COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

BitLocker, FileVault and Full-Disk Encryption

Recovery Keys, Escrow and What the Encrypted Drive Really Does and Does Not Protect

An encrypted drive looks, to the untrained eye, like the end of the road. BitLocker on the Windows laptop, FileVault on the Mac, LUKS on the Linux server: the disk is scrambled, and without the key it is noise. But full-disk encryption is far less of an obstacle than its reputation suggests, because it was designed to be recoverable. In a managed environment, the recovery key is almost always held somewhere: in the directory, in the device-management console, in a cloud account, in an escrow store the organisation set up precisely so that a forgotten password would not mean a lost laptop. The examiner's first move is not to attack the encryption but to find the key that already exists. Where no escrowed key exists, the drive may indeed be beyond reach, and the honest examiner says so. This guide sets out for UK lawyers how BitLocker, FileVault and their peers actually work, where their recovery keys live, how to obtain them lawfully, and how to tell the genuinely inaccessible drive from the one that is open with a key already in the client's possession.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Encrypted-drive examinations are routine laboratory work: locating BitLocker, FileVault and LUKS recovery keys in directories, device-management consoles and escrow stores, imaging the decrypted volume lawfully, and stating honestly where no key exists and the drive is genuinely beyond reach: reported under CPR Part 35 and CrimPR Part 19, with the recovery position established before any attack on the encryption is contemplated.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ENCRYPTED-DRIVE EXAMINATION | RECOVERY-KEY & ESCROW ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: FULL-DISK ENCRYPTION IS DESIGNED TO BE RECOVERABLE, AND IN A MANAGED ENVIRONMENT THE RECOVERY KEY ALMOST ALWAYS EXISTS SOMEWHERE THE ORGANISATION CONTROLS: THE EXAMINER'S FIRST TASK IS TO FIND THAT KEY, NOT TO ATTACK THE ENCRYPTION, AND ONLY WHERE NO ESCROWED KEY EXISTS IS THE DRIVE GENUINELY BEYOND REACH

How it works (§3): BitLocker (Windows), FileVault (macOS) and LUKS (Linux) encrypt the whole volume, protecting data at rest so a lost or stolen device reveals nothing; the volume is unlocked at boot by a passphrase, a hardware key tied to a secure chip, or a recovery key, and the encryption itself is sound: the security is real, and so is the recovery design behind it. **Where the keys live (§4):** BitLocker recovery keys are commonly escrowed to the directory or the cloud account and visible in the management console; FileVault keys can be held as institutional recovery keys or escrowed to the organisation or the user's cloud account; LUKS and server encryption keys sit in key-management and escrow systems: the managed device almost always has its key held where the organisation can retrieve it, precisely so a forgotten password never bricks a laptop. **Obtaining and imaging (§5):** the key retrieved lawfully from the store the organisation controls, the volume decrypted and imaged forensically, and the whole documented, so the "encrypted" drive is opened with a key already in the client's possession, no compulsion of any custodian required. **No key (§6):** where the device is personal and unmanaged, or the escrow was never configured, and the passphrase is genuinely unknown and strong, the drive may be beyond reach, and the honest examiner states that plainly rather than promising an attack that will not succeed (guide 117 §3). **Deployment (§7):** the recovery position, whether a key exists, established at the outset so the disclosure strategy is built on it, the drive opened lawfully where a key exists, and the estate's redundancy (guides 95, 117 §6) relied on where it does not.

- **Encryption is recoverable by design:** full-disk encryption was built so a forgotten password would not lose the data.
- **Find the key, do not attack the lock:** the managed device's recovery key almost always exists in a store the organisation holds.
- **Directory, console, cloud, escrow:** the four places a BitLocker or FileVault recovery key usually lives.
- **No escrow, maybe no access:** a personal, unmanaged, strongly-protected drive may be genuinely beyond reach, stated honestly.
- **Establish the recovery position first:** whether a key exists governs the whole disclosure strategy.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: encryption built to be recovered

Full-disk encryption exists to solve a specific problem: a laptop is lost or stolen, and the organisation does not want its data readable by whoever finds it. The design goal is that the device at rest, powered off, reveals nothing without the key. That goal is achieved, and achieved well: modern full-disk encryption is genuinely strong, and a drive protected by it, taken in isolation, is noise. This is why an encrypted drive intimidates: it looks like the lock of guide 117 at its most impregnable.

