conversion factors and other information about Mach Absolute Time, which differ between Intel and Apple Silicon hardware, and between Intel code running using Rosetta 2 and native ARM code on Apple Silicon systems.

This first line states which architecture the code was run on, then gives the two integers for the Mach timebase correction, and the correction factor; multiply raw time values by that to scale them from ticks to nanoseconds. Finally, it gives the current raw time, and that time after correction.

To discover the factors applied to Intel apps running in Rosetta 2 translation on an Apple Silicon Mac, force Mints to **Open using Rosetta** on that Mac.

# Unified log information



```
Mints Unified Log Info

Unified log information:

Check of log files at /var/db/diagnostics:
 11 items in the path /var/db/diagnostics;
 51 files in the Persist folder;
 337 files in the Special folder;
 100 files in the Signpost folder;
 9 files in the timesync folder.
There are 257 folders in the /var/db/uuidtext folder.

The oldest log entry has a datestamp of 2022-12-19T17_27_22Z, 1.712 days ago.
```

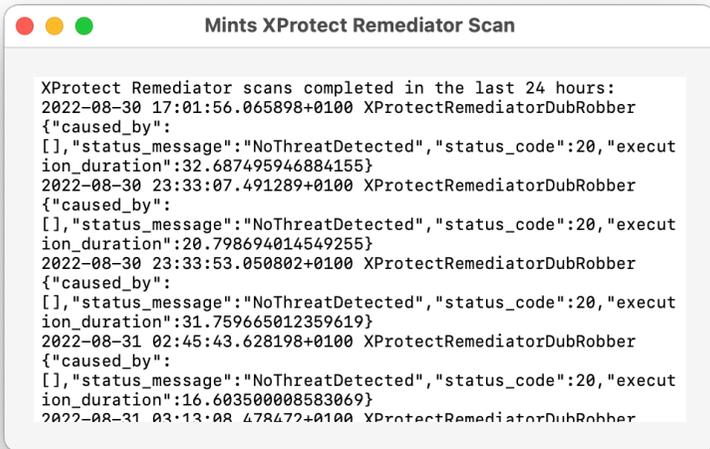
This window displays key information about the Unified log, including the contents and structure of the folders used to store the log. The main log contents are at `/var/db/diagnostics`, with UUID content in `/var/db/uuidtext`.

Within the main folder:

- **Persist** contains the main log files in tracev3 format, typically maintained to around 525 MB in more than 50 files;
- **Special** contains additional log files in tracev3 format. These are progressively weeded over time until they're eventually removed;
- **Signpost** contains signpost entries only;
- **timesync** contains time synchronisation data essential for datestamping of log entries;
- **HighVolume** is generally not used.

The datestamp of the first log entry in the oldest log file in the Persist folder is given, with the period currently covered by log entries from that time.

# XProtect Scans (Catalina and later)



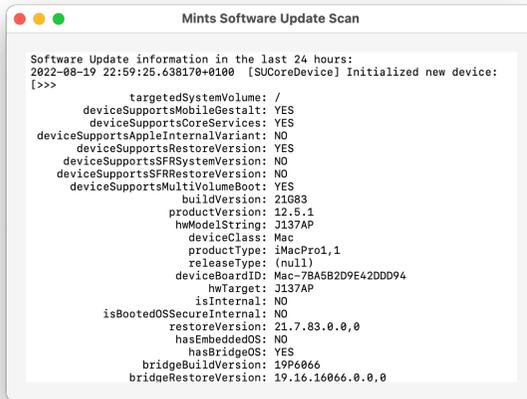
```
Mints XProtect Remediator Scan

XProtect Remediator scans completed in the last 24 hours:
2022-08-30 17:01:56.065898+0100 XProtectRemediatorDubRobber
{"caused_by":
[], "status_message": "NoThreatDetected", "status_code": 20, "execut
ion_duration": 32.687495946884155}
2022-08-30 23:33:07.491289+0100 XProtectRemediatorDubRobber
{"caused_by":
[], "status_message": "NoThreatDetected", "status_code": 20, "execut
ion_duration": 20.798694014549255}
2022-08-30 23:33:53.050802+0100 XProtectRemediatorDubRobber
{"caused_by":
[], "status_message": "NoThreatDetected", "status_code": 20, "execut
ion_duration": 31.759665012359619}
2022-08-31 02:45:43.628198+0100 XProtectRemediatorDubRobber
{"caused_by":
[], "status_message": "NoThreatDetected", "status_code": 20, "execut
ion_duration": 16.60350008583069}
2022-08-31 03:13:08.478477+0100 XProtectRemediatorDubRobber
```

