COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

External Storage Devices as Evidence

What Memory Sticks, External Drives and Cards Reveal: Copied Files, Timestamps, Deleted Data and Attribution

The previous guide proved the connection from the computer's side. This one examines the object itself: the memory stick delivered up under order, the external drive found in the desk, the memory card from the camera. A storage device carries its own testimony: the files it holds, the files it used to hold, timestamps that tell the copying story from the receiving end, traces of the machines it met, and the marks of attempts to clean it. This guide explains what a laboratory extracts from external storage, how device-side and machine-side evidence lock together, how deletion and reformatting are penetrated, what SSDs and flash media change about recovery, and how to frame attribution honestly when the object could have been in anyone's pocket.

⏱ Estimated reading time: 26 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. External media pass through the laboratory in volume: delivered up under order, seized in searches, or produced voluntarily: from single memory sticks to drawers of unlabelled drives, including physically damaged and deliberately destroyed units recovered at component level.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | MEDIA EXAMINATION & DATA RECOVERY | DAMAGED-DEVICE RECOVERY | CPR PART 35 EXPERT REPORTS

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: THE DEVICE IS DIRECT EVIDENCE; TREAT IT LIKE THE EXHIBIT IT IS

Machine-side USB analysis (guide 47) proves that a device met a computer; the device itself proves what came of the meeting. Examined properly: write-blocked, imaged, hashed, per this series' chain-of-custody discipline: external media yield four strata. **Contents:** the current files, hash-comparable to the source system's so that "the tender file on his stick" is a mathematical identity, not a resemblance. **History:** deleted files and folders, recoverable from file-system remnants and unallocated space with odds that depend heavily on media type: mechanical external drives recover generously; TRIM-governed SSDs and some flash media forget fast: plus reformat archaeology, where prior volumes and their dates survive beneath the current one. **The copy story:** timestamps on external media encode transfer events: creation times on the device marking when files arrived, wholesale trees sharing a single write window betraying a bulk copy, source-side modified times surviving the journey and proving the originals' vintage. **Provenance:** the device's own traces of the machines and accounts it met: system-generated folders and artefacts written by hosts, volume identity matching the LNK records on examined computers, occasionally host-written metadata naming machines outright. Locking device-side and machine-side strata together produces the strongest exfiltration (or exoneration) cases this series deals with. The honest limit is the pocket problem: a portable object proves its own history, not its carrier's identity; attribution is built from possession, the interlocking machine records, and content, and is expressed with exactly that structure.

- **Pursue the object early and handle it properly:** delivery-up converts inference to direct evidence, and a documented intake (photographed, write-blocked, hashed) keeps it admissible: guides 35 and 47's advice, converging.
- **Hash comparison is the closer:** device files matched to source-system files by hash end arguments about "similar documents"; the request to the examiner is comparison against named sources, not just a listing.
- **Media type sets recovery expectations:** mechanical drives and older sticks: good deleted-data odds; modern SSDs with TRIM: poor after short delay; memory cards: variable: the scoping call establishes which case you have before anyone promises the court recovered files.
- **Reformatting is rarely the end:** prior file systems, their creation dates and their content fragments survive routinely (guide 47's Example 3); a reformat after an order is a dated act of response, and usually a gift.
- **Damaged is not destroyed:** snapped sticks, drilled drives and immersed cards frequently yield at component level; physical destruction attempts are themselves powerful evidence, and the laboratory documents both the state and the recovery.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the object in the evidence bag

Sooner or later the case produces a thing: a stick surrendered at the disciplinary, a drive couriered under a consent order, a card found in a drawer during the search. The temptation is domestic: plug it in and look. Every instinct in this series says otherwise: plugging unprotected media into an ordinary computer writes to it (mounting, indexing, antivirus scans all touch the volume), changes timestamps that may be the very evidence, can trigger TRIM housekeeping on SSDs that erases recoverable data, and hands the other side a contamination argument gift-wrapped. The object goes to the laboratory as found, and comes back as an image plus a report.

