COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

What Evidence Can Be Recovered from a Windows Computer?

Deleted Files, USB History, Logins, Browsing, Execution Traces and the Timeline They Build

A Windows computer is a diary that its user never reads: every login, every program run, every file opened, every USB stick inserted and every website visited leaves traces in places most users have never heard of. For lawyers, that diary answers litigation's recurring questions: who did what, on which machine, when, and what happened to the documents that are no longer there. This guide tours the principal Windows evidence sources in plain English: what each artefact records, what it can and cannot prove, how deleted material comes back, and how an examiner assembles thousands of individual traces into a timeline a court can follow.

⏱ Estimated reading time: 28 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. Windows examination is the bread and butter of the laboratory: employee data theft, fraud, unauthorised access, document forgery and attribution disputes, examined from forensic images and reported under CPR Part 35 and CrimPR Part 19. Its eDiscovery arm, **e-discovery.uk**, integrates device-level findings into disclosure-scale review.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | WINDOWS ARTEFACT EXAMINATION | DELETED DATA RECOVERY | CPR PART 35 EXPERT REPORTS | COURT-EXPERIENCED EXPERT WITNESSES

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: WINDOWS RECORDS FAR MORE THAN USERS CREATE

The documents a user saves are a fraction of what a Windows computer knows. Around them, the operating system maintains dozens of records for its own housekeeping: registry entries logging every USB device ever connected; event logs recording logons, logoffs and system changes; shortcut files and jump lists remembering every document opened, including documents on drives long since removed; execution artefacts (Prefetch, Shimcache, Amcache, UserAssist, SRUM) recording which programs ran and when; browser databases holding history, searches, downloads and cached pages; and, beneath the file system, the recoverable remains of deleted files in the Recycle Bin, unallocated space, shadow copies and system restore data. None of this was designed as evidence; all of it functions as evidence, because it was created automatically, for operational reasons, by software with no stake in the litigation. The examiner's craft is threefold: recover it from a forensic image without altering it, interpret each artefact within its real limits (most prove that an account did something, not that a person did), and correlate thousands of entries into a timeline in which independent artefacts confirm one another. For lawyers, the practical rule is symmetrical: assume the machine remembers what your opponent claims never happened, and assume it also remembers what your client hopes it has forgotten.

- **Deletion is rarely destruction:** deleted files persist in the Recycle Bin, in unallocated space until overwritten, in Volume Shadow Copies, in temporary and cache copies, and in the metadata that records they once existed: even an unrecoverable file usually leaves a recoverable name, date and trace of its deletion.
- **The USB record is close to indelible in ordinary use:** Windows logs connected devices in multiple independent places (registry device keys, setupapi logs, event logs), with make, model, serial number and connection times: the backbone of most data-theft cases.
- **Attribution is layered, not assumed:** artefacts attach to user accounts; tying an account session to a human uses logon records, authentication types, and the surrounding activity pattern: and the honest report says which layer each conclusion rests on.
- **Anti-forensics usually leaves its own trail:** cleaning tools, mass deletions, clock changes and reinstalls are themselves recorded or inferable, and destruction evidence can matter more than the destroyed material, particularly after a preservation duty has arisen.
- **Everything below assumes a forensic image:** the acquisition, hashing and custody disciplines of earlier guides in this series; artefacts examined on a live original are evidence being altered while it is read.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the machine remembers

A departing employee copies the client database to a USB stick, deletes the copy from his desktop, empties the Recycle Bin, and hands the laptop back clean. On the screen, nothing remains. On the disk, nearly everything does: the registry recorded the stick's make, model and serial number and the minute it was first and last connected; shortcut files record the database file being opened from a volume with that stick's serial; the deletion left Recycle Bin metadata naming the file, its size and the moment it was deleted; and the file's content may still lie in unallocated space, recoverable in whole or part. The employee's clean screen and the examiner's rich disk are the same computer: the difference is where each of them looked.

