Scientific Working Group on Digital Evidence

SWGDE Mac OS X Tech Notes

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) 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 change

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall 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; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the user's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived for future reference, as needed, in accordance with that organization's policies.

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 the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

SWGDE Mac OS X Tech Notes

Table of Contents

1. Scope

The scope of this document is to describe the procedures for imaging and analyzing Macintosh computers. This document is restricted to the OS X operating system.

This document includes a discussion of OS X (Mac OS) and does not include a discussion of iOS, which is used on portable Apple devices such as iPods, iPads, iPhones, and Apple TV.

2. Overview of Mac OS X

Mac OS X has come preloaded on Macintosh computers since 2002. It has undergone a series of point upgrades since that time.

2.1 Versions:

10.0 Cheetah
10.1 Puma
10.2 Jaguar
10.3 Panther
10.4 Tiger
10.5 Leopard
10.6 Snow Leopard
10.7 Lion
10.8 Mountain Lion

Versions 10.0 through 10.5 can run on PowerPC or on Intel-based platforms. From 10.6 forward, an Intel-based platform is required.

2.1.1 Cheetah (OS X)

Cheetah introduced the dock. It offers native support for .pdf format and integrated email client (Mail). It included Address Book, a word processor called TextEdit, and the Aqua interface (a GUI theme). It introduced protected memory, which prevented cascading memory faults between programs. It introduced the Sherlock Desktop and Internet Search. The OS is built on XNU, which is a UNIX-like operating system built on the Darwin platform. It introduced Apple Script, a scripting tool and programming interface.

2.1.2 Puma (OS X.1)

Puma has an integrated DVD player. It allows for screen capturing. It contains Apple Script Studio, an upgrade to Apple Script. It introduced Finder, a search tool.

2.1.3 Jaguar (OS X.2)

Jaguar introduced Rendezvous (later became Bonjour) which allows the computer to communicate with other devices. It introduced CUPS (Common UNIX Printing System), allowing the computer to connect to any print device. Jaguar also introduced journaling,

allowing the operating system to keep track of what it's doing to help prevent file system corruption and increase stability. A revamped Finder was introduced, and iChat debuted.

2.1.4 Panther (OS X.3)

Panther updated Finder to include the Spotlight search engine. It has fast user switching, which allows for swapping between users without the necessity of user logouts. iChat was updated to allow video chatting. The Safari browser was introduced and File Vault was introduced. File Vault permits the user to encrypt their home folder. Font Book, a font manager, was included in this version as well.

2.1.5 Tiger (OS X.4)

Tiger introduced updated versions of Mail and Spotlight. Automator, a batch processing creator, was introduced, which allows the user to string numerous commands together creating an automated process.

2.1.6 Leopard (OS X.5)

Leopard introduced Time Machine, an incremental and full system backup. It also includes Spaces, which allows for virtual desktops. Spotlight was again updated. Quick Look was introduced; this allows for previewing the contents of a file without opening it. Boot Camp was introduced. Boot Camp allows a user to install another operating system alongside the Mac OS.

2.1.7 Snow Leopard (OS X.6)

Snow Leopard introduced 64-bit computing. Most operating system enhancements were speed related. Snow Leopard includes Quick Time 10, which was formerly Quick Time Pro.

2.1.8 Lion (OS X.7)

Lion supported full disk encryption utilizing File Vault. Mission Control replaced the "All Windows Expose" feature and gave an overview of all running applications. The user experience became more iOS-like. Lion introduced the Mac App Store and Apps, which were full screen applications. It introduced Launch Pad, which displayed an iOS-like grid of installed applications. Users can make multiple pages and group applications into folders, similar to iOS. Multi-Touch gestures were supported using a touch-enabled input device.

2.1.9 Mountain Lion (OS X.8)

The Mountain Lion interface was designed to emulate features of the iPhone and therefore includes integration of iCloud services. iChat was replaced by Messages; Messages supports the iMessage service, which is currently used on iPhones. Documents in iWork can be synched to the user's iCloud account. Time Machine can create rotating backups on more than one medium.