This window lists all reports recorded in the Unified log over the last 24 hours from the new anti-malware scanners built into XProtect Remediator in macOS Catalina and later. Not all scans result in reports, but those that do should appear in this list. Each entry reports the date and time of the report, the scanning module involved, then the report exactly as it appears in the log. This may give a reason for that scan, then gives the result, and the time taken in seconds.

Further information about this new security feature is available on the Eclectic Light Company blog.

# Software Update



```
Mints Software Update Scan

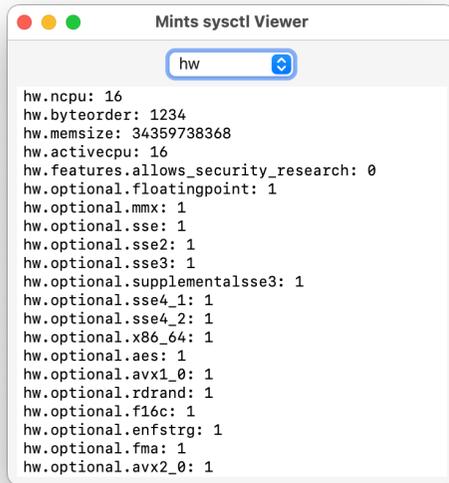
Software Update information in the last 24 hours:
2022-08-19 22:59:25.638179+0100 [SUCoreDevice] Initialized new device:
[>>>
    targetedSystemVolume: /
    deviceSupportsMobileGestalt: YES
    deviceSupportsCoreServices: YES
deviceSupportsAppleInternalVariant: NO
    deviceSupportsRestoreVersion: YES
    deviceSupportsSFRSystemVersion: NO
    deviceSupportsSFRRestoreVersion: NO
    deviceSupportsMultiVolumeBoot: YES
        buildVersion: 21683
        productVersion: 12.5.1
        hwModelString: J137AP
        deviceClass: Mac
        productType: iMacPro1,1
        releaseType: (null)
    deviceBoardID: Mac-7BA5B2D9E42DD094
        hwTarget: J137AP
        isInternal: NO
    isBootedOSSecureInternal: NO
        restoreVersion: 21.7.83.0.0,0
        hasEmbeddedOS: NO
        hasBridgeOS: YES
        bridgeBuildVersion: 19P6066
        bridgeRestoreVersion: 19.16.16066.0.0,0
```

This window displays the results of looking up details of firmware, T2 BridgeOS, Secure Firmware Restore (DFU mode), and fallback Recovery currently installed. This is obtained from a log entry made by one of the subsystems of Software Update. It works in Monterey and Ventura, most probably in Big Sur, and possibly older versions of macOS, and with Intel Macs with or without T2 chips, Apple silicon Macs, and macOS running in a virtual machine.

Note that the Recovery System referred to here *isn't* the paired Recovery volume which is part of the boot volume group in Monterey and later on Apple silicon Mac, and on all Intel Macs. On Apple silicon Macs running Big Sur, this is the primary Recovery, as in macOS 11 they don't have a paired Recovery volume. On Apple silicon Macs running Monterey and later, with is the fallback Recovery system installed on a hidden container on the internal SSD, and engaged by a double-press-and-hold of the Power button, instead of the normal Recovery system engaged by simply pressing and holding the Power button. Paired Recovery should match the main macOS version.

This is particularly useful when run after a macOS update, when it can show versions before and after the update has been installed.

