COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

# File Wiping, Anti-Forensics and the Evidence They Leave Behind

## When the Attempt to Destroy Evidence Becomes the Evidence

Some parties do not merely delete. They install a secure-erase utility and run it over the folder; they use a privacy cleaner on their browser; they encrypt the container, reset the phone, reinstall the operating system, set the clock back, swap the drive. Anti-forensics is the deliberate use of tools and techniques to defeat examination, and it is far more common in civil litigation than most lawyers expect: the departing employee, the director facing a claim, the party with a hold notice on the desk. Two facts govern it. First, it works: properly wiped data is unrecoverable and the honest examiner says so. Second, it announces itself: every anti-forensic act leaves artefacts of its own: the tool's installation, its execution, the pattern of what it erased, the routine records that stop, the timing against the dispute: and courts treat deliberate destruction after a duty arose as among the gravest conduct a litigant can commit. This guide sets out for UK lawyers the anti-forensic techniques encountered in practice, the traces each leaves, the honest limits of recovery, and the deployment of destruction evidence in spoliation, employment, fraud and criminal proceedings.

⏱ Estimated reading time: 25 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. Anti-forensic examination is a recurring instruction: the wiped laptop, the reset phone, the cleaned browser, the encrypted volume that appeared mid-dispute: examined for the tool, the execution, the extent and the timing, with the honest statement of what was destroyed and what survives, and reported under CPR Part 35 and CrimPR Part 19 where destruction is the issue.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ANTI-FORENSICS EXAMINATION | WIPING & RESET ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

# In this guide

§ 0 1 · ORIENTATION

# Executive summary

THE HEADLINE POINT: ANTI-FORENSICS DESTROYS CONTENT AND CREATES EVIDENCE OF DESTRUCTION: THE EXAMINATION READS THE TOOL, THE EXECUTION, THE EXTENT AND THE TIMING, STATES HONESTLY WHAT IS GONE, AND LETS THE COURT DRAW THE INFERENCE THAT DELIBERATE DESTRUCTION AFTER A DUTY AROSE INVITES

**The techniques (§3):** secure-erase and wiping utilities that overwrite files or free space; privacy and history cleaners that purge browser, application and system records; encryption applied to containers or volumes to place data beyond examination; factory resets, operating-system reinstalls and drive replacements that discard whole environments; and obfuscation: renaming, hiding, moving to unexpected media, clock manipulation (guide 108 §6) and log clearing. **The traces (§4):** tools are installed (installer records, program entries, registry keys), executed (prefetch, application logs, execution artefacts, the tool's own settings and targets), and leave patterns (overwritten regions with characteristic content, free-space wipes of identifiable extent); routine artefacts stop or restart empty (the cessation signature of guide 106 §5); and the platform records the act where the device could not (audit logs of resets, account purges, encryption enablement). **What survives (§6):** a competent wipe is unrecoverable and the report says so; but the wipe is rarely complete (targets missed, journals untouched, backups and syncs unreached), and the estate's redundancy (guides 95, 103) holds copies the destroyer never controlled: recovery is scoped honestly, from what the tool did not reach. **Deployment (§7):** the destruction dated against the preservation duty (guide 95 §6), its selectivity and timing read for intent, and the finding carried into adverse inference, strike-out, contempt, employment and fraud proceedings (guides 95 §7, 97, 98): with the innocent explanations: routine device hygiene, security policy, personal-data disposal before any duty: considered and excluded on the record.

- **Wiping works and confesses:** the content is gone; the tool's installation, execution and pattern remain.
- **Cessation is a signature:** histories that stop at a date, or restart empty, mark the cleaning as surely as the tool does.
- **Platforms record what devices cannot:** resets, purges and encryption enablement are logged server-side.
- **The estate is redundant:** what the destroyer controlled is gone; what they did not is the recovery route.
- **Timing decides consequence:** destruction after the duty is spoliation with grave remedies; before it, hygiene with an explanation.

