COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Can You Prove a USB Drive Was Connected?

The Registry Trail, the Serial Number, the Timeline: and What Connection Does Not Prove

Yes: on an ordinarily used Windows computer, the connection of a specific USB storage device is one of the most provable events in digital forensics, recorded in several independent places with make, model, serial number and times. This short, focused guide: a companion to the broader Windows evidence guide: walks through exactly how the proof is assembled, artefact by artefact; how one physical stick is identified across several machines; how connection evidence is timed, corroborated and presented; what the record honestly does not establish on its own; and how both claimant and defence teams should use it.

⏱ 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. USB connection analysis features in a large share of its employment, IP-theft and fraud casework, on both sides: building the connection-and-access timeline for claimants, and testing overclaimed versions of it for the defence, under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | USB & EXFILTRATION ANALYSIS | CPR PART 35 EXPERT REPORTS | COURT-EXPERIENCED EXPERT WITNESSES

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: CONNECTION IS PROVABLE; MEANING IS BUILT

Windows records USB storage connections for its own housekeeping in at least four independent places: registry device keys (manufacturer, model, serial, device timestamps), the setupapi installation log (first-ever connection, to the second), Windows event logs (connect and disconnect events where the relevant channels are enabled), and the mounted-volume records that tie the device to a drive letter and a volume identity. Because these records are created by different subsystems for different purposes, they corroborate one another: a challenge to any one must explain the others. The device's **hardware serial number** makes the proof portable: the same physical stick is identifiable on every Windows machine it ever touched, so a connection timeline can span the office desktop, the boardroom laptop and: after delivery-up: the home PC. Around the connection sits the evidence that gives it meaning: shortcut files and jump lists recording documents opened from the device's volume; shellbags recording its folders browsed; file-system and journal traces of copying; and the session context (who was logged in) that starts attribution. And there the honest limits begin: connection proves a device was present, not who inserted it and not, by itself, what was copied to it: copying is usually established as a pattern (connection, plus access to the files, plus volume and timing consistency, plus: decisively: the files found on the recovered stick), and the careful formulation of that pattern is what separates the report that survives cross-examination from the one that creates it.

- **The proof is layered by design:** four independent recorders; deleting or altering one leaves the others, and the tampering itself tends to show.
- **Serial numbers travel:** device identity is cross-machine; the exfiltration story is told across every computer the stick met, and the stick itself is the closing exhibit: pursue delivery-up early.
- **Timing is bracketed honestly:** first connection is logged to the second; last connection and intermediate sessions are established from the artefact set with per-artefact semantics stated: not every artefact records every insertion, and the report says which shows what.
- **Defence uses the same stack:** no connection in the disputed window, an IT-owned device, or access limited to innocuous files: the record exonerates as readily as it convicts, per this series' recurring payslips example.
- **Speed matters less here than elsewhere, but is not free:** the registry trail is durable through ordinary use, but event logs rotate and machines get reissued: preserve and image on the usual clock.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: one stick, one afternoon, one question

The client's suspicion is always specific: he came in on Saturday, he had a stick, the tender file was gone by Monday. The legal question is whether suspicion can become proof: and with USB storage on Windows, it usually can, because the operating system cannot help itself. To make plug-and-play work, Windows must remember devices; to make drive letters stable, it must remember volumes; to make "recent files" work, it must remember what was opened and from where. None of these features was built for court, which is precisely their value: the record was kept by machinery with no stake in the dispute, before anyone knew there would be one.

The craft is in assembly and restraint. Assembly, because the persuasive exhibit is not one registry key but the convergence: the same serial in the device records, the setupapi log, the event log and the volume records, bracketed by a logon session and surrounded by access artefacts. Restraint, because the record's edges are real: it does not photograph the hand on the stick, it does not itemise every byte copied, and an examiner who claims otherwise hands the other side its best afternoon. This guide teaches both.

§ 0 3 · THE RECORDERS

The artefact stack: where connection is recorded

RECORDER	WHAT IT HOLDS, AND ITS ROLE IN THE PROOF
Registry device keys (USBSTOR and related)	Per-device entries created at installation: manufacturer, product, revision and the hardware serial; associated device timestamps interpreted per Windows version. The backbone identity record: durable, per-machine, surviving the device's removal and most casual "clean-ups".
setupapi.dev.log	The driver-installation diary: the device's first-ever connection to this machine, date and time to the second, with the serial in the entry. The anchor for "when did this stick first meet this computer?": routinely decisive where the first connection is itself the story (the Saturday, the notice period, the day before resignation).
Event logs (device / driver channels)	Connect and disconnect events with timestamps where the relevant channels are enabled (coverage varies by Windows version and configuration): where present, the per-session record: each insertion and removal, not just the first.
Mounted-volume and drive-letter records	The link from hardware to file system: volume name, volume serial and assigned letter. The junction that lets access artefacts (which reference volumes) be tied back to the physical device.
Supporting cast	User-hive traces tying the device's volume to a specific account's activity; shellbags for its folders; LNK/jump lists for its files; Windows Search and antivirus scan records that sometimes log paths on the device: each adding a strand, per guide 41.