This asymmetry defines Windows forensics. The operating system is a compulsive note-taker: not because Microsoft anticipated litigation, but because features need memory: recent-files lists need records of opened files, plug-and-play needs records of devices, performance features need records of program launches. Each feature's memory is an artefact, and because the artefacts are independent (different features, different files, different formats), they corroborate each other in a way no single record could. A story that has to be consistent with the registry, the event logs, the link files, the execution traces and the browser database at once is a story with very little room to be false, and that is precisely what makes a well-examined Windows machine so decisive in court.

§ 0 3 · WHAT DELETION LEAVES

Deleted files and where they hide

- **The Recycle Bin is a folder, not a void:** deleted files move there with metadata recording original path, size and deletion time; even after emptying, those metadata records and the files' content are often recoverable from the disk regions involved.
- **Unallocated space is the great archive:** deleting a file releases its disk space for reuse but does not erase it; content persists until overwritten, which on large modern drives can be months or years. Examiners recover intact files where file-system records survive, and carve content (documents, images, fragments) from raw space where they do not. One honest caveat of the modern era: on SSDs, background housekeeping (TRIM) erases released space far faster, so recovery windows are shorter and sometimes closed: an examiner will say which world a given machine lives in.
- **Volume Shadow Copies are time machines:** Windows periodically snapshots volumes for restore and backup features; a shadow copy holds earlier versions of files, and files deleted since, exactly as they stood at the snapshot moment: routinely the recovery route for material long gone from the live file system, and the subject of a dedicated guide later in this series.
- **Copies outlive originals:** temporary files, autosaves, print spools, email attachments cached on opening, and application caches scatter duplicates that survive the original's deletion; the "destroyed" spreadsheet frequently persists as last Tuesday's autosave.
- **Even absence testifies:** file-system records ($MFT entries, USN journal), Recycle Bin metadata and recency artefacts prove that named files existed, when they were created, modified and deleted, and sometimes in what volume: so mass deletion on the eve of proceedings is provable as an event with a timestamp, whatever became of the content, and that finding often does more work than the files would have.

§ 0 4 · THE PLUG-IN RECORD

USB devices and external media history

- **What Windows records, automatically:** for every USB storage device ever connected: manufacturer, model and serial number (registry device keys); first connection (setupapi.dev.log, with date and time); recent connection windows (registry, event logs); the drive letter assigned; and the volume name and serial of the file system on the stick.
- **What connects device to documents:** shortcut (LNK) files and jump lists record files opened, including the volume serial of the drive they lived on: matching a document's LNK volume serial to a specific stick's registry record is how "he opened the client list from that exact device" is proven.
- **What it does and does not prove:** the record proves connection (which device, which machine, when) and access (which files were opened from it); it does not, by itself, log every file copied to the device: copying leaves quieter traces (folder access artefacts, timestamps, occasionally journal entries), so the honest formulation is often "the device was connected at 16:42; the following files were accessed from or in proximity to it; the pattern is consistent with copying": corroborated, in strong cases, by finding the files on the stick itself if it is recovered.
- **Cross-machine matching:** serial numbers make devices trackable across computers: the stick that touched the office desktop on Friday and the home laptop on Sunday is one stick, provably, and delivery-up of the physical device then closes the loop.
- **The defence reading:** the same records exonerate: no connection during the disputed window, a device that belongs to IT's imaging routine, or LNK evidence showing only payslips opened, per this series' recurring examples: the artefact is neutral; the pattern decides.

