Scientific Working Group on Digital Evidence

MacOS Tech Notes

SWGDE 13-F-002-2.0

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address

d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

MacOS Tech Notes

Table of Contents

1. Purpose....2
2. Scope....2
3. Limitations....2
4. Overview of macOS/Mac OS X....2
   4.1 Versions....2
5. Acquisitions....4
   5.1 iCloud Acquisition....4
6. Analyzing Apple Computers....5
   6.1 File System....5
   6.2 Directory Structure....6
   6.3 Application Data....15
   6.4 Additional System Artifacts....19
7. References....19
8. History....21

1. Purpose

This document is to provide forensic examiners with a functional knowledge for imaging and analyzing Apple laptops and computers running the macOS operating system.

2. Scope

This document is intended to serve as a guide for digital forensic examiners, from novice to intermediate, who are trained and experienced in the examination of computer operating systems and seek to obtain direction and familiarization with macOS systems and associated forensic artifacts. This document is limited to the macOS operating system (i.e., Mac OS X, macOS).

3. Limitations

This document will not cover other Apple operating systems, such as iOS, tvOS, or iPadOS. This document was prepared with the available resources at the time of publishing. As with all technology, this is an ever-evolving field with frequent innovation. The macOS outline presented here is interpreted with regard to a standard installation and cannot account for the wide variety of installations available to a user. Each macOS environment may vary and not comply with the information contained herein.

The digital forensic examiner is responsible for their examinations and should always verify findings and leads. This document is not intended as a step-by-step guide for conducting a thorough forensic examination, nor legal advice. Always seek guidance regarding applicable governing policies and laws.

4. Overview of macOS/Mac OS X

MacOS (previously known as Mac OS X) has been natively installed on Apple computers upon production since 2002, called Mac OS X starting in 2011, and macOS starting in 2016. It has undergone a series of point upgrades since that time. Apple has also implemented hardware updates and changes that directly affect the examination of various generations of machine releases.

The macOS ecosystem is controlled by Apple through internet communications, and has limited system customization for the user, depending on the type of devices the user has purchased and configuration relative to their iCloud account. A forensic examiner should understand that this concept exists concerning any Apple product, and while not in the scope of this document, an examiner should consider these parameters concerning their examination.

4.1 Versions

For macOS version history, see Table 1.

Version	Name	Processor / Security	Introduced
10.0	Cheetah	PowerPC	Dock; Address Book; TextEdit
10.1	Puma	PowerPC	Screen Capturing; Finder Search
10.2	Jaguar	PowerPC	Bonjour; CUPS; iChat
10.3	Panther	PowerPC	Safari; FileVault; iChat video; Spotlight
10.4	Tiger	PowerPC/Intel	Automator; x86 Architecture
10.5	Leopard	PowerPC/Intel	Time Machine; Quicklook; Bootcamp
10.6	Snow Leopard	Intel	64-bit Architecture; AppStore
10.7	Lion	Intel	Launchpad; Mission Control; FileVault FDE
10.8	Mountain Lion	Intel	Notes; Reminders; Messages; Notification Center
10.9	Mavericks	Intel	iCloud Keychain; Maps; iBooks; Tags
10.10	Yosemite	Intel	Handoff; Continuity
10.11	El Capitan	Intel	Split View; Metal
10.12	Sierra	Intel	Siri; Storage Optimization; Apple Pay
10.13	High Sierra	Intel/T2	HEIC; APFS; Metal 2
10.14	Mojave	Intel/T2	Dark Mode; Stocks; News; Home; Stacks
10.15	Catalina	Intel/T2	Music; Podcasts; Movies; Sidecar; Find My; Screen Time; Voice Control
11	Big Sur	Silicon ARM	iOS application support
12	Monterey	Silicon ARM	Shortcuts; Universal Control
13	Ventura	Silicon ARM	Freeform; Weather
14	Sonoma	Silicon ARM	Game Mode, Interactive Widgets, Safari Profiles

Version	Name	Processor / Security	Introduced
15	Sequoia	Silicon ARM	Integrates Apple Intelligence; Passwords App introduced, iPhone mirroring.
26	Tahoe	Silicon ARM	Runs on 2019 and later Macs; Apple Intelligence integration enhancements, Shortcuts, Clipboard, and Spotlight enhanced.