§ 0 4 · WHICH STICK

Identifying the specific device: serials and volume identity

- **The hardware serial is the fingerprint:** assigned by the manufacturer, embedded in the device, reported identically to every Windows machine: the registry entries on the office desktop and the home laptop naming the same serial are naming the same physical object, and the report can say so plainly.
- **The exception is noted, not feared:** a minority of cheap devices lack unique serials; Windows flags these (generating instance identifiers of a recognisable form), the examiner identifies the situation, and identity is then built from the volume layer and timing instead: weaker alone, workable in convergence.
- **Volume identity is the second signature:** formatting a stick creates a volume with its own serial and label; LNK files and other artefacts record volume serials of the media that files were opened from. Hardware serial identifies the object; volume serial identifies its file system: together they survive even the counter-move of reformatting (the hardware serial persists; the volume change itself is a dated event in the trail).
- **The recovered device closes the loop:** delivery-up of the stick allows the laboratory to read its serials directly, match them to every machine's records, and examine its contents: including deleted material: against the source files' hashes: the endgame that turns a connection case into a copying case, and the reason the physical device is pursued in every order this series drafts.

§ 0 5 · WHEN

Timing: first, last and in-between connections

- **First connection:** the setupapi entry, to the second, corroborated by device-key creation: the cleanest timestamp in the stack, and often the case's hinge.
- **Subsequent sessions:** assembled from event-log connect/disconnect pairs (where enabled), registry timestamps whose per-version semantics the examiner states (some update on later events, some do not), and the surrounding activity: LNK creation times for files opened from the volume, shellbag interaction times, journal entries: each a dated touchpoint of the device being present and in use.
- **Session bracketing:** connection evidence is framed inside the logon session (guide 41's Security-log work): the stick connected at 16:41 during an interactive session of account X that began 16:38: the sentence that carries attribution's first two links.
- **The clock discipline as ever:** UTC storage, local display, machine clock verified: and where timing is the battlefield (did the connection precede or follow the meeting?), the report shows the conversion working.
- **Honest gaps:** where event channels were off and registry semantics give only first-and-latest, the report brackets ("connected on at least the following occasions") rather than inventing a complete diary: the formulation that cross-examination cannot improve on.

§ 0 6 · FROM PRESENCE TO COPYING

From connection to files: what access evidence adds

- **Files opened from the device:** LNK files and jump lists recording documents on the stick's volume (path, volume serial, timestamps): proof the device was not merely present but used, and of what was touched on it.
- **Folders browsed:** shellbags for the device's directory tree: including folders since deleted, including trees whose names ("Client Backup", "GK backup") become exhibits in themselves.
- **Copying's quieter traces:** Windows keeps no single "copied to USB" log; copying is evidenced as a pattern: source files accessed in the window; destination volume present; occasionally journal and application traces (archive tools run, per guide 41's execution artefacts; Explorer copy dialogs in RAM if captured); and volumetrics (SRUM's per-application activity) consistent with transfer. The report assembles and labels the pattern as such.
- **The stick's own contents:** where recovered: the files, their hashes matching the source system's, their timestamps telling the copy story from the receiving end; where not recovered, the absence is a submission point (why has the device not been produced?) rather than a proof gap the claimant must apologise for.
- **Defence symmetry throughout:** the same artefacts establishing that only personal files were opened, that the device was IT's imaging drive on the IT calendar's date, or that the "copying window" contains no source-file access at all: the pattern method serving whichever side the facts do.

