SUMURI

Best Practices Guide

P.O. Box 121 Magnolia, Delaware 19962, USA • hello@sumuri.com • +1 302.570.0015 • www.sumuri.com

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

Disclaimer: Before using any new procedure, hardware, or software for forensics, examiners must do their own validation and testing before working on real evidence.

This Best Practice Guide is summarized from **SUMURI's Macintosh Forensic Survival Courses (MFSC),** which are **vendor-neutral** training courses taught to law enforcement, government, and corporate examiners worldwide.

More information about SUMURI can be found at **SUMURI.com.**

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

Why Use a Mac for Forensic Analysis?

Until the release of SUMURI's RECON LAB (our fully featured forensic suite), no other forensic tool has properly parsed or utilized the correct timestamps for macOS. This indicates that every Mac exam completed using any other forensic tool since 2005 has used timestamps that the Mac ignores.

This is only one example of improperly interpreting or missing an extremely important artifact entirely by other forensic tools.

It is imperative to understand the importance of using macOS in forensic exams and possible missed data using non-native solutions.

Apple Extended Attributes

Most examiners are familiar with metadata, such as EXIF information, found in pictures and videos. Apple Extended Attributes are special metadata created only within macOS to search for the macOS search utility, Spotlight.

Apple Extended Attributes contain extremely valuable information for investigations, and Windows cannot see this special metadata. Most Windows forensic tools ignore or have a limited ability to display Apple Extended Attributes as they cannot natively support them. Those that show some Apple Extended are using an open-source solution based on reverse engineering.

The purpose of Apple Extended Attributes is to help examiners find files, not the other way around. Reversed engineered, non-native solutions implemented in non-Mac native forensic tools require the examiner to find a file first then ask for the Apple Extended Attributes. Using a Mac-native or a forensic solution developed natively on a Mac, use Mac-native libraries to overcome these limitations.

Additionally, not all "Mac" forensic tools have been developed natively on the Mac. Most of these forensic tools were ported from Windows or Linux applications, including the same limitations of forensic tools when running on Windows and Linux.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

Images and data collected by SUMURI's RECON ITR and processed by RECON LAB provide the most extensive views of Apple Extended Metadata in addition to viewing natively with a Mac.

Understanding Apple Extended Metadata is critical to investigations.

Viewing Proper Timestamps

Apple's macOS utilizes Apple Extended Attributes timestamps in favor of its POSIX (Unix) timestamps. It is easier for most forensic tools to extract the Unix timestamps from Mac's Catalog File. As stated previously, these are not the timestamps that Apple utilizes. MacOS uses Apple Extended Metadata timestamps. Examples of these timestamps include download dates and when a human opened a file instead of a system event.

Both RECON ITR and RECON LAB, being natively designed on a Mac, allow the examiner to process and use Apple Extended Metadata timestamps in the analysis.

Viewing Files Natively

There are many file types and artifacts proprietary to macOS.

For example, Applications in macOS are actually "bundle" files. Everything needed for the application to run is found within the bundle file. What looks and appears to a single file to the Mac user is thousands of innocuous files and folders. These bundle files are expanded in traditional forensic tools, adding tens of thousands of unnecessary artifacts to your case.

Additionally, macOS's Quick Look natively supports viewing hundreds of file types without requiring the original application to be installed.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

Apple File System (APFS)

Apple File System (APFS) is a proprietary file system from Apple and is utilized for macOS, iOS, watchOS, and tvOS. APFS is natively and fully supported on macOS High Sierra (10.13) and above. APFS has no native support within Windows operating systems or forensic tools. Any support for APFS on Windows or Windows forensic tools requires reverse engineering using non-native technologies. These solutions found in non-native tools and environments range from no support at all to limited support.

Using macOS to work with its file systems (such as APFS) is logical as it will always be supported 100% of the time natively.

Local Time Machine Snapshots (APFS)

Time Machine is a utility in macOS used to create backups. Users must activate Time Machine and use a local or remote disk to store backups (the Time Machine disk). If the Time Machine disk is not available, the backups are stored locally to the computer. These "local" backups are known as "Local Time Machine Snapshots" in APFS and are referred to as APFS Snapshots.

An examiner should not expect to find Local Time Machine Snapshots in every case. They will only exist when the conditions described above have been met.

