

CVTR-2026-001

Apple Forensic Acquisition

Nick Stoltzfus

Senior Cybersecurity Engineer, nick.stoltzfus@crimsonvista.com

Follow this link to find similar works: <https://www.crimsonvista.com/crimson-labs>

©2026 Crimson Vista, Inc.

This Technical Report is brought to you for free and open access by Crimson Vista, Inc. and can be used for non-commercial purposes without restriction.

Apple Forensic Acquisition

CRIMSON VISTA TECHNICAL REPORT CVTR-2026-001

September 10, 2026

Nick Stoltzfus

Senior Cybersecurity Engineer

With the rise of personal Apple devices at the corporate and private levels, a corresponding increase in need for Mac/iOS forensic examiners is required, especially at the corporate, judicial, and legal domains. This Technical Report highlights some of the challenges and solutions encountered during Apple Device acquisition.

Apple device acquisition is constrained by three technical layers: APFS structure, hardware-backed encryption, and version-specific security controls.

On current Macs and iPhones, acquisition scope depends on the following variables:

- Device State
- OS Version
- Chip Generation
- Credentials Access
- Recovery Material
- Pre-unlocked Session Access

For example, the device state may be turned on, off, remote, or inoperative. The OS version will determine the encryption level of the file system which, in connection with the Chip generation, will define the presence of a Secure Enclave or T2 encryption. If the owners of the devices are unable to provide credentialed access to the system including access to a recovery key, options for acquisition will be severely limited.

APFS Forensic Acquisition

With the deprecation of the 30+ year HFS+ old file system as early as MacOS High Sierra in 2017, Apple needed a file system that would serve their customers moving forward. Thus, Apple introduced the APFS file system with built-in encryption, speedy SSD read-writes, and increased reliability via snapshots and containers rather than rigid partitions.

Because APFS uses copy-on-write metadata, snapshots, clones, space sharing, and native encryption, all things that alter the physical storage of the data. The effort required to perform forensic inspection of data on APFS volumes is large. Storage state is not represented by a simple fixed-partition model. Snapshot state can preserve earlier file-system views, clones can cause multiple logical files to share underlying storage, and volume size no longer maps cleanly to exclusive physical allocation inside a container. Acquisition and interpretation therefore need to be APFS-aware at the container, volume, and metadata level.

On macOS 10.15 and later, the startup APFS container includes multiple volumes, including Preboot, VM, Recovery, and the System-Data pair. This means evidence relevant to startup, recovery, and user activity is

distributed across several APFS volumes rather than a single startup partition. The examiner must correctly identify the role of each volume and preserve the volume-group relationship during acquisition and parsing.

On macOS 11 and later, Apple added the Signed System Volume (SSV). The system volume is cryptographically signed, and macOS verifies its integrity at runtime. This affects acquisition because the system volume is no longer just read-only in practice; it is sealed against tampering and must be interpreted as part of Apple's verified boot and runtime trust chain. As a result, post-Big-Sur (the OS introduced in 2020) Mac forensics began placing greater emphasis on the writable Data volume, APFS metadata, unified logs, and targeted artifacts instead of standard file system forensics found on NTFS or ExFAT file systems.

Sample APFS Container:

```
APFS Container (1 found)
|
+-- Container disk3
=====
APFS Container Reference: disk3
Size (Capacity Ceiling): 500.0 GB
Capacity In Use By Volumes: 210.3 GB
+--> Volume disk3s5s1 Macintosh HD (System, Sealed, Read-Only)
+--> Volume disk3s1 Macintosh HD - Data (Data)
+--> Volume disk3s4 Preboot (Preboot)
+--> Volume disk3s3 Recovery (Recovery)
+--> Volume disk3s6 VM (VM)
```

The practical consequence is that APFS acquisition is no longer just "image the disk and parse the files." The examiner must use the tools available to reconstruct the blocks inherent to the APFS system, including any clones, snapshots, or alternative files.

This can result in multiple file-system source files working together to produce a single output file. For example, a time snapshotted base file combined with a change offset file yields a copy containing changes from the original.

MacOS version changes, FileVault, and the T2 transition

Catalina changed Mac acquisition by separating system and user data into distinct APFS volumes. Big Sur extended that model with SSV. These changes reduced the value of older workflows that depended on booting external environments and treating the startup disk as a single writable file system.

FileVault remains the primary at-rest protection layer on macOS. Apple states that FileVault uses AES-XTS to encrypt full volumes. Apple's platform security documentation also ties FileVault key protection to hardware-backed security, including Secure Enclave-based protections and sealed-key mechanisms on supported systems. A raw storage image from a FileVault-enabled system may still be unusable unless the examiner also has access to decryption material such as the user password, a recovery key, or a live unlocked state.

