COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Browser History and Internet Artefacts

What the Browser Records, What It Means, and What It Does Not Prove

A web browser is one of the most revealing artefacts on any device, and one of the most frequently misread. It records the pages a user visited and when, the terms they searched, the sites they logged into, the files they downloaded and a mass of supporting data: cookies, cached pages, autofill entries, saved passwords and session records. In the right hands this reconstructs intention, research, preparation and knowledge with striking clarity. But browser evidence is also a minefield of misinterpretation. A URL in the history does not always mean a person deliberately went there; pages load resources from dozens of other sites automatically; a timestamp is in a time zone that must be established; and private-browsing modes, multiple profiles and shared devices all complicate the simple story of one person, one visit. This guide sets out for UK lawyers what browsers actually record and where, how those artefacts are collected and interpreted, and, above all, how to tell what browser evidence genuinely proves from what it only appears to.

⏱ 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. Browser and internet-artefact analysis is core laboratory work: reconstructing web history, searches and downloads across Chrome, Edge, Firefox and Safari, recovering deleted browsing records, and, critically, distinguishing deliberate user action from automatic background activity: reported under CPR Part 35 and CrimPR Part 19, with the meaning and the limits of each artefact set out so a court is neither misled by, nor deprived of, the evidence.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | MULTI-BROWSER ARTEFACT ANALYSIS | DELETED-HISTORY RECOVERY | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: a browser records visits, searches, downloads and much more with great clarity, but a URL in the history is not proof that a person deliberately went there, so the central skill is separating deliberate user action from automatic background activity and stating each artefact at its honest weight.

What it records (§3): visited URLs and times, searches, downloads, cookies, cached pages, autofill, saved passwords and sessions, across Chrome, Edge, Firefox and Safari, held in databases on the device and synced to the account. **Action versus automation (§4):** pages load dozens of resources automatically, adverts and redirects create history the user never chose, and prefetch and background sync add entries, so the presence of a URL is not, by itself, a deliberate visit. **Collecting and recovering (§5):** the artefacts are collected from the browser databases and often recovered when deleted, from unallocated space, caches and cloud sync (guides 4, 111). **Interpretation (§6):** the meaning of an artefact depends on how it arose, and attribution to a person depends on profile, timing and corroboration, not on the URL alone. **Deployment (§7):** proving knowledge, intent, research or preparatory acts, and rebutting the over-read history that automatic activity so often produces.

- **The browser is a detailed diary:** visits, searches, downloads, logins, cookies and cached pages, timestamped.
- **A URL is not an intention:** pages auto-load resources; adverts, redirects and prefetch create unchosen history.
- **Deleted history often survives:** in unallocated space, caches, related databases and cloud sync.
- **Attribution needs more than a URL:** profile, timing, session and corroboration place the person, not the address alone.
- **Interpretation is the skill:** the honest weight of each artefact depends on how it actually arose.

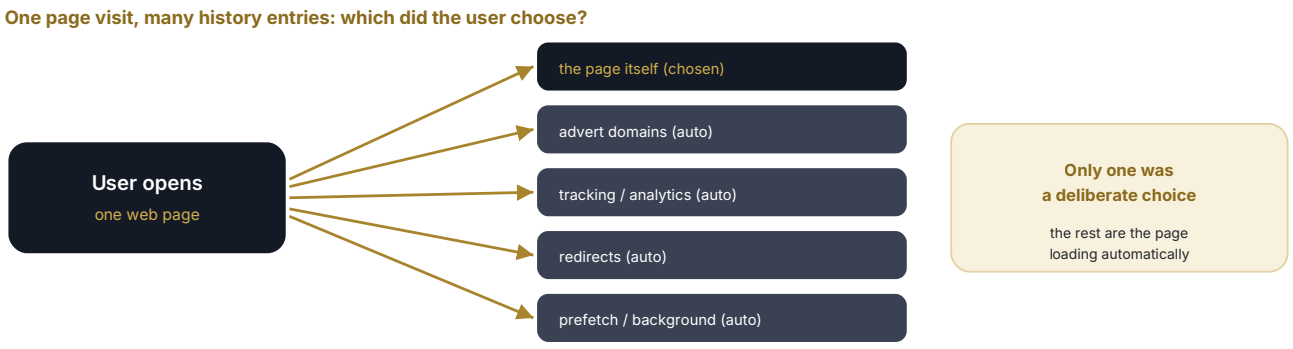

Figure 1 - a single deliberate visit generates many history and cache entries automatically; the interpretive task is to tell the one chosen URL from the many the page loaded on its own.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: a URL is not an intention

Browser evidence looks deceptively simple. Here is a list of web addresses, each with a date and time; surely it shows what the person looked at, and when. That intuition is right often enough to be dangerous, because it is also wrong often enough to convict or exonerate on a false basis. The trouble is that a modern web page is not one thing but dozens: open a single news article and the browser silently fetches adverts from ad networks, tracking scripts from analytics companies, images from content-delivery networks, and follows redirects through intermediary domains, all of which can leave entries in the browser's records. The user chose to open one page; the machine visited many. A history or cache full of domains the user never heard of is the normal result of ordinary browsing, not evidence of deliberate interest in each.