But there is a second design goal that the intimidation obscures: the same organisation that encrypts its laptops does not want a forgotten password to turn a working machine into a paperweight. So full-disk encryption is built to be recoverable. When BitLocker or FileVault is enabled in a managed environment, a recovery key is generated and, in almost every properly run deployment, escrowed: stored in the directory, the device-management console, or a cloud account, so that IT can unlock a device whose user has forgotten their password or left the company. The recovery key is the point. It means that in the corporate context, the "encrypted" drive is very rarely locked in any practical sense: the organisation holds the means to open its own device, and the examiner's job is to find that means, not to break the encryption. The genuinely inaccessible encrypted drive, personal, unmanaged, no escrow, a strong unknown passphrase, exists, but it is the exception, and the honest examiner distinguishes it from the far more common drive that is open with a key already in the client's hands. This guide is that distinction and how to act on it.

§ 0 3 · HOW IT WORKS

How BitLocker, FileVault and LUKS actually work

- **BitLocker (Windows):** encrypts the volume, with the encryption key protected by one or more protectors: a hardware security chip (the TPM) that releases the key at boot on a trusted machine, optionally a PIN or passphrase, and a recovery key generated at setup: the recovery key the escrowed fallback that unlocks the drive when the normal protector cannot (a moved disk, a changed configuration, a forgotten PIN).
- **FileVault (macOS):** encrypts the startup volume, unlocked at login by the user's password, with a recovery key generated at enablement that can be a personal recovery key shown to the user, an institutional recovery key held by the organisation, or a key escrowed to the organisation's management or the user's cloud account: the recovery key again the fallback the design provides.
- **LUKS and server encryption:** Linux full-disk encryption and enterprise server and storage encryption, unlocked by passphrases or key files, with keys typically held in key-management systems and escrow: the recovery design implemented through the organisation's key management rather than a consumer console.
- **Hardware-backed keys:** the security chip (TPM on Windows, the secure enclave on Apple silicon) that ties the encryption to the specific machine and releases the key only in a trusted state: strong protection that is exactly why the escrowed recovery key matters, because moving the disk to another machine defeats the hardware protector and requires the recovery key.
- **The common thread:** all three encrypt soundly and all three are built with a recovery mechanism, because unrecoverable encryption is a business risk no organisation accepts: the recovery key is not a weakness but a designed feature, and it is the examiner's route in.

§ 0 4 · WHERE THE RECOVERY KEYS LIVE

Where the recovery keys live: directory, console, cloud and escrow

- **The directory:** BitLocker recovery keys are commonly escrowed automatically to the organisation's directory (on-premises or cloud), retrievable by an administrator against the specific device: the first place to look for a managed Windows laptop's key, and often the only place needed.
- **The device-management console:** mobile-device-management and endpoint-management platforms store BitLocker and FileVault recovery keys against enrolled devices, visible to administrators: the console the organisation already uses to manage the fleet holding the key to each encrypted member of it.
- **The cloud account:** a BitLocker key escrowed to the user's or organisation's cloud account, and a FileVault key escrowed to the user's cloud account or the organisation's management: the key held in the account rather than on the device, retrievable through the account by consent, recovery or order (guide 117 §6).
- **Institutional and escrow keys:** FileVault institutional recovery keys deliberately generated so the organisation can unlock any managed Mac, and key-escrow systems for server and LUKS encryption: the organisation's deliberate provision for exactly this situation.
- **The printed or stored personal key:** the personal recovery key the user was shown at setup and may have printed, saved to a file, or stored in a password manager (guide 51): the key in the custodian's own records, sometimes produced on a simple request where the custodian is cooperative.

