COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Should a Computer Be Imaged While Running or Switched Off?

Volatile Data, Encryption and the Most Consequential Button in Forensics

For years the rule was simple: pull the plug and image the drive cold. Full-disk encryption ended that era. Power off a running BitLocker or FileVault machine without the credentials and the evidence may seal itself permanently; leave it running carelessly and every minute changes the data. Between those hazards sits a decision that must be made at the machine, by someone competent, and recorded: capture the memory, assess the encryption, then choose. This guide explains volatile data, what lives only in RAM, how BitLocker and FileVault change the calculus, the honest risks of both live and offline acquisition, and the at-the-machine framework that keeps the decision defensible.

⏱ Estimated reading time: 28 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. Its examiners make the live-or-offline call at machines every week: RAM captures ahead of shutdowns, live acquisitions of encrypted and production systems, and classic write-blocked dead-box imaging where that is the cleaner path, each decision logged under the NPCC principles and, where criminal-justice work requires, the Forensic Science Regulator Code. Its eDiscovery arm, **e-discovery.uk**, builds the same judgment into collection planning at disclosure scale, so nobody's first encounter with an encrypted laptop happens at the laptop.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ISO 27001-ALIGNED SECURITY | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | RAM CAPTURE & LIVE ACQUISITION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: ASSESS FIRST, CAPTURE MEMORY IF YOU CAN, AND LET ENCRYPTION DECIDE THE REST

Whether to image a computer running or switched off is no longer a matter of habit; it is a risk decision with permanent consequences in both directions. A machine that is **off stays off**: it is transported and imaged write-blocked, the cleanest acquisition there is, but if its disk is encrypted the recovery credentials must be located before anyone expects to read the image. A machine that is **on and unlocked** is a fleeting opportunity: memory can be captured (running processes, network connections, unsaved work and, critically, the decryption keys of mounted encrypted volumes), the encryption state can be assessed, and a live or logical acquisition of the decrypted data can be taken before any shutdown, because powering off an encrypted machine without credentials may seal the evidence permanently. A machine that is **on and locked** offers narrower options and a hard rule: do not guess passwords. Every path changes something or loses something; the discipline is that the choice is made by a competent person, at the machine, on an assessed basis, and recorded so it can be explained: the NPCC second principle, applied at the most consequential button in forensics.

- **"Pull the plug" is a legacy rule.** It optimised for disk integrity in an unencrypted world; with BitLocker on by default across modern corporate Windows estates and FileVault across Macs, the same reflex now risks converting readable evidence into ciphertext with no key.
- **RAM is evidence, and it evaporates.** Memory holds what no disk image will: live sessions, cloud tokens, chat state, unsaved documents, running malware, and mounted-volume keys. If the machine is on and the matter may need any of that, memory capture comes first, always.
- **Credentials are a collection task, not an afterthought.** Recovery keys are routinely escrowed (Active Directory and Entra for BitLocker, institutional or iCloud escrow for FileVault) and passwords lawfully obtainable from custodians; hunting them belongs in the plan before anyone stands at a machine.
- **Live acquisition is legitimate, footprint and all.** Running tools on a live system changes it; done competently, the changes are small, known, logged and explicable, and courts accept exactly that. The indefensible version is not the footprint but the silence about it.
- **Lawyers own the pre-decision:** ensuring nobody untrained touches a powered-on machine, that credentials and escrow are pursued in parallel, and that the standstill instruction now includes the sentence "if it is on, leave it on and call; if it is off, leave it off."

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the button and its consequences

Picture the moment this guide exists for. A director has been suspended; his laptop sits on his desk, lid open, screen unlocked, Teams still signed in. Three people have opinions. The office manager wants to shut it down "so nothing changes". The IT technician wants to have a look around first "while we can". The HR adviser wants it locked in a cupboard tonight and dealt with later. Each instinct destroys something:

- **Shutting it down** discards everything in memory: the open documents, the sessions, the connections, and (if the disk is encrypted, as it almost certainly is) potentially the practical ability to read the disk at all, unless someone can produce the credentials or the escrowed recovery key.
- **Having a look around** writes hundreds of changes under the very user profile in dispute: access times updated, caches touched, and a defence gift-wrapped ("the company was all over this machine after I left").
- **The cupboard overnight** leaves an unlocked, network-connected machine running: remote wipe reachable, sync continuing, screen lock or sleep about to change the state anyway, and the volatile evidence decaying with every hour.