# Sysctl Info

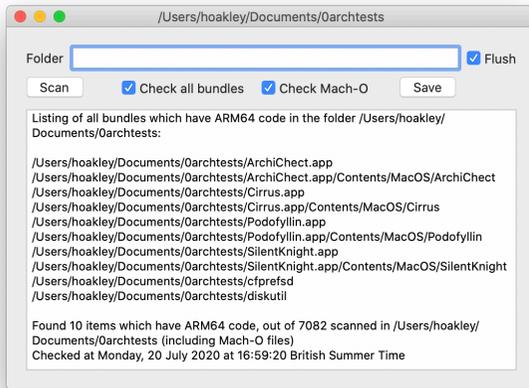


```
hw.ncpu: 16
hw.byteorder: 1234
hw.memsize: 34359738368
hw.activecpu: 16
hw.features.allows_security_research: 0
hw.optional.floatingpoint: 1
hw.optional.mmx: 1
hw.optional.sse: 1
hw.optional.sse2: 1
hw.optional.sse3: 1
hw.optional.supplementalsse3: 1
hw.optional.sse4_1: 1
hw.optional.sse4_2: 1
hw.optional.x86_64: 1
hw.optional.aes: 1
hw.optional.avx1_0: 1
hw.optional.rdrand: 1
hw.optional.f16c: 1
hw.optional.enfstrg: 1
hw.optional.fma: 1
hw.optional.avx2_0: 1
```

This window displays the output from the command tool `sysctl`, arranged by topic. This lists around a thousand different settings in the hardware and software of each Mac. These are named using a dot-based system, and to make it easier to locate those you're most interested in, there's a popup menu that selects which top-level category is displayed in the view below.

Detailed accounts of many of the entries are given in Apple's developer documentation, and in a page on the Eclectic Light blog. To make this accessible, there's a command in the **Help** menu **sysctl Information** that will open the page in your default browser.

# Universal binary checker (Mojave and later)



Before scanning for Universal software, decide whether you just want apps scanned, or whether you want all code-containing bundles scanned. To scan apps only, leave the checkbox labelled **Check all bundles** unchecked; to scan all bundles, ensure it is ticked (the default).

Next, decide whether you want all executable (Mach-O) code files scanned too. These include dynamic libraries (dylibs), command tools, and other code which is not delivered in a bundle. To scan all executable code, ensure that the checkbox labelled **Check Mach-O** is ticked (the default); for a basic scan, leave that checkbox unchecked. Scanning all bundles and all Mach-O files will take significantly longer.

Then decide which folder you wish to scan. You can select that in either of two ways:

- leave the **Folder** text box empty, and click on the **Scan** button. You will then be prompted to select the folder using the normal Open File dialog;
- enter a standard path into the **Folder** text box. You can use the standard shortcut of ~ to indicate your Home folder. Once you have entered the path, click on the **Scan** button to start the scan. If the **Flush** checkbox is ticked when you do this, the path in the **Folder** text box will be cleared when the scan starts; if you uncheck the **Flush** checkbox, your path will be left for you to edit it for the next scan.

→ [Universal binary checker](#) (concluded)

## Universal binary checker *(concluded)*

Scanning takes time. If you put the root path / in the **Folder** text box, this can take many minutes, even an hour or so. You may wish to scan top-level folders like /Applications one at a time rather than attempting to scan your entire Mac. During this period, the window shows a busy ‘spinner’ next to the **Scan** button, and you can work normally with other apps. Give the app time to complete its scan, and once complete it will display the results.

Scanning takes plenty of memory. Because of the deep traversal which it uses, Mints consumes memory by the GB in order to check every nook and cranny in the folder it is scanning. This should work fine with virtual memory, though. Again, you can reduce this by performing scans on smaller folders.

When a scan is complete, the title of the window will change to show the folder which has just been scanned. Change the size of the text in the output using ⌘+ to make it larger, to a maximum of 60 points, or ⌘– to make it smaller, to a minimum of 4 points.

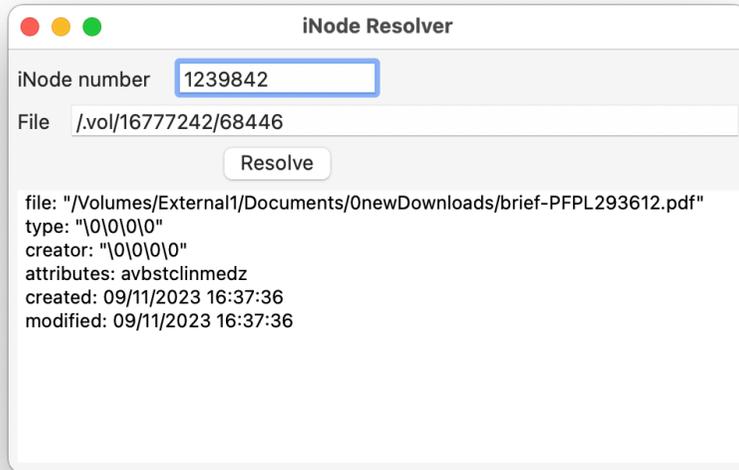
To save the results of a scan as a text file, click on the **Save** button, or use the **Save...** command in the **File** menu. You will then be prompted to select the name of the text file.