Table 1. Version History Chart (Credit: SWGDE)

5. Acquisitions

Regarding Apple computer device acquisitions, the examiner must conduct a thorough physical examination of the device. An examiner must identify the generation of the hardware before making any interactions or changes. Apple computers and laptops have introduced various hardware changes, which greatly differ in how to obtain a forensic image, e.g., Apple Silicon M1/M2 Advanced RISC (Reduced Instruction Set Computing) Machine (ARM). Other considerations to include are varying combinations of Apple computer hardware, security architecture, firmware passwords, file system, operating system, encryption, and booting options. These are all contributing factors that may modify a digital forensic examiner's method of acquisition. For best practices of Apple device acquisition, refer to *SWGDE 23-F-005-1.0 Best Practices Apple macOS Forensic Acquisition* [1].

5.1 iCloud Acquisition

Introduced in 2011, iCloud backups store system and application data similar to Time Machine backups. With iCloud backups, synchronized data is not contained within the backup file. To supplement the backup file, an examiner should also obtain the synced data using best practice methods. It should be researched what the data limit of an iCloud account is. Depending on the Apple ID's storage volume in iCloud, this may affect backup volume or quality. One method to obtain the iCloud data is via a legal request process (e.g. Court Orders, and Search Warrants), however, not all situations require this mode of acquisition, such as a consent of iCloud access and provided credentials.

Another method of accessing iCloud data is by using a Mac device to log into the iCloud. iCloud backups will be downloaded in an iTunes format, unless "restore original file names" was selected prior to backup. All devices logged into the iCloud user account can be backed up to the iCloud, and the iCloud will only keep the two most recent backups (Snapshots) generated. The choice can be made to download an entire backup or just parts that are considered essential. [2]

With the release of macOS 15, Sequoia introduced Temporary Backups, which expands the storage capacity of the iCloud capacity for the purpose of transferring device data to a new device. Be sure to research Apple policies for the current data retention policy at the time of acquisition. [3]

6. Analyzing Apple Computers

6.1 File System

Apple computers can use the UFS, FAT, exFAT, Hierarchical File System (HFS), HFS+, or HFSX, and Apple File System (APFS) file systems. Mac OS X v10.4 and earlier generally use UFS, while the newer operating system versions generally use HFS+. HFS stands for Hierarchical File System.

Files maintained by the HFS file system are made up of at least two parts: the data fork and the resource fork. The data fork contains the file content, and the resource fork can contain a variety of metadata and other data structures. If a file created on an HFS file system is copied to a file system that does not support resource forks, the resource fork will be separated as a hidden file or lost entirely. The HFS file system generally does not use file fragmentation; most files occupy contiguous sectors. This results in ease of file carving but may lead to difficulty in deleted file recovery.t.

APFS, the default file system for Apple computers using macOS 10.13 or later, features strong encryption, space sharing, snapshots, fast directory sizing, and improved file system fundamentals. While APFS is optimized for the Flash/SSD storage used in recent Mac computers, it can also be used with older systems with traditional hard disk drives (HDD) and external, direct-attached storage. macOS 10.13 or later supports APFS for both bootable and data volumes.

APFS allocates disk space within a container (partition) on demand. When a single APFS container has multiple volumes, the container's free space is shared and is automatically allocated to any of the individual volumes as needed. Additionally, an examiner can specify reserve and quota sizes for each volume. Each volume uses only part of the overall container, so the available space is the total size of the container minus the size of all the volumes in the container. [4]

6.1.1 System Date and Time

Apple computers utilize Extensible Firmware Interface (EFI), which is based on the Unified Extensible Firmware Interface (UEFI). To preserve the data integrity, an examiner should determine the system date and time through the Terminal located in the startup menu under Utilities. Using command key combinations to access the startup menu or pressing and holding power for M1/M2 Silicon. Enter the *date* command in the Terminal. Apple computer systems do not contain a BIOS or an implementation of UEFI in the same way Windows systems do. The system date and time can be obtained by booting the computer into Single User Mode or Startup Manager (Holding down the "Command" and "S" keys at boot time) and running the *date* command in Terminal.