The correct move is none of the three: photograph the screen, keep the machine awake and off the network if remote wipe is a realistic risk (a decision itself requiring thought), touch nothing else, and get a competent examiner to it, who will capture memory, assess encryption and choose the acquisition path on evidence. The rest of this guide explains what that examiner is weighing, so the lawyer in the room can recognise the right process, insist on it, and later defend or attack the choice that was made.

§ 0 3 · WHAT EVAPORATES

Volatile data: what lives only in memory

Volatile data is everything that exists only while power flows. In descending order of fragility:

- **RAM contents:** running processes and their data; unsaved and open documents; clipboard contents; chat and webmail sessions as rendered; cached passwords and authentication tokens for cloud services; and the decryption keys of any encrypted volume currently mounted: the single item that most changes acquisition strategy. Malware, if present, often lives here and nowhere else.
- **Network state:** active connections, remote sessions, mapped drives and VPN tunnels: who or what this machine is talking to right now, which in exfiltration and intrusion cases can be the story itself.
- **Running-system state:** logged-in users, open files, mounted devices and containers: the configuration of the moment, reconstructable only partially from disk afterwards.
- **Semi-volatile traces:** some memory content reaches disk on its own: the pagefile, and on machines that hibernate, the hibernation file, which is a copy of RAM frozen at the moment of hibernation. These sometimes rescue a case where no live capture happened, and a later guide's insider-trading clipboard example came from exactly such a source.

Memory capture is the acquisition answer: a small validated tool reads RAM into a hashed evidence file, taking minutes. It is performed first, before anything else is touched, because every other action (including the capture itself, modestly) changes memory; the tool's own footprint is known, documented and accepted practice. Whether memory matters enough to shape the whole approach depends on the matter: in an exfiltration, intrusion or encryption scenario, almost always; in a dispute purely about last year's emails, rarely, and the framework in §7 weighs exactly that.

§ 0 4 · THE GAME CHANGER

Encryption changes everything: BitLocker, FileVault and friends

- **The core distinction: encrypted at rest versus unlocked in use.** Full-disk encryption protects data when the machine is off; while it runs unlocked, the data is transparently decrypted and the key material sits in memory. Power-off flips the state: the running, readable estate becomes ciphertext, and the question becomes whether anyone can produce the key.
- **BitLocker (Windows):** on by default across modern corporate Windows. Protectors vary (TPM-only machines boot to the login screen and can often be imaged and unlocked with escrowed keys; TPM-plus-PIN and password-protected volumes will not open without their secrets). The saving grace is escrow: corporate estates routinely back recovery keys into Active Directory or Entra ID, and personal machines into the user's Microsoft account. The recovery-key hunt (IT, directory, account portals) is therefore a day-one task, not a post-imaging discovery.
- **FileVault (macOS):** the Mac equivalent, with recovery keys held personally, in iCloud, or via institutional keys under device management. Apple Silicon's architecture ties storage to the specific machine, which raises the stakes of hardware handling and makes credential recovery even more central; the Mac guide later in this series expands on this.
- **Container and volume encryption (VeraCrypt and kin):** encrypted containers mounted as drives while in use, invisible or inert when closed. A live machine with a mounted container is the only easy moment to acquire its contents (or capture the key from RAM); after dismount or shutdown, access depends entirely on the password or on key material recovered from memory captures and hibernation files.
- **The strategic consequence:** encryption converts the live-versus-offline question from preference to arithmetic. Running and unlocked plus encrypted equals acquire now (memory, then the decrypted estate) or be certain of the credentials before anyone touches power. Off plus encrypted equals leave it off and hunt keys before promising anyone a readable image. The examiner's first assessment at any machine is exactly this state.

