MacOS And Apple Silicon Forensics

Modern Macs present unique challenges for forensic acquisition due to hard w are encryption and secure boot. This guide details why traditional imaging fails, how live logical acquisition is performed, and the importance of credentials and cooperation. It also covers common mistakes, technical limitations, and where else evidence may reside.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/macos-and-apple-silicon-forensics

MACOS & APPLESILICON · A GUIDE FOR UK LAWYERS macOS and Apple Silicon Forensics The Mac That Cannot Be Imaged the Old Way: Encryption, Secure Boot and Live Acquisition COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: no disk to pull 03 How modern Macs store and protect data 04 Why the old imaging approach fails 05 How a Mac is acquired today 06 Credentials, cooperation and honest limits 07 Deployment: preservation, seizure and the estate 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary hardware-encrypted and its boot is locked down, so it is acquired live and logically on the running, unlocked machine with the credentials obtained by cooperation or lawful compulsion, and what it yields, and does not, is stated honestly.

§ 02 · FIRST PRINCIPLES The problem in plain English: no disk to pull

§ 03 · HOWITSTORESANDPROTECTSDATA How modern Macs store and protect data SOLDERED FLASH HW ENCRYPTION SECURE ENCLAVE SECURE BOOT ICLOUD

§ 04 · WHYOLDIMAGINGFAILS Why the old imaging approach fails

§ 05 · HOWITISACQUIREDTODAY How a Mac is acquired today

§ 06 · CREDENTIALSANDHONESTLIMITS Credentials, cooperation and honest limits

§ 07 · DEPLOYMENT Deployment: preservation, seizure and the estate

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE I CLOUD I PHONE / MACHINE / THE MAC APPLE DELETED / (LIVE) ACCOUNT RECOVERABLE PAIRED TIME IPAD BACKUPS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEMACSWITCHEDOFF, ANDTHELESSONLEARNED EXAMPLE2 · THELIVEACQUISITIONDONERIGHT EXAMPLE3 · THEHONESTLIMITANDTHEESTATETHATANSWERED

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTION FOR AM AC AC QUISITION

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The Mac acquisition checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Can you just image the Mac's hard drive like any other computer? What is the single most important thing when seizing a Mac? Is a live logical acquisition as good as a full image? The Mac is locked and we do not have the password. Can you break in? If we cannot access the Mac, is the evidence lost? Does this apply to older Intel Macs too?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

Can you just image the Mac's hard drive like any other computer?

Not on Apple Silicon (§4). The storage is soldered to the board, so there is nothing to remove; it is hard w are- encrypted, so it is unreadable at rest without the machine and its keys; and secure boot blocks the old trick of imaging it from external media. The classic pull-and-image method simply does not work. The Mac is instead acquired live and logically, on the running, unlocked machine, which is where its data is readable (§5).

What is the single most important thing when seizing a Mac?

Keep it powered on and unlocked (§7, Example 1). A running, unlocked Apple Silicon Mac can be acquired; a switched-off, locked one may be an encrypted brick without the credentials. The reflex from old training, to power a machine down, is exactly wrong here. So the machine is kept awake and unlocked, prevented from locking or sleeping into a locked state, protected from remote wipe, and acquired as soon as possible while access lasts.

Is a live logical acquisition as good as a full image?

For a modern Mac it is the correct and defensible method, not a compromise (§5, Example 2). Because no physical image is obtainable, the live logical or targeted collection, taken from the unlocked machine, hashed, documented and validated, is the sound approach, and done properly it is as accountable and reproducible as a classic image. The rigour, integrity, documentation, validation, is unchanged; only the technique adapts to a machine whose data is readable only while it runs.

The Mac is locked and we do not have the password. Can you break in?

Honestly, usually not by direct attack on a powered-off Apple Silicon machine (§6, Example 3). The credible answer is not a promise to crack it but the lawful alternatives: obtain the password by cooperation or an order (guide 117), and reach the same data through the iCloud account and any backups, which often hold much of it (§8). A reputable expert states this limit plainly rather than overpromising, and pursues the routes that actually work.

If we cannot access the Mac, is the evidence lost?

Often not (§8, Examples 1 and 3). A Mac sits in a tightly integrated Apple estate: iCloud holds synced files, mail, messages and photos; the paired iPhone or iPad holds the same messages and libraries; and Time Machine or other backups hold prior states. Reached through the account or the other devices by consent or lawful process, these frequently hold much of the same evidence. The Mac being inaccessible is a setback, not usually the end of the enquiry.

Does this apply to older Intel Macs too?

Partly (§3). Older Intel Macs may have removable storage and different boot behaviour, so some classic techniques can still apply, though File Vault encryption and the T-series security chips on later Intel models bring similar constraints. Apple Silicon machines are the fullest expression of the new reality, soldered, hard w are- encrypted, secure-booted, but the direction of travel is the same, and every Mac is assessed on its specific model, chip and configuration. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd

Source: https://e-discovery.uk/library/macos-and-apple-silicon-forensics. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.