§ 0 5 · WHO WAS SIGNED IN

Logins, accounts and who was at the keyboard

- **The Security event log** records logons and logoffs per account with timestamps and types: interactive at the keyboard, remote desktop, network, unlock: each type telling a different story about where the human was; failed attempts are logged too, with the account tried and the source.
- **Session context frames every other artefact:** artefacts belong to accounts (each user's registry hive, LNK files, browser profile are separate), so establishing which account was in an interactive session during the disputed window is the frame into which file, execution and browsing evidence then slots.
- **Account attribution versus human attribution:** the machine proves the account; the human layer is built from authentication type (a password typed at the keyboard, a badge-in record, a VPN log), exclusivity of credential knowledge, behavioural consistency (the session reads webmail belonging to one person), and elimination (who else was in the building, on the VPN, awake). The multi-user family computer example from this series' companion guide is the standing caution: shared machines need this layer done properly, and the honest expert says so.
- **Remote access changes the question:** RDP sessions, remote-support tools and VPN connections appear in their own artefacts; "someone else accessed my machine" is a testable hypothesis, not a rhetorical refuge, and the logs usually settle it one way or the other.
- **Timing precision:** logon/logoff pairs bracket sessions to the second, which is what lets a timeline say not just what happened but that it happened inside one identifiable sitting.

§ 0 6 · WHAT WAS OPENED

Files opened, folders browsed: the recency artefacts

- **Shortcut (LNK) files:** Windows creates one for nearly every document opened, recording the target's full path, its size, its timestamps at the moment of opening, and the volume (with serial) it lived on: LNK files survive the target's deletion, so they are the standing proof that named files existed and were opened, where, and when.
- **Jump lists:** per-application recent-document lists (Word's, Explorer's, the PDF reader's), storing sequences of opened items with timestamps: effectively a per-program diary of what the user worked on, ordered.
- **Registry recency keys:** recent docs, typed paths (locations the user typed into Explorer's address bar), open/save dialog history: small artefacts that answer pointed questions, such as whether a user navigated deliberately to a specific network share.
- **Folder access traces (shellbags):** the registry remembers folders browsed (including on removable drives and network shares, including folders since deleted) with window-position housekeeping that incidentally proves the folder was viewed: the artefact that shows someone browsing the HR share's salary folder, or the stick's "Client Backup" directory, even after both are gone.
- **Read together:** recency artefacts answer the litigation staple "did he ever open it?": the contract he denies seeing, the design file before its twin appeared at a competitor, the folder of confidential material browsed on the last afternoon: with the honest limit that they prove opening and browsing, not reading comprehension or purpose.

§ 0 7 · WHAT WAS RUN

Programs run: the execution artefacts

- **The family:** Prefetch (per-program launch files with run counts and recent run times), Shimcache and Amcache (compatibility and inventory databases recording executables present and executed), UserAssist (per-account registry counts of programs launched via the interface), and SRUM (the system resource monitor, logging per-application usage including network bytes, hourly, for weeks): independent records, different mechanisms, one question: what ran, when, how often, under which account.
- **Why lawyers should care:** execution artefacts are how you prove the use of the tools that matter: the cleaning utility run at 23:40 the night before imaging; the cloud-sync client that uploaded the take; the archiving tool that built the export; the unauthorised remote-access program; the accounting package opened during the falsification window.
- **Deleted programs leave records:** uninstalling or deleting an executable does not purge Prefetch, Shimcache, Amcache or UserAssist entries; the eradicated wiping tool is usually still named, with run times, in three separate places.
- **SRUM's quiet power:** per-application network usage means "this machine uploaded 4.2 GB via the browser between 21:00 and 22:00 on the 14th" is often provable from the device alone: the volumetric corroboration exfiltration cases want.
- **Limits stated plainly:** execution proves launch, not everything done inside the program; counts and timestamps have per-artefact quirks (some record last run only, some are updated on events other than execution); the examiner reports from the artefact's actual semantics, which is exactly the cross-examination ground where a careful report beats a confident one.