The scanner performs a deep traversal of the chosen folder, using `Bundle.executableArchitectures` to list executable architectures for each bundle. To check for Mach-O code files, it first inspects the ‘magic’ initial four bytes of every file. If it finds that they are `0xfeedface`, it then directly inspects the subsequent Fat Architecture slices to check whether the supported architectures include ARM64.

# Window menu: Visual Look Up window

To test or investigate Visual Look Up, in addition to the log window provided by Mints, you'll need to perform Visual Look Ups. This is made easy by opening this browser window within this app. It automatically opens a special test page on the Eclectic Light Company blog, containing various images for you to use in your tests. This is a normal browser window, so can be used to navigate anywhere else, although it doesn't support bookmarks, manual entry of URLs, or other conveniences.

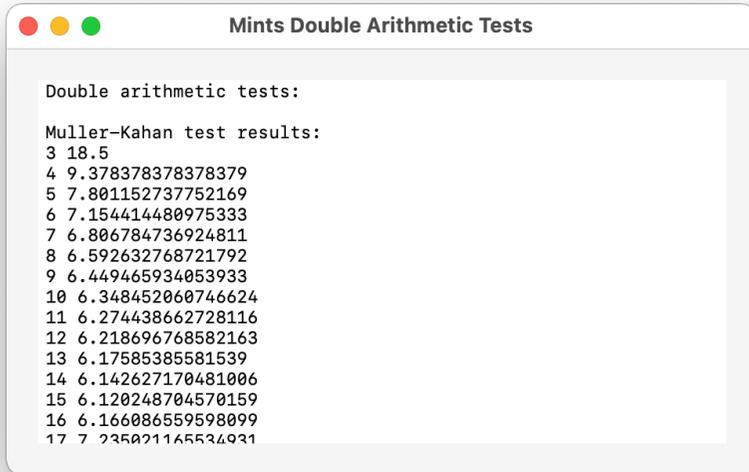
## Data... menu: Inode



This resolves inode numbers given in a volfs path to a regular file path, primarily to help you interpret APFS errors. It requires you to drag and drop a file from the *same* APFS volume onto its view. It then displays the volfs path for that file in the **File** text box.

To resolve the regular file path, paste its **Inode number** in the text box above, then click on the **Resolve** button. A few seconds later it then displays the file path and other information in the scrolling text view below, using the command `GetFileInfo`. If you don't enter an inode number, it resolves the path for the file that you dropped onto its view. Attributes shown are explained in `man GetFileInfo`.

## Data... menu: Double



```
Mints Double Arithmetic Tests

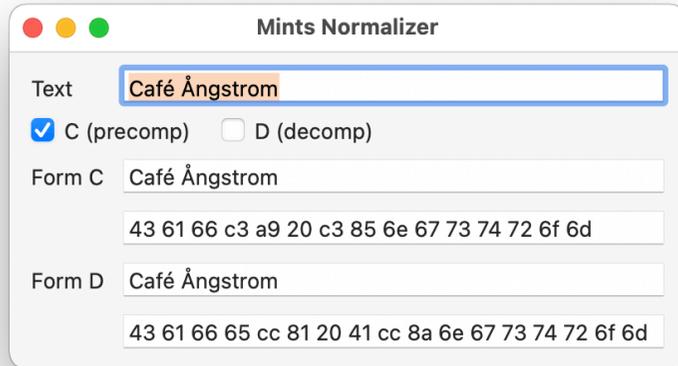
Double arithmetic tests:

Muller-Kahan test results:
3 18.5
4 9.378378378378379
5 7.801152737752169
6 7.154414480975333
7 6.806784736924811
8 6.592632768721792
9 6.449465934053933
10 6.348452060746624
11 6.274438662728116
12 6.218696768582163
13 6.17585385581539
14 6.142627170481006
15 6.120248704570159
16 6.166086559598099
17 7 235021165534031
```

This suite of tests looks at floating point arithmetic using the standard Swift type **Double**. These include the results of ‘difficult’ tests which normally generate inaccurate results, including the Muller-Kahan test, the Chaotic Bank, and the Rump test. For each, the standard result generated by modern Intel processors is given. The final group of tests demonstrates how calculating in different orders can induce numeric errors.

