COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Android Encryption, Secure Boot and Lock-Screen Protections

Why a Modern Android Phone Locks Like a Vault, and Why the Key Is Almost Always the Credential

Modern Android phones are encrypted by default, and the encryption is tied to the user's lock-screen credential and to a hardware security chip that refuses to give up the keys without it. The phone's boot process is verified so that its software cannot be tampered with to bypass those protections, and rate-limiting, lockouts and wipe-on-failure guard the credential itself. The result is that a locked, modern Android phone is very often a vault whose only key is the credential its owner knows. Older devices and some models are weaker, and the state of the phone when seized, powered on and previously unlocked, or cold and locked, can matter enormously. For the lawyer, this reframes the question from "can the phone be cracked?" to "can the credential be lawfully obtained, and what is the phone's state?" This guide sets out for UK lawyers how Android encryption, verified boot and lock protections work, how they differ across devices and states, what they mean for acquisition, and how the credential, not the exploit, is usually the way in.

⏱ 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. Android security is central to its mobile work: understanding each device's encryption, verified boot and lock protections, recognising when a phone is a vault whose key is the credential, distinguishing the states in which more or less is possible, and pursuing lawful access through the credential rather than reckless attempts that risk a wipe. The analysis sets honest expectations and is reported under CPR Part 35 and CrimPR Part 19, with the device's security state explained.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ANDROID ENCRYPTION & LOCK ANALYSIS | LAWFUL CREDENTIAL-LED ACCESS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: a modern Android phone is encrypted by default with keys tied to the lock-screen credential and guarded by a hardware security chip, its boot verified against tampering and its credential guarded by lockouts, so a locked modern device is very often a vault whose only key is the credential, which reframes the question from "can it be cracked?" to "can the credential be lawfully obtained, and what state is the phone in?"

Encryption (§3): file-based encryption by default, with keys derived from the credential and protected in hardware, so the data is unreadable without it. **Verified boot and the chip (§4):** the boot process checked against tampering, and a security chip that refuses to release keys without the credential, defeating software bypasses. **Lock protections and state (§5):** rate-limiting, lockouts and wipe-on-failure guard the credential, and the device's state (powered on and previously unlocked versus cold and locked) changes what is possible. **The credential is the key (§6):** lawful access through the credential, by cooperation or compulsion, is usually the way in. **Deployment (§7):** handling a locked Android phone to preserve every possibility, without reckless attempts that risk a wipe.

- **A vault with one key:** encryption tied to the credential and a hardware chip.
- **Boot is verified:** the software cannot be tampered with to bypass protection.
- **The credential is guarded:** lockouts and wipe-on-failure make guessing dangerous.
- **State matters enormously:** powered-on and previously unlocked beats cold and locked.
- **The key, not the exploit:** lawful access through the credential is usually the way in.

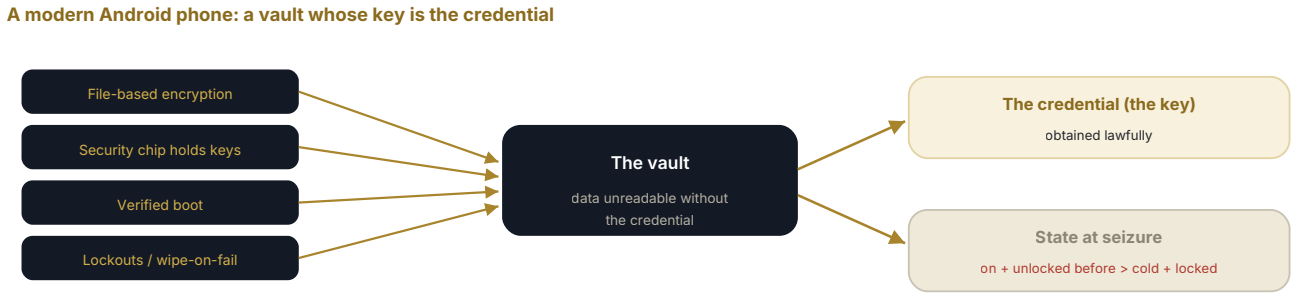

Figure 1 - encryption, a hardware key chip, verified boot and lockouts make a modern Android phone a vault, whose key is the lawfully obtained credential and whose state at seizure decides how much else is possible.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: a vault with one key

