MAC FORENSICS BEST PRACTICES

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

SUMURI Mac Forensics Best Practices Guide

Disclaimer

This Best Practices Guide is provided as a professional reference for forensic examiners handling Apple macOS systems.

- Before applying any procedure to live evidence, **you must validate and test it within your own lab environment**.
- macOS security, hardware, and file systems evolve rapidly. Always confirm tool compatibility with the latest macOS and hardware (Intel, T2, and Apple Silicon).

This guide is based on **SUMURI's Macintosh Forensic Survival Courses (MFSC)** and ongoing real-world casework with law enforcement, government, and corporate examiners worldwide.

Why Use a Mac for Mac Forensics

Key reasons to use macOS for forensic analysis:

- **Apple Extended Metadata & Attributes**
    - Proprietary macOS data such as Spotlight indexes, quarantine flags, download origins, and "last opened by user" times remain invisible or incomplete in non-native tools.
    - Only **Mac-native tools**—developed using Apple's own frameworks—can parse these correctly.
    - RECON ITR and RECON LAB preserve this metadata fully, without relying on reverse engineering.

- **Timestamps That Matter**
    - In HFS+ (macOS Extended), forensic tools often extracted POSIX/Unix timestamps from catalog files, ignoring Apple's extended metadata.
    - With **APFS**, Apple changed how timestamps and extended metadata are stored—but the same **principle applies**: many third-party tools continue to expose only the easiest POSIX timestamps, not the rich context macOS itself uses.
    - Examples: true download times, quarantine events, and user-action "last opened" dates.
    - Without **Mac-native examination**, investigators risk misinterpreting or completely missing timeline evidence.
- **APFS and Proprietary Functionality**
    - **APFS is a proprietary, closed-source file system**. Apple has not disclosed all functionality or data structures.
    - Any tool claiming APFS support outside macOS is doing so through **reverse engineering**, which means incomplete or unreliable access.
    - By contrast, **a Mac examining a Mac**—or RECON ITR/RECON LAB built natively for macOS—ensures 100% access to APFS volumes without interpretation errors.
- **APFS Snapshots (Local Time Machine Snapshots)**
    - When a backup disk isn't present, APFS stores system snapshots locally. These are often overlooked by non-native tools.
    - Snapshots preserve past system states, giving investigators time-machine-like visibility into user activity. **Files deleted previously by the user may still be found in Local Time Machine snapshots, making them a critical artifact in many investigations.**
    - Only Mac-native tools, such as RECON ITR and RECON LAB, can properly identify, image, hash, and analyze these snapshots with confidence—no reverse engineering required.

- **Encryption (FileVault, Secure Enclave)**
    - With FileVault 2 and hardware-backed encryption on T2 and Apple Silicon, **passwords are critical**. Without them, physical imaging is impossible.
    - With proper credentials, RECON ITR acquires decrypted images; RECON LAB processes and analyzes them.

Bottom line: To get **100% of the data, accurately, and without guesswork**, you must use a Mac to examine a Mac. Anything else relies on incomplete reverse engineering of proprietary Apple technology.

Encryption & the Importance of Passwords

Encryption is the single most important factor in modern Mac examinations. With the introduction of FileVault 2, the T2 Security Chip, and Apple Silicon processors with the Secure Enclave, **passwords and Recovery Keys are the keys to accessing evidence**. Without them, forensic acquisition is limited or completely impossible.

FileVault 2

What it is:

FileVault 2 is Apple's full-disk encryption, introduced in macOS Lion (10.7).

How it works:

Entire volumes are encrypted with XTS-AES-128. The encryption keys are stored in the Secure Enclave (on T2 and Apple Silicon) or in firmware/OS on older Intel models.

Enabling FileVault:

macOS prompts users to enable FileVault during setup. On newer Macs, FileVault may be enabled by default.

Decryption options:

- **User password** (login password for an authorized account)
- **Recovery Key** (created during initial setup)
- **iCloud credentials** (if the option to allow unlocking with Apple ID/iCloud was enabled at setup)

Best Practice:

- If FileVault is active and you have one of these credentials, use **RECON ITR** at collection to acquire a decrypted image.
- Alternatively, acquire the encrypted volume and later decrypt in **RECON LAB** using the same credentials.