MacOS has in-built native solutions to identify and process Local Time Machine Snapshots which are not supported by any other operating system.

RECON IMAGER (included with RECON ITR) and RECON LAB are the only solutions that can display, image, hash, and analyze Local Time Machine Snapshots in Macs with or without T2 Security Chips or Apple Silicon.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

FileVault

FileVault (Version 2) is the macOS full volume encryption that does not have any backdoors. FileVault can be mounted and decrypted with the user's login password or Recovery Key (created when users initially enable FileVault).

Using native macOS tools, examiners can acquire decrypted images at the time of collection. Additionally, examiners can easily decrypt forensic images of Macs with FileVault at the time of processing when using macOS.

RECON LAB allows the examiner to decrypt the forensic image of a Mac encrypted with FileVault natively using either the password or Recovery Key.

Support for Other File Systems

Mac is based on UNIX, whose origins have existed since the late 1960s. Whatever the Mac can mount, it can process.

MacOS natively supports APFS, macOS Extended (HFS+), MS-DOS FAT, ExFAT, and NTFS (as read-only).

Using freely available open-source FUSE solutions or third-party Paragon Software drivers, just about any file system can be mounted and processed on a Mac, including Linux EXT2, EXT3, and EXT4.

Full versions of RECON LAB include Paragon Software's Mac ToolBox and extFS for Mac.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

Helpful Hints

Before starting a new case using a Mac, please refer to these helpful tips.

Use macOS Extended for Evidence Drives

MacOS can support various file systems; however, in testing, we find the best results using macOS Extended (HFS+) for the evidence drive.

If examiners want to mount a macOS Extended evidence drive within a Windows environment, consider using HFS+ for Windows drivers from Paragon Software. These drivers are provided to you if you purchase RECON LAB.

If examiners create logical images of Mac data to any non-Mac file system, they will lose critical Apple Extended Metadata.

Use Apple Disk Image Format (.dmg) for Imaging Evidence

Apple Disk Images (.dmg) created with RECON ITR or PALADIN are formatted as RAW image formats that can load into any forensic tool that supports RAW images. The Mac natively supports these .dmg images.

Although Expert Witness Formats (.E01, .Ex01) can be mounted on a Mac, the process requires the use of FUSE drivers. FUSE acts as an interpreter to mount non-native file systems. Using FUSE adds an unnecessary layer between the forensic image and the macOS, causing additional problems that can be avoided using the native .dmg format for forensic images.

Avoid Segmentation of Forensic Image Files

Depending on what method is used, the Mac can support segmented image files. However, with extremely large disk sizes found in modern devices, it is possible to create thousands of segments that may cause issues. If possible, avoid segmenting forensic images and use a single file instead.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

Step by Step - Mac Forensics

STEP ACTIONS	DESCRIPTION
STEP-1:	PRE-SEARCH INTELLIGENCE Find out as much as you can about your target: • Number and types of Macs (MacBook, iMac, or Mac Pro) • Operating System Version (for collecting/processing volatile data and Copy Over Procedure) • Type/s and the number of ports • Does it contain a T2 Security Chip with Secure Boot? • Does it contain an Apple Silicon processor? • Is FileVault Active? • Can passwords be obtained?
STEP-2:	ISOLATE Assign one trained Digital Evidence Collection Specialist to handle the electronic evidence to minimize contamination and the Chain of Custody. Prohibit anyone else from handling the devices.
STEP-3:	ALWAYS ASK FOR THE PASSWORD Most newer Macs have enhanced security features such as Apple Silicon, T2 Security Chips, APFS File Systems, Secure Boot, FileVault, and more. Anyone or a combination of these security features can stop you from getting the data. ALWAYS ASK FOR THE PASSWORD.
STEP-4:	IF COMPUTER IS ON - LOCK SCREEN ACTIVE Options are: • Ask for the Password - Confirm password and proceed to Step-6. • Restart to Image RAM - Connect a RAM Imaging Utility to the Mac such as RECON IMAGER. Conduct a soft-restart (do not power off if possible and image the RAM). **Note - This will not work with Macs with Apple Silicon and T2 Security Chips with Secure Boot enabled.**