People still imagine that a forensic laboratory can "crack" a locked phone, and for many older devices that was true. For a modern Android phone it is, in the ordinary case, no longer the right picture. A modern Android device is encrypted by default: its data is scrambled on the storage, and the keys needed to unscramble it are derived from the user's lock-screen credential, the PIN, pattern or password, and protected inside a dedicated hardware security chip that will not release them without that credential. Its boot process is verified, so that the operating system cannot be quietly replaced or modified to bypass these protections. And the credential itself is guarded: too many wrong attempts trigger escalating delays, lockouts and, on many devices, the wiping of the phone. Put together, a locked, modern, up-to-date Android phone is very often a vault whose only key is the credential its owner knows.

This reframes the practical question. It is no longer "can the laboratory break in?" but "can the credential be lawfully obtained, and what state is the phone in?" The first half of that question is legal as much as technical: the credential is obtained through the owner's cooperation, through lawful compulsion where the law provides for it, or through other lawful means, and never through reckless guessing that risks wiping the very evidence sought. The second half is about the device's state, which matters enormously. A phone seized powered on and previously unlocked since it last booted is in a materially different state from one that is cold and locked: in the former, certain keys may still be resident and certain acquisitions possible that are impossible in the latter, which is why the seizure disciplines of keeping the device powered and isolated (guide 145) carry over to Android in full. And, because Android is a fragmented landscape (guide 161), all of this varies: older devices, some models and some configurations are weaker, and a device's specific version and hardware decide how strong its vault really is. The task, then, is to understand how Android's encryption, verified boot and lock protections work, to assess this device's strength and state, to pursue the credential lawfully, and to handle the phone so that no possibility is lost. This guide sets out how.

§ 0 3 · HOW ANDROID ENCRYPTION WORKS

How Android encryption works

- **Encrypted by default:** modern Android encrypting the device's storage by default, so the data at rest is unreadable without the keys, the baseline protection (guide 133): the default encryption.
- **File-based encryption:** modern devices encrypting per file with keys tied to the user's credential, so different data is unlocked at different stages and user data is protected until the credential is entered (§5): the per-file model.
- **Keys derived from the credential:** the encryption keys derived from the lock-screen credential combined with hardware secrets, so the credential is the root of access (§6): the credential-rooted keys.
- **Hardware-protected keys:** the keys protected in a security chip that performs the credential check and refuses to release keys without it, defeating attempts to extract keys from software (§4): the hardware protection.
- **Older devices differ:** older devices using weaker or whole-disk schemes, or lacking hardware protection, so the encryption's strength is assessed per device (guide 161): the device-specific strength.

Figure 2 - the credential, combined with a hardware secret and checked by the security chip, releases the keys that make the encrypted data readable; without it, the data stays sealed.

§ 0 4 · VERIFIED BOOT AND THE CHIP

Verified boot and the security chip

- **Verified boot:** the boot process checking each stage of the software against a trusted signature, so a tampered or replaced operating system is detected and refused, closing the route of bypassing protections by modifying the software (guide 139): the tamper check.
- **The security chip:** a dedicated chip (a secure element or trusted environment) holding keys, checking credentials and enforcing limits, isolated from the main system, so keys cannot be read out by ordinary software (guide 133): the hardware vault.
- **Rate-limiting in hardware:** the chip enforcing delays and attempt limits on credential checks, so brute-force guessing is slowed or blocked at the hardware level (§5): the hardware throttle.
- **Bootloader state:** whether the bootloader is locked or unlocked affecting what can be loaded and what the device permits, so its state is part of the assessment (guide 161): the bootloader factor.
- **Strength varies by device:** the presence and strength of these protections varying by maker, model and generation, so this device's boot and chip protections are assessed specifically (guide 161): the per-device assessment.