T2 Security Chip

- **What it is**: Apple's T2 chip integrates the Secure Enclave, disk controller, and cryptographic functions. It appears in most Intel Macs manufactured between 2018–2020.
- **Impact on forensics**:
    - Storage is always encrypted at rest.
    - Decryption keys are stored inside the Secure Enclave and never leave it.
    - Without the correct password, forensic imaging will only produce encrypted data.
    - Secure Boot prevents external devices from booting unless settings are changed in Recovery Mode with the proper password.

Best Practice:

1. **Obtain the password whenever possible.**
    - Without it, imaging is not possible on a T2 Mac.
    - Validate password accuracy before proceeding—do not risk lockout with repeated attempts.
2. **If you have the password, disable Secure Boot first.**
    - Boot into Recovery Mode.
    - Use Startup Security Utility to disable Secure Boot and allow booting from external media.
    - Once disabled, boot directly into **RECON ITR** on external media and acquire a decrypted forensic image.
3. **If disabling Secure Boot is not possible, use Target Disk Mode (TDM).**
    - Put the T2 Mac into Target Disk Mode by holding **T** at startup.
    - Connect it via Thunderbolt/USB-C to another forensic Mac.
    - On the examiner's Mac, run **RECON ITR**, disable Disk Arbitration, and image the connected T2 Mac.

⚠️ **Warning:** Too many failed password attempts can permanently lock the Secure Enclave, making evidence inaccessible. Only attempt a password entry if you are certain it is correct.

Apple Silicon & the Secure Enclave

- **What it is**: Apple Silicon (M1, M2, M3, M4 families) integrates the CPU, GPU, and Secure Enclave directly on the SoC (System on Chip).
- **Impact on forensics**:
    - Every Apple Silicon Mac uses the Secure Enclave for disk encryption and authentication.
    - Target Disk Mode is no longer supported. Instead, Apple introduced **Sharing Mode** for limited SMB access.
    - Full forensic imaging requires administrator-level credentials.
- **Acquisition options**:
    - **RECON ITR bootable media** can boot Apple Silicon Macs, provided the examiner has the admin password. This allows full imaging in DMG or sparseimage format.
    - **RECON ITR Live Imaging** can also be performed from a logged-in system when passwords are available.

Best Practice:

- Always collect admin passwords at the scene.
- Without a valid password, forensic acquisition is not possible.
- With credentials, boot into RECON ITR or use Live Imaging to acquire a **decrypted DMG** or sparseimage of the storage.

Passwords & Recovery Keys

Most critical evidence: The single most important action an examiner can take at the start of an investigation is to obtain valid passwords or Recovery Keys.

Types of passwords and credentials:

- macOS account password(s)
- Firmware (EFI) or Recovery password (older Macs)
- FileVault Recovery Key
- Apple ID / iCloud credentials *(can unlock FileVault if the user enabled the option during setup)*

Best Practice:

- Validate passwords immediately.
- Do not guess—incorrect entries can trigger lockouts, especially on T2 and Apple Silicon Macs.

Summary of Best Practices

- **Always ask for the password.** Without it, modern Macs cannot be fully imaged.
- **Validate immediately.** Confirm password accuracy before proceeding with imaging.
- **Image decrypted whenever possible.** RECON ITR can acquire decrypted DMG images at collection time.
- **Decrypt later if needed.** RECON LAB can decrypt FileVault volumes from forensic images when credentials are available.
- **Never brute force at the scene.** Excessive failed attempts risk locking the device or triggering security mechanisms.

- **Document everything.** Record which passwords were provided, who provided them, and how they were validated.

✅ **Key takeaway**: On modern Macs, **encryption is the rule, not the exception**. Without valid credentials, examiners will not be able to access or analyze evidence. Passwords and Recovery Keys are the foundation of successful Mac forensics.

Imaging Best Practices

Imaging is the foundation of any forensic investigation. On modern Macs (APFS, T2, Apple Silicon), the choice of **format, evidence drive, and workflow** determines whether all data is preserved or critical artifacts are lost. To ensure integrity, examiners must stay entirely within the **Mac-native environment** and use **Mac-native formats**.