§ 0 7 · THE EDGES

What connection evidence does not prove

- **Not the hand:** the record proves the machine met the device during a session of an account; the person holding the stick is the attribution chain's human layer, built per guide 41 (authentication, exclusivity, pattern, elimination): never assumed from ownership of the desk.
- **Not the contents at the time:** what the stick held when connected is known only from access traces and, later, the device itself; a connection alone says nothing about what, if anything, moved.
- **Not intent:** people connect sticks for slides, photographs and chargers; the pattern (which files, which timing, whose device, what followed) carries the inference, and the report leaves the adjectives to counsel.
- **Not completeness:** the artefact stack has horizons (event rotation, per-version semantics); "the only connections were…" is claimed only where the surviving records genuinely support it.
- **And not immunity from context:** IT imaging routines, backup drives, shared machines and departmental sticks generate innocent connection records daily; the examiner canvasses the alternatives before the lawyer pleads the sinister one: the CPR 35 duty and the strategic one aligned.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the one computer in isolation. A USB event's evidence extends across: every other machine the device touched (home PCs, second work machines: the serial travels); the device itself (contents, deleted material, its own timestamps); the source systems whose files were accessed (file-server audit and snapshots, per guide 43); endpoint-management and security tooling (device-control logs, DLP alerts, antivirus scans of removable media: where deployed, an independent corporate record of insertions with user and machine); the domain's authentication layer (who was logged on where); backups of the examined machine (older registry hives and event logs extending the trail's reach); and, in VDI estates, the session layer's redirection records (guide 46). When the primary machine is unavailable: reissued, wiped, or its logs rotated: these paths reconstruct the event from its other witnesses.

EVIDENCE	EXAMINED PC	OTHER PCS (SAME SERIAL)	THE DEVICE ITSELF	CORPORATE TOOLING (DLP / DEVICE CONTROL)	BACKUPS OF THE PC	DELETED / RECOVERABLE
Connection (identity, first time)	Y	Y, per machine	Own timestamps: partial	Y where deployed	Y (older hives/logs)	Registry trail durable
Per-session insertions	Where channels enabled	Likewise	n/a	Often Y	Extends rotation reach	Log rotation limits
Files accessed from device	Y (LNK, shellbags)	Y	Y (contents, recents)	Sometimes (scan paths)	Y	LNK survives deletion
What was copied	Pattern evidence	Pattern evidence	Y: the closing proof	DLP: sometimes itemised	Pattern at earlier dates	Device deleted files: often carvable
Who was at the keyboard	Session records	Session records	n/a	User field in alerts	Y	Varies

Fallback strategy in one line: if the machine is gone, follow the serial (other computers), the corporate tooling (device-control and DLP records), the backups (older hives and logs), and above all the device: delivery-up converts every gap in the machine-side story into the stick's own testimony.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE SERIAL THAT CROSSED THREE MACHINES

A recruiter denied ever moving candidate data: "I don't even own a memory stick." The registry stack said otherwise, three times: a device (make, model, serial ending 4C7F) first connected to her office desktop at 17:52 on her penultimate day (setupapi), with LNK files recording the candidate database export opened from its volume; the same serial on the boardroom laptop two days earlier for eleven minutes; and: after delivery-up of devices from her home under order: the stick itself, plus her home PC's registry showing serial 4C7F first connected the evening of the penultimate day at 21:14. The stick's contents hash-matched the export. Three machines, one serial, one evening: the denial was withdrawn by amendment, and the case became about remedy.

EXAMPLE 2 · THE CONNECTION THAT WAS IT ALL ALONG

An employer's investigator reported "a mass-storage device connected for 47 minutes" on a suspended manager's PC and the disciplinary proceeded on exfiltration. The defence examination read the same records further: the device's registry identity was a one-terabyte external drive of the model IT purchased in bulk; its serial appeared across nine other machines on dates matching the IT team's published re-imaging calendar; the 47-minute window contained a technician's admin logon, not the manager's; and the manager's own account showed no session that day (he was suspended, badge records agreeing). The "exfiltration" was the deployment team preparing his machine for reallocation. The dismissal failed for want of reasonable investigation: the stack had named the innocent explanation in its first four fields.

EXAMPLE 3 · THE REFORMAT THAT DATED ITSELF

Facing delivery-up, a defendant produced his stick freshly formatted: "nothing on it, never was." The layers disagreed politely. Hardware serial: matched the office machine's records across six connections in the notice period. Volume history: the office LNK files recorded a volume serial from those dates; the produced stick's current volume serial differed, and its file-system creation timestamp fell two days after the delivery-up order was served. Carving the device recovered fragments of the pricing workbook, hash-matching pages of the original. The reformat had not erased the story; it had added a chapter, dated, about response to the order: which the judge addressed in terms at the costs hearing.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **"Connected" reported as "copied":** the overclaim this guide exists to prevent; the pattern method, or nothing.
- **Innocent-device blindness:** Example 2's IT drive; the model-and-calendar check skipped.
- **Attribution from the desk:** the session layer ignored; the account's owner named for a technician's logon.
- **Timestamp semantics flattened:** per-version registry behaviour ignored, "last connected" asserted from a field that does not mean that on this build.
- **The device not pursued:** months of machine-side argument while delivery-up: the closing exhibit: goes unsought.
- **Cross-machine reach unused:** the serial's travels to home and second machines never followed.
- **Corporate tooling forgotten:** DLP and device-control logs: sometimes an itemised transfer record: never requested.
- **Slow preservation:** the machine reissued, event logs rotated, and the durable registry left carrying the case alone.