§ 0 5 · LOCK PROTECTIONS AND STATE

Lock-screen protections and the device's state

- **The credential types:** PIN, pattern, password and biometrics as credentials, with biometrics usually unlocking only after a first credential entry since boot, so the underlying PIN or password is the true key (§6): the credential hierarchy.
- **Lockouts and wipe-on-failure:** escalating delays, lockouts and, where configured, wiping after repeated failures, so guessing the credential is dangerous and can destroy the evidence (§7): the guessing hazard.
- **Before first unlock and after:** a device that has not been unlocked since boot holding user data sealed, and one unlocked at least once since boot holding certain keys resident, so the two states differ greatly in what is possible (guide 145): the state divide.
- **Powered on versus cold:** a device powered on and previously unlocked preserving possibilities that are lost if it powers off or reboots, so it is kept powered and isolated (guide 145): the keep-it-on rule.
- **Network isolation:** the device isolated from networks to prevent remote lock or wipe and to preserve its state, as on iOS (guide 145): the isolation rule.

§ 0 6 · THE CREDENTIAL IS THE KEY

The credential is the key: lawful access

- **The credential unlocks everything:** the lawfully obtained credential unlocking the device, releasing the keys and enabling the deepest acquisition the device permits, so it is the single most valuable thing to obtain (guide 162): the master key.
- **By cooperation:** the owner providing the credential voluntarily, the cleanest route, often secured by explanation of the consequences of refusal (guide 117): the consensual route.
- **By lawful compulsion:** where the law provides, a party compelled to disclose the credential, with the consequences of non-compliance, so the credential is obtained by legal process (guide 117): the compelled route.
- **By other lawful means:** credentials lawfully found elsewhere, in the estate, in records, or through lawful technical methods where they exist for the device, never by reckless guessing (guide 140): the lawful alternatives.
- **Never risk a wipe:** no attempt that could trigger lockout or wipe made without expert assessment, so the evidence is never destroyed in trying to reach it (§5): the do-no-harm rule.

§ 0 7 · DEPLOYMENT

Deployment: what to do with a locked Android phone

- **Preserve the state:** the phone kept powered on, isolated from networks and untouched, so a previously-unlocked state and resident keys are not lost (guide 145): the state preserved.
- **Assess this device:** the model, version, security hardware, bootloader and lock state assessed to determine the vault's strength and what is possible (guide 161): the assessed vault.
- **Pursue the credential lawfully:** the credential sought by cooperation or compulsion as the primary route, since it opens everything (§6): the key pursued.
- **Acquire when unlocked:** once unlocked, the deepest acquisition the device permits taken promptly, before it locks or changes (guide 162): the window used.
- **Turn to the estate meanwhile:** the Google account, backups and estate pursued in parallel, so the case progresses even while the vault is closed (§8): the parallel estate.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a locked, encrypted Android phone is a sealed node, and the estate around it is the way to the evidence while, or if, the vault stays closed. The device holds the data, sealed behind the credential. But the Google account (guide 161) syncs messages, photos, backups, location history and app data reachable lawfully and independently of the device's lock; the manufacturer's cloud holds backups and synced data; local and cloud backups hold the device's contents, an encrypted local backup with its own credential; a paired wearable holds shared data; the counterparts hold their side of communications; and the credential itself may be recoverable from the estate, from other devices, records or the owner's own storage. The discipline is to preserve the sealed device's state so nothing is lost, pursue the credential lawfully as the key, and in parallel reach the estate, so that a closed vault does not stall the case and the evidence flows from wherever it can be lawfully obtained. When the phone is sealed, the account and backups often hold most of what it does; when the credential cannot be obtained, the estate is the route; and when it can, the device opens fully.

EVIDENCE	LOCKED DEVICE (SEALED)	UNLOCKED DEVICE	GOOGLE ACCOUNT	BACKUPS / MANUFACTURER CLOUD	PAIRED / COUNTERPART	CREDENTIAL SOURCE
Messages	Sealed	Y: at depth	Y: if synced	Y: if backed up	Y: counterpart	n/a
Photos / files	Sealed	Y	Y: Google Photos/ Drive	Y	Shared copies	n/a
Location / app data	Sealed	Y	Y: history, app backups	Some	Wearable	n/a
Deleted data	Sealed	Y: if deep	Earlier states	Pre-deletion backup	Their copy	n/a
The credential	n/a	n/a	Account recovery aids	Backup credential	Other devices / records	Y: owner, records, estate