§ 0 2 · FIRST PRINCIPLES

# The problem in plain English: destruction is an act, and acts are recorded

A party who wipes a laptop believes they have subtracted evidence from the case. What they have done is exchange one kind of evidence for another. The files are gone: the examiner will confirm it. But the wiping program was downloaded on a date, installed under a profile, run at a time, pointed at particular folders, and the system recorded most of that without being asked. The browser history that ends abruptly on the day the letter of claim arrived is not an absence; it is a dated event. The phone reset to factory settings the evening before it was due to be handed over carries the reset timestamp in its own firmware. Anti-forensics converts the question "what did the documents say?" into "why did you destroy them, and when?": and courts find the second question easier to answer against the destroyer than the first ever was.

This guide is not a manual for either side of that exchange. It is a description of the techniques an examiner encounters, the artefacts each leaves, the honest boundary of what can be recovered, and the legal weight of a destruction finding: so that the lawyer facing a suspiciously clean device knows what to ask for, and the lawyer advising a client under a hold notice knows what to say, with force, about the consequences of cleaning up.

§ 0 3 · THE TECHNIQUES

# The techniques: wiping, cleaning, encryption, resets and obfuscation

- **File and free-space wiping:** utilities that overwrite a file's content before deleting it, or overwrite all unallocated space to destroy previously deleted residue: the classic secure-erase category, with methods ranging from single-pass zeroing to multi-pass patterns, and scope from a single file to an entire volume.
- **Privacy and history cleaners:** tools that purge browser histories and caches, application recent-file lists, system logs, thumbnail caches, jump lists and temporary files: marketed as maintenance, deployed as concealment: the category most often found on the "tidied" laptop of guide 106 Example 2.
- **Encryption as concealment:** containers and volumes encrypted after a duty arose, keys withheld, or full-disk encryption enabled on a device previously unencrypted: data placed beyond examination rather than destroyed: with its own legal consequences (guide 117-118's territory) and its own timing evidence.
- **Resets, reinstalls and replacements:** factory resets on phones and tablets, operating-system reinstalls on computers, drive swaps and device "losses" (guide 95 Example 2): whole environments discarded, with the reset or install date recorded by the device or platform and the pre-reset state sometimes surviving in backups and syncs.
- **Obfuscation and manipulation:** renaming files to innocuous names or wrong extensions, moving data to unexpected media, steganographic hiding, timestamp manipulation (guide 108 §6), log clearing (guide 99 §10), and account or channel deletion on platforms: concealment rather than destruction, defeated by content-based searching and the platform's own records.

§ 0 4 · THE TRACES

# The traces: installation, execution, patterns and the negative space

- **Installation artefacts:** installer downloads in browser histories (the search for "secure delete" often surviving in the very history later cleaned), installation records in program registries and package managers, application folders, shortcuts and uninstall entries (sometimes the tool uninstalled but its uninstall record retained): the tool's arrival, dated.
- **Execution artefacts:** Windows prefetch files recording each run with timestamps and run counts; application event logs; the tool's own logs, settings and job files listing targets and methods; registry most-recently-used entries; macOS and mobile equivalents: the tool's use, dated and often scoped.
- **Overwrite patterns:** wiped regions filled with zeros, fixed patterns or random data in contiguous extents inconsistent with normal deletion residue; the boundaries of a free-space wipe visible against surviving unallocated content; file-system entries whose content is overwritten but whose metadata (names, sizes, dates) persists in the MFT (guide 106 §4): the wipe's extent, mapped.
- **The cessation signature:** browser, application and system histories that end at a date and restart empty or sparse; jump lists and recent-file entries with a gap; event logs cleared (itself a logged event on Windows); thumbnail caches rebuilt: the cleaning's date fixed from what stopped: guide 95 §3's negative space, at its most eloquent.
- **The journal the tool forgot:** file-system change journals and volume shadow copies frequently untouched by wiping tools focused on file content: the names and deletion transactions of wiped files preserved in structures the tool never targeted (guide 106 Example 2's 3,100 names).

