APFS And The Apple File System

APFS, used on Macs, iPhones, and iPads, preserves deleted and prior data states more often than expected. This guide details how copy-on-write, snapshots, and clones work, where evidence resides, and how to recover and interpret this information for legal proceedings, highlighting common mistakes and technical limits.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/apfs-and-the-apple-file-system

APFS & APPLEFILESYSTEM · A GUIDE FOR UK LAWYERS APFS and the Apple File System Snapshots, Clones and Containers: Where Deleted Data Hides on Apple Devices COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM DELETED-DATA RECOVERY CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary The headline point: APFS, the file system on every modern Mac, iPhone and iPad, uses copy-on-write, snapshots and clones, so deleted and earlier versions of data survive more often, and in different places, than intuition suggests, and snapshots in particular can preserve whole prior states of the device.

§ 02 · FIRST PRINCIPLES The problem in plain English: a file system that keeps the past

§ 03 · HOWAPFSWORKS How APFS works: containers, copy-on-write, clones CONTAINER VOLUMES COPY-ON-WRITE CLONES SNAPSHOTS

§ 04 · SNAPSHOTS Snapshots: the treasure of prior states

§ 05 · RECOVERINGDELETEDANDEARLIERDATA Recovering deleted and earlier data

§ 06 · INTERPRETATIONANDHONESTLIMITS Timestamps, interpretation and honest limits

§ 07 · DEPLOYMENT Deployment: prior versions, deletion and timelines

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE LIVE APFS MACHINE / I CLOUD I PHONE / LOCAL DELETED / SNAPSHOTS RECOVERABLE TIME PAIRED BACKUPS IPAD

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEDELETEDDOCUMENTASNAPSHOTKEPTWHOLE EXAMPLE2 ·

THEEARLIERVERSIONTHATEXPOSEDTHEEDIT EXAMPLE3 · THECLONETHATWASNOTTWODOCUMENTS

§ 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 · INSTRUCTIONFORANAPFSANA LY SIS

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The APFS checklist Red flags When to involve a digital forensic expert 2 and 3,

§ 6). The findings are dated using snapshots as checkpoints, assessed in context, and corroborated

§ 13 · COMMON QUESTIONS Frequently asked questions If a file was deleted from an Apple device, is it recoverable? What is an APFS snapshot, and why does it matter? Can we prove a document was altered after it was signed? Why does it matter whether something is a clone? How urgent is preserving an Apple device for APFS recovery? Do APFS timestamps tell us exactly when things happened?

§ 14 · REFERENCE Glossary APFS 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

If a file was deleted from an Apple device, is it recoverable?

Often, and more reliably than on older systems (§4, §5, Example 1). APFS uses copy-on-write, so changes write new data and leave old data recoverable, and it takes snapshots, point-in-time pictures of the whole file system, that frequently hold deleted files and earlier versions intact. A document gone from the live file system is very often recovered whole from a snapshot that predates its deletion, or from remnants in free space, provided the device is preserved before the data is overwritten or the snapshots pruned.

What is an APFS snapshot, and why does it matter?

A snapshot is a frozen picture of the entire file system at a moment in time (§4). The operating system and Time Machine create them automatically, so a device usually holds several without the user knowing. They matter because they can preserve files as they were at a past moment, including material since deleted or altered, making them the richest source of prior states on an Apple device and a powerful way to prove what existed on the device, and when.

Can we prove a document was altered after it was signed?

Frequently, using APFS (§5, §7, Example 2). Because APFS retains earlier data, a prior version of the document can often be recovered from a snapshot or copy-on-write remnants, and compared with the version relied on. If the comparison shows a change made after the purported date, that exposes the alteration or backdating (guide 109). The interpretation is done carefully, reading timestamps and clone relationships correctly, so the comparison rests on a sound understanding of each recovered version.

Why does it matter whether something is a clone?

Because a clone is not an independent copy (§3, §6, Example 3). APFS clones share the same underlying data until one is changed, so two apparent copies may really be one object with two names, not two separate duplicates that were made and moved. Mistaking a clone for independent duplication overstates the facts. Establishing the clone relationship before drawing conclusions about copying or distribution is essential to an accurate account, which is why interpretation matters as much as recovery.

How urgent is preserving an Apple device for APFS recovery?

Quite urgent (§4, §5). Copy-on-write remnants survive only until their space is reused, and snapshots are pruned over time, so continued use of the device steadily erodes what can be recovered. Preserving the device promptly, and acquiring it while snapshots and remnants remain, maximises recovery. As with the Mac acquisition itself (guide 131), the device should be preserved without c are less use, and the sooner it is examined, the more of its past survives.

Do APFS timestamps tell us exactly when things happened?

They are valuable but must be read with care (§6). APFS records several timestamps per file, which help build timelines, but copy-on-write and cloning mean a timestamp may not mean what it appears to at first glance, since a change writes new structure. So the metadata is interpreted by someone who understands APFS behaviour, and findings are stated at honest

confidence, using snapshots as reliable dated checkpoints where possible, rather than reading raw timestamps at face value. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 15 of 17