§ 0 8 · THE ONLINE RECORD

Browsing, searching and the online record

- **Browser databases** (Chrome, Edge, Firefox) hold history with visit times and counts, searches typed, downloads with source URLs and saved paths, autofill, cookies and session data, per profile, and often synchronised across a user's devices: the intent evidence of the modern case: what was searched for, in what sequence, before what act.
- **Cached content:** pages and images stored locally for speed survive as evidence of what was actually displayed, sometimes long after the site changed or the history was cleared; webmail fragments and web-app content (personal email, cloud drives, chat services used in-browser) frequently persist in cache and appear nowhere else on the machine.
- **Cleared history is not cleared evidence:** deletion of browser history is itself detectable (gaps, database internals), and the underlying records are often recoverable from database free space, shadow copies or the sync service's other devices; meanwhile DNS caches, session files and the cache tell overlapping stories.
- **Downloads bridge worlds:** the download record ties an internet source to a disk file (URL, timestamp, saved path), connecting the online act to the file-system evidence around it: for both incriminating material and its innocent explanation (the automatic download, the drive-by, the shared machine).
- **The usual honesty:** browsing proves the account's session displayed or fetched content, with attribution built per §5; and search history is read in context: people search for what alarms them as well as what they intend.

§ 0 9 · THE SYSTEM'S DIARY

Event logs and the system's own diary

- **What they are:** structured logs the system and applications write continuously: security (logons, privilege use, audit events), system (boots, shutdowns, time changes, device and service events), application (program-level events), plus dozens of specialised operational logs (remote desktop, PowerShell, task scheduler, USB-related channels).
- **The questions they answer:** when the machine was on and off (bracketing all other claims); when the clock was changed (the backdating tell, logged with old and new time); when services and scheduled tasks ran; when remote sessions connected and from where; when logs themselves were cleared: an event that writes its own conspicuous entry.
- **Rotation and reach:** logs have size limits and overwrite oldest-first, so their reach back in time varies from weeks to years by channel and activity; shadow copies and backups extend reach by preserving earlier log states: a preservation point worth acting on early.
- **Corroboration hub:** in timeline work, event logs are the spine other artefacts hang on: the file opened (LNK) inside the session (Security log) after the boot (System log) with the stick connected (device events): four sources, one minute, one story.

§ 10 · ASSEMBLY

Building the timeline: from artefacts to narrative

- **The method:** every artefact's timestamps are extracted and normalised into one chronology (UTC with declared local conversion, per this series' standing clock discipline), across file system, registry, logs, browser and execution sources: often hundreds of thousands of events, filtered to the windows that matter.
- **Corroboration is the craft:** a single artefact can be misread; a cluster cannot easily be: the 16:38-16:51 window that contains the logon, the stick's connection, the folder browse, the LNK creations, the archive tool's execution and the logoff is a narrative because six independent recorders agree, and the expert report presents exactly that convergence.
- **Timestamp semantics matter:** created, modified, accessed and record-change times mean specific things and are moved by specific operations (copies, extractions from archives, restores change some and not others); tampering (backdating) tends to leave internal inconsistencies (file-system internals, log sequence, the clock-change event) that timeline work exposes: the forgery cases of this series turn on precisely this.
- **The deliverable for lawyers:** not the artefact dump but the annotated chronology: each entry sourced to its artefact, each inference graded (proves / consistent with / cannot exclude), exhibit-referenced, and readable by a judge: the format in which Windows evidence actually wins cases.

§ 11 · IN THE WILD

Worked examples

EXAMPLE 1 · THE LEAVER, THE STICK AND THE FIFTEEN MINUTES

A sales director resigned and denied taking anything. His laptop's image told the last afternoon's story in six artefacts: 16:38 interactive logon (Security log); 16:41 a USB stick's first-ever connection to that machine (registry and setupapi, with make, model and serial); 16:42-16:49 shellbags recording browsing of the CRM export folder and a folder on the new volume named "GK backup"; LNK files created for the pipeline spreadsheet and client list, their volume serial matching the stick; 16:47 execution of an archiving utility (Prefetch, UserAssist); 16:51 logoff. Delivery-up of the stick, ordered on that evidence, found the archive, hash-matching the company originals. The claim settled at the door with undertakings and costs; the fifteen minutes had been recorded by five independent features, none of which he had known were watching.