Fallback strategy in one line: preserve the sealed device's state, pursue the credential lawfully as the key, and in parallel reach the Google account, backups and counterparts, so a closed vault does not stall the case.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE CREDENTIAL THAT OPENED THE VAULT

A modern, fully patched Android phone was seized locked. Its §3 encryption, §4 security chip and verified boot made it, in the ordinary sense, uncrackable, a vault. The §6 credential-led approach was taken: the phone was §7 preserved powered on and isolated, and the credential was pursued by lawful compulsion (guide 117). Once obtained, it §6 released the keys, and the deepest §7 acquisition the device permitted was taken promptly, a full file system with deleted data (guides 162, 155). No exploit was needed or possible; the key was the credential. The lesson is §6's: on a modern Android phone the credential is the master key, opening what no software bypass can, so it is pursued lawfully, by cooperation or compulsion, as the primary route, and the device is preserved and then acquired promptly once it opens.

EXAMPLE 2 · THE REBOOT THAT LOST THE WINDOW

A phone was seized powered on and had been unlocked since boot, a §5 state in which certain keys were resident and a valuable acquisition was possible without the credential. Before the examiner reached it, someone powered it off, and on restart it was in the §5 before-first-unlock state, its user data sealed and the window gone (guide 145). The credential was not available, and what had been possible was now impossible. The §7 estate, the Google account and backups, had to supply what the device would have (guide 161). The lesson is §5's: the device's state at seizure matters enormously, a powered-on, previously-unlocked phone preserves possibilities that a reboot destroys, so it is kept powered on and isolated from the moment of seizure, and no one powers it off, reboots it or lets its battery die.

EXAMPLE 3 · THE GUESS THAT WOULD HAVE WIPED THE EVIDENCE

Someone proposed simply trying likely PINs on a locked phone. The §5 lock protections made this dangerous: the device enforced §4 hardware rate-limiting and escalating lockouts, and was configured to §5 wipe after repeated failures, so guessing risked destroying the very evidence sought. Per §6, no such attempt was made; the credential was pursued lawfully, and the §8 estate reached in parallel. The evidence was preserved because no one gambled with it. The lesson is §6's: the credential is guarded by lockouts and wipe-on-failure, so reckless guessing can wipe the phone, and no attempt that could trigger lockout or wipe is made without expert assessment, the do-no-harm rule that keeps the evidence intact while the lawful route is pursued.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Expecting the phone to be "cracked":** the outdated assumption, when the credential is the only key on modern devices (Example 1, §2).
- **Powering off or rebooting the device:** destroying a previously-unlocked state and its possibilities (Example 2, §5).
- **Guessing the credential:** risking lockout or wipe by trying PINs (Example 3, §6).
- **Not pursuing the credential lawfully:** neglecting cooperation or compulsion as the primary route (§6).
- **Failing to isolate the device:** allowing a remote lock or wipe over the network (§5).
- **Assuming all Androids are equally strong:** not assessing this device's specific protections (§3, §4).
- **Stalling on the sealed device:** not reaching the estate in parallel (§7, §8).
- **Missing the acquisition window:** not acquiring promptly once the device is unlocked (§7).

Technical limitations

- **Modern devices are genuine vaults:** without the credential, a modern, patched device may be inaccessible: the core limit (§2).
- **State is decisive and fragile:** a reboot can close a window permanently (§5).
- **Lockouts and wipe are real:** guessing can destroy evidence (§5).
- **Strength varies by device:** older or weaker devices may permit more (§3).
- **Protections evolve:** each Android generation strengthens the vault (§4).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the phone locked, and is the credential known or obtainable, since it is the key to everything?
- What state is it in, powered on and previously unlocked, or cold and locked, and has it been kept powered and isolated?
- Is the Google account and are backups available, to reach the evidence while the vault is closed?

Ask your opponent

- Please preserve the device at Schedule 1 powered on, isolated from networks and unaltered, and provide the lock-screen credential to enable lawful access.
- Please confirm the device's model, version, security state and whether it has been powered off or rebooted since seizure.
- Please preserve and disclose the associated Google account and backups.