Image Formats

- **Apple Disk Image (.dmg) – Preferred**
    - Fully supported by macOS natively.
    - Preserves Apple Extended Metadata and APFS integrity.
    - Compatible with RECON ITR, RECON LAB, and any forensic tool that supports RAW/DD format.
    - Depending on encryption and system type, DMGs may not always be a “raw” bitstream but remain forensically sound and universally usable in Mac-native workflows.

- **Sparseimage / Sparsebundle**
    - Alternative Mac-native formats.
    - Expand dynamically as data is written.
    - Useful when working entirely within the Mac-native environment.
    - Supported by RECON tools for acquisition and analysis.
- **E01/Ex01**
    - Strongly discouraged.
    - Requires reverse-engineered support layers to mount (e.g., FUSE).
    - Anytime you leave the Mac-native environment, you **can lose or will lose information**, especially Apple Extended Metadata.
    - Should only be used if mandated by outside requirements, with clear documentation of their limitations.

✅ **Best Practice:** Always use **DMG (preferred)** or **sparseimage/sparsebundle**. Avoid E01/Ex01 unless forced.

Evidence Drive Formats

- **APFS – Best for Mac-only analysis**
    - Provides 100% preservation of Mac-native artifacts.
    - Recommended when all imaging and examination will be performed within macOS using RECON ITR and RECON LAB.

- **HFS+ – Use only if cross-platform access is needed**
    - Preserves Apple Extended Metadata.
    - Useful if evidence must be accessed by Windows-based examiners with HFS+ drivers.
    - Still reliable, but slightly less future-proof than APFS.

⚠️ **Note on Logical Collections:** When performing *logical exports* (copying out files instead of imaging a disk), do **not** use FAT, ExFAT, or NTFS as destination file systems. These cannot fully preserve Apple Extended Metadata and will result in loss of critical forensic data.

Segmentation of Forensic Images

- Modern Macs often contain terabyte-scale SSDs. Segmenting images into thousands of small files increases the chance of corruption or access issues.
- While macOS can technically handle segmented DMGs, **a single continuous file is strongly recommended**.

✅ **Best Practice:** Avoid segmenting forensic images unless absolutely necessary due to storage constraints or external requirements.

Mounting Forensic Images

When mounting images for examination on macOS, it is critical to maintain integrity by locking the original image and using shadow files.

- **Locking the Image**
    - Use **(Command + I)** → “Lock” to set the DMG as read-only.

Mounting a Single DMG with Shadow File

```
hdiutil attach -noverify -noautofsck IMAGE.DMG -shadow
```

-
    - Ensures all writes are redirected to a temporary shadow file, leaving the original image untouched.

- **Fusion Drive (Non-APFS) Mounting Example**

Mount the SSD portion first:

```
hdiutil attach -readonly -nomount -imagekey
diskimage-class=CRawDiskImage /Volumes/DEST/SSD_FUSION/SSD_FUSION.dmg
```

Then mount the platter portion:

```
hdiutil attach -readonly -nomount -imagekey
diskimage-class=CRawDiskImage
/Volumes/DEST/PLATTER_FUSION/PLATTER_FUSION.dmg
```

    - Once both are attached, use Disk Utility to check mount status. If gray, right-click and select “Mount.”

✅ **Best Practice:** Always lock forensic images and mount with a shadow file. Never mount writable.

Imaging Checklist

1. Confirm system type (Intel, T2, Apple Silicon).
2. Obtain and validate passwords (FileVault, admin, Recovery Key).
3. Disable Secure Boot when possible, or use Target Disk Mode.
4. Use **RECON ITR** to acquire a **DMG** (preferred) or **sparseimage/sparsebundle**.
5. Save to an **APFS evidence drive** (or HFS+ if Windows review required).
6. Avoid segmentation—use a single file.
7. Lock the image and mount with a shadow file before examination.
8. Document every step for reproducibility.