→ [Floating Point Explorer](#)

## Data... menu: Normalizer

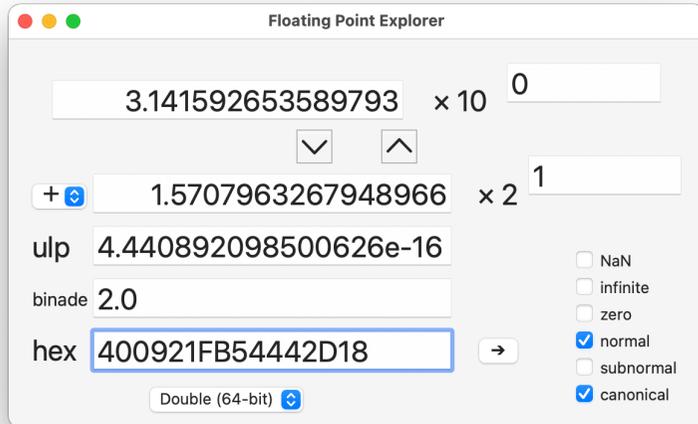


The Mints Normalizer window helps you address problems with normalization forms in Unicode text, most particularly in file paths and names. Paste (or type) the text into the top text box and press Tab or Return. Mints then shows whether the text complies with Unicode Normalized Form C ('precomposed') and/or D ('decomposed'). Following that, it gives the Form C normalized form of that text, both in characters and in UTF-8, and the same for the Form D normalized form.

To use this to normalize Unicode text, for example, to Form D for use with a Mac file system, paste the text into the top box, and copy the text shown in the Form D box below.

More extensive information about normalization is available in my free app Apfelstrudel.

# Floating Point Explorer



This window helps you work with IEEE 754 32- and 64-bit floating-point numbers. Enter any number in one of three formats:

- **Radix 10**, expressed as *significand* × 10<sup>*index*</sup>, such as 1.234 × 10<sup>2</sup> representing 123.4, in the upper row, then click on the **down** button or press the down cursor key to see it below using a radix of 2 as represented internally, and in hexadecimal at the foot.
- **Radix 2**, expressed as *significand* × 2<sup>*index*</sup>, such as 1.5 × 2<sup>2</sup> representing 6.0, in the middle row, then click on the **up** button or press the up cursor key to convert it to radix 10 in the row above, and in hexadecimal at the foot.
- **Hexadecimal**, packed in 4 or 8 bytes according to standard single and double formats, then click the **→ right** button on the right of the hex box or press the right cursor key to convert it to both radix 10 and 2 formats above.

→ [Floating Point Explorer](#) (concluded)

## Floating Point Explorer *(concluded)*

To help you convert hex formats, you can include white space to make them easier to enter and read, e.g. 4009 21FB 5444 2D18. That will be stripped when the hex is converted. Hex values are also automatically padded with zeros at the left, to the expected number of bytes according to the length of its hex representation.

In addition to showing those three formats of numbers, the window also displays the ulp, binade, and checkboxes identify special representations, such as NaN (not a number), infinities, zeros, and whether the number is normal or subnormal. Terms used comply with IEEE 754:

- **ulp** is the unit of the least significant digit in this value's significand; for most, this is the difference between that number and the next greater representable number.
- **binade** is the number with the same index, but with a unit significand.

Switch number format between 32-bit single-precision and 64-bit double using the popup menu at the foot of the window, following which conversions will be made into the format you set.

# Updates

Whenever you open Mints, it may check to see if an update is available. This *doesn't* use the popular Sparkle mechanism for updating in place, but works as detailed here.

Once Mints has successfully completed its integrity check, it checks whether update checking has been turned off in its preferences file. If that has, it abandons any attempt to check for updates. If checking is allowed, it then checks when it last checked for updates. If that was more than 12 hours ago, it continues to perform the check. It then connects to my GitHub server, from where it downloads a list of current versions of my apps. It doesn't upload any data to the GitHub server at all, and no statistics beyond GitHub normal connection figures are collected either: no personal identifiers are recorded. If there is an update available, Mints then checks that its location is on this WordPress blog, and posts a dialog which invites you to download the update.