§ 0 5 · OBTAINING AND IMAGING

Obtaining the key lawfully and imaging the decrypted volume

- **Establish ownership and management first:** whether the device is company-owned and managed (recovery key almost certainly escrowed) or personal and unmanaged (recovery key may not exist anywhere the client can reach): the question that decides whether this is a simple retrieval or a genuine access problem (guide 117 §3).
- **Retrieve the key from the store the client controls:** for a managed device, the administrator retrieves the recovery key from the directory, console or cloud account against the device identifier: the client opening its own device with its own key, no compulsion of any custodian and no attack on the encryption.
- **Image the decrypted volume forensically:** the volume unlocked with the recovery key and imaged with a write-blocker or by a forensic decrypt-and-image process, hashed and documented (guides 2, 3): the decrypted image as sound and admissible as any other, the decryption step recorded as part of the method.
- **The independent-examiner option:** where the device is personal or mixed-use, or privilege and private data are in play, the recovery key used by an independent examiner who images and discloses only the relevant material (guides 97 §7, 115 §7, 117 §4): the drive opened without handing the whole of it to the opponent.
- **Document the recovery method:** the source of the key, the decryption step, the hash of the decrypted image and the chain of custody: the "encrypted" drive's opening fully explained, so no suggestion of unauthorised access or alteration can arise (guide 117 §7's self-help prohibition observed).

§ 0 6 · WHEN THERE IS NO KEY

When there is no key: the genuinely inaccessible drive

- **The unmanaged personal device:** a personally owned laptop with FileVault or BitLocker enabled by the user, never enrolled in any management, with the recovery key known only to the user and not escrowed anywhere the client can reach: the drive genuinely dependent on the user's key, obtainable only by their cooperation or a compulsion order (guide 117 §4 to §5).
- **The misconfigured or bypassed escrow:** a managed environment where escrow was not enabled, failed, or was deliberately bypassed by a technical user who suppressed key backup: the key that should exist not existing, established by checking the stores rather than assumed: sometimes itself a finding about the user's conduct.
- **The honest limit:** where no escrowed key exists and the passphrase is genuinely unknown and strong, the drive is, honestly, beyond reach by brute force: the examiner states this plainly rather than promising an attack that modern encryption defeats (guide 100's honest-limits discipline, guide 117 §3).
- **The reach-around still applies:** even a genuinely locked drive rarely holds the only copy: the cloud backups, syncs, server-side platforms and counterpart copies of guide 117 §6 frequently deliver the evidence while the drive stays shut: the encrypted drive reduced to its local-only residue.
- **Refusal as evidence:** where a key genuinely exists in the custodian's hands and they refuse it, the civil compulsion and adverse-inference machinery of guide 117 §4 applies: the withholding costly even if the drive is never opened.

§ 0 7 · DEPLOYMENT

Deployment: the recovery position, disclosure and honest limits

- **Establish the recovery position early:** whether a recovery key exists, and where, determined at the outset, because it governs everything: a key in the directory means routine collection, no key means the guide 117 access strategy: the disclosure plan built on the recovery reality, not on assumption.
- **The corporate default is access:** in most corporate matters the encrypted drive is openable with the organisation's own escrowed key, and the intimidating "the laptop is encrypted" objection dissolves on checking the console (Example 1): the encryption a non-issue where the key was escrowed as designed.
- **Honest limits where they apply:** for the genuinely unmanaged, unescrowed, strongly-protected drive, the honest statement that it is beyond reach, coupled with the estate reach-around and, where a key exists in the custodian's hands, the compulsion routes (guide 117): the position stated truthfully, neither over-promising access nor abandoning the reachable estate.
- **Admissibility of the decrypted image:** the decrypted volume imaged and hashed with the recovery method documented, so the opened drive is admissible and its integrity unchallengeable: lawful, key-based decryption producing evidence as sound as an unencrypted image (guides 2, 3).
- **The preventive lesson:** the organisation advised, as a matter of readiness, to ensure recovery-key escrow is enabled and the keys retrievable, so that a future dispute finds the keys where they should be: the encryption that protects the data at rest not becoming the obstacle to lawful access when access is needed.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: an encrypted drive is one node, and the key that opens it and the data it holds are both usually reflected elsewhere in a managed estate. The drive holds the local and deleted material behind the encryption. The recovery key sits in the directory, the management console, the cloud account or an escrow store, almost always for a managed device. The same data is reflected in the cloud backups made before or despite the encryption, the synced copies on other devices, the server-side mailbox, drives and SaaS, and the counterparts' copies. The discipline is to check the recovery stores first, because the managed drive is typically open with a key the organisation holds, and then, whether or not the drive opens, to map the estate that holds the same data unencrypted. When the drive is managed, its own key opens it; when the drive is unmanaged and truly locked, the estate carries the case and a custodian-held key becomes adverse-inference evidence if refused; when escrow was suppressed, that suppression is itself a finding about conduct. The encrypted drive intimidates in isolation and dissolves in context.

