BitLocker FileVault And Full Disk Encryption

Full disk encryption, such as BitLocker and FileVault, is often recoverable, particularly in managed environments where recovery keys are typically escrowed. This guide details how these systems work, where keys reside, and how to lawfully obtain and image decrypted volumes for litigation or investigation. It also addresses scenarios where keys are genuinely absent.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/bitlocker-filevault-and-full-disk-encryption

FULL - DISKENCRYPTION · A GUIDE FOR UK LAWYERS Bit Locker, File Vault and Full-Disk Encryption Recovery Keys, Escrow and What the Encrypted Drive Really Does and Does Not Protect COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES ENCRYPTED-DRIVE EXAM IN AT I ON RECOVERY-KEY & ESCROW ANALYSIS CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: encryption built to be recovered 03 How Bit Locker, File Vault and LUKS actually work 04 Where the recovery keys live: directory, console, cloud and escrow 05 Obtaining the key law full y and imaging the decrypted volume 06 When there is no key: the genuinely inaccessible drive 07 Deployment: the recovery position, disclosure and honest limits 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 THE HEADLINE POINT: FULL - DISKENCRYPTIONISDESIGNEDTOBERECOVERABLE, AND INAMANAGEDENVIRONMENTTHERECOVERYKEYALMOSTALWAYSEXISTSSOMEWHERE THEORGANISATIONCONTROLS: THE EXAMINER ' SFIRSTTASKISTOFINDTHATKEY, NOTTOATTACKTHEENCRYPTION, ANDONLYWHERENOESCROWEDKEYEXISTSISTHE DRIVEGENUINELYBEYONDREACH

§ 02 · FIRST PRINCIPLES The problem in plain English: encryption built to be recovered

§ 03 · HOW IT WORK S How Bit Locker, File Vault and LUKS actually work

§ 04 · WHERETHERECOVERYKEYSLIVE Where the recovery keys live: directory, console, cloud and escrow

§ 05 · OBTAININGANDIMAGING Obtaining the key law full y and imaging the decrypted volume

§ 06 · WHEN THERE IS NO KEY When there is no key: the genuinely inaccessible drive

§ 07 · DEPLOYMENT Deployment: the recovery position, disclosure and honest limits

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION COUNTERPART LOCAL- ENCRYPTED RECOVERY- CLOUD SERVER-SIDE DRIVE KEY STORES BACKUP PLATFORMS SYNCED / DELETED / COPIES ONLY

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEBITLOCKERLAPTOPTHATWASOPENALLALONG EXAMPLE2 · THESUPPRESSEDESCROWTHATTOLDITSOWNSTORY EXAMPLE3 · THEPERSONALMACBOOKANDTHEHONESTLIMIT

§ 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 (or the reluctant party) Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTION FOR AN ENCRYPTED - DRIVEEXAMIN AT ION

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The encrypted-drive checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions The laptop is Bit Locker encrypted. Is the data lost? Where exactly do we find a recovery key? Can you break Bit Locker or File Vault if there is no key? A managed device's recovery key is missing from the console. What does that mean? The device is personal and the person will not give the key. Now what? Is a decrypted image as good as evidence as an unencrypted one?

§ 14 · REFERENCE Glossary LUKS TPM 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

The laptop is Bit Locker encrypted. Is the data lost?

Almost certainly not, if it is a managed company device: Bit Locker recovery keys are routinely escrowed to the directory or the management console at setup, precisely so IT can unlock a device whose password is forgotten (§4, Example 1). The first step is to retrieve that key from the store the or g an is at i on controls, decrypt and image the volume: no attack on the encryption, no compulsion of any custodian, just the key the client already holds.

Where exactly do we find a recovery key?

Four common places (§4): the organisation's directory (on-premises or cloud), the device-management console, a cloud account the key was escrowed to, and dedicated escrow or key-management stores. For File Vault there may also be an institutional recovery key the or g an is at i on deliberately holds. And the custodian may have a printed or saved personal recovery key in their own records. Check these before treating the drive as locked.

Can you break Bit Locker or File Vault if there is no key?

No, not by brute force in any useful time, if the encryption is sound and the passphrase is strong (§6): modern full-disk encryption is genuinely secure, which is the whole point of it. The honest examiner says so rather than promising an impossible attack (guide 117 §3). But a truly keyless drive is the exception, usually a personal, unmanaged device, and even then the same data often exists unencrypted in the estate (§8).

A managed device's recovery key is missing from the console. What does that mean?

It is worth investigating, because it should be there: escrow may have been misconfigured or failed, or it may have been deliberately suppressed by a technical user before leaving (§6, Example 2). The management logs usually show which, and a deliberate suppression of the escrow key is itself evidence of obstruction, deployed alongside any anti-forensic findings (guide 110). The absent key can be part of the case, not just a problem.

The device is personal and the person will not give the key. Now what?

The guide 117 machinery: a civil disclosure order requiring them to provide the key or enable access, on independent-examiner terms that protect their private data, with adverse inference available if they refuse without good reason (§6, Example 3). Meanwhile the estate reach-around, backups, syncs, server-side platforms, counterparts, often supplies most of the material without the drive (§8). The honest limit on the drive does not mean the case is lost.

Is a decrypted image as good as evidence as an unencrypted one?

Yes, when done properly: the volume is unlocked with the law full y retrieved recovery key, imaged and hashed, and the decryption method documented (§5), so the decrypted image's integrity is unchallengeable and its provenance clear. Lawful, key-based decryption produces evidence every bit as sound and admissible as an image of an unencrypted drive: the encryption is simply a step that was opened with the proper key. cflab. u k · e-disc ove r y. u k