On top of this sit further complications. Timestamps are stored in a particular time base and must be converted correctly before a visit is placed in the day. Private-browsing modes leave a different, sparser trace. Multiple browser profiles, and multiple users on a shared device, mean the history may not belong to the person assumed. Prefetching and background synchronisation add entries for pages that were never displayed. And deleted history is frequently recoverable, but a recovered fragment carries even less inherent context about how it arose. The consequence is that browser evidence is genuinely powerful, it can show searches, downloads, logins and knowledge with real force, but only when an examiner separates what the user deliberately did from what the browser did automatically, and states each at its true weight. This guide is about making that distinction reliably.

§ 0 3 · WHAT THE BROWSER RECORDS

What the browser records, and where

- **History and visits:** visited URLs with timestamps and visit counts, and the transition type recorded by the browser, whether the user typed the address, clicked a link, was redirected or the page was prefetched, which is central to distinguishing action from automation (§4): held in the browser's history database.
- **Searches:** search terms entered, often preserved in the history and in dedicated keyword tables: among the most probative artefacts, showing what a user actively sought (guide 96's timeline discipline).
- **Downloads:** downloaded files with source URLs, destinations and times: evidence of what was obtained and from where, and a deliberate act more reliably than a mere page load.
- **Cookies, cache and sessions:** cookies showing sites interacted with, cached pages preserving what content actually looked like, and session data showing what was open: rich context, but much of it created automatically (§4).
- **Autofill, passwords and accounts:** saved form data, credentials and signed-in accounts, evidencing account ownership and use (guide 105), and the sync account through which history reaches the cloud (§5, §8).

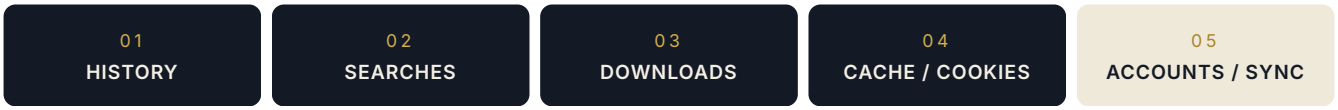

Figure 2 - the browser's principal artefact families, from the deliberate (searches, downloads) to the largely automatic (cache, cookies), each read at its own weight.

§ 0 4 · ACTION VERSUS AUTOMATION

Deliberate action versus automatic activity

- **Transition types:** browsers record how a URL was reached, typed, clicked, redirected, reloaded, prefetched, and this transition data is the primary means of telling a deliberate visit from an automatic one: the single most important interpretive artefact (§3).
- **Page resources are not visits:** the adverts, trackers, images and scripts a page loads can appear in caches and related records, and must not be read as deliberate visits to those domains (Figure 1): the commonest over-read.
- **Redirects and pop-ups:** a single click can chain through several domains and open pop-ups, generating history for pages the user never intended or saw: the chain reconstructed, not each link counted as a choice.
- **Prefetch and background sync:** browsers pre-load pages they predict the user might open and sync in the background, creating entries for content never displayed: automatic activity distinguished from viewing.
- **Dwell, sequence and corroboration:** how long a page was open, the sequence of deliberate navigation, and corroboration from searches and downloads together indicate genuine user engagement, far better than a bare URL: the honest reading built from context, not address (§6).

§ 0 5 · COLLECTING AND RECOVERING

Collecting and recovering browser artefacts

- **Collect the browser databases:** the history, download, cookie, cache and autofill databases collected from the device with integrity preserved and hashed, across every browser and profile present, not just the default one (guides 2, 3).
- **Recover deleted history:** deleted browsing records frequently recoverable from unallocated space, database free pages, cache remnants and related artefacts, because deletion is often incomplete (guide 4): the erased history reconstructed where it survives.
- **Reach the synced account:** browser history synced to the account (a browser account, or the platform account) recoverable from the cloud even where the device record was cleared, an independent copy reached through the account (guides 111 to 114, §8).
- **Preserve related system artefacts:** DNS cache, system logs and other operating-system records that corroborate or contextualise browser activity collected alongside (guide 105): the browser read against the system, not in isolation.
- **Handle private browsing realistically:** private-mode sessions leave sparser but not always zero traces, in memory, DNS and related artefacts, so their limits are stated honestly and the estate is used to fill the gap (§6, §8).