§ 0 5 · THE CLASSIC PATH

Offline (dead-box) acquisition: strengths and risks

- **What it is:** the machine powered off (or already off), storage removed or accessed via boot-safe methods, imaged through a write blocker into a verified forensic container. The source is never booted; nothing on it changes.
- **Strengths:** the cleanest evidential story ever told: zero alteration, perfect repeatability, the gold standard for contested devices, and procedurally simple to defend. Deleted material, artefacts and unallocated space are captured exactly as the last shutdown left them.
- **Risks and costs:** everything volatile is already gone, including mounted-container keys; an encrypted disk yields ciphertext until credentials or recovery keys are produced, which can mean delay or, at worst, permanent lockout; hardware realities intrude (soldered storage, hardware-bound encryption on modern laptops and Macs, RAID members that mean nothing imaged alone); and taking a live business machine down has operational cost the plan must own.
- **Its proper domain:** machines found off (leave them off); unencrypted or credential-secured devices where volatile data is not in play; and the contested device where maximum-integrity imaging is the priority and the credential position is already known. The classic error is applying it by reflex to a running encrypted machine, which is §10's first story.

§ 0 6 · THE MODERN NECESSITY

Live acquisition: strengths and risks

- **What it is:** acquisition from the running system: memory capture first, then, as the matter requires, a live image of the disk (reading the decrypted data through the running OS) or a targeted logical acquisition of the decrypted estate, all with validated tools run from external media, logged as they go.
- **Strengths:** it captures what only exists now: memory and its keys, the decrypted contents of encrypted volumes, network and session state, and the running truth of the machine. For encrypted devices without assured credentials, it is not merely stronger; it may be the only path to readable evidence.
- **Risks, honestly stated:** the tools have a footprint (processes run, small writes occur, memory shifts); the target moves while acquired (a live image is a snapshot of motion, and hashes attach to the image taken, not to a frozen source); a hostile environment can interfere (malware, dead-man scripts, remote access still open); and the whole exercise demands competence: this is precisely the "accessing original data" the NPCC second principle governs, and the operator must be able to explain every change their presence caused.
- **Managing the risks:** minimal-footprint validated tools; a fixed order of operations (most volatile first); network isolation decided deliberately (against remote wipe, weighed against cloud-session evidence that isolation kills); contemporaneous logging of every action and time; and, where feasible, following the live acquisition with a dead-box image once credentials are secured, giving the case both the decrypted estate and the pristine artefact layer.

§ 0 7 · THE DECISION

The at-the-machine decision framework

The examiner's sequence, which the lawyer's plan should anticipate and the record should show:

S1 **photograph machine and screen; note power state, lock state, visible applications, network connections, external media; record time against reference clock.**

OFF →	**It stays off.**	Label, bag, transport; image dead-box through a write blocker. In parallel: establish encryption status and hunt credentials and recovery keys (custodian, IT, directory escrow, account portals) before anyone expects a readable image.
ON + UNLOCKED →	**The fleeting opportunity.**	Prevent sleep and screen lock (a deliberate, logged act); decide network isolation (remote-wipe risk versus live-session evidence); **capture memory first**; assess encryption from the running system; if encrypted or containers are mounted, acquire the decrypted estate (live image or targeted logical) before any power event; then shut down by the method the situation justifies (graceful shutdown writes tidily but triggers scripts; hard power-off freezes disk state but discards the tidy-up: the choice is recorded either way) and complete with a dead-box image where warranted.
ON + LOCKED →	**Narrow options, hard rules.**	Do not guess passwords (lockouts and, on managed devices, wipe policies punish attempts). Memory capture may still be possible and worthwhile by technical means where justified; otherwise pursue credentials and escrowed keys, weigh waiting against risk, and treat power-off as the last resort taken only with the credential position understood.
ASLEEP / HIBERNATING →	**Ambiguous, treat with care.**	Sleep is memory alive on low power (waking it is an option with consequences; letting it die is a shutdown by neglect); hibernation has already written memory to disk, which is good news for the dead-box path. Identify which state before acting, and log the reasoning.

Two constants across every branch: **memory first** whenever it is available and could matter, because no later step can recover it; and **the log**, because every branch involves judgment, and judgment undocumented is judgment attackable.