§ 0 5 · MOBILE, CLOUD AND PLATFORM ANTI-FORENSICS

# Mobile, cloud and platform anti-forensics

- **Phone resets:** factory resets record their timestamp in device firmware and setup artefacts; the platform's account records the device's re-enrolment; and the pre-reset state survives in cloud backups (iCloud, Google) taken before the reset, and in the counterparties' copies of every message (guide 95 Example 2): the reset dated, and often defeated.
- **Message and app deletion:** deleting conversations in messaging apps leaves database freelist residue (guides 63-66, 145-175), server-side records on platforms that keep them, and the counterpart's intact copy: with disappearing-message features and deletion-for-everyone commands logged as events on several platforms.
- **Cloud purges:** emptying recycle stages, deleting accounts, removing channels and revoking shares are audited actions with acting accounts and timestamps (guides 101, 103, 106 §3): the destruction recorded server-side by the platform the destroyer used to do it.
- **Encryption enablement and key withholding:** the enabling of device or container encryption is logged locally and often by device management; the withholding of keys after a disclosure order is a conduct question with its own consequences (guide 118): the data unreachable, the act visible.
- **Log clearing:** Windows records the clearing of its event logs as an event; cloud audit logs cannot be cleared by users at all; and SIEM and forwarding copies survive local clearing: the attacker's and the insider's favourite technique, defeated by the layer above it (guide 99 §8).

§ 0 6 · WHAT SURVIVES

# What survives: the honest limits of recovery and the estate's redundancy

- **The honest limit:** a competently executed overwrite destroys the content: single-pass zeroing on modern media is sufficient, and the examiner does not promise recovery from wiped regions: the finding is "wiped, unrecoverable, dated" and its weight is in the last word.
- **Incomplete wipes:** tools miss targets (files open at the time, alternate data streams, system-protected areas), skip journals and shadow copies, and leave metadata residue: what the tool did not reach is recovered by the ordinary methods (guides 95 §5, 106 §4).
- **Solid-state and mobile storage:** flash media's wear-levelling and over-provisioning can preserve copies the tool's overwrite never touched, while TRIM and encryption-based erasure can destroy more than expected: the medium's behaviour established before recovery is scoped or foreclosed.
- **The estate's redundancy:** sync mirrors, cloud versions (guide 102), backups, counterpart copies, other members' Teams and chat copies (guide 101), email recipients, and platform-side records: the copies the destroyer did not control: guide 103 §6's reconstruction, with the wipe as the reason it is needed.
- **The device's own memory of the wipe:** even where nothing substantive survives, the §4 traces do: the finding "this device was wiped with this tool on this date, targeting these locations, and the following routine records ceased" is complete evidence in itself.

§ 0 7 · DEPLOYMENT

# Deployment: timing, intent and the consequences of proven destruction

- **The duty clock:** the destruction dated from §4-§5's artefacts and set against contemplation, the letter of claim, the hold notice and any order (guide 95 §6): destruction after the duty is spoliation; before it, the innocent explanations of §10 are considered.
- **Intent from selectivity and sequence:** a wipe targeting the disputed project folder alone, run the evening after the hold notice, following a search for "permanently delete files": the artefacts supplying the consciousness the law requires: guide 95 §4's selectivity, with the tool's job file as the exhibit.
- **Civil consequences:** adverse inference calibrated to the proven destruction; costs; strike-out where a fair trial is impossible; contempt where an order was breached; and the practical collapse of the destroyer's credibility on every other issue: guide 95 §7's ladder, climbed faster on anti-forensic evidence than on any other.
- **Employment, regulatory and criminal:** the departing employee's cleaner as misconduct and springboard evidence (guide 97); the regulated firm's record destruction as a reporting breach; perverting the course of justice where the destruction relates to criminal proceedings: flagged for specialist advice as the findings reach them.
- **Advising the client under a hold:** the preventive deployment: the hold notice that names cleaning tools, resets and encryption as prohibited acts, explains that they leave traces, and states the consequences: the most effective anti-anti-forensic measure is the client who has read this section.