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

STEP-4:	IF COMPUTER IS ON - LOCK SCREEN ACTIVE Options are: • Ask for the Password - Confirm password and proceed to Step-6. • Restart to Image RAM - Connect a RAM Imaging Utility to the Mac such as RECON IMAGER. Conduct a soft-restart (do not power off if possible and image the RAM). **Note - This will not work with Macs with Apple Silicon T2 Security Chips with Secure Boot enabled.**
STEP-5:	COMPUTER IS OFF Collect the computer using best practices for the collection of electronic evidence. Prepare for imaging (refer to Step-12).
STEP-6:	COMPUTER IS ON - DESKTOP IS ASSESSABLE - LOOK FOR DESTRUCTIVE PROCESSES Look for signs of destructive processes such as wiping utilities, erasing free space, etc. If destructive processes are running, options are: • Attempt to stop the destructive process. Use Force Quit, if possible (Command + Option/Alt + Esc keyboard combo).
STEP-7:	COMPUTER IS ON - DESKTOP IS ASSESSABLE - COLLECT VOLATILE INFORMATION Using a trusted and validated tool (not the source computer's tools), collect Volatile Data such as running processes, network connections, unsaved documents. RECON ITR has automated Volatile Data collection features.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

STEP-8:	COMPUTER IS ON - DESKTOP IS ASSESSABLE - CHECK FOR HIDDEN DESKTOPS OR RUNNING VIRTUAL MACHINES Check for running virtual machines and open files on other desktops (macOS supports up to 16). If a Virtual Machine is found running, use the VM software to “Save a snapshot” (keep in mind the will create a new file or could overwrite an existing snapshot). Treat the VM as a new computer following the best practices for responding to a live system for that OS.
STEP-9:	COMPUTER IS ON - DESKTOP IS ASSESSABLE - CHECK FOR ENCRYPTION When the user is logged in, data on any mounted encrypted volumes are accessible. Check to see if any of the mounted volumes are encrypted (Command + I). If encrypted, copy the data from the encrypted volumes to an HFS formatted volume to preserve metadata (can use “rsync” command) or Live Imaging built into RECON ITR. Using System Preferences -> Security and Privacy -> FileVault, check to see if FileVault is ON or OFF. If found ON, copy the data from the encrypted home directory to an HFS formatted volume to preserve metadata. RECON ITR includes Live Imaging and Triage tools to assist with this step.
STEP-10:	COMPUTER IS ON - DESKTOP IS ASSESSABLE - IMAGE RAM Image RAM using a tool that supports the running macOS version such as RECON ITR. ***Special Note - imaging Mac RAM can sometimes cause a kernel panic and requires the admin password. Make sure that you image Mac RAM last.***

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

STEP-12:	OBTAINING SYSTEM DATE AND TIME With the system OFF, power on the system holding down the Option/ALT key to check for the presence of a Firmware Password (boot level password). If you do not see a lock, power off the system by holding down the power key. If the Mac does not contain Apple Silicon or a T2 Security Chip, power on the system again, holding the (Command + S) keys. Once you see text, you can let go. This is Single User Mode. If the Mac does contain Apple Silicon or a T2 Security Chip, you will need the password to enter Single User Mode. At the command prompt, type: date Power off the system by holding down the power key until the system turns off.
STEP-13:	IMAGING macOS Extended (RECON IMAGER included with RECON ITR) Image the Mac by booting to RECON ITR USB. RECON ITR automatically interprets the Core Storage volume. Depending on your case, you can image the physical disks, individual volumes, or the derived Core Storage Volume. • DMG format - .dmg is recommended for mounting and processing on a Mac natively. The .dmg image made by RECON IMAGER is also a RAW image that can be imported into any forensic tool.
STEP-14:	IMAGING - FUSION DRIVE RECON IMAGER included with RECON ITR) Most tools see Fusion Drives as two separate drives (usually a combination of an SSD, spinning hard disk, or an additional SSD). RECON ITR will automatically interpret any synthesized file systems properly, which are derived from the two individual disk volumes.