3. Imaging Macintosh Computers

3.1 Boot Options

3.1.1 Press and hold "C" during start up: boots from a CD, DVD, or USB drive

3.1.2 Press and hold "D" during start up: starts up in Apple Hardware Test (a suite of diagnostics that will test the computer's hardware)

3.1.3 Press and hold "Option-Command-P-R" until the startup sound occurs a second time: resets the NVRAM (resets hardware settings to factory default)

3.1.4 Press and hold "Option" during start up: starts up in Start Up Manager where the user can select a volume from which to boot (volumes will be displayed with icons and volume names; note that Linux volumes will appear as Windows volumes)

3.1.5 Press and hold "Eject", "F12", or hold the mouse/track pad button: ejects any removable media

3.1.6 Press and hold "N" during start up: attempts to start up from a compatible network server (NetBoot)

3.1.7 Press and hold "T" during start up: starts up in Target Disk Mode (only for FireWire/Thunderbolt capable equipment)

3.1.8 Press and hold "Shift" during start up: starts up in Safe Boot Mode and temporarily disables login items (displays only required kernel extensions and disables many functions such as the DVD player and USB support; mostly used for operating system repairs)

3.1.9 Press and hold "Command-V" during start up: starts up in Verbose Mode (only used for troubleshooting start up problems)

3.1.10 Press and hold "Command-S" during start up: starts up in Single User Mode (command line only; can be used to obtain the computer's date and time by typing "date" with no quotation marks)

3.1.11 Press and hold "Option-N" during start up: starts up from NetBoot Server using the default boot image

3.1.12 Press and hold "Command-R" during start up: starts from Lion Recovery

3.1.13 Press and hold "X" during start up: starts from Mac OS X partition by default and bypasses any other partitions

3.2 Suggested Boot Order to Determine System Configuration

Boot the system by holding the Option key to determine:

- If a BootCamp partition exists.
- If there is a firmware password installed.

If no firmware password or BootCamp partition exists, continue with the imaging process options described below.

If a firmware password exists, the examiner must either remove the firmware password or remove the hard drive for imaging.

If a Windows-based examination machine is used to image a Mac that contains a BootCamp partition while booted in Target Disk Mode, the OS will mount the partition, thus writing to it. If the examiner encounters this configuration and fails to use a hardware write blocking method, Windows will write a \RECYCLER or \$RECYCLE.BIN folder to the NTFS or FAT partition of the source media.

3.3 Media Imaging

3.3.1 Remove hard drive for imaging

Utilize imaging hardware or software to acquire the drive's content. See *SWGDE Best Practices for Computer Forensics V3* for more information.

Considerations:

- Not every device has an easily-accessible hard drive.
- MacBook Airs may contain a hard drive, a solid state drive, or NAND flash.
- If there are multiple hard drives present, there may be a hardware or software RAID.

3.3.2 Boot to forensically sound boot media (CD/DVD or USB)

Attach an external target drive to the suspect system and hold down the "C" key to boot from forensically sound media for acquisition.

Considerations:

- Not all forensic boot media are capable of booting a Mac computer.
- Not all Macs have optical media drives.
- Boot media must match the OS X processor version.
- If a Boot Camp partition has a Windows operating system installed, there is the possibility that the Windows operating system will boot rather than the forensically sound boot media.

3.3.3 Boot into Target Disk Mode (TDM)

Start the suspect computer by holding down the "T" key during the boot sequence. Upon entering Target Disk Mode, attach an examination computer to the suspect system via the FireWire or Thunderbolt port.

Considerations:

- Target Disk Mode is *not* write protected, so a write blocker may be necessary. Target Disk Mode essentially allows a user to see the computer as a mass storage device. Data ***can*** be written to disks while in Target Disk Mode.
- Not all Mac computers can be placed in Target Disk Mode. Target Disk Mode requires either a Firewire or Thunderbolt interface, which not all Mac computers have. See http://support.apple.com/kb/HT1661 for a current list of Target Disk Mode capable systems.
- For all legacy PATA based Macs, Target Disk Mode will only show the examiner the master hard drive.

4. Analyzing Macintosh Computers

4.1 Aspects Unique to Mac Computers

4.1.1 File System

Macintosh computers can use the UFS, FAT, exFAT, HFS, HFS+, or HFSX 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.

The HFS file system generally does not use file fragmentation; most files occupy contiguous sectors. This results in ease of file carving but difficulty in deleted file recovery after a certain point.

Files in 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 out as a hidden file or lost entirely.

4.1.2 System Date and Time

Macintosh computers do not contain a BIOS as Windows systems do. The system date and time can be obtained by booting the computer into Single User Mode (Holding down the "S" key at boot time) and typing the **date** command at the command prompt.

4.1.3 Plists versus Registry Files

Unlike the Registry found on Windows machines, Mac OS and applications store user and system configuration data in various plist files across the drive. The contents of plist files can be binary, ASCII data, or XML. Viewers exist to examine binary plist information on a Windows machine.

4.2 Default Applications of Potential Forensic Interest

4.2.1 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.