EXAMPLE 2 · THE DELETION THAT PROVED MORE THAN THE DOCUMENTS WOULD HAVE

A respondent under a preservation notice delivered his laptop for imaging three weeks late. The examination could not recover much content: TRIM on the SSD had done its work. But the metadata layer was intact: file-system records showed some fourteen hundred files deleted in one twenty-minute window, two days after the notice's receipt (its read receipt was in the mailbox); Prefetch and UserAssist showed a cleaning utility downloaded (browser record, with the search "permanently delete files" an hour earlier) and run twice in the same window; and the event log recorded the Recycle Bin policy being changed to bypass it. The court drew the adverse inference the pattern invited and struck out the defence on the spoliation application: the destroyed documents were never seen, and were never needed.

EXAMPLE 3 · THE SHARED OFFICE COMPUTER AND THE ACCOUNT THAT WAS NOT HIM

A warehouse supervisor was dismissed for offensive material found on a shared office PC, the employer's case resting on "it was on his computer". The image reframed the possessive: four accounts, but the material sat under a generic shared login used by the whole shift. The timeline layered attribution properly: the files' download times (browser record under the shared account) fell in three windows; badge records put the claimant off-site for two of them; and in the third, the same session's webmail cache showed another named employee's personal inbox open concurrently. The tribunal found the dismissal unfair for want of reasonable investigation: the machine had never said what the employer heard it say, and the account/human distinction of §5 decided the case.

§ 12 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **IT looks first:** a well-meaning administrator browsing the live machine, updating access times, populating recency artefacts and triggering TRIM: the classic pre-instruction damage this series' preservation guides exist to prevent.
- **"It was on his computer" as attribution:** Example 3's error: account, session and human conflated in one possessive pronoun.
- **Overclaiming the USB record:** asserting "copied" where the artefacts prove "connected and accessed"; the careful formulation survives cross, the confident one creates it.
- **Reading timestamps naively:** treating a copy's creation date as the document's origin, or an access time as human reading, without the operation-semantics layer.
- **Waiting out the artefacts:** months of delay while logs rotate, shadow copies age out and SSD housekeeping runs; Windows evidence is perishable at the edges, and instruction speed is recovery rate.
- **The single-artefact case:** building on one record where the discipline is convergence; the timeline, not the trace, is the evidence.
- **Ignoring the exculpatory sweep:** examining only for the client's theory; the same disk usually contains the other side's best points, and the CPR 35 duty (and good strategy) is to know them first.

Technical limitations

- **SSDs shorten the deleted-content window:** TRIM erases released space in the background; metadata and artefact layers survive, content recovery is machine-and-timing dependent, and the examiner reports which.
- **Artefact reach varies:** logs rotate, recency lists cap, Prefetch holds finite entries, SRUM spans weeks; every artefact has a horizon, and absence beyond it proves nothing.
- **Encryption gates everything:** BitLocker-protected disks need credentials or recovery keys (the escrow disciplines of guide 33) before any of this exists to examine.
- **Windows versions differ:** artefact locations, formats and even existence shift across versions and configurations (some enterprise builds disable features); findings are version-specific and the report says so.
- **Cloud redirection thins the local record:** files living in synced cloud folders may leave placeholder-level traces locally, with the substantive record in the tenancy: the pointer to this series' cloud guides, and to collecting both sides of the sync.

§ 1 3 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Where is the machine now, who has touched it since the events, and has IT "had a look"? (The contamination question, first, always.)
- Is it a shared or single-user machine, and what accounts exist? (The attribution terrain.)
- Is the disk encrypted, and do we hold the recovery keys? (The gate before everything.)

Ask your opponent

- Please confirm the device has been preserved unused since [date], and provide the forensic image (or the device for imaging) with chain of custody.
- Please identify all user accounts and all persons with access to the machine in the relevant period.
- If any deletion, cleaning or reinstallation has occurred since the duty to preserve arose, please give particulars: when, by whom, using what, and on whose instruction.