Modern macOS systems utilize *Apple Cocoa Core Data* timestamps, initially upon release, are 32-bit integers representing the number of seconds since January 1, 2001, 00:00:00 GMT, also

known as *Mac absolute time* and *CF Absolute Time*. Depending on the macOS version, Apple Cocoa Core Data timestamps may not be a 32-bit integer, and may be using seconds, milliseconds, microseconds, or nanoseconds to generate the timestamp. Mac systems previously used the following timestamp calculations:

- MacHFS timestamps are a 32-bit integer that represents the number of seconds since January 1, 1904, 00:00:00 GMT.
- MacHFS+ extended timestamps are in nanoseconds since January 1, 2001, 00:00:00 GMT.
- macOS Classic is calculated in seconds since January 1, 1904, 00:00:00 GMT.

Modern macOS systems utilize internet connectivity to maintain an accurate clock, and there is no internal Complementary Metal-Oxide-Semiconductor (CMOS) clock on modern Apple computers.

6.2 Directory Structure

While there are differences among versions, most Mac operating systems roughly conform to the File System Hierarchy Standard (FHS) detailed below. The root level of the system drive is commonly referred to simply as "root," is represented by the "/" character and will commonly contain directories listed in Table 2. [5]

Directory	Description
/.Trash(es)	Temporary storage of user-deleted files. The system hides this directory from the user by default.
/.vol	Volume-specific file identifiers (i.e., inode numbers).
/Applications	Installed applications including pre-installed Apple software, local system utilities, and user-installed applications. This directory is visible to the user.
/bin	Essential command-line binaries.
/cores	Core Dumps, if the service is enabled.
/dev	Essential device files (e.g., mount points).
/Library	System wide directory for applications that share resources to store data files, caches, resources, and preferences. This directory is visible to the user.
/Network	Data identifying computers in the local area network. This directory is visible to the user.
/private	Parent directory in older versions of Mac for the /etc, /tmp, and /var.
/sbin	Temporary files created by the system and applications.

Directory	Description
/System	System resources required by the operating system to function including startup items. This directory is visible to the user.
/Users	User account directories for storing user-specific data. This directory is visible to the user.
/tmp	Temporary files created by the system and applications. The system hides this directory from the user by default.
/usr	Non-essential command-line binaries.
/var	Variable data (e.g., log files, caches, temporary application data, lock files). The system hides this directory from the user by default.
/Volumes	Mount points for physical and virtual disks and volumes in the local file system. The system hides this directory from the user by default.

Table 2. File System Hierarchy Standard (FHS) (Credit: SWGDE)

6.2.1 /Library

This folder contains settings and logs for applications. This folder is differentiated from /users/<username>/Library in that it contains settings universal to the machine rather than settings associated with a specific user account.

6.2.2 Hidden Folders

In addition to the root directories hidden by the system by default, the macOS adopted the UNIX convention to automatically hide folders whose name starts with the period (.) character, often referred to as “dot directories”. An example of the hidden dot directories is the “/.Trash”.

6.2.2.1 /.Trash or /.Trashes

This subfolder contains deleted files that are capable of being restored by the user. This subfolder functions much like the Recycle Bin on a Windows computer.

- /.Trashes - Trash at the root of any media connected to a Mac, used for files deleted from specific volume
- /users/<username>/.Trashes - user specific Trash for items deleted by user on local system

6.2.3 /Users

Referred to as the User Home directory, which has a directory created for each user. More specifically /users/<username>/ is where most applications store user-specific data, such as configuration files, lists, Documents, Downloads, and Desktop folders. The Plist files within the User folder often contain user preferences and settings. Other files of interest are .bash_history

and .zsh_history. This directory can reveal user activity, preferences, command line events, and other insights attributed to the user. This directory can contain the user's documents, movies, music, pictures, downloads, and other user-created files.

See Table 3 below for a list of common natively-installed directories within root/users/<username>/ (to be represented with placeholder "~/") that can be featured in a macOS environment. An examiner should be mindful that some of these directories may be hidden when analyzing a live machine and not a processed forensic image.