§ 0 8 · THE WIDER MAP

# Source architecture: where else the evidence lives

Per this series' source-architecture discipline: anti-forensics is an attack on one layer of a redundant estate, and the examination reads every layer the attack did not reach. On the device: the tool's installation and execution artefacts, the overwrite patterns, the journals and shadow copies the tool skipped, the cessation signature in routine histories, the firmware's reset record. On the platform: audit events for purges, resets, encryption and account changes; version ladders and recycle stages; the account's sign-in context at the time of the act. In the estate: sync mirrors, backups, counterparts' copies, other members' chat copies, email recipients. In the physical and behavioural world: the person's own messages about "clearing things up", the search history for the tool, the badge record placing them at the machine, the purchase of a new drive. When the device is a wiped shell, the platform still logged the purge; when the platform account is gone, the counterparts still hold the messages; when everything the party controlled is clean, the timing, the tool and the silence are the case.

| QUESTION | DEVICE ARTEFACTS | PLATFORM AUDIT + RECORDS | ESTATE REDUNDANCY | BEHAVIOURAL + PHYSICAL LAYER | JOURNALS + SHADOW COPIES | WIPED / UNRECOVERABLE |
|---|---|---|---|---|---|---|
| **Was a tool used, when** | Y: install + execution records | Device-management logs | n/a | Download + search history; purchases | Tool files' own creation entries | The tool rarely wipes itself |
| **What was targeted** | Y: job files, overwrite extents | Purge events name items | The copies that survive show what was hit | "Clearing the project folder" | Y: names + deletion transactions | Content gone; names often not |
| **When, against the duty** | Y: timestamps; cessation date | Y: event timestamps | Last-sync bracket | Messages + presence records | Journal sequence | Reset firmware stamp |
| **What the material was** | Metadata residue | Version ladders, recycle stages | Y: counterparts, backups, mirrors | References in others' messages | Shadow-copy content sometimes | n/a |
| **Who did it** | Profile context | Y: acting account + session | n/a | Y: the person's own words + presence | n/a | n/a |

Fallback strategy in one line: when the content is wiped, prove the wipe from the tool, the journal and the cessation; date it from the artefacts; recover the material from the estate the destroyer never controlled: and let the timing speak.

§ 0 9 · IN THE WILD

# Worked examples

**EXAMPLE 1 · THE FREE-SPACE WIPE AND THE SEARCH THAT PRECEDED IT**

A defendant in a fraud claim delivered his laptop under a disclosure order. The examination found an unallocated space filled almost entirely with zeros: a free-space wipe of the whole volume: and a user folder with nothing relevant. The §4 traces reconstructed the rest: a browser history (itself partially cleaned, but with the search-engine session cookies intact) showing searches for "permanently delete files so they cannot be recovered" three days after the order; the download and installation of a wiping utility that evening; prefetch entries for two executions over the following two days; the tool's job file listing "free space" and "Documents\Projects" as targets; and the change journal, untouched, recording the deletion of 1,400 named files from the Projects folder in the minutes before the first execution. The estate's redundancy (a SharePoint sync client's server-side ladder) recovered 1,100 of the files; the remaining 300 were gone. The court drew the inference on the wipe evidence, and the defendant's credibility did not survive the exhibit that listed the search terms.