QUESTION	ENCRYPTED DRIVE	RECOVERY-KEY STORES	CLOUD BACKUP	SYNCED / COUNTERPART COPIES	SERVER-SIDE PLATFORMS	DELETED / LOCAL-ONLY
The key to open it	Held by protector	Y: directory, console, cloud, escrow	n/a	n/a	n/a	n/a
Documents	Behind encryption	Opens the drive	Y: synced copy	Y: shared copies	Y: drives, SaaS	Local-only files
Messages	Behind encryption	Opens the drive	Y: pre-encryption backup	Y: counterparts	Y: mailbox, chat	Local caches
Local-only / deleted	Y: drive only, once open	Opens to reach it	Sometimes	n/a	Version history	Y: once decrypted
Was escrow suppressed	Configuration on device	Y: absence is the finding	n/a	n/a	Management logs	n/a

Fallback strategy in one line: check the recovery-key stores first because the managed drive is usually open with the organisation's own key; where no key exists, map the estate that holds the same data unencrypted, and treat a refused custodian-held key as evidence.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE BITLOCKER LAPTOP THAT WAS OPEN ALL ALONG

An employer's IT team reported that a departed employee's company laptop was "BitLocker encrypted and inaccessible", and the litigation team feared a compulsion fight for the password. The §4 first check dissolved the problem in ten minutes: the laptop had been enrolled in the company's own endpoint-management platform, which had escrowed the BitLocker recovery key to the directory automatically at setup, exactly as designed. The administrator retrieved the recovery key against the device's identifier, and the §5 process unlocked and imaged the decrypted volume forensically, hashed and documented. No password was compelled, no encryption was attacked, and no custodian cooperation was needed: the employer had held the key to its own device the entire time. The lesson is §2's: in a managed environment the encrypted drive is very rarely locked in any practical sense, and the first move is always to check the recovery stores, not to reach for a court order.

EXAMPLE 2 · THE SUPPRESSED ESCROW THAT TOLD ITS OWN STORY

In an intellectual-property dispute, a technically sophisticated departing engineer's managed Mac was returned FileVault-encrypted, and the recovery key was not in the management console where every other device's key sat. The §6 investigation established why: the engineer had, shortly before leaving, altered the device's configuration to suppress the escrow of the recovery key to the organisation, so that the key that should have been retrievable was not: an act recorded in the management logs and inconsistent with any innocent explanation. The drive itself was, for the moment, genuinely inaccessible (§6's honest limit). But the §8 estate carried the case: the engineer's mailbox, the corporate cloud drive and the code repositories held the relevant material server-side, and the suppression of the escrow key became evidence in its own right, a deliberate step to obstruct access, deployed alongside the guide 110 anti-forensic findings. The missing key was not the end of the matter; it was part of the case.