If you click on the **Download** button, it then points your default browser at that update, which should trigger the update to be downloaded to your normal downloads folder. The update is received as a regular Zip archive, and is exactly the same as you would download from the Downloads page here. It also carries a quarantine flag, so that when you unZip it and install the app inside, it undergoes normal first run 'Gatekeeper' security checks. If you click on the **Ignore** button, Mints won't remind you about it again for another 12 hours.

An additional item at the end of the **Help** menu explains the update status. If no update check is performed, or the check fails, the last item reads **Update not checked**. If the check is performed and update information is obtained, even when no update is available or you decline to download it, that menu item reads **Checked for update** and is ticked (but still disabled).

You can customise this behaviour by changing Mint's preferences. The keys to use are:

- `noUpdateCheck`, a Boolean. When set to `true`, this disables all update checking. Default is `false`.
- `updateCheckInt`, a real number (Double). When set to a value greater than 1.0, the minimum time interval between checks, in seconds. Default is 43200, which is 12 hours. If you set it to any value less than 1, Ulbow will reset it automatically to that default.

To change either of these, use a Terminal command of the form

```
defaults write co.electiclight.Mints updateCheckInt '10'
```

which works properly through the preferences server `cfprefsd`.

# Further Information

The monospace font using in versions of macOS up to and including Mojave is `monospacedDigitSystemFont`; that used in Catalina and Big Sur is `monospacedSystemFont`, which is unfortunately not available in earlier versions of macOS. Both are used in their regular weight.

Predicates used to obtain log extracts include:

- `subsystem == "com.apple.clouddocs" OR subsystem == "com.apple.cloudkit" OR subsystem == "com.apple.mmcs" OR processImagePath CONTAINS[c] "cloud" OR processImagePath CONTAINS[c] "bird" OR processID = 0 (for iCloud in macOS 13 and earlier)`
- `subsystem == "com.apple.FileProvider" OR subsystem == "com.apple.cloudkit" OR subsystem == "com.apple.mmcs" OR processImagePath CONTAINS[c] "cloud" OR processImagePath CONTAINS[c] "bird" OR processID = 0 (for iCloud in macOS 14)`
- `subsystem == "com.apple.TCC" OR subsystem == "com.apple.launchservices" OR subsystem == "com.apple.securityd" OR subsystem == "com.apple.sandbox" OR processImagePath CONTAINS[c] "tccd" OR processImagePath CONTAINS[c] "sandboxd" OR processID = 0 (for TCC)`
- `subsystem == "com.apple.TimeMachine" OR (subsystem == "com.apple.duetactivityscheduler" AND eventMessage CONTAINS[c] "Rescoring all") OR (subsystem == "com.apple.xpc.activity" AND eventMessage CONTAINS[c] "com.apple.backupd-auto") OR eventMessage CONTAINS[c] "backup" OR eventMessage CONTAINS[c] "Time Machine" OR eventMessage CONTAINS[c] "TimeMachine" (for Time Machine)`
- `subsystem == "com.apple.duetactivityscheduler" OR subsystem CONTAINS "com.apple.xpc" OR processID = 0 (for DAS scheduling)`
- `subsystem == "com.apple.spotlightserver" OR subsystem CONTAINS "com.apple.spotlightindex" OR subsystem CONTAINS "com.apple.DiskArbitration.diskarbitrationd" OR processImagePath CONTAINS[c] "mdworker_shared" OR processImagePath CONTAINS[c] "mds_stores" (for Spotlight)`