4.2.2 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. The associated plist file is located in:

/Users/<User Name>/Library/Preferences/com.apple.appstore.plist

4.2.3 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.

4.2.4 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 suspect media to avoid making writes.

4.2.5 FaceTime

FaceTime is a video calling application that includes a text-based chat function. It was 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.

4.2.6 FileVault

Prior to Mac OS X Lion, FileVault encrypted the user's home directory.

Beginning with Mac OS X Lion, FileVault 2 encrypts the entire volume rather than just the user's home directory.

It must be turned on by the user and utilizes AES-128 bit encryption. The type of file produced by the encryption varies by Mac OS X version:

- Mac OS X Tiger: Encrypted data is placed into a flat file called a sparse image. The home folder is encrypted when the user logs out or shuts down the system.
- Mac OS X Leopard and Snow Leopard: Encrypted data is placed into a sparse bundle. This file contains a folder structure within it. Sparse bundles break images into smaller 8MB files called bands. The home folder is encrypted when the user logs out or shuts down the system.
- Beginning with Mac OS X Lion the entire volume is encrypted. If the Mac has multiple user accounts, FileVault 2 will ask which accounts are authorized to encrypt the volume. Each user can decrypt the volume using an encryption key stored in the user's Keychain. The user can store his/her recovery key with Apple.

4.2.7 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.

4.2.8 iCal / Calendar

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

4.2.9 iChat / Messages

iChat (renamed Messages in OS X 10.8) is an instant messaging application that supports audio, video, and screen-sharing capabilities. iChat was an AIM client built into Mac OS X.

iChat/Messages logs are found in the user's /Documents folder. Examiners may be able to recover account configuration information, recent chats, files transferred, saved chat transcripts, and SMS messages from the com.apple.iChat.plist file.

4.2.10 iPhoto

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.

The default location for the iPhoto Library is located in:

/Users/<User Name>/Pictures/iPhoto Library

4.2.11 iTunes

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.

The default location of the iTunes library is located in: /Users/<User Name>/Music/iTunes/

The associated plist file is located in:

/Users/<User Name>/Library/Preferences/com.apple.iTunes.plist

4.2.12 Image Capture

Image Capture is an application that enables users to upload pictures from digital cameras or scanners that are either connected directly to the computer or connected to the network. The associated plist file is located in:

/Users/<User Name>/Library/Preferences/com.apple.Image_Capture.plist

4.2.13 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.

sers 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.

4.2.14 Mail

Examiners may be able to recover stored email messages and recently used email addresses (both recipient and sender) in the Mail application.

The file com.apple.mail.plist contains information regarding accounts, user names, associated full names, and email port numbers.

The file searchhistory.plist contains information regarding keyword searches used within the Mail client. It also contains the date and time that the searches were conducted.

4.2.15 Photobooth

An application that uses the computer's built in camera to take video or still pictures which the user can manipulate. The images are stored in the user's /Pictures/Photobooth folder. The associated plist file is located in:

/Users/<User Name>/Library/Preferences/com.apple.PhotoBooth.plist

4.2.16 Preview

The default file viewer in Finder for image files and .pdf documents. It includes some basic editing features for image files.

Preview retains a history of recently opened files and user-created bookmarks at:

/Users/<User Name>/Library/Preferences/com.apple.Preview.LSSharedFileList.plist.

4.2.17 QuickTime

A proprietary multimedia player capable of playing audio, video, and image files. It can create video files using the computer's webcam or screen recordings. A list of recently played files is contained at:

/Users/<User Name>/Library/Preferences/com.apple.QuickTimePlayerX.LSSharedFileList.plist.

4.2.18 Apple Remote Desktop

Apple Remote Desktop (ARD) is installed by default starting with Mac OS X Leopard. It allows users to remotely control or monitor other computers over a network.

The file: /Library/Preferences/com.apple.RemoteDesktop.plist contains MAC addresses, date of last connection, remote system serial number, remote system machine type (including operating system version and number), and IP addresses.

4.2.19 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.

Safari v2: Cache files are swap files contained in numbered folders. They will show date, time, and URL information for the cache file as well as a preview of the webpage.

Safari v3: All data is in a SQLite database found under the user's /Library/Safari or /Library/Caches folders. There are several .plist files of interest contained in these folders, including: bookmarks.plist, downloads.plist, history.plist, lastsession.plist, and topsite.plist.

Safari v4: This version incorporates coverflow to view the top sites, which are still recorded in the topsites.plist file. The user's /Library/Caches/Metadata/Safari/History folder contains internet history files with the file extension .webhistory. Also in this folder are bookmark files with the file extension .webbookmark.