§ 0 8 · BEYOND THE LAPTOP

Servers, sleep states and special cases

- **Production servers are not switched off.** The business impact is unjustifiable and RAID arrays image poorly as separated disks. Server acquisition is live or logical by design: memory where intrusion is in play, targeted acquisition of the relevant shares and databases, VM snapshots where the estate is virtualised (a clean parallel path: snapshot the guest, acquire the snapshot, production undisturbed), and the server's logs collected alongside. The servers and virtualisation guides later in this series expand each.
- **Mobile devices run their own rules:** phones are effectively always-on encrypted devices whose acquisition windows are governed by lock state and OS version; the instinct that matters is isolation (airplane mode, Faraday) against remote wipe, and the mobile guides treat the rest.
- **Machines mid-activity:** a computer found actively transferring, wiping or communicating presents the rare case where intervention (pulling network, even power) may be justified to stop ongoing destruction, accepting the volatile loss: a recorded judgment call, made on what was observable at the time.
- **The second visit problem:** live opportunities rarely recur. A machine acquired lightly today and returned to use will not present the same memory, sessions or mounted containers again; if the matter's gravity is uncertain, err toward capturing the fleeting layer while it exists.

§ 0 9 · THE PAPER

Recording the decision: NPCC principle 2 in action

- **The principle:** where accessing original data is necessary, the person doing so must be competent and able to explain the relevance and implications of their actions. Live acquisition is this principle's home ground: the footprint is legitimate exactly to the extent it is understood, minimised and recorded.
- **What the record shows:** the state found (photographs, times, observations); the assessment made (encryption indicators, credential position, volatile-data value, isolation decision); the actions taken in order, with tools, versions and times; the changes those actions are known to cause; the hashes of everything captured; and the shutdown method chosen with its reason.
- **Why it wins later:** a challenge to live acquisition succeeds against silence ("what else did you change?") and fails against a log ("these processes, these writes, this footprint, all documented, none touching the material in issue"). The other side's expert, given the record, verifies rather than speculates, and verified footprints end arguments.
- **The lawyer's checkpoints:** before: is a competent person making this call, to a written plan? After: does the file contain the state photographs, the decision log and the hashes? In attack: does the opponent's file contain them, and if not, what exactly happened at their machine, and who says so?

§ 10 · IN THE WILD

Worked examples

EXAMPLE 1 · THE PLUG PULLED ON BITLOCKER

An operations manager, suspended in a procurement fraud inquiry, left his laptop running and unlocked. A security officer, following decade-old training, held the power button until it died and locked it in the safe: textbook, once. The disk was BitLocker-encrypted with TPM plus PIN; the manager declined to provide the PIN; and the recovery key was in none of the escrows, because the machine had been rebuilt outside policy two years earlier. The unlocked, readable estate that had sat open on the desk (including, per a colleague's witness statement, a spreadsheet of side-company payments on screen) became ciphertext at the moment the button was held. The inquiry proceeded on server-side fragments; the disk has never been read. Total distance between the evidence and its loss: one competent hour that was never called for.

EXAMPLE 2 · THE RAM CAPTURE THAT HELD THE KEY

In a fraud investigation, a suspect's laptop appeared clean until a 40 GB extensionless file of pure noise turned up in a games folder: a VeraCrypt container, dismountable and passwordless. What saved the case was sequence: the examiner who attended the seizure had captured memory before shutdown as routine. The capture held the container's master key material; the volume was mounted from the key; and the decrypted contents (a second set of accounts) became the exhibit around which the matter resolved. Nothing about the container was known when the memory was taken. The capture was ten minutes of standard discipline, performed because the machine was on and the rule is memory first.

EXAMPLE 3 · THE LIVE ACQUISITION THAT SURVIVED CHALLENGE

A defendant company's key server could not be powered down, so acquisition was live: memory, then targeted collection of the disputed database and shares, tools run from external media, every action timed in the log. Eighteen months later the claimant's expert alleged the acquisition had "contaminated" the server and the data could not be relied on. The response exhibited the acquisition record: the tool set and versions, the known footprint (named processes, listed writes, none within the database files), the hash schedule, and the running-state photographs. The claimant's expert, invited to identify any artefact inconsistent with the log, identified none; the challenge was abandoned in the joint statement. The footprint was real, disclosed and irrelevant, which is exactly what the record existed to show.