The second temptation is narrative: the stick contains the client list, therefore he stole it. The device's evidence is richer and more careful than that: *when* the list arrived (during employment or after the injunction?), *from where* (timestamps and volume traces pointing at which machine), *what else* travelled with it, *what was deleted* and when, and *whose usage* the surrounding content reflects. The examined object either assembles the story or complicates it: both outcomes are worth having before pleadings say things evidence must then live up to.

§ 0 3 · INTAKE

Getting the device examined: intake, imaging, integrity

- **Documented receipt:** the exhibit record opens on arrival: photographs of the device, markings and serials; condition noted (including damage and tamper signs); custody transfer recorded: guide 35's regime, applied to an object small enough to lose.
- **Write-blocked imaging:** the device is read through hardware write-protection into a verified image (hashed at acquisition, verified thereafter); all examination happens on copies; the original returns to the exhibit store. Where media are failing, imaging adapts (sector-by-sector persistence, component-level work) per guide 44's damaged-array discipline.
- **Encrypted media meet guide 33:** BitLocker To Go, hardware-encrypted drives and encrypted containers on the volume need keys or passwords: hunted through the usual routes, compelled where orders allow, and noted as a stated limitation where absent.
- **The comparison set travels with the instruction:** device examination lands hardest when the laboratory also holds the source material (or its hashes): name the systems and files the device should be compared against in the instruction itself.

§ 0 4 · WHAT IS THERE

What the live file system tells you

- **Inventory with metadata:** every current file and folder, with sizes, timestamps and hashes: the exhibit-ready listing, filtered to the issues, and hash-matched against sources to separate identical copies from lookalikes and from edited descendants.
- **Structure speaks:** folder trees mirroring the employer's share ("Projects/Live/Tender 2026"), names like "backup" and "old laptop", and organisational habits that match (or fail to match) a claimed owner: content-as-conduct evidence, used with restraint.
- **Embedded metadata rides along:** Office authorship, revision and company fields inside the copied documents (per this series' metadata guide, ahead) often name the source environment outright: the claimant company in every document property is an eloquent inventory.
- **Host droppings map the itinerary:** system folders and files written by the computers the device met (Windows system-volume folders, Mac metadata files and trash folders, camera DCIM structures) sketch what kinds of machines used it, corroborating the machine-side serial trail and sometimes extending it to machines never examined.

§ 0 5 · WHEN IT GOT THERE

Timestamps on external media: reading the copy story

- **Creation on the device = arrival:** a file copied to external media typically takes a new creation time (the copy moment) while keeping its source modified time: so "created 22:41 on 3 March, modified 14:02 on 11 January" reads as "an 11 January document, copied here at 22:41 on 3 March": the two-clock signature of transfer, and the backbone of copy chronology.
- **Bulk copies cluster:** hundreds of files created within one tight window, tree intact, is a single drag of a folder: the shape of an exfiltration event, timeable to minutes and matchable to a guide 47 connection record on the source machine.
- **File-system semantics are stated, not assumed:** FAT/exFAT (most sticks and cards) record timestamps in local time with coarse resolution and no time zone; NTFS-formatted externals behave like guide 41 describes: the examiner declares the format's rules before the chronology is argued, and reconciles device clocks against host clocks where offsets appear.
- **Backdating meets the usual ladder:** manipulated timestamps on media face the internal-consistency checks of this series' backdating analysis: file-system internals, embedded metadata, and the interlocking machine-side records that a device-side edit cannot reach.