✅ **Key takeaway:** Imaging must always be performed with **Mac-native formats (DMG, sparseimage, sparsebundle) saved to APFS/HFS+ evidence drives**. This ensures full preservation of Apple Extended Metadata and APFS integrity—something non-native environments cannot guarantee.

Step-by-Step Mac Forensic Workflow

This section provides a practical, **step-by-step playbook** for conducting Mac forensic acquisitions. Following these steps ensures consistent, defensible results while minimizing the risk of data loss or alteration.

STEP 1: Pre-Search Intelligence

Before handling the target Mac, gather as much information as possible:

- **Type of Mac** (MacBook, iMac, Mac Studio, Mac Pro, etc.)
- **Processor** (Intel, T2 Security Chip, or Apple Silicon)
- **Operating System version** (important for volatility collection and compatibility)
- **FileVault status** (is full-disk encryption enabled?)
- **Passwords available?** (system password, FileVault, Recovery Key, Apple ID/iCloud)
- **Peripherals and ports** (Thunderbolt, USB-C, legacy ports)

⚠️ **Critical:** On Apple Silicon and T2 Macs, **passwords are mandatory**. Without them, full imaging is not possible.

STEP 2: Isolate

- Assign one trained examiner to handle the Mac.
- Prohibit others from interacting with the device.
- Maintain chain of custody documentation from the moment evidence is seized.

STEP 3: Password Acquisition

- Always request all relevant passwords and Recovery Keys.
- Test passwords carefully. **Do not attempt repeated guesses** — too many failed attempts can lock the system or trigger security policies.
- Validate accuracy at the earliest safe opportunity.

STEP 4: If the Computer is On – Locked Screen

Options:

- **If password is known**: Validate it and proceed to access the desktop.
- **If password is unknown**: Do not attempt multiple guesses. Secure the device and move to offline imaging procedures.
- **RAM acquisition**: Not feasible on modern Macs (T2 or Apple Silicon). Only possible on legacy Intel systems, which are increasingly rare.

STEP 5: If the Computer is Off

- Collect and secure the device using best practices for electronic evidence.
- Prepare imaging media and RECON ITR before powering on the Mac.

STEP 6: If the Computer is On – Desktop Accessible – Check for Destructive Processes

- Look for signs of wiping tools or free-space erasure in progress.
- If detected, attempt to stop them using **Force Quit** (Command + Option + Esc).
- Document the activity with screenshots or photographs.

STEP 7: Collect Volatile Information (If Logged In)

If the system is accessible and safe to interact with:

- Collect volatile data (processes, network connections, unsaved documents) using **RECON ITR's automated volatile data collection**.
- Save volatile data to external media.

STEP 8: Check for Hidden Desktops or Virtual Machines

- macOS supports multiple desktops (up to 16). Check Mission Control for additional active desktops.
- Look for running VMs. If found:
    - Use the VM's native software to **Save a Snapshot** (this typically creates a file on the same system being examined).
    - Treat the VM as a separate computer and follow OS-appropriate best practices.

STEP 9: Check for Encryption

- If logged in, encrypted volumes are accessible.
- Use **Command + I** on mounted volumes to check encryption status.
- If encrypted, copy critical data to an **APFS or HFS+ evidence drive** (using `rsync` or RECON ITR's Live Imaging).
- Check **System Settings** → **Security & Privacy** → **FileVault** to confirm FileVault status.

STEP 10: Imaging by Platform

Intel Macs (no T2)

- Boot directly to **RECON ITR USB**.
- Image using DMG format.

T2 Macs

1. **Preferred option**: With the password, boot into Recovery Mode and **disable Secure Boot**, then boot externally into **RECON ITR** and image.
2. **Fallback option**: If Secure Boot cannot be disabled, use **Target Disk Mode**. Connect to an examiner Mac, disable Disk Arbitration, and image with RECON ITR.

Apple Silicon Macs

- Always require an admin password.
- Boot directly into **RECON ITR** using external boot if allowed.
- Alternatively, use **RECON ITR Live Imaging** from a logged-in system.
- SMB "Sharing Mode" may provide limited access, but is not a substitute for full imaging.

STEP 11: System Date and Time Verification

- If possible, confirm the system date/time by booting to Recovery or Single User Mode (Intel only).
- Document system time for reporting accuracy.