**EXAMPLE 2 · THE PHONE RESET THE NIGHT BEFORE HANDOVER**

A respondent to an employment claim was ordered to deliver her phone for imaging. The phone arrived in factory-fresh condition. The §5 examination read the firmware's reset timestamp: 23:41 the evening before handover; the platform's account records showed the device re-enrolled at 23:58 with a new backup baseline; and the pre-reset iCloud backup: taken automatically at 02:00 two nights earlier and not yet overwritten: was obtained under order and restored, yielding the message threads the claim concerned, including a thread in which the respondent told a friend she was "going to wipe it, they'll never know". The reset was dated to the hour; the material was recovered from the backup she had not thought to delete; and her own message supplied the intent. Guide 95 Example 2's lesson, from the other chair.

**EXAMPLE 3 · THE CLEANER THAT WAS ROUTINE, AND THE ALLEGATION THAT FAILED**

An employer alleged that a departed manager had run a privacy cleaner to destroy evidence, citing the tool's presence and a sparse browser history. The manager's examiner ran the §7 timing and the §10 innocent-explanation analysis: the cleaner had been installed four years earlier under the firm's own IT-approved software list, its scheduled task had run weekly throughout (prefetch and task-scheduler history showed 200-odd executions on a Sunday cadence), the browser history's sparseness matched the weekly cadence exactly, and the final execution was the routine Sunday run: two days before the manager knew of any dispute. The change journal showed no bulk deletion; the sync mirror held the manager's work files complete. The tool was present; its use was routine and pre-dated the duty; the allegation failed with costs. Anti-forensic tools are not anti-forensic acts, and the examination distinguishes them.

§ 10 · WHERE IT GOES WRONG

# Common mistakes and technical limitations

## Common mistakes

- **Recovery promised:** lawyers and clients told wiped data "can usually be recovered": §6's honest limit ignored, expectations mismanaged.
- **The wipe unexamined:** "the laptop was empty" reported without the tool, execution and cessation evidence that makes emptiness a finding.
- **Timing unread:** destruction proven but never dated against the duty: the consequence left on the table.
- **Tool presence pleaded as destruction:** Example 3's allegation: the routine cleaner accused without execution history or journal evidence.
- **The estate unsearched:** the wiped device treated as the only source while the sync ladder and the backup held the material.
- **Devices powered on:** the reset phone or wiped laptop booted by IT "to check", overwriting residue and shadow copies the examination needed.
- **Hold notices silent on cleaning:** clients never told that resets, cleaners and encryption are prohibited and traceable: §7's preventive deployment skipped.
- **Encryption treated as a dead end:** the key-withholding conduct question and the enablement timing never pursued.

## Technical limitations

- **Competent wiping is final:** overwritten content on modern media is not recovered: the report states it, and the case proceeds on the destruction evidence instead.
- **Flash media behaves unpredictably:** wear-levelling may preserve, TRIM may destroy: the medium's actual behaviour tested, not assumed.
- **Sophisticated actors clean the traces too:** tools that wipe their own prefetch and journal entries exist; the cessation signature and the platform layer remain, and the report says which tests were run.
- **Attribution follows guide 106:** the wipe attributes to a profile and session; the person needs the corroboration lattice.
- **Encrypted data is unreachable without keys:** lawful-access and key-disclosure questions (guides 117-118) are legal, not technical, and are planned as such.

§ 11 · INTERROGATORIES & DRAFTING AIDS

# Questions to ask · Suggested wording

## Ask your client

- Has anyone run cleaning software, reset a device, reinstalled a system or enabled encryption since the dispute arose: and if so, on whose instruction?
- What routine maintenance tools and scheduled tasks were in place before the dispute: the Example 3 baseline?
- Where do the sync mirrors, backups and counterpart copies of the affected material sit: the §6 redundancy, mapped now?

## Ask your opponent

- Please confirm whether any secure-deletion, wiping, privacy-cleaning or history-clearing software has been installed on or executed against [devices] since [date], identifying the software, installation and execution dates, and the locations targeted, and disclose the software's logs and configuration files.
- Please confirm whether [devices] have been factory-reset, reinstalled, re-imaged, replaced or encrypted since [date], with dates, the person responsible, and the reason, and identify all backups, synchronised copies and platform records of the pre-reset state.
- Please confirm preservation of [devices] unpowered and unaltered pending forensic imaging, and of all platform audit logs, backups and synchronised copies relating to them.