§ 0 6 · WHAT WAS THERE

Deleted data: recycle folders, unallocated space and the SSD problem

- **Deletion on removable media is usually immediate but shallow:** most systems bypass the recycle bin for removable volumes: the entry is dropped, the content remains in unallocated space until overwritten: so recovery odds track subsequent usage, not time alone. (External drives treated as fixed disks, and Mac-used media with trash folders, add a recoverable intermediate stop.)
- **Recovery has two gears:** file-system remnant recovery (names, paths, dates and content: the full story) and carving (content without names: guide 44's method), applied in that order, with results labelled by gear so the report's claims match the technique's yield.
- **Reformat archaeology:** a quick format writes a new empty index and touches little else: prior volume structures, their creation dates and swathes of prior content remain findable: the layered history that dated guide 47's Example 3, available on most FAT/exFAT media and many NTFS externals.
- **The SSD and TRIM caveat, honestly:** external SSDs and some high-end sticks implement TRIM-style housekeeping when hosts support it: deleted content may be genuinely unrecoverable within hours: the same caveat as guide 41's internal-drive discussion, and the reason recovery promises wait for the scoping call. Mechanical external drives, mainstream sticks and cards remain the generous end of the spectrum.
- **Wiping tools leave their signature:** patterned overwrites, vendor-tool remnants and the timing of a wipe (free space zeroed the day after the letter) convert lost content into conduct evidence: spoliation's device-side fingerprint.

§ 0 7 · WHOSE HAND

Whose device, whose hand: attribution on portable media

- **The pocket problem, named:** the device authenticates nothing about its carrier: no logons, no accounts, no sessions of its own. Attribution is assembled around it: possession (where found, who produced it, purchase records), the machine-side interlock (guide 47's serial trail placing it in the suspect's sessions on the suspect's machines), and content (personal documents, photographs, filenames and structures tying usage to a person).
- **The interlock is the engine:** device volume serial matching the LNK records on his desktop; arrival timestamps on the device matching connection windows in his logon sessions; host droppings matching his machines' platforms: each correspondence a weld between object and user that no "not mine" survives intact.
- **Shared and departmental media get shared-asset treatment:** the office backup drive touched by five people is framed like guide 43's shared folder: the report maps who could and did, by session, and resists the singular pronoun until the welds justify it.
- **Defence work reads the same welds in reverse:** a device never seen in the accused's sessions, content reflecting another user, arrival times in windows the accused can alibi: the interlock exonerates with the same mechanics, and the laboratory is instructed for exactly that as often as not.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the device in isolation. External-media evidence spans: the object itself; every computer it met (machine-side records per guide 47, plus the copied files' sources); the source systems and their servers (originals, access audit, snapshots per guide 43); corporate device-control and DLP tooling (insertion and transfer records); cloud sync services if the device's content was also synchronised anywhere; backups of the machines involved (older machine-side records); counterpart devices (a second stick in the same story, the home PC the files moved on to); and purchase and issuance records (who bought or was issued the object). When the primary source is unavailable: the device never produced, destroyed, or unreadable: these paths carry the case, and the machine-side stack alone frequently suffices for connection-and-access findings while the device's absence does its own evidential work.

EVIDENCE	THE DEVICE	SOURCE MACHINE(S)	SOURCE SERVERS / CLOUD	CORPORATE TOOLING	ONWARD DEVICES	DELETED / RECOVERABLE
Copied files (content)	Y: direct	Originals + access artefacts	Originals, versions, audit	DLP: sometimes itemised	Y if moved on	Device unallocated: media-dependent
Copy timing	Y (arrival timestamps)	Y (connection + access windows)	Access logs where enabled	Y where deployed	Second-hop timestamps	Varies
Device itinerary	Host droppings	Y (serial records, per machine)	n/a	Insertion logs	Y (their own records)	Registry durable
Deletion / wiping on device	Y (remnants, wipe signatures)	Sometimes (tool execution traces)	n/a	Sometimes	n/a	Gear-dependent
User attribution	Content indications	Y (sessions: the welds)	Account records	User field in alerts	Possession context	Varies