Technical limitations

- **Coverage varies by build and configuration:** event channels, registry semantics and artefact presence differ across Windows versions; findings are stated per this machine's reality.
- **No native byte-level copy log:** absent DLP-class tooling, copying is pattern-proved; the report's language reflects it.
- **Serial-less devices exist:** identified as such and handled through volume identity and convergence.
- **Non-storage devices tell less:** phones in charge-only mode and MTP connections leave different, thinner trails than mass storage: the examiner distinguishes the classes rather than borrowing conclusions across them.
- **Anti-forensics leaves marks but takes data:** registry cleaning and log clearing are usually detectable (and dated), but a competently scrubbed machine may retain only fragments: the cross-machine and corporate layers then carry the proof.
- **Macs and Linux differ:** this guide is Windows; the Mac guide's mounted-volume artefacts do parallel work with different persistence.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which machines could the individual have used, and where are they now? (The serial's itinerary needs the fleet preserved.)
- Is device-control, DLP or endpoint-security tooling deployed, and what do its logs show for the period?
- What legitimate USB activity (IT imaging, backups, departmental drives) should we expect to find and exclude?

Ask your opponent

- Please deliver up all USB storage devices in [name]'s possession or control, and identify any disposed of since [date], with particulars.
- Please preserve and produce forensic images of [machines], and confirm no re-imaging, reissue or clean-up has occurred since [date].
- Please disclose device-control and DLP records for [name] in [period].

Ask your eDiscovery / forensic provider

- Which recorders are present and enabled on these builds, and what will each honestly support?
- How will the report formulate copying: pattern elements, and their individual strength here?
- What does the cross-machine and device plan look like: which serials to chase, which orders to seek?

SUGGESTED WORDING · INSTRUCTION FOR USB CONNECTION ANALYSIS

> "Please examine the images of [machines] and report on: (1) all USB storage devices connected in [period], with make, model, serial and, per device, the first connection time and such further connection occasions as the artefacts support, stating the basis and limitations of each; (2) the logon sessions within which each relevant connection occurred; (3) files and folders accessed from each device's volume, and any pattern of source-file access, archiving or transfer activity consistent or inconsistent with copying to the device; (4) legitimate explanations canvassed, including IT and backup device fleets, with the checks performed; and (5) upon delivery-up, the examination of the device(s) against the foregoing, including recovered deleted content and hash comparison to source. Please express copying conclusions as evidenced patterns and distinguish, throughout, connection, access and transfer."

§ 12 · QUICK CONTROL

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

The USB evidence checklist

- ☐ All candidate machines preserved and imaged before reissue; event-log rotation halted
- ☐ Full recorder stack examined: registry, setupapi, event channels, volume records: convergence shown
- ☐ Device identified by hardware serial; volume identity mapped; serial-less cases flagged and handled
- ☐ Timing anchored on setupapi for first connection; further occasions bracketed with stated semantics
- ☐ Connections framed in logon sessions; attribution built in layers, never assumed
- ☐ Access evidence assembled: LNK, jump lists, shellbags, execution and volumetric context
- ☐ Innocent fleets checked: IT drives, backup routines, shared devices: and excluded on evidence
- ☐ Corporate device-control / DLP records requested where deployed
- ☐ Cross-machine trail followed; delivery-up of the device pursued early
- ☐ Copying expressed as a labelled pattern; the report's limits stated before the other side states them

Red flags

- A report leaping from "connected" to "stole".
- An exfiltration case with the physical device never sought.
- Connection findings with no session framing.
- A device model matching the IT department's own fleet, unremarked.
- A stick produced freshly formatted after an order (Example 3: date the volume).
- Machines reissued mid-dispute; "we needed the laptop back".
- Timestamps asserted without per-version semantics.

When to involve a digital forensic expert

At preservation, to hold the fleet and the logs while they still cover the window; at analysis, because the stack's strength is convergence and its danger is semantics: both examiner's work; at the order stage, to specify delivery-up and the device examination that closes the loop; and at review, whenever the other side's case rests on USB findings: Examples 2 and 3 are, between them, most of what our defence instructions in this area look like, and the distance between what the artefacts say and what enthusiastic reports claim remains the most reliably productive ground in device litigation. Reported, throughout, under CPR Part 35 / CrimPR Part 19 with the edges stated.