EXAMPLE 3 · THE PERSONAL MACBOOK AND THE HONEST LIMIT

A claimant in an employment matter had done some work on a personally owned MacBook with FileVault enabled by her, never enrolled in any employer management, the recovery key known only to her. The employer demanded the laboratory "decrypt it". The §3 and §6 honest assessment was clear: the encryption was sound, no escrowed key existed anywhere the employer could reach, and brute force would not open a strong passphrase in any useful time. Rather than promise an impossible attack, the examiner stated the position plainly (§6): the drive was accessible only with the claimant's own key or by her cooperation. The §7 route was the guide 117 machinery, a disclosure order requiring her to provide the key or enable access, on independent-examiner terms protecting her private data, with adverse inference available if she refused without good reason. The honest limit was stated, the estate reach-around was pursued for what existed elsewhere, and the lawful compulsion route was used for the residue: no false promise of decryption was made.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Treating a managed encrypted drive as locked:** Example 1's fear: a compulsion fight contemplated when the recovery key sat in the client's own directory all along.
- **Not checking the recovery stores:** the directory, console, cloud and escrow left unchecked, the simplest route to access skipped in favour of attacking the encryption (§4).
- **Promising to decrypt the unmanaged drive:** Example 3's demand: an impossible brute-force attack promised on a sound, unescrowed, strongly-protected drive (§6).
- **Missing the suppressed escrow as a finding:** Example 2's engineer: the absent key treated only as an obstacle, not recognised as evidence of deliberate obstruction.
- **Booting the device to check:** the encrypted laptop powered on and logged into by IT "to see", altering the drive and its artefacts before forensic imaging (guides 108, 110).
- **Self-help decryption attempts:** unauthorised attempts to access the drive rather than lawful key retrieval or compulsion (guide 117 §7).
- **The estate ignored:** a genuinely locked drive treated as the only source while backups, syncs and server-side platforms held the same data (§8).
- **Escrow readiness never advised:** the organisation not advised to ensure recovery-key escrow is enabled and retrievable, so a future dispute finds the keys missing.

Technical limitations

- **Sound encryption is sound:** BitLocker, FileVault and LUKS with strong protectors and no escrowed key are not brute-forceable in useful time: the honest limit, stated where it applies.
- **Hardware protectors tie the key to the machine:** moving the disk defeats the TPM or secure-enclave protector and requires the recovery key, which is exactly why the escrowed key matters (§3).
- **Escrow depends on configuration:** a key is escrowed only if the environment was configured to escrow it; unmanaged and misconfigured devices may have no retrievable key (§6).
- **Personal cloud escrow needs the account:** a key escrowed to the user's personal cloud account is reached only through that account, by consent or order (guide 117 §6).
- **Decryption must preserve integrity:** the decrypt-and-image process is documented and hashed so the decrypted image's integrity is unchallengeable (§5).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the encrypted device company-managed, so a recovery key is almost certainly escrowed, or personal and unmanaged, where it may not be?
- Have the directory, device-management console, cloud account and escrow stores been checked for the recovery key against this device?
- If a managed device's key is missing, was escrow suppressed or misconfigured, and is that itself relevant?

Ask your opponent (or the reluctant party)

- Please confirm whether the encrypted device(s) are managed such that a BitLocker, FileVault or equivalent recovery key is escrowed to a directory, management console, cloud account or escrow store, and if so provide the recovery key or enable access.
- Please confirm whether any recovery-key escrow was disabled, suppressed or removed in respect of the device(s), and if so when, by whom and why.
- Where no escrowed key exists, please provide the passphrase or recovery key necessary to access the relevant material, on terms that an independent examiner access the device and disclose only the relevant material.

Ask your eDiscovery / forensic provider

- Is this device managed, and is its recovery key retrievable from a store the client controls?
- If the key is missing from a managed device, does the configuration show escrow was suppressed?
- Where the drive is genuinely locked, what does the estate hold unencrypted, and what exists only on the drive?

SUGGESTED WORDING · INSTRUCTION FOR AN ENCRYPTED-DRIVE EXAMINATION

> "We instruct you to examine the encrypted device(s) identified at Schedule 1. Please: (1) establish whether each device is company-managed or personal, and whether a BitLocker, FileVault or equivalent recovery key is escrowed to the directory, device-management console, cloud account or an escrow store the client can lawfully access; (2) where a recovery key is available, retrieve it lawfully, decrypt and forensically image the volume, and document the source of the key, the decryption method, the hash of the decrypted image and the chain of custody; (3) for any managed device whose key is unexpectedly absent, establish whether recovery-key escrow was disabled, suppressed or removed, and when and by whom, treating any such act as potentially relevant; (4) where no recovery key exists and the passphrase is genuinely unknown, state that position honestly rather than attempting an unfeasible attack, and identify the material available from backups, synchronised copies and server-side platforms instead; and (5) where access requires a key held only by a custodian, advise on the lawful routes to compel or obtain it. Do not power on or alter any device before forensic imaging."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The encrypted-drive checklist