§ 11 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The reflex power-off** of a running encrypted machine, by security staff, IT or well-meaning managers: the modern era's single most expensive habit.
- **The look-around:** browsing the live machine under the disputed profile before any capture, seeding the file with post-dispute activity.
- **Memory skipped** because "we only need the documents", discovered to matter when the container, the session or the deletion question surfaces later.
- **Password guessing at locked machines,** burning lockout counters and, on managed devices, walking into wipe policies.
- **Credentials hunted after imaging:** the readable-image promise made to the client before anyone checked what BitLocker would say about it.
- **Isolation unconsidered:** the machine left online for remote wipe, or yanked offline in a way that destroyed the live cloud sessions that were the evidence.
- **Graceful-versus-hard shutdown unrecorded:** either can be right; unexplained, either is a cross-examination theme.
- **Untrained live work:** IT staff running admin tools across the estate "to acquire it", with a footprint nobody can now separate from the events in issue.

Technical limitations

- **Memory capture is imperfect by nature:** RAM changes during the capture, some regions resist acquisition, and the tool's own presence occupies space; the product is an evidentially excellent approximation, not a frozen instant, and honest reports say so.
- **Live images are snapshots of motion:** hashes verify the image taken, not a stilled source; the acquisition log carries the burden a write blocker carries in the dead-box world.
- **Encryption sometimes wins:** no credentials, no escrow, no memory capture, no hibernation file can mean no access, lawfully and finally; the examiner's evidenced statement of that position is itself the deliverable, and compelled-disclosure routes (in civil orders or, in criminal contexts, RIPA Part III machinery) are legal questions beyond this guide's scope.
- **Hostile environments deceive:** a compromised machine can misreport to live tools; where intrusion is the issue, findings from live acquisition are corroborated against disk, logs and network sources before weight is put on them.

§ 12 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which relevant machines are currently on, off, or in unknown states, and who can keep them exactly as they are until the examiner arrives?
- What disk encryption does the estate use, and where are recovery keys escrowed (Active Directory, Entra, MDM, account portals)? Can IT verify escrow for the specific devices today?
- Is remote wipe enabled for these devices, and who can suspend it without touching the machines?

Ask your opponent

- For each relevant device: in what power state was it found, who made the live-or-offline decision, and against what record?
- Was memory captured; if not, why not, and what volatile material may thereby be unavailable?
- Please provide the acquisition logs for any live acquisition, including tools, versions, times and the known footprint, and the shutdown method used for each machine.

Ask your eDiscovery / forensic provider

- Who attends powered-on machines, with what kit and what written order of operations?
- How do you decide network isolation, and how is that decision recorded?
- What is your memory-capture tool's validated footprint, and how is it disclosed in reports?
- If the device proves encrypted without credentials, what exactly will you do, in what order, and what will you tell us at each stage?

SUGGESTED WORDING · ADDITION TO THE CLIENT STANDSTILL INSTRUCTION

> "For any computer or device relevant to this matter: if it is switched on, leave it switched on, do not close the lid, do not log off, do not let anyone use or examine it, and telephone us immediately; if it is switched off, leave it switched off and secure it as it is. Do not attempt passwords on any locked device. Please also ask IT, without touching the devices, to (a) confirm what disk encryption applies and where recovery keys are held, and (b) suspend any remote-wipe capability for the listed devices, confirming both in writing. The difference between a readable and an unreadable machine can be decided by these steps in the next hour."

SUGGESTED WORDING · INSTRUCTION TO THE EXAMINER ATTENDING A LIVE MACHINE

> "You are instructed to attend and assess the device in its current powered-on state and to proceed in accordance with good practice, namely: recording the state found by photograph and note before any interaction; capturing volatile memory before other acquisition steps; assessing encryption status and any mounted containers from the running system; acquiring the decrypted estate by live or targeted means where encryption so requires; determining and recording the network-isolation and shutdown decisions with reasons; and completing dead-box imaging thereafter where appropriate. All tools, versions, actions and times are to be logged contemporaneously, all captures hashed, and any changes caused by your presence identified in your note. Please report the credential and escrow position for the device before any power-off it if it can be safely deferred."