- `subsystem == "com.apple.AppStore" OR subsystem == "com.apple.AppleMediaServices" OR subsystem == "com.apple.appstored" OR subsystem == "com.apple.JetEngine" OR processID = 0 (for the App Store)`
- `subsystem CONTAINS[c] "com.apple.diskmanagement" OR subsystem CONTAINS[c] "com.apple.mobileaccessoryupdater" OR subsystem CONTAINS[c] "com.apple.DiskArbitration.diskarbitrationd" OR senderImagePath CONTAINS[c] "IOAccessoryManager" OR senderImagePath CONTAINS[c] "apfs" (for Disk Mount)`
- `subsystem == "com.apple.VisionKit" OR subsystem == "com.apple.espresso" OR subsystem == "com.apple.siri.argos" OR subsystem == "com.apple.mediaanalysis" OR subsystem == "com.apple.CoreRecognition" OR subsystem == "com.apple.trial" OR subsystem == "com.apple.pegasuskit" OR subsystem == "com.apple.coreml" OR processImagePath CONTAINS[c] "mediaanalysisd" (for Look Up)`
- `subsystem == "com.apple.trial" OR subsystem == "com.apple.triald" OR subsystem == "com.apple.cloudkit" OR processImagePath CONTAINS[c] "triald" OR processImagePath CONTAINS[c] "mediaanalysisd" (for Trial)`
- `subsystem == "com.apple.SoftwareUpdateMacController" AND eventMessage CONTAINS[c] "Initialized new device:" (for Software Update)`
- `subsystem == "com.apple.XProtectFramework.PluginAPI" AND category == "XPEvent.structured" (for XProtect scans).`

The log show command used for Trial and Look Up includes the return of Signposts, and log contents have the category field prefixed, as extensive use is made of categories in log entries for these sub-systems.

Extensive information about Mints and the unified log is available from the [Eclectic Light Company blog](#), and the [product page](#) in particular. That can be accessed through the **Mints Support** command in the **Help** menu too.

# Change list

1.19:

- replaced CloudDocs with FileProvider in iCloud log extracts, when running in macOS Sonoma.

1.18:

- added hex support to the Floating Point Explorer.

1.17:

- fixes a bug in the information about sudo vulnerabilities
- added Floating Point Explorer.

1.16:

- added sysctl Information.

1.15:

- added inode resolution to the Data menu.

1.14:

- fixes a crashing bug in Disk Check if an unmounted volume is selected
- updates xattr handling to remove deprecations.

1.13:

- fixes a crashing bug in Disk Check if a network or non-local volume is selected.

1.12:

- added Disk Check feature.

1.11:

- added Disk Mount log access.

1.10:

- added Unified log information
- removed app integrity checking.

1.9:

- added XProtect Remediator scan feature.

1.8:

- added Software Update feature.

1.7:

- added Trial log access.

1.6:

- added Look Up log access
- added Visual Look Up browser window
- built for 12.3 and earlier using Xcode 13.3.

- 1.5:
  - added Boot feature to discover boot times
  - added Unicode Normalizer to Data menu
  - improved Spotlight search test window handling
  - added QoS where relevant.
- 1.4:
  - added App Store log access
  - added Window/Data... menu with a single window for Doubles.
- 1.3:
  - improved opening log checks to detect time formatting errors.
  - refactored the display of log entries to reduce memory requirements and increase performance.
  - brought all time formatting into line with latest changes in macOS 11.
- 1.2:
  - added opening log checks to protect against macOS bugs.
- 1.1:
  - added busy spinner and search timing to Spotlight test
  - added sudo test to the Environment feature.
- 1.0:
  - additional files for Spotlight test
  - added mdimporter info for Spotlight test
  - first full release.
- 1.0b11:
  - added Environment info window
  - added Spotlight section, complete with test files
  - laid out main window more systematically.
- 1.0b10:
  - added many new items to the Mac Info feature, with support for Apple Silicon Macs too.
- 1.0b9:
  - added DAS Scheduling log browser
  - revised Volume Info and corrected its coverage and information
  - fixed a bug in Mac Info which resulted in crashing if that Mac's logic board had no serial number.
- 1.0b8:
  - added Mac Info feature
- 1.0b7:
  - added Volume Info feature
  - added Keychain Info feature
  - added support for saving via menu command to main windows.
- 1.0b6:
  - added Mach Absolute Time feature
  - minor tweaks to the interface.
- 1.0b5:
  - changed algorithm used by Universal Binary Checker to stop using lipo
  - Universal App for for Intel and Apple Silicon Macs.
- 1.0b4:
  - changed standard log text colours to black/white, red, blue, green
  - added Universal Binary Checker for 10.14 and above.
- 1.0b3:
  - tried to fix further bug opening log windows in Sierra.
- 1.0b2:
  - fixed weird bugs in the log window nib.
- 1.0b1:
  - first beta release, with iCloud, TCC and Time Machine log browsers.

28 February 2024.