Ask your eDiscovery / forensic provider

- Which artefact families will you examine for our questions, and what are their horizons on this machine's configuration?
- Will the timeline deliverable grade inferences (proves / consistent with / cannot exclude) per entry?
- What is recoverable given the drive type and elapsed time, honestly, before we budget the examination?

SUGGESTED WORDING · INSTRUCTION FOR A WINDOWS EXAMINATION

> "Please examine the forensic image of [device] and report on: (1) all indications of removable storage devices connected between [dates], with identifiers and connection times; (2) files and folders accessed in that period, including from removable or network volumes, and any evidence of copying, archiving or transfer of [categories]; (3) user sessions in the period, with account, logon type and duration, and the evidential basis for attributing each session to an individual; (4) programs executed, including any cleaning, wiping, archiving, remote-access or synchronisation utilities; (5) internet activity relevant to [issues], including searches and downloads; (6) deleted material relevant to the above, recovered or evidenced by metadata, with dates and methods of deletion; and (7) a consolidated timeline of the foregoing in UTC and local time, with each entry sourced and each inference graded. Please state the limitations applicable to each finding, including artefact horizons and drive-type effects, and preserve and exhibit all underlying artefacts."

§ 14 · QUICK CONTROL

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

The Windows evidence checklist

- ☐ Device preserved unused from the moment the question arose; no IT browsing, no reissue, no rebuild
- ☐ Forensic image taken with hashing and custody per this series; encryption keys secured
- ☐ Accounts and access mapped before attribution claims are made
- ☐ USB and external-media history examined where transfer is in issue; devices themselves pursued for delivery-up
- ☐ Recency artefacts (LNK, jump lists, shellbags) swept for the files and folders in issue
- ☐ Execution artefacts checked for cleaning, archiving, sync and remote-access tools
- ☐ Browser record examined for intent, downloads and webmail/cloud traces
- ☐ Event logs preserved early (they rotate); clock-change and log-clear events checked
- ☐ Deleted-material recovery attempted across Recycle Bin, unallocated space and shadow copies, with drive-type honesty
- ☐ Findings assembled as a graded, sourced timeline; exculpatory findings identified and faced

Red flags

- The machine "tidied up", rebuilt or reissued after the dispute arose.
- A cleaning utility in the execution record near a preservation date.
- Clock-change or log-cleared events inside the disputed window.
- Attribution resting on machine possession alone in a shared environment.
- An opponent's expert report quoting artefacts without stating their limits.
- Months of unexplained delay between preservation duty and imaging.

When to involve a digital forensic expert

Immediately when a Windows machine's history may matter: the artefact layers are perishable (logs rotate, shadow copies age, TRIM runs), and the examiner's first contribution is stopping the loss. Thereafter for the examination itself, which is interpretation as much as extraction: artefact semantics, attribution layering and timeline assembly are where cases are won and where amateur readings are dismantled: and for the CPR Part 35 / CrimPR Part 19 report that presents convergence a court can act on. Defensively, instruct an examiner whenever an opponent's case rests on device findings: the gap between what Windows artefacts prove and what enthusiastic reports claim they prove is, in our experience, the most reliably productive ground in digital-evidence litigation.

§ 15 · COMMON QUESTIONS

Frequently asked questions

Can deleted files really be recovered, and for how long?

Often, and it depends: on drive type (hard drives hold released content until overwritten, months or years; SSDs erase it in background housekeeping, days or less), on activity since, and on the parallel routes: Recycle Bin remnants, shadow copies, temporary and cached duplicates, backups. Two honest constants: the metadata layer (that files existed, and when they were deleted) survives far longer than content; and every week of delay closes doors. Instruct early and let the examiner report which doors this particular machine still has open.

Can the computer prove who was using it, rather than which account?

Not alone, and no honest expert claims it can: the machine proves account sessions. The human layer is built around them: authentication type and credential exclusivity, corroborating records (badges, VPN, CCTV, phones), and in-session behaviour (whose webmail, whose files, whose patterns): usually to a comfortable civil standard, sometimes beyond. What decides cases is doing that layer explicitly: Example 3 is what happens when a party skips it, and §5 is the discipline that survives cross-examination.