STEP 12: Mounting Forensic Images

- Always **lock DMG images** before examination.
- Use **shadow files** to prevent alteration:

```
hdiutil attach -noverify -noautofsck IMAGE.DMG -shadow
```

- **Fusion Drives (APFS or HFS+):**
    - When imaged properly, RECON LAB will automatically recognize and mount Fusion Drives, including APFS Fusion volumes.
    - This eliminates the need to manually attach SSD and platter portions.
    - If using macOS without RECON LAB, you may still need to mount components individually and recombine with Disk Utility.

✅ **Best Practice:** Whenever possible, rely on **RECON LAB** to automatically mount and interpret complex Mac storage, including Fusion Drives. This ensures accuracy and reduces examiner error.

STEP 13: Indexing & Search

Enable Spotlight indexing for manually mounted forensic images:

```
mdutil -i on /Volumes/VOLUME_NAME
```

- Use Finder + Spotlight to conduct native searches, preserving Apple Extended Metadata.

STEP 14: Reporting

- **Screenshots**:
    - Full screen: Command + Shift + 3
    - Selected area: Command + Shift + 4
    - Window: Command + Shift + 4 + Spacebar
- **PDF Export**: Command + P → Save to PDF.
- **Copy-Over Procedure**:
    - Create a new admin account on examiner Mac.
    - Copy suspect application artifacts into the new account.
    - Launch and document applications via screenshots or PDFs.
    - Delete or archive the account afterward.

✅ **Key takeaway:** The workflow begins with **password acquisition** and flows into **Mac-native imaging (DMG, sparseimage, sparsebundle)** using **RECON ITR**, with platform-specific considerations for Intel, T2, and Apple Silicon Macs. Every step must be documented and performed natively to guarantee forensic soundness.

Indexing & Searching with Spotlight

Spotlight is Apple's native search and indexing service, tightly integrated with macOS. Forensic examiners should leverage Spotlight because it provides access to Apple Extended Metadata that is not fully available through non-native tools. Proper indexing and searching can reveal critical artifacts such as download origins, quarantine flags, or document metadata that may otherwise be overlooked.

Enabling Spotlight Indexing on Forensic Images

When a forensic image (DMG, sparseimage, or sparsebundle) is mounted, indexing must be manually enabled:

```
mdutil -i on /Volumes/VOLUME_NAME
```

- Replace `/Volumes/VOLUME_NAME` with the path to the mounted image.
- Spotlight will begin indexing the volume, creating a `.Spotlight-V100` directory.
- This index allows macOS to surface extended attributes and relationships between files in the same way the user experienced them on the original system.

⚠️ **Best Practice:** Always confirm indexing is on for manually mounted forensic images before conducting searches. This ensures all available Apple Extended Metadata is accessible.

Performing Native Spotlight Searches

Once indexing is enabled, searches can be performed through:

- **Finder** → Spotlight Search Bar (Command + F)
- **Command-line searches** using `mdfind`

Isolating Search Scope

- Use Finder's advanced search (Command + F) to restrict scope:
    - Limit by directory or folder.
    - Filter by metadata attributes (kind, date opened, download date, etc.).
- Narrowing the scope ensures more precise results and reduces false positives.

Investigative Value of Spotlight

Spotlight indexes and Extended Attributes can reveal:

- **Download origins** — where files came from (browser, email, AirDrop, etc.).
- **Quarantine status** — whether files were flagged as potentially harmful.
- **User activity** — "last opened by" timestamps separate from POSIX/Unix times.
- **Hidden relationships** — files tied together through metadata links.

These artifacts are not fully or reliably exposed in non-Mac forensic tools. Using Spotlight within macOS guarantees the most accurate representation of what the user saw and did.

Best Practices

- Always enable Spotlight indexing before searching forensic images.
- Use both **Finder GUI searches** and **command-line `mdfind` queries** for thoroughness.
- Keep the search scope narrow to focus on directories or artifact sets of interest.
- Document queries and results with screenshots or exported metadata for reporting.

