Time Machine And MacOS Backup Analysis

e-discovery.uk, Computer Forensics Lab. Published 2026-09-02.
https://e-discovery.uk/library/time-machine-and-macos-backup-analysis

TIME MACHINE & MACOSBACKUPS · A GUIDE FOR UK LAWYERSTime Machine and macOS Backup AnalysisThe Second Machine That Remembers What the First One DeletedCOMPUTER FORENSICS LAB§ ABOUT THE AUTHORPREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAMPRIOR-STATE & VERSION ANALYSIS CPR PART 35 EXPERT REPORT SFULL CHAIN-OF-CUSTODY DOCUMENTATION§ CONTENTSIn this guide01 Executive summary02 The problem in plain English: a second machine that remembers03 How Time Machine and macOS backups work04 What backups preserve05 Recovering prior states and deleted data06 Authentication, dating and honest limits07 Deployment: the deleted file, the earlier version, the aged-out log08 Source architecture: where else the evidence lives09 Worked examples10 Common mistakes and technical limitations11 Questions to ask · Suggested wording12 Checklist and red flags · When to involve a digital forensic expert13 Frequently asked questions14 Glossary · References · Disclaimer · How a specialist laboratory can assist§ 01 · ORIENTATIONExecutive summaryThe headline point: Time Machine keeps regular, versioned backups of a Mac, so a backup is a secondmachine that remembers what the first one deleted, preserving deleted files, earlier document versions andaged-out artefacts at many past points, often outside the encryption and reach of the live machine.§ 02 · FIRST PRINCIPLESThe problem in plain English: a second machine that remembers§ 03 · HOW BACKUP S WORKHow Time Machine and macOS backups workCONFIGURED REGULAR BACKUP VERSIONED STATES EXTERNAL DRIVE RECOVER PASTSTATE§ 04 · WHATBACKUPSPRESERVEWhat backups preserve§ 05 · RECOVERINGPRIORSTATESRecovering prior states and deleted data§ 06 · AUTHENTICATIONANDHONESTLIMITSAuthentication, dating and honest limits§ 07 · DEPLOYMENTDeployment: the deleted file, the earlier version, the aged-outlog§ 08 · THEWIDERMAPSource architecture: where else the evidence livesEVIDENCE LIVE MAC MACHINE BACKUP / 3RD-PART YTIME ICLOUD CLONES /DRIVE SYNC BACKUPAPFS DELETED /SNAPSHOTS RECOVERABLE§ 09 · IN THE WILDWorked examplesEXAMPLE1 · THEDELETEDFILETHEBACKUPDRIVEKEPTEXAMPLE2 · THEEARLIERVERSIONTHATEXPOSEDTHEBACKDATINGEXAMPLE3 · THELOCKEDMACANDTHEBACKUPTHATANSWERED§ 10 · WHEREITGOESWRONGCommon mistakes and technical limitationsCommon mistakesTechnical limitations§ 11 · INTERROGATORIES & DRAFTING AIDSQuestions to ask · Suggested wordingAsk your clientAsk your opponentAsk your e Discovery / forensic providerSUGGESTED WORDING · INSTRUCTION FOR A BACKUP ANALYSIS§ 12 · QUICK CONTROLChecklist and red flags · When to involve a digital forensicexpertThe backup-analysis checklistRed flagsWhen to involve a digital forensic expert§ 13 · COMMON QUESTIONSFrequently asked questionsA file was deleted from the Mac. Can a backup still have it?Can backups prove a document was altered after it was dated?The Mac is locked and we cannot access it. Does that end things?Can a backup recover system logs that have rotated away?How reliable is a backup as evidence of timing?What if there is no Time Machine backup?§ 14 · REFERENCEGlossarySources and authoritative referencesDISCLAIMER§ HOW A SPECIALIST LABORATORY CAN

ASSISTWorking with Computer Forensics LabSpeak to a forensic examiner, not a salesperson.INSTRUCTTHELABNEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

Can a backup recover system logs that have rotated away?

Yes, that is one of its great strengths (

How reliable is a backup as evidence of timing?

Reliable, when authenticated and properly framed (

Source: https://e-discovery.uk/library/time-machine-and-macos-backup-analysis. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.