~/Applications	Contains applications and data about the application.
~/Desktop	Stores files and directories located on the desktop. This is not a shared folder unless a user has granted permission to another.
~/Documents	Stores personal files to the user and is not a shared directory unless the user gives permission to another. Natively contains iChat/Messages logs.
~/Documents/iChat (Historical Location) **~/Library/Messages/chat.db** **~/Library/Messages/Attachments** (Current Location)	Default save location for iChat and Messages application.
~/Downloads	Where downloaded files are stored by default. Includes downloads from browsers, applications and other sources.
~/Library	Contains user specific data, settings, preferences and/or application support files. Typically hidden by default. Within the User Library are multiple application directories, each will contain valuable forensic data within each sub directory. This directory will also contain a wealth of user-specific artifacts.

~/Library/Application Support	User-specific application data files that are maintained by each application and typically exclude user-defined data.
~/Library/Application Support/Screen Sharing	Contains artifacts regarding Screen Sharing.
~/Library/Application Support/MobileSync/Backup	Default location for local iPhone, iPod, and iPad backup data (“iTunes Backups”).
~/Library/Caches	Contains temporarily stored application data files written by software.
~/Library/Caches/com.apple.Safari/Cache.db	Contains data from websites visited via the Safari browser.
~/Library/Preferences	Contains user-specific application preferences.
~/Library/Preferences/com.apple.dock.db	Contains folders and network shares in the Dock application.
~/Library/Safari	Contains .plist files for internet bookmarks, internet download history, and internet browsing history.
~/Library/Images/iChat/Recent Pictures	Contains the user’s iChat profile pictures; however, if a user deletes this file, it may not affect their displayed account picture.
~/Library/Mail	May store locally-synced email messages and recently-used email addresses (both recipient and sender) in the Mail application. Other associated Mail artifacts.
~/Library/Mail/Mailboxes	In Mac OS X Snow Leopard this directory contains mailbox structure, e-mail messages, attachments, account settings, and .emlx files.

~/Library/Mail/V2/Mailboxes	Since Mac OS X Lion, this directory contains mailbox structure, e-mail messages, attachments, account settings, and .emlx files. Currently, macOS stores .emlx files within .mbox files in this directory.
~/Library/Mail/Downloads	May recover stored email messages and recently used email addresses (both recipient and sender) in the Mail application. Other associated Mail artifacts.
~/Library/Application Support/CallHistoryDB/CallHistory.storedata	See 6.3.6 FaceTime in this document for additional detail.
~/Library/Messages	Contains database for Messages application.
~/Library/Mobile Documents ~/Library/iCloud Drive	Contains data regarding synced Documents and Data features of iCloud. In more modern MacOS (typically Sierra and later) this directory is called iCloud Drive.
~/Library/StickiesDatabase	Stickies is an application for putting user-created notes on the screen. Stickies keep all information in the listed directory in a Rich Text Format.
~/Library/Containers/com.apple.Notes/Data/Library/ Notes/ NotesV1.storedata-wal	Contains SQLite Database files for locally stored Notes from the Notes application.
~/Library/Keychain	See 6.3.8 Keychain in this document for additional detail.
~/Movies	Contains video media files.
~/Music	Contains all audio media files.
~/Music/iTunes	Default location of iTunes.

~/Pictures	Contains picture and visual media files.
~/Pictures/Photos Library.photoslibrary	iPhoto is a digital photograph manipulation application. The user can import, organize, print, edit, and share digital photos. iPhoto stores images in a package file. Inside of the package file, original photos are stored in the /Originals folder; modified photos are stored in /Modified folder. From the package file, the examiner may obtain photo metadata and camera information (i.e., EXIF data). iPhoto creates thumbnails of all photos and saves them as thumb segment files. A /Data.noindex folder contains thumbnails of all photos associated with iPhoto.
~/Pictures/Photo Booth Library	Contains Picture files from Photo Booth application.
~/Public	Used for sharing files among all users on the device.
~/Sites	Used to store shared files and folders.

Table 3. Common User Home Directories (Credit: SWGDE)

6.2.4 Property Lists (i.e., plist)

While Registry data found on Windows machines is highly valuable, hierarchical, and organized, macOS stores user information within property list (plist) files throughout various operating system directories. Applications store user and system configuration data in various plist files across the drive as well. The contents of plist files may be stored in binary, ASCII data, or XML. Viewer software exists to examine binary plist information. See Table 4 for common plists to consider, however, plists are created every time a user or software creates a directory and is typically stored within that directory. Table 4 shows common plist locations for typical macOS installations, and a description of what artifacts may be found within the plist.