§ 13 · QUICK CONTROL

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

The live-or-offline checklist

- ☐ Standstill instruction issued in the on-stays-on, off-stays-off form; nobody touching machines
- ☐ Encryption estate and key escrow verified with IT in parallel, before power decisions
- ☐ Remote-wipe capability identified and suspended without touching devices
- ☐ Competent examiner attending powered-on machines with a written order of operations
- ☐ State photographed and logged before interaction; reference time recorded
- ☐ Memory captured first wherever available and potentially material; capture hashed
- ☐ Encryption and mounted containers assessed live; decrypted estate acquired before any power event where needed
- ☐ Isolation and shutdown decisions made deliberately and recorded with reasons
- ☐ Dead-box imaging completed where warranted once credentials secured; both acquisitions cross-referenced
- ☐ Full acquisition log, tool footprint disclosure and hash schedule filed as the decision's defence

Red flags

- "Security switched it off to be safe."
- An encrypted image delivered with no credential plan attached.
- Browsing history on the disputed profile dated after the dispute.
- No memory capture in a matter about deletion, exfiltration or containers.
- A locked device with a climbing failed-attempt counter.
- A live acquisition with no log, or a log written afterwards.
- An opponent's account of the machine's handling that has no photographs, no times and no named decision-maker.

When to involve a digital forensic expert

Before anyone touches a powered-on machine: this is the single scenario in the series where hours matter most, because the unlocked state is perishable and the wrong reflex is irreversible. Involve the laboratory the same day where a relevant machine is on, where encryption without assured credentials is suspected in any state, where remote wipe is plausible, where containers or exotic encryption may be present, and where a server or live system must be acquired without downtime. Involve them retrospectively where the other side's machines were handled by amateurs: an examiner's statement of what a reflex power-off or an untrained look-around cost, and of what the absent records would have shown, converts mishandling from anecdote into submission. And where the impossible has happened (the encrypted device with no keys), the examiner's evidenced no-access statement is the honest end of the line, and the beginning of the legal routes that lie beyond it.

§ 14 · COMMON QUESTIONS

Frequently asked questions

Is it ever right just to pull the plug?

Occasionally, as a recorded judgment: classically where destruction is visibly in progress (a wipe running, mass deletion under way) and stopping it outweighs everything volatile, or where the machine is known unencrypted and volatile data is genuinely irrelevant. What is never right is the reflex version: unassessed, unrecorded, by whoever was standing closest. The question the file must answer is not "was the plug pulled?" but "who decided, on what assessment, and where is it written?"

An employee's laptop is on their desk, unlocked, and they have just been suspended. What do we actually do in the next hour?

Photograph the screen as found; keep the machine awake if you can do so without exploring it (a deliberate mouse-nudge regime is legitimate and should be logged); do not read, open or close anything; decide with advice whether to disconnect the network (remote-wipe risk usually says yes for a managed device); have IT verify encryption and recovery-key escrow without touching the device; and get an examiner attending the same day. The unlocked state is the most valuable evidential window this matter will ever have; spend it on nothing except preserving it.

Does live acquisition contaminate the evidence?

It changes the machine, in small, known, documented ways: that is different from contamination. The forensic position, accepted by courts for years, is that a competent live acquisition's footprint is minimal, identified and separable from the material in issue, and the acquisition log exists to demonstrate exactly that. The evidential danger is not the footprint; it is the undocumented footprint, and the amateur one, neither of which can be separated from anything.

The laptop is asleep. Is that on or off?

On, for the purposes that matter: memory is powered and its contents (including any mounted-volume keys) survive, but the state is fragile: batteries die, and lids and timers can tip sleep into shutdown or hibernation. Treat a sleeping machine as a ticking version of the on-and-locked or on-and-unlocked case, identify which it will wake into, and get the examiner to it before the battery makes the decision instead. Hibernation, by contrast, has already written memory to disk, which the dead-box path can recover: the states differ, and the response should too.

We have the BitLocker recovery key but not the user's password. Is that enough?