The file cache.db, located in the user's /Library/Caches/com.apple.safari folder, is a SQLite database containing a list of internet history. It keeps screenshots of webpages visited by the user.

The file com.apple.safari.plist contains recent internet searches.

Safari v5: The file cache.db, located in the user's /Library/Caches/com.apple.safari folder, is a SQLite database containing a list of internet history.

The user's "/Library/Caches/com.apple.safari/Webpage Previews" folder contains .jpg files of previously-viewed webpages. The content of this folder is maintained even when the cache is cleared.

4.2.20 Spotlight

Spotlight is a system-wide desktop search feature that 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.

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.

4.2.21 Stickies and Notes

Stickies is an application for putting user-created notes on the screen. Stickies keep all information in the user's Users/<User Name>/Library/StickiesDatabase folder and are stored in a Rich Text format.

Notes is a notepad application that allows the user to save notes as files. Notes content can be synced with iPods, iPads, and iPhones. The notes are stored in the following folder location: /Users/<User Name>/Library/Containers/com.apple.Notes/Data/Library/Notes/NotesV1.storedata-wal

4.2.22 Time Machine

A backup utility 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 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.

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.

4.3 Folders of Potential Forensic Interest

4.3.1 Visible on Root

The default visible subfolders at the drive's root level are: /Applications, /Library, /System, /Network and /Users.

4.3.1.1 /Applications

This folder contains all installed applications.

4.3.1.2 /Library

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

4.3.1.3 /System

This folder contains the operating system. It also contains system start up items, display settings, and fonts.

4.3.2 Hidden Subfolders on the Root

The default hidden subfolders at the drive's root level of possible interest are: /.Trash or /.Trashes, /Volumes, /Temp, /var/tmp and, /.MobileBackups.

4.3.2.1 /.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/<User Name>/.Trashes - user specific Trash for items deleted by user on local system

4.3.2.2 /Volumes

This subfolder is the mount point for all attached volumes.

4.3.2.3 /Temp

This subfolder contains temporary files. Programs store temporary data at /var/tmp.

4.3.2.4 /var/vm

This subfolder contains the swap file and sleepimage. A sleepimage is much like a hibernation file on a Windows computer and is located in: /private/var/vm/sleepimage

4.3.2.5 /var/log

This folder contains a variety of logs. These include logs with detailed information about files that have been printed, installer logs, email logs, system logs (system events), and the disk utility log.

4.3.3 /User

A directory is created for each user. Most applications store user-specific data in this directory. The .plist files within the User folder often contain user preferences and settings. This directory can contain the user's documents, movies, music, pictures, downloads, and desktop files.

4.3.3.1 Default file paths of possible interest within the User folder include:

/Users/<User Name>/Applications/

/Users/<User Name>/Desktop/

/Users/<User Name>/Documents/

/Users/<User Name>/Downloads/

/Users/<User Name>/Library/

/Users/<User Name>/Movies/

/Users/<User Name>/Music/

/Users/<User Name>/Pictures/

/Users/<User Name>/Public/

/Users/<User Name>/Sites/

4.3.3.2 The /Users/<User Name>/Library folder contains internet history, webpage cache, email remnants, application history, application log files, and other files of possible interest.

4.3.3.3 In Snow Leopard, the /Users/<User Name>/Library/Mail/Mailboxes folder contains .emlx files. In Lion, the /Users/<User Name>/Library/Mail/V2/Mailboxes folder contains .emlx files.

4.3.3.5 The "/Users/<User Name>/Library/Images/iChat/Recent Pictures" folder contains the user's iChat profile pictures.

4.3.3.6 The /Users/<User Name>/Library/Safari folder contains .plist files for internet bookmarks, internet download history, and internet browsing history.

4.3.3.7 The /Users/<User Name>/Library/Caches/com.apple.Safari/Cache.db contains data from visited websites. In some versions of Safari, "/Users/<User Name>/Library/Caches/com.apple.Safari/Webpage Preview" contains images of visited websites.

4.3.4 Other artifacts which may be of interest during the forensic analysis.

4.3.4.1 Operating System Installation Date

/private/var/log/OSInstall.custom (OS X 10.5)

/private/var/db/.AppleSetupDone (OS X 10.6 and later) this file also contains the registration info entered by the user during initial setup

4.3.4.2 Operating System Version

/System/Library/CoreServices/SystemVersion.plist (OS X Client)

/System/Library/CoreServices/ServerVersion.plist (OS X Server) - not used with OS X 10.7 and later

4.3.4.3 Software Installation

/Library/Receipts/InstallHistory.plist - history of installed applications and updates

/Library/Preferences/com.apple.SoftwareUpdate.plist - last software update

4.3.4.4 Current Time Zone

/etc/localtime (link file pointing to current time zone)

/Library/Preferences/.GlobalPreferences.plist

4.3.4.5 Auto-Login and Last Login User Info

/Library/Preferences/com.apple.loginwindow.plist

/private/etc/kcpassword - auto-login password

4.3.4.6 Printing

/private/var/spool/cups - completed and unfinished print jobs (print system uses PDF files)

4.3.4.7 Deleted Users

/Library/Preferences/com.apple.preferences.accounts.plist

4.3.4.8 Attached Media

/Users/<User Name>/Library/Preferences/com.apple.sidebarlists.plist - history of attached media, volumes devices, etc.

4.3.4.9 Email

/Users/<User Name>/Library/Mail

/Users/<User Name>/Library/Mail Downloads

4.3.4.10 iPhone/iPod

/Users/<User Name>/Library/Application Support/MobileSync/Backup - folder where iPhone, iPod Touch and iPad sync their data

/Users/<User Name>/Library/Application Support/MobileSync/Backup/*UUID*/Info.plist - contains info on the exact device synced (Backup), modified date of this file is the last time it was synced

/Users/<User Name>/Library/Preferences/com.apple.iPod.plist - all iOS and iPod devices connected for this account, includes iOS version , IMEI, etc.

4.3.4.11 User Auto-Launch Items

/Users/<User Name>/Library/Preferences/loginwindow.plist

4.3.4.12 Network Settings

/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

/Library/Preferences/SystemConfiguration/NetworkInterfaces.plist - Available network interfaces including MAC address on OS X 10.8

/Library/Preferences/SystemConfiguration/com.apple.NetworkInterfaces.plist - Available network interfaces including MAC address

/Library/Preferences/SystemConfiguration/com.apple.preferences.plist - Network Configuration for each interface (not on OS X 10.8)

/Library/Preferences/SystemConfiguration/preferences.plist - network interface configuration and Back To My Mac information

4.3.4.13 User Configuration

/Users/<User Name>/Library/Preferences/com.apple.finder.plist - Recent searches, Trash setting, view settings, recent folders

/Users/<User Name>/Library/Preferences/com.apple.dock.plist - Applications in the Dock

/Users/<User Name>/Library/Preferences/.com.apple.dock.db - folders and network shares in the Dock

/Users/<User Name>/Library/Preferences/com.apple.desktop.plist - Desktop picture

/Users/<User Name>/Library/Preferences/com.apple.recentitems.plist - recent documents, applications, and network connections

4.3.4.14 Screen Sharing

/Users/<User Name>/Library/Application Support/Screen Sharing

4.3.4.15 Bluetooth History

/Library/Preferences/com.apple.Bluetooth.plist

4.3.4.16 Instant Messaging

/Library/Preferences/com.apple.iChat.AIM.plist

/Library/Preferences/com.apple.iChat.plist

/Library/Preferences/com.apple.iChat.SubNet.plist

/Users/<User Name>/Library/Preferences/com.aol.aim.plist

/Users/<User Name>/Library/Preferences/com.adiumX.adiumX.plist

/Users/<User Name>/Library/Preferences/com.apple.iChat.AIM.plist

/Users/<User Name>/Library/Preferences/com.apple.iChat.plist

/Users/<User Name>/Library/Preferences/com.apple.SubNet.plist

/Users/<User Name>/Library/Preferences/com.skype.skype.plist

/Users/<User Name>/Library/Preferences/com.yahoo.messenger3.plist

/Users/<User Name>/Library/Preferences/com.yahoo.messenger3.Users.*screenname*.plist

/Users/<User Name>/Documents/iChat - default save location for iChat and Messages application

/Users/<User Name>/Library/Messages - database for Messages app

4.3.4.17 iCloud

/Users/<User Name>/Library/Mobile Documents - sync of “Documents and Data” feature of iCloud

4.3.4.18 Virtual Memory

/private/var/vm/swapfile0

5. References

www.appleexaminer.com

support.apple.com

www.blackbagtech.com/resources.html

Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit - Syngress Press (ISBN 1597492973)

SWGDE Mac OS X Tech Notes

History

Revision	Issue Date	Section	History
1.0	09/13/2013	All	Completed drafting document; voted to release as a Draft for Public Comment
1.0	09/14/2013	All	Formatted and released as a Draft for Public Comment