✅ **Key takeaway:** Spotlight is not just a convenience — it is a **forensic necessity**. By using Spotlight natively on macOS, examiners access metadata and relationships that non-native tools cannot replicate, ensuring a complete and accurate investigation.

Reporting Best Practices

Once evidence has been imaged and examined, accurate and defensible reporting is critical. For Mac forensics, the goal is to **present data in the same way the user would have seen it**, while ensuring that the examiner's actions are well-documented and repeatable.

The following best practices cover methods to capture, document, and present findings directly from the macOS environment.

Screen Captures

macOS provides several built-in shortcuts for creating forensic-quality screenshots. These should be used whenever possible to document findings visually.

Full Screen Capture

```
Command + Shift + 3
```

- Captures the entire screen.

Area Screen Capture

```
Command + Shift + 4
```

- Crosshairs appear, allowing the examiner to select a specific region.

Window Screen Capture

```
Command + Shift + 4 + Spacebar
```

- Cursor changes to a camera icon. Clicking a window captures only that window, preserving the context without clutter.

Best Practice:

- Save screenshots in **lossless PNG format** (macOS default).
- Immediately rename files with descriptive titles (e.g., `QuarantinedFileEvidence_2025-08-26.png`).
- Keep screenshots in the case folder alongside the forensic image.

Printing to PDF

macOS has a built-in option to “Print to PDF” from almost any application. This is especially useful for preserving search results, browser history, or Spotlight queries in a non-editable format.

- From the menu, select:
  File → Print → Save as PDF

Best Practice:

- Use PDFs to preserve large lists of search results or reports generated by RECON ITR/RECON LAB.
- Save PDFs with descriptive file names tied to case numbers and artifact type.

Copy-Over Procedure

Some artifacts, particularly **application data**, are best validated by running them inside a clean macOS environment. The Copy-Over Procedure allows the examiner to replicate the user's environment while preserving integrity.

Steps:

1. Create a new **administrator user account** on the examiner's forensic Mac.
2. Copy the suspect's application artifacts (e.g., Safari, Messages, or Mail data) from the forensic image to the new user account.
3. Log in as the new user.
4. Launch the application.
    - macOS will interpret the artifacts natively, exactly as the user would have seen them.
    - This ensures accurate rendering of proprietary data (chats, mailboxes, application states).
5. Document findings with **screenshots or Print-to-PDF**.
6. Log out of the temporary user account.
7. Remove or archive the account.

Best Practice:

- Always document the Copy-Over Procedure steps in your notes, including which artifacts were copied and how they were validated.
- Use this method for Mac-only artifacts that do not display correctly in non-native tools.

RECON Reporting Options

Both RECON ITR and RECON LAB provide integrated reporting features:

- Export results directly into **PDF or CSV** for case documentation.
- Automated bookmarking and tagging ensure that all evidence references are traceable.

Best Practice:

- Use RECON's reporting tools for structured exports (timelines, artifact summaries).
- Use macOS native reporting (screenshots, Copy-Over Procedure) for contextual validation.

General Reporting Guidelines

- **Clarity over volume:** Present only what is relevant to the investigation. Avoid overwhelming reports with unnecessary screenshots or metadata.
- **Maintain integrity:** Never alter evidence files during reporting. Always use locked images and shadow mounts.
- **Chain of custody:** Record how reports were generated, including tools and system versions.
- **Defensibility:** Reports should show both the artifact and the method used to validate it.

✅ **Key takeaway:** Forensic reporting in Mac environments should rely on **macOS-native methods** — screenshots, PDFs, and the Copy-Over Procedure — combined with RECON's structured exports. This dual approach ensures authenticity, accuracy, and forensic defensibility.

Helpful Hints

Before starting any new Mac forensic case, review these reminders to ensure efficiency, completeness, and forensic soundness.

Stay Mac-Native

- Always use **a Mac to examine a Mac**.
- Rely on **Mac-native formats (DMG, sparseimage, sparsebundle)** for imaging.
- Be careful of using non-Mac tools that rely on **reverse engineering APFS**, as they risk missing or misinterpreting artifacts.