Ask your eDiscovery / forensic provider

- How strong is this device's vault, encryption, chip, boot and lock protections, and what is possible in its current state?
- What is the lawful route to the credential, and what can the estate supply meanwhile?
- Has any attempt been made that risked lockout or wipe?

SUGGESTED WORDING · INSTRUCTION FOR A LOCKED ANDROID DEVICE

> "We instruct you in relation to the locked Android device at Schedule 1 relevant to Schedule 2. Please: (1) preserve the device's state, keeping it powered on, isolated from all networks and unaltered, and ensure it is not powered off, rebooted or allowed to discharge; (2) assess this specific device's encryption, security hardware, verified boot, bootloader and lock protections, and its current state (whether unlocked since boot), and advise what is possible in that state with and without the credential; (3) pursue the lock-screen credential lawfully, by the owner's cooperation or lawful compulsion or other lawful means, as the primary route, making no attempt that could trigger lockout or wipe; (4) once the device is unlocked, take the deepest lawful acquisition it permits promptly, before it locks or changes; and (5) in parallel, identify and reach the Google account, backups, manufacturer cloud and counterparts to supply the evidence while the device is sealed, and present findings at honest confidence with the device's security state explained."

§ 12 · QUICK CONTROL

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

The locked-Android checklist

- ☐ Device kept powered on from seizure; never powered off or rebooted
- ☐ Device isolated from all networks
- ☐ This device's encryption, chip, boot and lock protections assessed
- ☐ Current state (unlocked since boot?) established
- ☐ Credential pursued lawfully as the primary route
- ☐ No guessing or attempt risking lockout or wipe
- ☐ Deepest acquisition taken promptly once unlocked
- ☐ Google account, backups and estate reached in parallel
- ☐ Credential sought lawfully in the estate and records
- ☐ Device's security state and limits explained in the report

Red flags

- An expectation that the phone will be "cracked": Example 1.
- The device powered off, rebooted or allowed to die: Example 2.
- PINs guessed on a device with lockouts or wipe: Example 3.
- The credential not pursued by cooperation or compulsion.
- The device left on a network, risking remote wipe.
- All Androids assumed equally strong.
- The case stalled on the sealed device with the estate ignored.

When to involve a digital forensic expert

From the moment a locked Android device is seized, because its state is fragile and the wrong action, a reboot, a guess, a network connection, can lose the evidence permanently: the expert preserves the device powered on, isolated and untouched (Example 2, §5, §7), assesses this specific device's encryption, security chip, verified boot and lock protections and its current state to determine what is possible (§3, §4), and pursues the credential lawfully, by cooperation or compulsion, as the master key that opens what no bypass can, making no attempt that risks lockout or wipe (Examples 1 and 3, §6). Once the device opens, the deepest acquisition it permits is taken promptly (guide 162), and in parallel the Google account, backups and counterparts are reached so a closed vault does not stall the case (§8). Findings, and the device's security state, are reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Through **cflab.uk** and **e-discovery.uk**, locked-device work treats the modern Android phone as the vault it is, preserving its state, pursuing its one key lawfully, and reaching the evidence through the estate while the vault stays shut.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can a laboratory just crack a locked Android phone?

For a modern, patched device, usually not, and the picture has changed (§2, Example 1). Modern Android phones are encrypted by default with keys tied to the lock-screen credential and held in a hardware security chip that will not release them without it; verified boot prevents the software being tampered with to bypass this; and lockouts guard the credential. So a locked modern device is very often a vault whose only key is the credential. Older or weaker devices may permit more, which is why each device is assessed specifically, but the ordinary expectation is that the credential, not an exploit, is the way in.

So what do we do with a locked phone?

Preserve its state, pursue the credential lawfully, and reach the estate meanwhile (§7). The phone is kept powered on, isolated from networks and untouched, so a previously-unlocked state and its possibilities are not lost. The credential is pursued as the master key, by the owner's cooperation or by lawful compulsion where the law provides, never by guessing. Once unlocked, the deepest acquisition the device permits is taken promptly. And in parallel, the Google account, backups and counterparts are reached, so the case progresses even while the vault is closed.

Why does it matter whether the phone was powered off?

Because state decides what is possible, and a reboot can close a window permanently (§5, Example 2). A phone that has been unlocked at least once since it booted holds certain keys resident and may permit acquisitions that are impossible on a phone that is cold or has not been unlocked since boot, whose user data is fully sealed. Powering off or rebooting a previously-unlocked phone returns it to the sealed state and destroys those possibilities. So from seizure the device is kept powered on, charged and isolated, and no one reboots it.

Can't we just try the likely PINs?

No, that can wipe the evidence (§5, §6, Example 3). The credential is guarded by hardware rate-limiting, escalating lockouts and, on many devices, wiping after repeated failures, so trying PINs risks locking the device for long periods or destroying its contents entirely. No attempt that could trigger lockout or wipe is made without expert assessment. The credential is obtained lawfully instead, by cooperation, by compulsion, or by other lawful means such as finding it in the estate or records, so the evidence is never gambled away in the attempt to reach it.

How is the credential obtained lawfully?

By cooperation, compulsion or other lawful means (§6, guide 117). The cleanest route is the owner providing it voluntarily, often after the consequences of refusal are explained. Where the law provides, a party can be compelled to disclose the credential, with consequences for non-compliance. And credentials are sometimes lawfully found elsewhere, in other devices, records or the owner's storage, or reachable through lawful technical methods that exist for some devices. Whichever route, it is lawful and non-destructive, because the credential is the key to everything and the evidence must not be risked in obtaining it.

If the phone stays locked, is the case stuck?

Not necessarily, because the estate is reached in parallel (§8). A sealed device is one node; the Google account syncs messages, photos, backups, location history and app data reachable lawfully regardless of the device's lock; manufacturer and local backups hold the device's contents; a paired wearable holds shared data; and counterparts and providers hold their records. Reached while the credential is pursued, these frequently supply most of what the device would, so a closed vault does not stall the case, and if the credential is ultimately obtained, the device then opens fully as well.

§ 14 · REFERENCE

Glossary

File-based encryption
Per-file encryption tied to the credential.

Credential
The PIN, pattern or password unlocking the device.

Security chip / secure element
Hardware holding keys and checking credentials.

Verified boot
Boot-time checking of software against tampering.

Bootloader
The low-level loader; locked or unlocked state matters.

Before first unlock
The sealed state of a device not yet unlocked since boot.

After first unlock
The state with certain keys resident after one unlock.

Lockout
Escalating delays after failed credential attempts.

Wipe-on-failure
Erasing the device after repeated failed attempts.

Lawful compulsion
Legal process requiring disclosure of a credential.

Sources and authoritative references

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

- cflab.uk, digital forensics services (Android encryption and lock analysis, lawful credential-led access, 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 (device-state preservation and lawful access 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
- Android Open Source Project, encryption, verified boot and hardware-backed security documentation: source.android.com, encryption · source.android.com, verified boot
- Regulation of Investigatory Powers Act 2000, Part III (disclosure of protected information) and NPCC digital evidence guidance: legislation.gov.uk, RIPA Part III · npcc.police.uk
- Forensic Science Regulator, Code of Practice v2 and ISO/IEC 27037 · CPR Part 35: gov.uk, FSR Code · iso.org, 27037 · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Locked-device work at the laboratory treats the modern Android phone as the vault it is. From seizure, the device is preserved powered on, charged, isolated from all networks and untouched, because a previously-unlocked state holds possibilities that a single reboot destroys and a network connection invites a remote wipe (Example 2, guide 145). This specific device's encryption, security chip, verified boot, bootloader and lock protections are assessed, together with its current state, to determine what is possible with and without the credential (guide 161). The credential is pursued lawfully as the master key, by the owner's cooperation, by lawful compulsion where the law provides, or by other lawful means including its recovery from the estate, and no attempt that could trigger lockout or wipe is ever made, so the evidence is never gambled away in reaching it (Examples 1 and 3, guide 117). Once the device opens, the deepest acquisition it permits is taken promptly (guide 162), and in parallel the Google account, backups, manufacturer cloud and counterparts are reached so that a closed vault does not stall the case. Findings, and the device's security state and limits, are reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding reframe is the one this guide set out: not "can it be cracked?" but "can the key be lawfully obtained, and what state is the phone in?"

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