Fallback strategy in one line: no device? Run the machine-side stack, the corporate tooling and the source-server audit for connection, access and pattern, pursue onward devices and cloud copies for the content, and put the non-production itself before the court: the absent exhibit is a submission, not a dead end.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE TWO-CLOCK SIGNATURE AND THE INJUNCTION DATE

A consultant enjoined from using client materials produced his external drive "for inspection, voluntarily", confident it showed only his own work product. The two-clock reading undid him: ninety-one files carried modified dates from his engagement period but creation dates on the drive from six weeks *after* the injunction: copied onto this device, from somewhere, well after the order bit. The somewhere emerged from the files' embedded metadata (his co-defendant's initials in the revision history) and the drive's host droppings (a Windows machine matching the co-defendant's laptop, whose guide 47 records completed the interlock). Voluntary inspection became committal territory: the device had dated the breach and named the accomplice's machine.

EXAMPLE 2 · THE SNAPPED STICK, RECOVERED

Confronted at a disciplinary, an employee snapped his memory stick in half in front of witnesses: dramatic, and forensically optimistic. The halves went to the laboratory in an exhibit bag; component-level work read the storage directly; and the reconstructed volume held the payroll export (hash-matched), a folder of applications to competitors, and: in unallocated space: an earlier deleted copy of the same export from three weeks prior, establishing the taking predated the confrontation. The destruction act itself, witnessed and photographed, ran alongside the recovered content in the tribunal bundle. Physical destruction had converted a document case into a document case plus a conduct case.

EXAMPLE 3 · THE DRIVE THAT CLEARED HER

A finance manager was accused when the year-end pack surfaced on a competitor's desk: she had a company external drive, and the employer's investigator equated possession with guilt. The laboratory examination inverted it: the drive's content and structure reflected the finance *team's* shared use (four users' personal folders, per the department's own naming); the pack's copy on the drive carried an arrival timestamp inside a connection window that guide 47 analysis placed in a colleague's logon session on the shared workstation; and her own sessions showed the drive connected only for the month-end backups her role required, files hash-verified as exactly those backups. The colleague's home PC, later delivered up, held the onward copy. The welds that convict had, assembled honestly, acquitted: and identified the leak.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Plugging it in to look:** timestamps altered, TRIM triggered, contamination argued: the domestic reflex, indulged.
- **Listing without comparing:** an inventory delivered with no hash-match against sources: the question half-answered.
- **Reading FAT timestamps as NTFS:** local-time, coarse-resolution semantics ignored; chronologies built on the wrong rules.
- **Possession pleaded as attribution:** the pocket problem waved away; Example 3's investigator, everywhere.
- **Recovery promised before media type is known:** the SSD caveat discovered in the witness box.
- **The interlock never built:** device examined, machines examined, nobody joining the welds.
- **Damaged devices abandoned:** Example 2's halves binned as hopeless by someone who never asked a laboratory.
- **Loose exhibit handling:** a pocketable object with no custody record: guide 35's cautionary tales in miniature.

Technical limitations

- **TRIM and wear-levelling on SSDs/flash** can make deletion genuinely final; stated per media, per timing.
- **FAT-family metadata is thin:** no ownership, no audit, coarse times: the format most sticks use records the least.
- **Carved recoveries lack names and dates:** gear-two results are labelled as such and used accordingly.
- **Hardware-encrypted and locked devices** without credentials may be unreadable at any effort level: the limitation is stated and the architecture paths take over.
- **Host droppings identify platforms, not people:** corroboration, not attribution, and reported at that weight.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What devices exist or existed: issued, personal, departmental: and can purchase or issuance records be found?
- What should the device contain if the innocent explanation is true: and what must it not?
- Which source files and systems should the laboratory hash-compare against?

Ask your opponent

- Please deliver up [devices], unaltered, and confirm none has been connected to any computer, formatted, wiped or disposed of since [date]; if any has, give particulars.
- Please identify all external storage devices used by [name] in connection with [matter] in [period], including devices no longer held, with dates and circumstances of disposal.
- We put you on notice that laboratory examination will address deleted content, prior volumes and wiping activity; conduct in respect of the devices will be relied on accordingly.