Operating System	
/System/Library/CoreServices/SystemVersion.plist	macOS version and OS details.

/System/Library/CoreServices/ServerVersion.plist (Not used with OS X 10.7 and later)	OS Version details.
Software Installation	
/Library/Receipts/InstallHistory.plist	History of installed applications and updates.
/Library/Preferences/com.apple.SoftwareUpdate.plist	Last software update.
Time zone	
/Library/Preferences/.GlobalPreferences.plist	Contains system wide timezone details, settings, preferences and other various behaviors. *This is a hidden file.*
Auto-Login and Last Login User Info	
/Library/Preferences/ com.apple.loginwindow.plist	Contains configuration settings for the system's login window, including auto login settings. Also contains a list of allowed and denied users, and any login or logout scripts.
Deleted Users	
/Library/Preferences/ com.apple.preferences.accounts.plist	Contains account details.
App Store	App Store is a link to an Apple website allowing users to purchase, download, and update applications. The user's download history is maintained by Apple, and artifacts may be located in the iTunes application plist.
~/Library/Preferences/com.apple.appstore.plist	Contains user-specific configuration and metadata for the Mac App Store.

iTunes Or Music	A media player application used for playing, downloading, saving, and organizing digital music and video files on desktop or laptop personal computers. It is also used to download applications (apps) from the iTunes Store. iTunes is used to manage content on, and create backup copies of, iPods, iPhone, iPod Touch, and iPad devices. Since Catalina this application received a name change to Music.
~/Library/Preferences/com.apple.iTunes.plist	Stores user-specific preferences and settings for the iTunes application.
iPhone/iPod artifacts	These are all user-specific artifacts.
~/Library/Application Support/ MobileSync/Backup/*UUID*/Info.plist	Contains information regarding the specific device and the device's synced backup, the modified date of the backup, and the last time it was synced.
~/Library/Preferences/com.apple.iPod.plist	iOS and iPod devices connected for this account, including iOS version, IMEI, etc.
Auto-Lauch	
~/Library/Preferences/loginwindow.plist	User-specific file documenting items that are set to Auto-Launch.
Network Settings	The following are all system-wide artifacts. *With the release of macOS 15 Sequoia, a Wi-Fi feature has been added where the Media Access Control (MAC) Address will change to prevent long-term tracking.*
/Library/Preferences/com.apple.alf.plist	Firewall settings.
/Library/Preferences/SystemConfiguration/ com.apple.airport.preferences.plist	Airport (Wireless) Settings.
/Library/Preferences/SystemConfiguration/com.apple. nat.plist	Internet Sharing Settings.

/Library/Preferences/SystemConfiguration/com.apple.network.identification.plist	Historical Network TCP/IP Assignments with timestamps.
/Library/Preferences/SystemConfiguration/com.apple.smb.server.plist	Server Message Block (SMB) and network folder browsing settings.
/Library/Preferences/SystemConfiguration/NetworkInterfaces.plist	Available network interfaces (including the MAC address on OS X 10.8).
/Library/Preferences/SystemConfiguration/com.apple.NetworkInterfaces.plist	Available network interfaces, including the MAC address.
/Library/Preferences/SystemConfiguration/com.apple.preferences.plist	Network Configuration for each interface (not available on OS X 10.8).
/Library/Preferences/SystemConfiguration/preferences.plist	Network interface configuration and Back To My Mac information.
User Configuration	
~/Library/Preferences/com.apple.finder.plist	Recent searches, trash settings, view settings, and recent folders.
~/Library/Preferences/com.apple.dock.plist	Applications in the Dock, user-specific.
~/Library/Preferences/com.apple.desktop.plist	Desktop picture capture.
~/Library/Preferences/com.apple.recentitems.plist	Recent documents, applications, and network connections.
Bluetooth History	
/Library/Preferences/com.apple.Bluetooth.plist	System-wide Bluetooth settings.
Instant Messaging	
/Library/Preferences/com.apple.iChat.AIM.plist	System-wide settings and preferences regarding the iChat application.
/Library/Preferences/com.apple.iChat.plist	System-wide settings and preferences currently for the iMessage application.
/Library/Preferences/com.apple.iChat.SubNet.plist	System-wide messaging network settings.

