Start

Scrub helps protect the privacy of sensitive documents and other files, by removing data and metadata which may leak their contents. Those include:
- **extended attributes**, which can reveal where a document was downloaded from and when, among other things,
- **versions**, which can reveal previous versions with content which has since been removed or changed,
- **QuickLook previews**, which can show documents stored on an encrypted volume without the protection of that encryption *(not in Mojave or later)*,
- **Spotlight metadata**, containing keywords and other indexed content,
- file creation and modification dates.

For example, you might use an external encrypted disk to store and work on documents containing very sensitive information. You could use Scrub to remove old versions from those, empty and disable QuickLook's caches, and disable Spotlight indexing on that volume.

⚠️ Scrub is not intended for the novice, nor for those who don't understand the consequences of its powerful features. Used inappropriately, it can and will destroy data which you may be unable to recover or replace. But used wisely, it can ensure that sensitive files don't give anything away. For some users, such as journalists, it should provide valuable protection to documents which you really don't want others to access.

Scrub is no substitute for storing sensitive files on a securely encrypted disk. It is intended to enhance the protection of files which are already themselves stored securely.

➔ Audit   ➔ Scrub   ➔ Warnings   ➔ Tips & Tricks   ➔ Updates & Change list

Audit

To open a file, folder or volume:
- use the **Open** command in the **File** menu to select it
- click on the **Open** button in any Scrub window
- drag and drop that file/folder/volume onto Scrub's icon in the Finder or Dock.
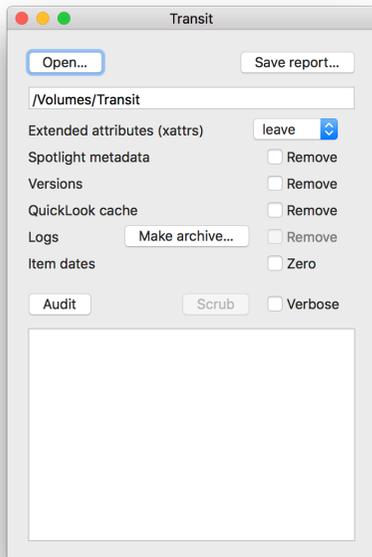
Before you can Scrub a file/folder/volume you must check it by clicking the **Audit** button. This examines all the items in the file/folder/volume, reports how many have extended attributes and versions, and lets you make an informed decision as to what you wish to Scrub.

➔ [Audit report](#)　　➔ [Scrub](#)　　➔ [Warnings](#)

The Eclectic Light Company blog – https://eclecticlight.co

Audit report

The audit reports the state of QuickLook caching, the number of files found with old versions, the number of files found with xattrs, and any items found in the following list of types (UTIs):

- com.apple.application-bundle – these are apps
- com.apple.installer-package-archive – these are installer packages
- com.apple.generic-bundle – these are folders posing as files
- com.apple.aperture.library
- com.apple.migratedaplibrary
- com.apple.migratedphotolibrary
- com.apple.photos.library
- com.apple.garageband.project
- com.apple.itunes.ipa
- com.apple.imovielibrary
- com.apple.imovieevent
- com.apple.finalcutprolibrary
- com.apple.finalcutproevent

Items which are reported as having one of those UTI types are those which are most liable to damage by removing xattrs, changing the date of creation, etc.

Scrub
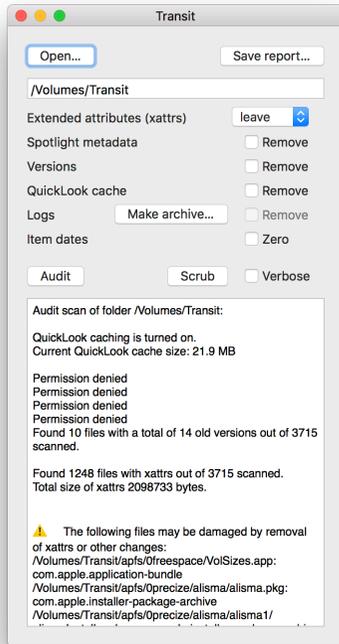
Once you have run an audit on the file/folder/volume, decide which data to remove.

➜ [Warnings](#) ➜ [Extended attributes](#) ➜ [Spotlight metadata](#) ➜ [Versions](#) ➜ [QuickLook cache](#) ➜ [Logs](#) ➜ [Tips & Tricks](#)

Item dates changes the creation and last modification dates for the file, or all items in the folder/volume, to 01:00 on 1 January 1970.