If someone used a wiping tool, is the evidence gone?

The targeted content may be; the event rarely is. Wiping tools appear in execution artefacts (Prefetch, UserAssist, Amcache) with run times, their acquisition often sits in the browser record, mass deletions leave file-system and journal traces, and configuration changes are logged. Post-duty destruction then does its own damage: adverse inferences, strike-out exposure, and Example 2's outcome: courts treat proven spoliation, provably timed, as loudly as the missing documents would have spoken.

The laptop has been used for months since the events. Is examination pointless?

No: it re-weights toward the durable layers. Registry device history, LNK and shellbag records, execution artefacts, and event-log reach often survive routine use for long periods; deleted-content recovery and short-horizon artefacts suffer most. The examination scopes to what the elapsed time left, and the report states horizons honestly: months of use narrows the window, it does not board it up.

Does any of this work on a Mac, or on cloud-stored files?

The philosophy transfers, the artefacts differ: macOS keeps its own equivalents (covered in the next guide in this series), and files living in cloud tenancies leave their substantive record server-side, where platform audit logs and versions do the work (the cloud guides that follow). The Windows machine remains evidentially rich even in cloud-centric estates: sync clients, local caches and the artefact families above record the local half of every story: but complete answers usually mean collecting both halves.

What does a Windows examination cost and how long does it take?

Scoped work on defined questions (a leaver's last month, a USB window, an attribution dispute) is typically days of examiner time on a fixed estimate, after imaging; full-timeline work on multi-year questions scales with the ambition. The economical route is the instruction wording in §13: precise questions, graded findings, stated limits: which buys conclusions rather than tooling output, and usually answers in one report what open-ended "look at everything" instructions answer in three.

§ 16 · REFERENCE

Glossary

Amcache / Shimcache
System databases recording executables present and run; survive the program's deletion.

Event logs
The system's structured diaries: security, system, application and specialised channels.

Jump list
Per-application recent-items record with timestamps.

LNK (shortcut) file
Auto-created record of an opened file: path, timestamps, size and source volume serial.

Prefetch
Per-program launch records with run counts and times.

Recycle Bin metadata
Records of deleted files: original path, size, deletion moment: often outliving the content.

Shellbags
Registry traces of folders browsed, including deleted, removable and network folders.

SRUM
Resource-usage database: per-application activity and network volumes, hourly, for weeks.

TRIM
SSD housekeeping that erases released space, shortening deleted-content recovery windows.

Unallocated space
Disk regions released by deletion, holding recoverable content until reused.

UserAssist
Per-account registry counts and times of programs launched via the interface.

Volume Shadow Copy
Point-in-time volume snapshot preserving earlier file versions and since-deleted files.

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 (Windows examination, deleted data recovery, USB and execution artefact analysis, timeline reporting under CPR Part 35 / CrimPR Part 19): cflab.uk/digital-forensics-services · the digital-evidence guide for defence lawyers and guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection and Phase 04 · Processing (device-level findings integrated into disclosure review): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- 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 (expert evidence): justice.gov.uk, Part 35 · justice.gov.uk, CrimPR Part 19

DISCLAIMER

This publication provides general information about Windows forensic artefacts as at August 2026. Artefact behaviour varies with Windows versions, configurations and hardware, 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

Windows examination is the laboratory's core discipline: forensic imaging under full custody, then artefact work across every family in this guide: deleted-data recovery calibrated to the drive's realities, USB and transfer analysis, session attribution built in layers, execution and browsing evidence, and the graded, sourced timeline that turns a disk into a narrative. We report under CPR Part 35 and CrimPR Part 19, state limits as plainly as findings, and are as often instructed to dismantle overclaimed device evidence as to build it. Urgent preservation (before logs rotate and SSDs housekeep) can usually be arranged within days. Through **e-discovery.uk**, device findings integrate into disclosure-scale review, so the machine's story and the document story are told as one. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.

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