~ /Library/Preferences/com.aol.aim.plist	User-specific AOL AIM account preferences.
~ /Library/Preferences/com.adiumX.adiumX.plist	User-specific preferences for Adium messaging application seen on OS X 10.7 and newer.
~ /Library/Preferences/com.apple.iChat.AIM.plist	User-specific settings and preferences regarding the iChat application account(s).
~ /Library/Preferences/com.apple.iChat.plist	User-specific preferences regarding the iMessage application.
~ /Library/Preferences/com.apple.SubNet.plist	User-specific messaging network settings.
~ /Library/Preferences/com.skype.skype.plist	User-specific Skype preferences and settings.
~/Library/Preferences/com.yahoo.messenger3.plist	User-specific Yahoo Messenger settings and preferences.
~/Library/Preferences/ com.yahoo.messenger3.Users.*screenname*.plist	User-specific account settings for Yahoo Messenger.

Table 4. Common plist Directory List (Credit: SWGDE)

6.2.5 Core Storage

Core Storage was introduced with OS X Lion (10.7) as a logical volume manager sitting between the whole disk partition scheme and the file systems used for specific partitions. It presents multiple partitions on multiple drives as if they were one logical volume. Core Storage provides for dynamic allocation of partitions while maintaining the existing file system. This provides a mechanism for in-place transformations (e.g., the full-disk encryption used by File Vault 2, or the process of dynamically extending a partition onto another disk).

The importance of Core Storage for forensics is that, on drives where enabled (default for Mac OS X Yosemite 10.10), the OS must be involved during the acquisition process; Linux boot media will no longer provide access to all partitions on the system. [6]

6.3 Application Data

6.3.1 Library Directories

System and user data associated with installed applications are predominantly located in the Library directories. These folders include the default macOS applications that come preinstalled on the system, applications installed through the App Store, and third-party applications installed from installer files.

6.3.2 Address Book / Contacts

Address Book (renamed Contacts in OS X 10.8) is a SQLite database containing contact information. This database contains the default Apple.com ID as well as any Apple.Mac or MobileMe accounts associated with the computer. Address Book/Contacts may also include associated images.

6.3.3 Continuity

The Continuity feature introduced with OS X Yosemite and iOS 8.1 includes the following: Handoff, Phone Calling, Instant Hotspot, AirDrop, and SMS. Handoff allows the user to start an email, document, or browsing session on an iOS device and continue the work on another device using a wide variety of apps. Continuity also allows the user to make and receive phone calls through a Mac computer via connection with an iPhone. Except for AirDrop, all Continuity functionality is dependent upon the devices being signed in to the same iCloud account. The Instant Hotspot feature is dependent upon the carrier support of Personal Hotspots.

6.3.4 Dashboard

A GUI interface used for hosting mini-applications known as widgets. Users can assign widgets to the Dashboard, or widgets may be assigned by default.

6.3.5 Disk Arbitration

Disk Arbitration is the daemon responsible for monitoring disks and updating the disk arbitration table. This service mounts and unmounts disks. It can be used to set a volume as read-only. It's important to turn disk arbitration off when connecting to evidence media to avoid making writes.

6.3.6 FaceTime

FaceTime is a video calling application first introduced with Mac OS X Lion. This application only works on Apple devices. It can be tied to the user's Apple ID or other email account. In OS X Yosemite, FaceTime allows users to make phone calls, and the call history is synced to all devices via iCloud.

6.3.7 Finder

Finder is the default file manager responsible for the overall management of files, disks, network volumes, and the launching of other applications. Spotlight (discussed below) is built into Finder.

After Mac OS X Leopard, Finder included Quick Look. This allows the user the ability to preview the contents of a file without opening it. The use of Quick Look on an unlocked volume (not read-only) will change a file's last accessed date and time. Quick Look creates its own SQLite database that stores the full paths and thumbnails of the data it references.

6.3.8 iCal / Calendar

iCal (renamed Calendar in OS X 10.8) is a personal calendar application. It is integrated with iCloud (formerly MobileMe).

6.3.9 Keychain

Keychain is a password management application that stores passwords, certificates, encryption keys, and secure notes. Passwords are stored in a separate database by user.