§ 13 · COMMON QUESTIONS

Frequently asked questions

How certain is device identification, really?

For devices with hardware serials: as certain as digital identification gets: the serial is manufacturer-embedded, machine-independent and recorded identically wherever the device goes; matching entries across machines and to the recovered stick is a like-for-like comparison the report can make without hedging. For the serial-less minority, identity is a convergence finding (volume identity, timing, model) and is expressed as such. The examiner tells you which class your device is in on day one.

Can someone delete the connection records?

Partially, with effort, and rarely cleanly: the records live in multiple stores with different clean-up resistance; consumer "privacy" tools miss several; and the scrubbing itself (cleaner execution in the artefacts, registry gaps with telltale shapes, cleared logs writing their own final entry) tends to be provable and dated. Meanwhile the cross-machine copies, the backups' older hives and any corporate tooling remain untouched. Post-duty scrubbing thus usually converts a connection case into a spoliation case: an upgrade for the other side.

The connection was two years ago. Too late?

Often not: the registry identity and setupapi anchor survive ordinary use for years, and backups can reach further. What fades is texture: event-log sessions rotate away, recency artefacts cap out: so the two-year case tends to establish the device and its first meeting firmly, with fewer intermediate occasions. Whether that suffices depends on what the case needs the timeline to carry: an examiner's scoping view, from the actual image, costs a day.

He says the stick was for personal photos. How is that tested?

On the access layer and the device: what the LNK files and shellbags show being opened from the volume (holiday folders or the CRM export); what the source systems record being touched in the connected windows; and, on delivery-up, what the stick holds and held (deleted material included) against the claim. Personal-use explanations are frequently true and frequently checkable: the pattern method neither presumes guilt nor takes assertions on trust, which is precisely why its findings carry weight in both directions.

Do phones connected by cable show up like memory sticks?

Differently: modern phones present as media devices (MTP) or charge-only, not mass storage; they leave their own connection records (device identity, times) but not drive letters or volume serials, and file movement through MTP leaves thinner machine-side traces. The examiner treats the classes separately: a phone-cable finding supports presence and, with access artefacts, use, but the mass-storage inferences do not transplant. Phone-side evidence (the mobile guides ahead) then carries what the PC side cannot.

What single step most strengthens a USB case?

Get the device. Delivery-up, sought early and enforced, converts every machine-side inference into direct evidence: contents, hashes, deleted files, the stick's own dates: and Example 3 shows even the destructive response to an order becoming evidence. Second place: preserve the whole fleet before reissue, so the serial's itinerary can be walked. Everything else in this guide works better with those two done, and limps without them.

§ 14 · REFERENCE

Glossary

Device key (USBSTOR)
Registry record of an installed USB storage device: make, model, serial.

Device control / DLP
Corporate tooling logging or blocking removable-media use; sometimes itemising transfers.

Delivery-up
The order producing the physical device: the machine-side story's closing exhibit.

Hardware serial
Manufacturer-embedded device identifier; identical on every machine: the fingerprint.

LNK volume serial
The opened file's source-volume identity recorded in shortcuts; ties documents to media.

MTP
Media-transfer mode used by phones; different, thinner trail than mass storage.

Pattern proof of copying
Connection + source access + timing + (ideally) device contents: labelled as a pattern.

setupapi.dev.log
Driver-installation log; the first-connection anchor, to the second.

Session framing
Placing the connection inside a logon session: attribution's first links.

Volume serial
Per-format file-system identity; changes on reformat, and dates the reformat.

Sources and authoritative references

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

- cflab.uk, digital forensics services (USB and exfiltration analysis, device examination on delivery-up, defence review of device findings, CPR Part 35 / CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · the defence lawyers' digital-evidence guide and library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection (device and endpoint sources within disclosure exercises): 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

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

USB analysis is bread-and-butter laboratory work, run to this guide's disciplines: the full recorder stack examined in convergence, devices identified by serial and volume, timelines session-framed and honestly bracketed, copying expressed as labelled patterns, innocent fleets checked before anything is pleaded, and the physical device pursued, received and examined against source hashes: reported under CPR Part 35 and CrimPR Part 19. We are instructed as often to test USB findings as to make them; Examples 2 and 3 are composites of that defence work. Cross-machine and corporate-tooling follow-through comes as standard, and through **e-discovery.uk** device findings integrate into wider disclosure exercises. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if machines are queued for reissue, call today.

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