STEP-15:	IMAGING (PALADIN) Image the Mac using PALADIN (non-T2 Security Chip Mac). • DMG format - .dmg is recommended for mounting and processing on a Mac natively. The .dmg image made by PALADIN is also a RAW image that can be imported into any forensic tool.
STEP-16:	IMAGING - FUSION DRIVE (PALADIN) Most tools see Fusion Drives as two separate drives (usually a combination of an SSD, spinning hard disk, or an additional SSD). Image both drives individually using PALADIN using a .dmg format. These images can be recombined on a Mac into a single volume. Remember to mount the SSD drive first. RECON LAB can automatically recombine Fusion drives that have been imaged separately.
STEP-17:	IMAGING - MACS WITH T2 SECURITY CHIP AND SECURE BOOT ENABLED Macs with T2 Security Chips have Secure Boot enabled, preventing booting from any external devices. To image Mac with Secure Boot enabled, put the source Mac into Target Disk Mode by holding down the “T” key on startup. Connect the source Mac to your forensic computer with the proper cable (ex. Thunderbolt) and boot your forensic computer with RECON ITR to image. Additionally, you can use RECON ITR running from the examiner’s Mac live. Use RECON ITR’s Disk Manager to disable Disk Arbitration, connect the source Mac in Target Disk Mode, open RECON IMAGER to image. Optionally, if you know the password, you can enter the Mac’s Recovery Mode and disable the Secure Boot and Booting from External Media to allow booting. Image the source Mac with the bootable version of RECON ITR.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

STEP-17:	IMAGING - MACS WITH AN APPLE SILICON PROCESSOR Newer Macs with Apple Silicon Processors will always require the administrator user password. Apple Silicon Macs cannot boot to external media and do not have Target Disk Mode. To image an Apple Silicon Mac, the examiner needs to log into an administrator account and image using any compatible commercial tool like RECON ITR's Live Imager. Apple Silicon Macs can also be attached to other Macs using the SMB connection available in Sharing Mode.
STEP-18:	MOUNTING FORENSIC IMAGE (DMG) - LOCK IMAGE Using (Command + l) "lock" the forensic image.
STEP-19:	MOUNTING FORENSIC IMAGE (DMG) - MOUNTING (SINGLE IMAGE) Locked forensic images on the Mac must be mounted using a shadow file. Example: hdiutil attach -noverify -noautofsck IMAGE.DMG -shadow
STEP-20:	MOUNTING FORENSIC IMAGE (DMG) - MOUNTING (FUSION DRIVE IMAGE) - NON-APFS The SSD drive must be mounted first. hdiutil attach -readonly -nomount -imagekey diskimage-class=CRawDiskImage /Volumes/DEST/SSD_FUSION/SSD_FUSION.dmg hdiutil attach -readonly -nomount -imagekey diskimage-class=CRawDiskImage /Volumes/DEST/PLATTER_FUSION/PLATTER_FUSION.dmg Once attached, use Disk Utility to check the mount. If the volume is gray, right-click and select mount.

hello@sumuri.com
+1 302.570.0015
helpdesk.sumuri.com
www.sumuri.com

STEP-21:	INDEXING To use Spotlight to search the forensic image, you must enable indexing of the mounted volume. Example: mdutil -i on replace_with_volume_name
STEP-22:	INDEX SEARCHES Navigate with the Finder to the directory or volume you would like to search. Begin searching using the Spotlight Search Bar in the Finder window (Command + F). Isolate the search to the directory you are interested in and use filters to find data.
STEP-23:	REPORTING OPTIONS - SCREEN CAPTURES • Full Screen Capture - (Command + Shift + 3) • Area Screen Capture - (Command + Shift + 4) • Window Screen Capture - (Command + Shift + 4 + Spacebar)
STEP-24:	REPORTING OPTIONS - PRINT TO PDF Use (Command + P) to print. Use the Option “Save to PDF.”

STEP-25:	REPORTING OPTIONS - COPY OVER PROCEDURE • It is recommended that you use the same version of macOS as the forensic image. This allows the user to view the data in a native format. • Create a new user account on your forensic Mac (needs to be an Admin user). • Copy out suspect Application artifacts to an external drive. • Switch to the new user account. Replace the new user Application data with the suspect's Application artifacts. • Launch each application of interest and document via PDF printing or screen captures. • When native reporting is complete, log out of the new user account and log into your forensic account. • Remove the new user account via System Preferences. You have the option to archive the new user account or delete it.