Evidence Drives

- **APFS** → Best for Mac-only analysis, preserves all metadata.
- **HFS+** → Use only when cross-platform access is required.
- ⚠️ **Never use FAT, ExFAT, or NTFS** for logical collections. These will lose Apple Extended Metadata.

Imaging Best Practices

- **Preferred format:** DMG.
- Use **sparseimage or sparsebundle** if flexibility is needed.
- Avoid segmentation — create single, continuous images whenever possible.
- Lock all images before mounting and use **shadow files** to prevent alteration.

Passwords Are Critical

- Collect and validate **system passwords, FileVault Recovery Keys, and admin credentials** at the scene.
- Without credentials, imaging is impossible on modern T2 and Apple Silicon Macs.
- ⚠️ **Never attempt repeated guesses** at the lock screen — too many failed attempts can trigger lockout or data loss.

Secure Boot & T2 Workflow

- If you have the password, **disable Secure Boot first** to allow external booting into RECON ITR.
- If that is not possible, use **Target Disk Mode (TDM)** as a fallback.
- Document the method chosen and why.

Apple Silicon Workflow

- Always requires the admin password.
- Use **RECON ITR external boot** when permitted.
- If not available, use **RECON ITR Live Imaging** from a logged-in system.
- Treat SMB “Sharing Mode” as very limited and not a replacement for imaging.

Indexing & Searching

- Enable Spotlight indexing on mounted forensic images before searching.
- Use both **Finder** (GUI) and **mdfind** (command-line) to query metadata.
- Document searches with screenshots or PDF printouts.

Reporting

- Use **macOS-native reporting methods**:
    - Screenshots (lossless PNG).
    - Print-to-PDF.
    - Copy-Over Procedure for application artifacts.
- Use RECON ITR and LAB reporting features for structured outputs.

Documentation & Defensibility

- Document every step: passwords collected, imaging method, mount commands, Spotlight queries.
- Maintain clear chain of custody for all images, reports, and exports.
- Ensure reporting shows both **what was found** and **how it was validated**.

✅ **Key takeaway:** Staying 100% Mac-native, obtaining passwords early, and documenting every step are the three pillars of successful Mac forensic examinations.

Why SUMURI

The Mac forensic landscape has changed dramatically with the adoption of **APFS, the T2 Security Chip, and Apple Silicon processors**. Examiners who attempt to use non-native tools or workflows risk missing critical artifacts, misinterpreting timelines, and losing metadata that could be vital to an investigation.

SUMURI was created to solve these problems.

Built Natively for macOS

- **RECON ITR** and **RECON LAB** are developed *on macOS for macOS*.
- They leverage Apple's own frameworks and libraries, ensuring 100% accurate parsing of Apple Extended Metadata, timestamps, and APFS structures.
- Unlike reverse-engineered tools, RECON products do not guess — they present the evidence as macOS itself records and interprets it.

Training and Expertise

- SUMURI's **Macintosh Forensic Survival Courses (MFSC)** are the most widely respected Mac forensic training programs worldwide.
- The **Certified Forensic Mac Examiner (CFME)** credential sets the standard for proficiency in Mac examinations.
- All SUMURI training is **vendor-neutral** at its core, emphasizing examiner skill, while simultaneously preparing professionals to use SUMURI's native tools to their fullest potential.

Examiner-Focused Approach

- SUMURI was founded by forensic examiners, for forensic examiners.
- Every workflow, from imaging with RECON ITR to analysis in RECON LAB, is designed to maximize accuracy and minimize examiner error.
- SUMURI continues to evolve alongside Apple, ensuring that its tools and training remain current as macOS changes.

Commitment to the Community

- SUMURI provides affordable, accessible solutions and has supported the forensic community globally for more than a decade.
- Free resources such as PALADIN (for legacy needs) and contributions to examiner education demonstrate SUMURI's mission to put examiners first.

✅ **Key takeaway:**
To perform accurate, defensible, and complete Mac forensic examinations in 2025 and beyond, investigators must use Mac-native tools and workflows. **SUMURI's RECON ITR, RECON LAB, and training programs are the gold standard for ensuring that no artifact is overlooked, no timestamp is misinterpreted, and no evidence is lost.**