Ask your eDiscovery / forensic provider

- What does media type mean for recovery odds here, before we plead anything?
- What comparison set do you need from us, and in what form?
- Can you build the machine-device interlock, and what additional images does that require?

SUGGESTED WORDING · INSTRUCTION FOR DEVICE EXAMINATION

> "Please examine the delivered device(s) and report on: (1) intake condition and integrity, with imaging method and hashes; (2) a metadata inventory of live content relevant to [issues], hash-compared against the source materials at Schedule B; (3) the copy chronology: arrival timestamps read under the applicable file-system semantics, bulk-copy windows, and correlation with the connection and session records from [machines]; (4) deleted content, prior volume structures and any wiping or formatting activity, with recovery gear and timing stated; (5) indications of the machines and platforms the device has been used with; and (6) attribution observations framed against possession, the machine interlock and content, distinguishing what the device itself establishes from what surrounding evidence supplies. Please state media-type recovery limitations expressly."

§ 12 · QUICK CONTROL

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

The external media checklist

- ☐ Devices pursued early: delivery-up sought, disposal questions asked on the record
- ☐ No one plugs anything in; exhibits bagged, custody opened, couriered to the laboratory
- ☐ Write-blocked imaging with hashes; originals to the exhibit store
- ☐ Media type established; recovery expectations set before pleadings promise
- ☐ Inventory hash-compared against named sources
- ☐ Copy chronology read under correct file-system semantics; bulk windows identified
- ☐ Deleted, reformatted and wiped layers examined; gears and timing labelled
- ☐ Machine-device interlock built across every available computer
- ☐ Attribution framed on possession + interlock + content; shared media mapped, not presumed
- ☐ Encrypted and damaged units routed to specialist handling, not abandoned

Red flags

- "I had a quick look at what's on it first."
- A device produced formatted, "for privacy".
- Devices "lost" or "thrown away" after the letter before action.
- An inventory with no source comparison.
- Chronologies silent on FAT time semantics.
- Possession equalling guilt in the particulars.
- A damaged device written off without laboratory assessment.

When to involve a digital forensic expert

Before the device is touched: intake discipline is where device cases are won or contaminated. At scoping, for the media-type conversation that calibrates every promise made to the court. At examination, for the strata this guide describes and the interlock that gives them force: laboratory work end to end. And whenever the object is damaged, encrypted or missing: component-level recovery, credential strategy and architecture-path fallbacks are specialist calls, and Example 2's halves are a standing argument against giving up early. Both instructing positions are routine: building the device case, or testing one: Example 3's inversion: under CPR Part 35 and CrimPR Part 19, with the pocket problem and media limits stated plainly.

§ 13 · COMMON QUESTIONS

Frequently asked questions

We have the stick. Do we still need the computers?

For a strong case, yes: the device supplies content and arrival times; the machines supply connection records, sessions and access artefacts: and the welds between them are what attribution stands on. A device alone proves what it holds and roughly when it arrived; paired with even one source machine it proves the corridor the files travelled and whose session the transfer sat inside. Ask for both in the same order wherever possible.

The files were deleted from the stick before it was handed over. Gone?

Frequently not: removable-media deletion is shallow (index dropped, content resident until overwritten), and sticks see little post-deletion writing in the ordinary course. Expect file-system remnant recovery first (names, dates, content) and carving behind it: unless the device is a TRIM-active SSD, where the honest answer arrives only after imaging. Reformatting changes little: prior volumes and content routinely survive quick formats, and the reformat's own date joins the chronology.

Can you tell which computer the files came from?

Often, by convergence: source-side modified times and embedded metadata carrying the origin environment; host droppings typing the platforms the device met; and, decisively, the machine-side interlock: the source computer's own records of this device's serial, connected in a session, with the very files accessed in the window the device says they arrived. Any single strand indicates; the convergence identifies: and the report will use exactly those verbs.