## Ask your eDiscovery / forensic provider

- What tool, what executions, what targets, what dates: and is the cessation signature consistent with them?
- What is genuinely unrecoverable, and what does the estate's redundancy still hold?
- Does the timing and selectivity support intent, or is Example 3's routine explanation live?

### SUGGESTED WORDING · ANTI-FORENSICS PARAGRAPH FOR A HOLD NOTICE

> "You must not delete, destroy, alter, conceal or encrypt any document or device that may be relevant to [the matter], and in particular you must not: run any secure-deletion, wiping, privacy-cleaning, history-clearing or 'optimisation' software on any computer, phone or storage device; reset, reinstall, re-image or replace any device; enable or change encryption on any device or container; delete accounts, messages, channels or files on any platform; or alter system clocks. These acts leave forensic traces that identify the software used, the time it was run and the material affected, and destruction of relevant material after this notice may result in adverse inferences, costs orders, strike-out of your case, or proceedings for contempt of court, and may constitute a criminal offence. If any such act has already occurred, or if routine maintenance or security processes may perform any such act automatically, you must inform [instructing solicitors] immediately so that preservation can be arranged."

§ 12 · QUICK CONTROL

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

## The anti-forensics checklist

- ☐ Devices sequestered unpowered; imaged before any examination
- ☐ Installation artefacts for cleaning and wiping tools searched
- ☐ Execution artefacts (prefetch, logs, job files, scheduled tasks) dated
- ☐ Overwrite patterns and free-space wipe extents mapped
- ☐ Cessation signature assessed across browser, application and system histories
- ☐ Change journal and shadow copies examined for skipped residue
- ☐ Platform records checked for resets, purges, encryption and account actions
- ☐ Estate redundancy searched: syncs, backups, counterparts, other members' copies
- ☐ Routine-maintenance baseline established before intent is inferred
- ☐ Each act dated against the preservation duty; finding graded

## Red flags

- Searches for "permanently delete" or wiping tools in the dispute period: Example 1's terms.
- Devices delivered factory-fresh or with suspiciously sparse histories: Example 2's phone.
- Unallocated space that is uniformly zeroed.
- Histories ending on the day of the letter of claim.
- Encryption enabled or keys "forgotten" after an order.
- Event logs cleared; the clearing event itself present.
- Allegations of wiping resting on tool presence alone: Example 3's failure.

## When to involve a digital forensic expert

Before the device is powered on, because booting overwrites what the wipe left; at examination, where the tool, execution, extent and cessation are read together and the honest limit of recovery stated (Examples 1-2); at reconstruction, where the estate's redundancy is worked for the material the wipe was meant to destroy; at assessment, where routine maintenance is distinguished from destruction before intent is pleaded (Example 3); and at deployment, where the dated finding is evidenced under CPR Part 35 or CrimPR Part 19 in spoliation, employment, fraud and criminal proceedings. Through **cflab.uk** and **e-discovery.uk**, anti-forensic examinations run from write-blocked acquisition to the graded, dated finding: and the preventive deployment of §7 is offered to every client under a hold, because the cheapest wipe is the one that never happens.

§ 13 · COMMON QUESTIONS

# Frequently asked questions

### The other side's laptop is completely empty. Can anything be recovered?

From wiped regions, honestly, no (§6); from what the tool missed (journals, shadow copies, alternate streams) and from the estate the party did not control (syncs, backups, counterparts), frequently a great deal (Example 1's 1,100 files). And the wipe itself, dated and scoped from the tool's artefacts, is often worth more than the content: courts infer against destroyers.