Users can create custom Keychains that can be stored anywhere, including on removable media. The custom Keychain stays encrypted until the user chooses to unlock it. This is differentiated from the user's Keychain, which is unencrypted when the user logs in to the local machine. Some applications that allow auto-filling obtain the encryption key from the Keychain. The Keychain may also show the wireless network SSIDs and Apple IDs associated with the user.

With the introduction of Mac OS X Yosemite, the Keychain may be synced through iCloud, which allows the user to share credentials with other Apple devices. The Keychain will also allow users to store credit card information, usernames, and website passwords entered into the Safari browser. Keychains may be critical to an investigation with regard to attribution of activities or what a user had access to. [7] With the release of macOS 15 Sequoia, Passwords as an application was released. This allows for authorization credentials to be managed across multiple Apple products and even Windows.

6.3.10 Safari

Safari is the default web browsing application. In newer versions of Mac OS X, notable items are contained in SQLite databases. Artifacts may include internet bookmarks, internet history, tabs and windows most recently opened, the last session, the user's search bar history, downloads, cookies, and webpage previews.

6.3.11 FS Events

File System Events (FSEvents) is the Application Programming Interface (API) that identifies file system changes. FSEvents, and its associated daemon, *fseventsd*, monitor critical file system changes and events in real time. FSEvents can be located, along with *fseventsd*, in the root of every volume. [8] Some categories that are monitored are seen in Table 5.

• User profile activity • User picture type files • User Document Type Files • Downloads activity • Trash Activity • Browser Activity	• Cloud Storage Box Activity • DS Store Activity • Saved Application State • Root Shell Activity • Guest Account Activity • Sudo Usage Activity • Bash Activity

• Mount Activity • Email Attachments • Cloud Storage Dropbox Activity	• Failed Password Activity • iCloud Synchronization Activity • Shared File Lists

Table 5. FSEvents Possible Artifacts List. (Credit:SWGDE)

Two key components of FSEvents functionality are *Spotlight* and *Security*.

6.3.12 Spotlight

Currently, Spotlight can be found at /Volumes/<drivename>/.Spotlight-V100. Spotlight is a hidden database that performs as a system-wide desktop search feature. The Spotlight database contains an index of all items and files on the system. Most user files on the Mac can be indexed by Spotlight. Every time a file is created, moved, copied, saved, or deleted Spotlight monitors and records these changes in the index. It also allows for searching of data contained within file metadata, including artifacts not readily available through regular file system navigation. [9]

Indexing the volume begins when the volume is mounted, except when that volume is optical media, a network volume, or a read-only drive. Spotlight may be disabled by the user. Spotlight in OS X Yosemite now includes features to search websites, maps, iTunes, and other content.

6.3.13 Security

Applications utilize the information provided by FSEvents to monitor suspicious or malicious activity.

6.3.14 Time Machine

A backup utility was introduced with Mac OS X Leopard. It is designed to work with the Time Capsule. After its initial backup of everything on the hard drive, Time Machine backs up files incrementally on the following schedule:

- Hourly backups: data modified in the past 24 hours
- Daily backups: data modified each day in the past month
- Weekly backups: everything older than a month until the disk runs out of space; at that point, the oldest backup is then deleted

Time Machine will back up deleted files if they have not been removed from Trash. Time Machine backups can be searched for files previously deleted from the Mac. Time Machine backups created when the backup device is unavailable will be stored on the local device under /.MobileBackups, a hidden folder.

Network backups will be stored as .sparseimage files while local backups will be stored in incremental folders. If multiple machines are backed up to the same Time Machine, each backup will be separated into folders named for the host machine name. [10]

6.4 Additional System Artifacts

/private/var/log/OSInstall.custom	Operating System Installation information on OS X 10.5.
/private/var/db/.AppleSetupDone	OS Installation info along with registration information entered by the user upon initial setup on OS X 10.6 and later.
/etc/localtime	System-wide current Timezone and Daylight Savings settings stored in binary format.
/private/etc/kcpassword	Auto-login password, the folder is hidden.
/private/var/spool/cups	completed and unfinished print jobs.
/private/var/vm/swapfile0	Virtual memory data.

Table 6. Additional System Artifacts (Credit: SWGDE)

7. References

[1] Scientific Working Group on Digital Evidence, *Best Practices Apple MacOS Forensic Acquisition*. 23-F-005-1.0 *SWGDE,* 2024, https://www.swgde.org/documents/published-complete-listing/23-f-005-swgde-best-practices-apple-macos-forensic-acquisition/.