The device belongs to the company but lived on a shared desk. Is attribution hopeless?

No: it is shared-asset work, per Example 3: map the users whose sessions the device appears in across the machine fleet, read the content's internal ownership signals, and time the disputed transfer against the session record. Shared possession widens the starting pool and the interlock narrows it: sometimes to one, sometimes to two-with-submissions: and a report that shows that narrowing honestly outperforms one that never admitted the pool existed.

What about memory cards from cameras, dashcams and phones?

Same laboratory treatment, distinct habits: DCIM structures and device-written metadata (camera model, sometimes GPS in the images themselves) make provenance unusually rich; FAT semantics govern times; deletion recovery is typically generous; and the card frequently outlives and contradicts the device it served ("the dashcam footage was overwritten" meets the card's unallocated space). Treat cards as first-class exhibits, not accessories: they decide cases about incidents, journeys and timelines with some regularity.

Our opponent simply has not produced the drive we know exists. What now?

Run the fallback line: machine-side records prove the device's existence, serial, and every connection (guide 47); corporate tooling and server audit prove access and pattern; onward copies are pursued where the content travelled. Then put the absence itself to work: specific disclosure and delivery-up applications, questions about disposal with dates, and the adverse-inference submission that a produced device would have answered. Non-production of a pocketable exhibit is rarely neutral, and courts are readier than opponents expect to say so.

§ 14 · REFERENCE

Glossary

Arrival timestamp
Creation time a file takes on the device at copy: the transfer moment.

Carving
Content recovery without file-system context; names and dates absent.

Component-level recovery
Reading storage chips directly from damaged devices.

DCIM structure
Standard camera folder layout; provenance signal on cards.

FAT/exFAT semantics
Local-time, coarse-resolution timestamp rules of most removable media.

Host droppings
System files written to media by computers it met; platform itinerary evidence.

Interlock
The welded correspondence between device-side and machine-side records.

Pocket problem
Portability's attribution gap: the object proves its history, not its carrier.

Reformat archaeology
Recovery of prior volumes, dates and content beneath a new format.

Two-clock signature
New creation + old modified time: the copy event, self-documented.

Wipe signature
Patterned overwriting and tool remnants evidencing deliberate destruction.

Write blocker
Hardware preventing any write during imaging; intake's first tool.

Sources and authoritative references

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

- cflab.uk, digital forensics services (media examination, data recovery including damaged devices, hash comparison and copy-chronology analysis, CPR Part 35 / CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection (device sources within disclosure exercises; "defensibility is built, not retrofitted"): e-discovery.uk/edrm/collection · Knowledge Centre: e-discovery.uk/knowledge
- e-discovery.uk, practice method: e-discovery.uk
- NPCC / College of Policing digital evidence guidance: college.police.uk, digital devices guidance · Forensic Science Regulator statutory Code: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 and ISO/IEC 17025: iso.org, 27037 · iso.org, 17025
- CPR Part 35 and CrimPR Part 19: justice.gov.uk, Part 35 · justice.gov.uk, CrimPR Part 19

DISCLAIMER

This publication provides general information about external storage devices as evidence as at August 2026. Recovery behaviour varies by media type, controller and usage, and the worked examples are fictional. 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. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

External media are received, imaged and examined at the laboratory daily: documented intake, write-blocked acquisition, hash comparison against your named sources, copy-chronology and deleted-layer analysis with media-type limits stated, and the machine-device interlock built across every image you can supply: including component-level recovery of snapped, drilled and immersed devices, and defence review of possession-equals-guilt reasoning. Reporting runs under CPR Part 35 and CrimPR Part 19. Through **e-discovery.uk**, device findings integrate into disclosure-scale exercises alongside every other source. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if a device is about to be handed over, examined in-house, or has just been dramatically destroyed, call first.

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