The introduction of the T2 chip marks the point where this became much more significant. T2-era Macs added hardware-backed secure boot and stronger integration between startup policy, key protection, and storage access. Magnet's current macOS workflows for T2 and Apple silicon systems center on live logical collection from a running machine rather than classic third-party boot-media imaging. This is an acquisition

constraint, not a tooling preference. When the device is locked, powered off, and protected by FileVault, the examiner may be able to capture encrypted storage without being able to derive readable user data.

For that reason, the most important pre-acquisition questions on a Mac are usually these:

- Is the device running?
- Is a user session unlocked?
- Is FileVault enabled?
- Is there a password, recovery key, escrowed key, or other lawful decryption source?
- Is the target Intel, T2-era Intel, or Apple silicon?

Those conditions determine whether the examiner can perform live collection, targeted logical acquisition, or only encrypted-at-rest imaging.

iOS version and hardware issues

On iOS, acquisition scope is even more state-dependent. The most universal workflow remains the local device backup. Apple states that encrypted local backups contain more data than unencrypted backups, including saved passwords, Wi-Fi settings, website history, Health data, and call history. Apple also states that encrypted backups do not include Face ID, Touch ID, or device passcode data. This makes encrypted backup the broadest generally available acquisition path in cooperative or consent-based cases.

However, backup acquisition is not equivalent to full file-system acquisition. Backup scope depends on what Apple exposes through the backup service and what remains protected by the current device security model. On modern iOS versions, especially on newer chips, full file-system access is not universally available through private tools or a single standard method. Instead, acquisition depth varies by device generation, OS version, and vendor-specific access method.

Elcomsoft's current documentation is a useful summary of the present technical landscape. It distinguishes among extended logical acquisition, agent-based low-level extraction, and bootloader-based extraction. Extended logical acquisition is documented for all devices and all iOS versions. Deeper agent-based extraction is available only on supported device/version combinations. Bootloader-based extraction is limited to selected older hardware. Their published support notes also describe version ceilings, hardware exclusions, and stability limitations for some modern devices.

The implication is that iOS acquisition cannot be described accurately as "logical versus physical" in the older, simpler sense. The correct model is layered access:

1. standard backup-based acquisition,
2. expanded logical collection of exposed files and logs,
3. deeper vendor-assisted extraction where hardware and OS support it.

That layered model better matches the current Apple security architecture and the actual capabilities published by current forensic vendors.

Where this leaves examiners

Modern Apple acquisition is determined first by access state and only second by software choice. On both macOS and iOS, the examiner must establish whether the device is unlocked, paired, live, encrypted, and running on hardware/firmware that supports only logical collection or also supports a deeper extraction path. There is no single workflow that applies uniformly to current Macs, current iPhones, older Intel Macs, T2-era Macs, and legacy checkm8-capable devices.

For Mac systems:

- APFS volume-group structure must be preserved.
- FileVault may render storage unreadable without decryption material.
- T2 and Apple silicon materially restrict traditional offline workflows.

For iOS devices:

- encrypted local backup is the most universal acquisition starting point,
- acquisition depth beyond backup is hardware/version specific,
- deeper access is typically vendor-assisted and not universally available,

For **macOS**, **Magnet Axiom Process and Examine** current tooling is strongest for analysis of Apple systems including Apple silicon systems. Their published materials position these products around logical collection and targeted acquisition rather than universal offline physical imaging of locked modern Macs. That makes them suitable for corporate investigations, insider-risk cases, and incident response where the Mac is accessible in a live state. However, in my experience, Magnet Axiom Process can run into many issues that cause corrupt or incomplete captures. **Cellebrite's Digital Collector** is able to perform better in more circumstances.

For **iOS**, if you'd like to stay in the Magnet Ecosystem **Magnet Axiom's Verakey** can perform iOS extraction. MSAB XRY Pro is another enterprise platform intended for broader extraction work, including workflows involving locked or encrypted devices where supported. These are lab-oriented products rather than general-purpose backup utilities.

Crimson Vista employs the above recognized tooling in our forensic investigations. Different tools work better under different constraints, **there is no one-size-fits-all solution.**

Best private or practitioner-controlled options

For **iOS**, the strongest private workflow is still an encrypted local backup performed through Finder, Apple Devices, or a compatible implementation such as `idevicebackup2` from `libimobiledevice`. `Libimobiledevice` documents support native iOS backup workflows, and MVT documentation (Mobile Verification Toolkit) explicitly notes that encrypted backups contain more data than unencrypted backups. This approach is scriptable, defensible, and broadly usable in consent-based acquisitions, but it does not replace full-file-system or vendor-assisted low-level methods.

For **macOS**, private workflows are much narrower on modern systems. Once lawful access is already established, live targeted collection and APFS-aware parsing remain effective. By contrast, private dead-box acquisition of a locked FileVault-enabled T2 or Apple silicon Mac is heavily constrained by encryption, startup security, and hardware-backed key protection. In those cases, private tooling is best used for validation, parsing, and post-collection analysis rather than as a universal acquisition bypass.