[2] Apple, Inc. "View and manage iCloud device backups." *Apple,* https://support.apple.com/guide/icloud/view-and-manage-backups-mm122d3ef202/icloud. Accessed 16 September 2025.

[3] Apple, Inc. "Get Temporary iCloud storage when you buy a new iPhone or iPad." *Apple,* https://support.apple.com/en-us/104980. Accessed 24 September 2024.

[4] Apple, Inc. "Add, delete, or erase APFS volumes in Disk Utility on Mac." *Apple,* https://support.apple.com/guide/disk-utility/add-delete-or-erase-apfs-volumes-dskua9e6a110/mac. Accessed 16 September 2025.

[5] Apple, Inc. "Folders that come with your Mac." *Apple,* https://support.apple.com/guide/mac-help/folders-that-come-with-your-mac-mchlp1143/mac. Accessed 17 September 2025.

[6] Wikimedia Foundation, Inc. "Core Storage." *Wikipedia,* https://en.wikipedia.org/wiki/Core_Storage. Accessed 17 September 2025.

[7] Apple, Inc. "Setup iCloud Keychain." *Apple,* https://support.apple.com/en-us/109016. Accessed 16 September 2025.

[8] Apple, Inc. “Core Services / File System Events.” *Apple*, https://developer.apple.com/documentation/coreservices/file_system_events. Accessed 16 September 2025.

[9] Apple, Inc. “Search for Anything with Spotlight on Mac.” *Apple,* https://support.apple.com/guide/mac-help/search-with-spotlight-mchlp1008/mac. Accessed 15 September 2025.

[10] Apple, Inc. “Backup your Mac with Time Machine.” *Apple,* https://support.apple.com/en-us/104984. Accessed 15 September 2025.

8. History

Revision	Issue Date	History
1.0 DRAFT	09/13/2013	Completed drafting document; voted to release as a Draft for Public Comment.
1.0 DRAFT	09/14/2013	Formatted and released as a Draft for Public Comment.
1.0 DRAFT	01/16/2014	Voted as Approved; no changes made.
1.0 DRAFT	02/06/2014	Formatting and tech edit performed for release as Approved.
1.1 DRAFT	06/06/2014	Added Mavericks OS X.9 version. Voted to release as a Draft For Public Comment.
1.1 DRAFT	06/12/2014	Updated disclaimer. Formatted and released as a Draft for Public Comment.
1.1	08/28/2014	No changes made; voted to publish as an Approved document.
1.1	09/05/2014	Formatting and technical edit performed for release as an Approved document.
1.2 DRAFT	01/15/2015	Added Yosemite OS X.10 version. Added general updates for Yosemite data. Voted for release as a Draft for Public Comment.
1.2 DRAFT	02/05/2015	Formatting/edit performed for release as a Draft for Public Comment.
1.3 DRAFT	06/04/2015	Added information regarding Core Storage to document. Voted for release as a Draft for Public Comment.
1.3 DRAFT	06/20/2015	Formatting/edit performed for release as a Draft for Public Comment.
1.3	09/17/2015	SWGDE voted to release as an Approved Document.
1.3	09/29/2015	Formatting and technical edit performed for release as an Approved Document.

2.0 DRAFT	01/12/2023	Updating of all sections to bring the content to current macOS versions.
2.0 DRAFT	06/15/2023	Updating of all sections to bring the content to current macOS versions.
2.0 DRAFT	01/11/2024	Updating of all sections to bring the content to current macOS versions.
2.0 DRAFT	05/16/2024	Updating of all sections to bring the content to current macOS versions.
2.0 DRAFT	09/18/2025	Updated all sections to bring the content to current macOS versions. Draft approved for SWGDE internal review.
2.0 DRAFT	01/12/2026	Updated to address Internal Review comments. Moved forward for SWGDE membership vote to release as a Draft for Public Comment.
2.0 DRAFT	02/17/2026	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment.
2.0 DRAFT	05/12/2026	Editorial updates.
2.0	06/18/2026	SWGDE voted to approve as a Final Approved Document.
2.0	07/14/2026	Formatted for release as a Final Approved Document.