For the disk, generally yes: the recovery key unlocks the volume for imaging and examination without the user's cooperation, which is precisely why verifying escrow early changes the whole strategy's risk. It will not, of course, open separately protected things that live inside (password-protected files, application-level encryption, mounted-container secrets), and it says nothing about a machine whose key was never escrowed. Hence the standing rule: confirm the key position per device, in writing, before anyone relies on it.

Should company policy change because of any of this?

Two cheap amendments repay themselves the first time they are needed: an incident rule that powered-on devices of departing or suspended staff are left on, isolated and referred (replacing the switch-it-off training of the unencrypted era), and an IT rule that encryption recovery keys are escrowed verifiably for every corporate device, audited annually. Both convert future versions of this guide's first worked example into its second.

§ 15 · REFERENCE

Glossary

BitLocker
Windows full-disk encryption; recovery keys commonly escrowed in Active Directory, Entra ID or Microsoft accounts.

Dead-box acquisition
Imaging a powered-off machine via write blocker; zero alteration, no volatile capture.

FileVault
macOS full-disk encryption; recovery via personal, iCloud or institutional keys.

Full-disk encryption
Encryption of an entire volume, transparent while unlocked, absolute while locked without keys.

Hibernation file
RAM written to disk at hibernation; a recoverable snapshot of memory for the dead-box path.

Live acquisition
Acquisition from a running system: memory first, then live or targeted collection of the (decrypted) estate.

Memory (RAM) capture
Hashed acquisition of volatile memory by a validated minimal-footprint tool.

Mounted container
An encrypted volume (e.g. VeraCrypt) open for use; readable, and its keys in RAM, only while mounted.

Network isolation
Deliberately disconnecting a device to prevent remote wipe or interference; a recorded trade-off.

Recovery key
The escrowed secret that unlocks full-disk encryption without the user's password.

TPM
The hardware module holding BitLocker keys; defines how a machine boots and what imaging yields.

Volatile data
Evidence existing only while power flows: memory, sessions, connections, keys.

Sources and authoritative references

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

- cflab.uk, digital forensics services (attendance at live machines, RAM capture, live and dead-box imaging under NPCC principles, encrypted-device handling and CPR Part 35 / CrimPR Part 19 reporting): cflab.uk/digital-forensics-services
- cflab.uk, the digital-evidence guide for defence lawyers (volatile data, RAM-held container keys and clipboard evidence in practice) and the lawyer guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (powered-on device handling within disclosure-scale collection planning): 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
- NPCC / College of Policing digital evidence guidance (the principles governing original-data access and audit trails): college.police.uk, digital devices guidance
- Forensic Science Regulator, statutory Code of Practice: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 (guidance on handling powered-on and powered-off devices) and ISO/IEC 17025: iso.org, 27037 · iso.org, 17025
- Microsoft, BitLocker recovery documentation, and Apple, FileVault documentation (key escrow and recovery routes): learn.microsoft.com, BitLocker recovery · support.apple.com, FileVault
- CPR Part 35 (experts) and CrimPR Part 19: justice.gov.uk, Part 35 · justice.gov.uk, CrimPR Part 19
- ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about live and offline digital evidence acquisition in the United Kingdom as at August 2026. The worked examples are fictional illustrations. Encryption behaviour varies by product, version and configuration; obtain specific advice for any real device. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Rules, standards and guidance change; always check the current text. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

The live-or-offline decision is a same-day service: our examiners attend powered-on machines with validated memory-capture and live-acquisition kits, photograph and assess before touching, capture the volatile layer, read the encryption position, and choose and record the path under the NPCC principles, completing with write-blocked dead-box imaging where the matter warrants both. We run the credential and escrow hunt in parallel with IT, advise on isolation against remote wipe, handle containers and exotic encryption, and deliver the acquisition log, footprint disclosure and hash schedule as a set built for challenge. Through **e-discovery.uk**, powered-on device handling is written into disclosure collection plans in advance, so the standstill instructions, escrow checks and attendance arrangements exist before the morning they are needed. Where the other side's machines were handled by reflex, we review their records (or their absence) and report what was lost, under CPR Part 35 / CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.

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