- ☐ Device ownership and management status established first
- ☐ Directory checked for escrowed BitLocker recovery keys
- ☐ Device-management console checked for BitLocker and FileVault keys
- ☐ Cloud account and escrow stores checked
- ☐ Custodian's own records checked for a printed or stored personal key
- ☐ Recovery key retrieved lawfully; no encryption attack attempted
- ☐ Decrypted volume imaged, hashed and the method documented
- ☐ Missing key on a managed device investigated as possible suppression
- ☐ Honest limit stated where no key exists and the passphrase is strong
- ☐ Estate mapped for the same data held unencrypted elsewhere

Red flags

- A managed encrypted device declared "inaccessible" without checking the recovery stores: Example 1.
- A recovery key missing from a managed device whose peers all have theirs: Example 2's suppression.
- A demand to brute-force an unmanaged, strongly-protected personal drive: Example 3.
- An encrypted device powered on by IT before imaging.
- Any self-help attempt to access the drive.
- Escrow found to have been disabled shortly before a departure.
- A locked drive treated as the only source while the estate held copies.

When to involve a digital forensic expert

At the outset, to establish the recovery position, whether and where a key exists, because it governs the whole disclosure strategy and often turns an intimidating "encrypted drive" into a routine retrieval (Example 1); before any device is powered on, because booting alters the drive; where a managed key is unexpectedly missing, to establish whether escrow was suppressed and whether that is a finding (Example 2); where the drive is genuinely unmanaged and locked, for the honest assessment and the estate reach-around rather than a false promise of decryption (Example 3); and at deployment, where the decrypted image's integrity and the recovery method are explained under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, encrypted-drive examinations begin by finding the key the organisation already holds, image the decrypted volume lawfully and defensibly, and state honestly where no key exists: because the encrypted drive is usually open with a key in the client's possession, and knowing that is worth more than any attempt to break the encryption.

§ 13 · COMMON QUESTIONS

Frequently asked questions

The laptop is BitLocker encrypted. Is the data lost?

Almost certainly not, if it is a managed company device: BitLocker 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 organisation 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 FileVault there may also be an institutional recovery key the organisation 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 BitLocker or FileVault 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 lawfully 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.

§ 14 · REFERENCE

Glossary

Full-disk encryption
Encryption of an entire volume, protecting data at rest.

BitLocker
Windows full-disk encryption, with escrowable recovery keys.

FileVault
macOS full-disk encryption, with personal and institutional keys.

LUKS
Linux full-disk encryption, with key-management escrow.

Recovery key
A fallback key that unlocks an encrypted drive.

Escrow
Storing a recovery key where the organisation can retrieve it.

TPM
A hardware chip releasing the key on a trusted machine.

Institutional recovery key
A key letting an organisation unlock any managed Mac.

Protector
A mechanism guarding the encryption key (TPM, PIN, recovery key).

Decrypt-and-image
Unlocking a volume and forensically imaging it.

Sources and authoritative references

The encrypted-drive disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (encrypted-drive examination, recovery-key retrieval and decrypt-and-image, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (encrypted-source collection and estate reach-around as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft, BitLocker recovery and key escrow guidance: learn.microsoft.com, BitLocker · Apple, FileVault and institutional recovery keys: support.apple.com, FileVault
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices: csrc.nist.gov, SP 800-111
- PD 57AD and CPR Part 31 (disclosure and control): justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35 · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Encrypted-drive work at the laboratory begins with the recovery position, because it usually changes the whole picture: for a managed device, the BitLocker or FileVault recovery key is almost always escrowed to the directory, the management console, a cloud account or an escrow store, and the intimidating "the laptop is encrypted" objection dissolves the moment those stores are checked (Example 1). The key is retrieved lawfully, the decrypted volume imaged and hashed with the method documented, and the collection proceeds as normal, no attack on the encryption, no compulsion of any custodian. Where a managed device's key is unexpectedly absent, the laboratory establishes whether escrow was suppressed and treats that as the finding it often is (Example 2). Where the drive is genuinely unmanaged and strongly protected, the honest limit is stated plainly and the estate reach-around and the guide 117 compulsion routes are used instead of a false promise of decryption (Example 3). Devices are never powered on before imaging, and access is never attempted by self-help. Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if an encrypted device has come in, the first and most useful question is simply: where is its recovery key, and does the client already hold it?

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace