

Macintosh System Artifacts

.bash_history This file maintains a set of commands entered in the terminal by the user	Root of /Users Home Directory
Attached Media	<i>/username/Library/Preferences/com.apple.sidebarlists.plist</i>
Bluetooth devices	<i>/username/Library/Preferences/com.apple.Bluetooth.plist</i>
Calendar Events User's iCal calendar events	<i>/Username/Library/Calendars/GUID/Events</i>
Custom Menus List of the custom "menus" installed by the user. Shows what runs when a user logs in.	<i>/username/Library/Preferences/com.apple.systemuiserver.plist</i>
Documents Directory	<i>/Username/Documents</i>
Entourage Database User is using Microsoft Office for Mac, and is using Entourage as the email client	<i>/username/Documents/Microsoft User Data/Office 2008 Identities/Main Identity/Database</i>
Entourage Mail Contacts	<i>/username/Library/Caches/Metadata/Microsoft/Entourage/2008/Main Identity/Contacts/0T/0B/0M/0K</i>
Entourage Mail Messages	<i>/username/Library/Caches/Metadata/Microsoft/Entourage/2008/MainIdentity/Messages/0T/0B/0M/0K/</i>
Home Directory	<i>/Users/Username</i>
iPhoto Library Modified version of photos	<i>/username/Pictures/iPhoto Library/Modified</i>
iPhoto Library Original version of photos	<i>/username/Pictures/iPhoto Library/Originals</i>
Login – Auto Login	<i>/Library/Preferences/com.apple.loginwindow.plist</i>
Login – Login Items List of applications that	<i>/username/Library/Preferences/com.apple.loginitems.plist</i>

Macintosh System Artifacts

automatically start when the user is logged in	
Logs – System	<p><i>/var/log</i></p> <p><i>/cups/access_log</i> - Printer Connection Information</p> <p><i>/cups/error_log</i> - Printer Connection Information</p> <p><i>/daily.out</i> - Network Interface History</p> <p><i>/samba/log.nmbd</i> - Samba (Windows based system) connection information</p>
Logs - User	<p><i>/username/Library/Logs/</i></p> <p><i>/DiscRecording.log</i> - Log of CD or DVD media burned using the Finder.</p> <p><i>/DiskUtility.log</i> - Log of CD or DVD media burned using the Finder, mount and unmount history of ISO or DMG image files, Permission Repair history. and hard disk partition information.</p> <p><i>/iChatConnectionErrors</i> - Log files here contain information of past iChat connection attempts. Data such as username, IP address, and Date&Time of the attempt</p> <p><i>/Sync</i> - Log files here will contain information on .Mac syncing, mobile devices such as iPods and cell phones, and Date&Time of the activities</p>
Mail.app Information on Mail.app setup including account names and where the email is stored locally	<i>/username/Library/Preferences/com.apple.mail.plist</i>
Network Information	<i>/Library/Preferences/com.apple.network.identification.plist</i>
Network Lookups Lookups, Whois, Ping and Port Scans	<i>/username/Library/Preferences/com.apple.NetworkUtility.plist.</i>
Photo Booth Photos captured with Webcam	<i>/username/Pictures/Photo Booth</i>
Pictures Directory	<i>/Username/Pictures</i>
Printers	<i>/username/Library/Preferences/com.apple.print.PrintCenter.plist</i>
Programs Directory	<i>/Applications</i>
Public Directory	<i>/username/Public</i>

Macintosh System Artifacts

If file sharing is enabled via any protocol, sharing is enabled on the Public directory	
Quicktime Recently Viewed Movie Files	/username/Library/Preferences/com.apple.quicktimeplayer.plist
Recent Items The 10 most recently run applications, connected server information, and documents recently accessed by the user	/Username/Library/Preferences/com.apple.recentitems.plist
Recently Opened Recently opened folders Last server connection from Finder Last "Go to Folder" selection	/Username/Library/Preferences/com.apple.finder.plist
Swap File	/private/var/vm
System Install Date Completion time	/private/var/log/OSInstall.custom
System Registration	/Username/Library/Assistants/Send Registration.setup
System Version	/System/Library/CoreServices/SystemVersion.plist
Trash Files moved to the trash by the logged on user	/username/.Trash
USB Devices Search for - kernel[0]: USBMSC Identifier	/var/log/kernel.log
User Contacts	/Username/Library/Preferences/AddressBookMe.plist
User Identification Examination of plists will show generateduid for user identification	/private/var/db/dslocal/nodes/Default/users
User Logon Information	/private/var/db/shadow/hash

Macintosh System Artifacts

<ul style="list-style-type: none">• Last logon date• Failed logons• Account creation date	GUID file with .state extension
User Logon Password Hash	/private/var/db/shadow/hash GUID file with no extension
Volumes information about all volumes mounted on the computer	/username/Library/Preferences/ByHost/com.apple.systempreferences/0017f2c9b67f.plist (Hex name will be different – this is the MAC address of the computer’s Ethernet adapter)
Wireless Networks	/Library/Preferences/com.apple.airport.preferences.plist

Safari Artifacts

Bookmarks	/username/Library/Safari/Bookmarks.plist
Bookmarks Backup	/username/Library/Caches/Metadata/Safari/Bookmarks
Browsing History	/username/Library/Safari/History.plist
Browsing History Backup	/username/Library/Caches/Metadata/Safari/History
Cache	/username/Library/Caches/com.apple.Safari/cache.db/tables/ cfurl_cache_blob_data (Expand to show Blob Data)
Cache URL Response	/username/Library/Caches/com.apple.Safari/cache.db/tables/ cfurl_cache_response (View HTML file)
Cookies	/username/Library/Cookies/Cookies.plist
Downloads History	/username/Library/Safari/Downloads.plist
Home Directory	/username/Library/Safari
Last Session	/username/Library/Safari/LastSession.plist
Preferences	/username/Library/Preferences/com.apple.Safari.plist

Firefox Artifacts

Bookmarks and Form History	/username/Library/Application Support/Firefox/ Profiles/ abcdef7g.default/formhistory.sqlite/tables/moz_formhistory (Profiles default directory name is randomly generated for each user)(View HTML file)
Bookmarks Backup	/username/Library/Application Support/Firefox/ Profiles/ abcdef7g.default/bookmarkbackup (Profiles default directory name is randomly generated for each user) (View files named bookmarks-yyyy-mm-dd.json)
Browsing History	/username/Library/Application Support/Firefox/ Profiles/ abcdef7g.default/places.sqlite/tables/moz_history (Profiles default directory name is randomly generated for each user)(View HTML file)
Cache	/username/Library/Application Support/Firefox/ Profiles/ abcdef7g.default/Cache (Profiles default directory name is randomly generated for each user)
Cookies	/username/Library/Application Support/Firefox/ Profiles/ abcdef7g.default/Cookies.sqlite/tables/moz_cookies (Profiles default directory name is randomly generated for each user)(View HTML file)
Downloads History	/username/Library/Application Support/Firefox/ Profiles/ abcdef7g.default/downloads.sqlite/tables/moz_downloads (Profiles default directory name is randomly generated for each user)(View HTML file)
Home Directory	/username/Library/Application Support/Firefox/Profiles/ abcdef7g.default
Stored Passwords	/username/Library/Application Support/Firefox/ Profiles/ abcdef7g.default signons3.txt file

Google Chrome Artifacts

Chrome Directory	/username/Library/ Application Support/Google/Chrome/
Chrome Cache	/Username/Library/Caches/com.google.Chrome/
Preferences	/username/Library/Preferences/com.google.Chrome.plist

VirtualBox Artifacts

VirtualBox Directory	/username/Library/VirtualBox/
VirtualBox Settings Contains information about recently run virtual machines	/username/Library/VirtualBox/VirtualBox.xml
VirtualBox Log File	/username/Library/VirtualBox/VBoxSVC.log
VirtualBox VM Directory	/username/VirtualBox VMs

Drop Box Artifacts

Drop Box Cache Folder	/username/Library/Caches/com.getdropbox.dropbox
Drop Box Config Database Information, such as Drop Box directory path and user email account	/username/.dropbox/Config.db
Drop Box Config Folder	/username/.dropbox
Drop Box File Cache Information about files stored in Drop Box directory.	/username/.dropbox/filecache.db
Shared Folder	/username/Dropbox

iChat Artifacts

Account Settings	/username/Library/Preferences/com.apple.ichat.plist
Saved Chats If chats are saved, they will be in directories named with the date of the chat Flag 1 – Incoming message Flag 5 – Outgoing message	/username/Documents/iChat
User Chat Picture	/username/Library/Caches/com.apple.iChat/Pictures/ PictureNameMap.plist

Apple Mail Artifacts

Mail Directory	/username/Library/mail
POP3 Mail Boxes	/username/Library/mail/pop.username@mailaddress.com
IMAP Mail Boxes	/username/Library/mail/Mailboxes

iPod Artifacts

Cache	/username/Pictures/iPhoto Library/iPod Photo Cache (Photos will have .ithmb extension. Photos needed converted using a program such as iThmbConv)
Syncing Clients	/username/Library/Application Support/SyncServices/Local/ Syncingclients.plist
History of iPhone and iPod Connectivity	/Library/Preferences/com.apple.iPod.plist
History of iPhone and iPod Connectivity for specifi user	/username/Library/Preferences/com.apple.iPod.plist

iPhone Backup Artifacts

Account Settings	<i>/username/Library/Application Support/MobileSync/Backup/GUID/Info.plist</i>
Address Book Contact Icons	<i>/username/Library/Application Support/MobileSync/Backup/GUID/cd6702cea29fe89cf280a76794405adb17f9a0ee.mddata/ABIImage/Blobs</i>
Address Book Information	<i>/username/Library/Application Support/MobileSync/Backup/GUID/31bb7ba8914766d4ba40d6dfb6113c8b614be442.mddata/ABPerson (Select HTML file)</i>
Backup Directory (MAC)	<i>/username/Library/Application Support/MobileSync/Backup/GUID</i>
Backup Directory (Windows)	<i>\Documents and Settings\username\Application Data\Apple Computer\Mobile Sync\Backup</i>
Calendar Information	<i>/username/Library/Application Support/MobileSync/Backup/GUID/2041457d5fe04d39d0ab481178355df6781e6858.mddata/_SqliteDatabaseProperties (Select HTML file)</i>
Call Log	<i>/username/Library/Application Support/MobileSync/Backup/GUID/ff1324e6b949111b2fb449ecddb50c89c3699a78.mddata/Call (Select HTML file)</i>
Notes	<i>/username/Library/Application Support/MobileSync/Backup/GUID/740b7eaf93d6ea5d305e88bb349c8e9643f48c3b.mddata/Note (Select HTML file)</i>
Text Messages <ul style="list-style-type: none"> • 2 – External Number • 3 – Local Number 	<i>/username/Library/Application Support/MobileSync/Backup/GUID/3d0d7e5fb2ce288813306e4d4636395e047a3d28.mddata/Group_member (Select HTML file)</i>
Voice Mail Log	<i>/username/Library/Application Support/MobileSync/Backup/GUID/992df473bbb9e132f4b3b6e4d33f72171e97bc7a.mddata/Voicemail (Select HTML file)</i>
Other Property Lists	Overview Tab > File Category > Other Known Types > Property List File
Address Book Listings	<i>b64e73540b6221bffc16b18f2205e1335e31d7d8.mddata</i>
Email Account Usage	<i>5fd03a33c2a31106503589573045150c740721dd.mddata</i>

Macintosh System Artifacts

Last Number Dialed	fb7786ced1add24313fa258c8e1ed041e24d52a4.mddata
Map Directions	b60c382887dfa562166f099f24797e55c12a94e4.mddata
Map Pin Drop	b88b75bddaa69139b66d948b7cbd4f41d9dd416d.mddata
Map Searches	a30335a2c0f0316c9610d868a527b2ade1911542.mddata
Purchase Information	3b2f19b7d02788a824d3d1f7b9ba5e4c7108485c.mddata
Safari Browsing History Lowest number is most recent	1d6740792a2b845f4c1e6220c43906d7f0afe8ab.mddata
Safari Cookies	1dd07f2fbb1169bed93c21047ca5616371ea4a04.mddata
Safari Searches	bd38afa30b5a43c146db02a46ee11d82cdc817fe.mddata
Safari Web Pages	9281049ff1d27f1129c0bd17a95c863350e6f5a2.mddata
Voice Mail	Conduct a search for files with header 23-21-41-4D-52-0A Files must be exported from case and renamed with .amr extension Use program such as AMR Player to listen to voice mails
Wireless Networks	34f7f8423d8f77bc812dd8d70f84c33a5caacbe8.mddata