### Can an expert tell the difference between routine clean-up and deliberate destruction?

Usually: routine tools run on schedules with long histories, target predictable locations and pre-date the dispute (Example 3); deliberate destruction is installed recently, executed in bursts, targets the disputed material selectively, and clusters around the duty date (Example 1): §7's timing and selectivity, with the journal showing whether bulk deletion preceded the run.

### A phone was factory-reset before handover. Is the evidence gone?

The device's contents, largely; the case, rarely: the reset is timestamped in firmware and re-enrolment records, pre-reset cloud backups often survive (Example 2), counterparties hold their copies of every message, and the platform logged the account's activity. The reset becomes the exhibit; the backup becomes the evidence.

### What if the data was encrypted rather than wiped?

Encryption conceals rather than destroys: the enablement is dated (§5), the data exists, and the withholding of keys after an order is a conduct question with serious consequences (guides 117-118): distinct from the technical impossibility of decryption, which the examiner states honestly. The court is told when, and asked to draw the conclusion.

### How should we warn a client not to do any of this?

Explicitly, in the hold notice, naming the acts (cleaning tools, resets, reinstalls, encryption, account deletion, clock changes), stating that they are traceable, and setting out the consequences: §11's paragraph. Clients under hold destroy evidence far more often from ignorance of the traces than from calculated risk; the warning removes the ignorance.

### Is running a wiping tool a criminal offence?

It can be, where it is done to pervert the course of justice in criminal proceedings, and in regulated contexts destruction of records may breach statutory duties: the civil consequences (adverse inference, strike-out, contempt where an order is breached) arise far more commonly and are severe in themselves (§7). The finding is evidenced the same way whichever track it reaches, and specialist advice is taken on the criminal edge.

§ 14 · REFERENCE

# Glossary

**Anti-forensics**
Deliberate techniques to defeat forensic examination.

**Cessation signature**
Routine records stopping or restarting empty at a date.

**Free-space wipe**
Overwriting all unallocated space to destroy deletion residue.

**Job file**
A wiping tool's saved record of targets and methods.

**Overwrite pattern**
The characteristic content a wipe leaves in erased regions.

**Prefetch**
Windows' record of program executions with timestamps and counts.

**Privacy cleaner**
Software purging histories, caches and recent-file records.

**Reset timestamp**
The firmware or setup record of a device's factory reset.

**Secure erase**
Overwriting file content before deletion.

**Shadow copy**
A volume snapshot often untouched by file-level wiping.

## Sources and authoritative references

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

- cflab.uk, digital forensics services (anti-forensics examination, wiping and reset analysis, 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 07 · Analysis (hold-notice drafting, redundancy mapping and destruction analysis as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- PD 57AD (preservation duty and disclosure certificate): justice.gov.uk, PD 57AD · CPR Part 31: justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization (what sanitisation achieves): csrc.nist.gov, SP 800-88 · NIST SP 800-86: csrc.nist.gov, SP 800-86
- Forensic Science Regulator, Code of Practice v2: gov.uk, FSR Code · ISO/IEC 27037: iso.org, 27037 · ICO, UK GDPR guidance: ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

# Working with Computer Forensics Lab

Anti-forensic examinations at the laboratory begin with the device unpowered and imaged write-blocked, because booting is the second wipe; the examination then reads the tool's arrival and execution, maps the overwrite extent, reads the cessation signature and the journal the tool forgot (Example 1's 1,400 names), pulls the platform's own record of resets and purges (Example 2's firmware stamp), and works the estate's redundancy for the material the wipe was meant to destroy: with the honest limit stated where content is truly gone. The routine-maintenance baseline is established before intent is pleaded (Example 3's Sunday cadence), and the dated finding is reported under CPR Part 35 or CrimPR Part 19. The laboratory also drafts the preventive paragraph of §11 for clients under hold. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a device has just come back suspiciously clean, the first instruction is the same as guide 108's: do not switch it on.

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