The **Verbose** checkbox gives full details of what has changed in the scrolling box below. To save the contents of the scrolling box at the bottom of the window to a text file, click on the **Save report** button.

Warnings

⚠️ None of Scrub's actions has any **Undo** available. Once xattrs, versions, and other information have been removed, they have gone for good. You should therefore ensure that you only use these options on files for which you have good, recent backups which retain all the data and metadata. For example, to preserve versions, use my free DeepTools to make a copy of the document with all its versions preserved.

⚠️ Scrub includes features which can render files unusable when used inappropriately. If you are unsure as to whether you should be using it, please don't until you fully understand its use, and its potential effects and side-effects.

⚠️ Scrub isn't intended for use on cloud storage such as iCloud Drive. The results of using it on any remote storage are unpredictable, and could damage files stored there.

⛔ **Never run Scrub on special folders such as Library or Applications**, even in your Home folder. Files in those folders may rely on xattrs, accurate file dates, and the like, to function normally. One quick Scrub could lead to lasting problems.

➜ [Audit](#)   ➜ [Scrub](#)

Extended attributes (xattrs)

These are stored on the same volume as the file, and can contain potentially revealing information about where a file was downloaded from, when, and using which app. Xattrs are also used to store all sorts of other information which can be retrieved using the right tools.
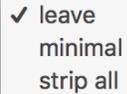
✓ leave
minimal
strip all

There are three options for removal of xattrs, selected in the popup menu:
- **leave** doesn't remove any xattrs, and leaves them all intact. This is the safest option in terms of compatibility, but may leave metadata available;
- **minimal** removes all xattrs apart from the following, which have significant value to macOS and some apps:
  - com.apple.LaunchServices.OpenWith
  - com.apple.metadata:com_apple_backup_excludeItem
  - com.apple.quarantine
  - com.apple.ResourceFork
  - com.apple.TextEncoding

- **strip all** removes all xattrs including those listed above. ⚠️ You should only use this if you are certain that it will not affect the security or usability of the files. It *cannot* strip com.apple.macl xattrs in 10.15 or 11.0, as those are protected by SIP.

➜ [Scrub](#)   ➜ [Spotlight metadata](#)

Spotlight metadata

These are indexes built to support Spotlight search, and contain words and other data extracted from files. They are stored on the same volume as the file, and can be used to indicate content. This item is only enabled when you are examining a file/folder/volume on a volume other than the startup volume (mounted in a macOS /Volumes mount point rather than in a path directly from the startup or root volume /). This is to ensure that you do not inadvertently disable Spotlight on your startup volume. Removing these indexes will prevent Spotlight from searching that entire volume, including all other files and folders.

If you opt to remove Spotlight metadata, you will be asked to authenticate with your admin password twice, in order for Scrub to perform the two commands needed to do this.

Spotlight is disabled using the commands
```
sudo mdutil -i off mountPoint
sudo mdutil -E mountpoint
```
It can be re-enabled using the command
```
sudo mdutil -i on mountPoint
```

➜ [Scrub](#)   ➜ [Versions](#)

Versions

These are automatically made and stored when you save a document in apps which support the macOS version system. Those versions are stored on the same volume as the file, and can be accessed to discover all previous versions of a document and its contents. They are valuable when you are actively working with a document, but also can reveal sensitive information which may have been included in a previous version of that document. Removing old versions doesn't affect the current version of that document, nor any Time Machine backups of it.

Removal of old versions is performed using the function `NSFileVersion.removeOtherVersionsOfItem(at: URL)`

➔ [Scrub](#)   ➔ [QuickLook cache](#)

QuickLook cache

This contains thumbnails and previews for display by QuickLook. Unusually, there is only one active cache, which is stored in a hidden folder on your startup volume. Even when you view documents on encrypted volumes, their thumbnails and previews will be stored here, and could easily leak sensitive data. Removing this cache makes thumbnails and previews slower to be displayed, as they have to be generated every time they are used, but it should prevent leakage of sensitive content. It applies to all volumes, not just the one containing the sensitive documents.

⚠️ Mojave and later protect the QuickLook Cache from prying eyes by turning it into a DataVault. Attempts to obtain information about that DataVault or to remove the cache are therefore blocked, and this feature is disabled in Scrub.

QuickLook cache handling is performed as follows.
The path to the QuickLook cache is determined from `NSTemporaryDirectory()`.
Total cache size is measured by performing a shallow traversal of the cache directory, and totalling the size of all items within it.
The command which clears the cache is `qlmanage -r cache`
Turning caching off is implemented by the command `qlmanage -r disablecache`
which changes the QLUseCache value in ~/Library/Preferences/com.apple.QuickLookDaemon.plist.
QuickLook caching can be re-enabled using the command
`qlmanage -r enablecache`

➔ Scrub   ➔ Logs

Logs

These only include the unified log in Sierra and later. This option is disabled until you have clicked on the adjacent button to **Make archive** (make a logarchive) of the current logs. You can then store that securely in case you need to refer back to it for any reason. The unified log does have a good degree of privacy, censoring potentially sensitive information, but has been known to leak encryption passwords at times, and reveals details of user activity and more.

Before Scrub can make a logarchive or remove logs, you will be prompted to enter your admin password so that the necessary commands can be run.

Removal of logs is performed using the command
`sudo log erase --all`
and making a logarchive using
`log collect --output filepath`

➜ [Scrub](#)　　➜ [Tips & Tricks](#)

Tips and Tricks

When performing an audit, and zeroing dates, Scrub performs deep traversals of the folder/volume selected, to identify every file and folder within it. This can take time, and considerable amounts of memory. To make the best use of multi-core processors, Scrub performs as much as possible in the background, and simultaneously. It therefore displays up to three 'busy spinners' between the **Audit** and **Scrub** buttons, each monitoring separate processes. The busy spinner at the left monitors xattr activity, that in the centre version activity, and that at the right UTI checking (during Audit) and date setting (during Scrub).

When you Audit and Scrub a volume rather than a folder, some of the folders examined have permissions which prevent normal access. These are reported as errors in the scrolling display, and are inevitable and normal.

It is easy to use Scrub with caution: run the first Audit, and select just one or two options to apply in the Scrub. Once those have been scrubbed, run another Audit, and decide on any further options to apply for a second Scrub. This is particularly useful when removing xattrs: you don't have to go straight to strip all during your first Scrub, but can go for **minimal**, then see how that has worked with another Audit.

Scrub is aimed primarily at folders and volumes full of normal documents, rather than complicated items such as apps, Photos libraries, and other packages. Look carefully through the Audit report to see if a Scrub might inadvertently damage something which is not a normal document, and move it out of the way if necessary.

Scrub is also a convenient way of removing old versions from large collections of documents. They can take a lot of space on your storage, and are now quick and simple to remove.

➔ [Scrub](#)   ➔ [Privacy protection](#)

Privacy protection in Mojave and later

Scrub is designed so that it will clean any item for which you have permissions. However, Mojave and later add restrictions to preserve the privacy of your personal data. If you want to use Scrub to edit any file or folder, including those in what macOS considers to be protected data, then you must add the app to the list of apps with **Full Disk Access** in the **Privacy** tab of your **Security & Privacy** pane.

If you don't do that, but try to access protected data, then you should be prompted to give consent to Scrub to do so; if you agree, it will then be added to the appropriate list of apps in the Privacy settings.

If Scrub crashes when you try to access any protected items, this is most probably because you need to add it to the Full Disk Access list.

⚠️ In Catalina and later, despite adding Scrub to the Full Disk Access list, some operations may still fail on removable (external) volumes. This is a limitation of macOS, and can prevent you from saving a logarchive to an external volume. You can work around that by saving it to ~/Documents and copying it to the external volume in the Finder.

➜ [Scrub](#)   ➜ [Updates & Change list](#)

Updates

To check for updates to Scrub and other apps, use the **Browse updates** command in the **Help** menu. This opens a special page on The Eclectic Light Company blog in which you can view current versions, and download any that you wish.

Change list

1.3:
- updated xattr code for compatibility.

1.2:
- Universal App for Big Sur and Apple Silicon
- removed QuickLook cache operations from Mojave and later to avoid failure and crashes, particularly in Big Sur.

1.1:
- fixes a crashing bug when running an audit in Catalina
- notes that 10.14 and later can't get QuickLook cache sizes
- updated Help book for Catalina behaviours.

1.0:
- checks code integrity after launching
- added Help book
- added link to Support page
- supports sizing of text
- ported to Swift 5 and Xcode 10.3
- improved saving of window size and position.

1.0b2:
- ported to Swift 4.2.1 and Xcode 10.1
- fixed bug in handling single files (at last)
- notarized for Mojave.

1.0b1:
- added UTI review in Audit
- tidied menus to remove Save and Save as
- tweaked window text and layout
- enabled log removal (Sierra and later)
- completed Dark Mode support
- ported to Swift 4.2
- built using Xcode 10ß.

1.0a1:
- initial release
- remove logs doesn't (intentionally).   4 June 2023.