Should A Computer Be Imaged While Running Or Switched Off

This guide explores the critical decision of whether to image a computer live or offline, focusing on volatile data, encryption, and the implications for forensic collection. It provides a framework for UK lawyers to navigate this complex choice, ensuring evidential integrity.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/should-a-computer-be-imaged-while-running-or-switched-off

LIVE & OFFLINEACQUISITION · A GUIDE FOR UK LAWYERS Should a Computer Be Imaged While Running or Switched Off? Volatile Data, Encryption and the Most Consequential Button in Forensics COMPUTER FORENSICS LAB E-DISCOVERY. UK

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

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the button and its consequences 03 Volatile data: what lives only in memory 04 Encryption changes everything: Bit Locker, File Vault and friends 05 Offline (dead-box) acquisition: strengths and risks 06 Live acquisition: strengths and risks 07 The at-the-machine decision framework 08 Servers, sleep states and special cases 09 Recording the decision: NPCC principle 2 in action 10 Worked examples 11 Common mistakes and technical limitations 12 Questions to ask · Suggested wording 13 Checklist and red flags · When to involve a digital forensic expert 14 Frequently asked questions 15 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: ASSESSFIRST, CAPTURE MEMORY IF YOU CAN, ANDLET ENCRYPTIONDECIDETHEREST

§ 02 · FIRST PRINCIPLES The problem in plain English: the button and its consequences

§ 03 · WHATEVAPORATES Volatile data: what lives only in memory

§ 04 · THEGAMECHANGER Encryption changes everything: Bit Locker, File Vault and friends

§ 05 · THECLASSICPATH Offline (dead-box) acquisition: strengths and risks

§ 06 · THEMODERNNECESSITY Live acquisition: strengths and risks

§ 07 · THEDECISION The at-the-machine decision framework

§ 08 · BEYONDTHELAPTOP Servers, sleep states and special cases

§ 09 · THE PAPER Recording the decision: NPCC principle 2 in action

§ 10 · IN THE WILD Worked examples EXAMPLE1 · THEPLUGPULLEDONBITLOCKER EXAMPLE2 · THERAMCAPTURETHATHELDTHEKEY EXAMPLE3 · THELIVEACQUISITIONTHATSURVIVEDCHALLENGE

§ 11 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes

Technical limitations

§ 12 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · ADDITIONTOTHECLIENTS TA NDSTILLINSTRUCTION SUGGESTED WORDING · INSTRUCTION TO THE EXAMINER AT TENDINGALIVEM AC HINE

§ 13 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The live-or-offline checklist Red flags When to involve a digital forensic expert

§ 14 · COMMON QUESTIONS Frequently asked questions Is it ever right just to pull the plug? the next hour? Does live acquisition contaminate the evidence? The laptop is asleep. Is that on or off? We have the Bit Locker recovery key but not the user's password. Is that enough? Should company policy change because of any of this?

§ 15 · REFERENCE Glossary 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

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 Bit Locker 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 exam in at i on 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. cflab. u k · e-disc ove r y. u k

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. 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 18 of 21