§ 0 6 · INTERPRETATION AND HONEST LIMITS

Interpretation, attribution and honest limits

- **Meaning depends on origin:** the weight of an artefact depends on how it arose, a typed search is strong, an auto-loaded advert domain is nearly meaningless, so each is interpreted by its transition and context, not counted equally (§4): the core discipline.
- **Attribution to a person:** browser records place activity in a profile on a device, not certainly in a person: the profile, the login state, the timing against known presence and corroborating evidence establish who was at the keyboard (guide 105).
- **Shared devices and profiles:** on a device used by several people, or with several profiles, the history may not belong to the assumed user: attribution tested, not presumed (guide 105's family-computer discipline).
- **Time zones and clocks:** browser timestamps converted correctly and reconciled with the system clock and other sources before a visit is placed in the day (guide 108).
- **State weight honestly:** the finding expressed at the level the artefact supports, "this search term was typed at this time in this profile", not "the defendant visited this site", where the evidence shows only an automatic load: the honesty that survives cross-examination (guide 100).

§ 0 7 · DEPLOYMENT

Deployment: knowledge, intent, research and concealment

- **Knowledge and intent:** searches and deliberate visits evidencing what a person knew, sought or planned, from research preceding an act to knowledge of a fact in dispute, deployed on the strength of the transition data and corroboration (§4).
- **Preparatory acts:** a sequence of deliberate searches and downloads showing preparation, in fraud, harassment and other matters, presented as a corroborated pattern rather than isolated URLs (guide 98).
- **Rebutting the over-read history:** the defence use, showing that URLs relied on by an opponent were automatic loads, redirects, pop-ups or another profile's activity, not deliberate acts by the client (Figure 1, §4): the misinterpretation exposed.
- **Concealment and deletion:** deliberate clearing of history, use of private mode or anti-forensic tools around a relevant time, established and dated against the duty to preserve (guides 110, 109): the attempt to hide as evidence in itself, honestly distinguished from routine housekeeping.
- **Corroboration across the estate:** browser activity aligned with downloads, files, messages and the synced account (§8), so a deliberate research or preparation narrative rests on convergent evidence, not the history alone.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the browser is one node, and the same web activity is reflected across the device, the account and the network. The device holds the browser databases, caches and the deleted remnants of them. But the synced browser or platform account holds an independent cloud copy of history and searches, often surviving a local deletion; the operating system holds DNS cache, logs and prefetch that corroborate or contextualise; other devices signed into the same account carry the synced history too; the network or provider may hold DNS and access logs; and the destinations themselves, the sites, the search provider, the download sources, hold server-side records reachable by lawful process. The discipline is to read the browser against these, because the account copy defeats a cleared local history, the DNS cache and logs corroborate a genuine visit, and the transition and system context distinguish the deliberate from the automatic. When local history is wiped, the sync account holds it; when private mode leaves little, DNS and memory artefacts may still show activity; and when a single browser is silent, another device on the same account speaks.

EVIDENCE	DEVICE BROWSER	SYNCED ACCOUNT (CLOUD)	OTHER SIGNED-IN DEVICES	OS / SYSTEM ARTEFACTS	NETWORK / DESTINATION	DELETED / RECOVERABLE
Visited URLs	Y: history db	Y: synced history	Y: same account	DNS cache, prefetch	Server / DNS logs	Often (unallocated, cache)
Searches	Y: keyword tables	Y: account activity	Y	n/a	Search-provider records	Often
Downloads	Y: download db + file	Sometimes	Sometimes	File-system artefacts	Source-site logs	Varies
Logins / accounts	Y: cookies, autofill	Y: account	Y	Credential stores	Site login logs	Limited
Private-mode activity	Sparse	Usually not synced	n/a	DNS, memory remnants	Server / DNS logs	Limited

Fallback strategy in one line: read the browser against the account, the system and the network; a cleared local history is often held in the sync account, and DNS, logs and other devices corroborate what a single browser cannot.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE ADVERT DOMAINS MISTAKEN FOR DELIBERATE VISITS

A prosecution alleged that a defendant had deliberately visited a series of illicit websites, relying on a list of domains found in the browser cache and history. The §4 transition analysis dismantled the claim: the great majority of the domains had no user-typed or clicked transition, they were adverts, trackers and redirect intermediaries loaded automatically by a small number of pop-up-laden pages the user had actually opened, exactly the Figure 1 pattern. The §6 honest reading showed that the deliberate visits were few and to different sites, and that the incriminating domains were the automatic exhaust of ordinary, if unwise, browsing, not chosen destinations. The transition data, dwell times and the redirect chains, reconstructed and explained, transformed a damning-looking list into a handful of automatic loads. The lesson is §4's: a URL in the cache or history is not a deliberate visit, the transition and the chain reveal what the user actually chose, and an unexamined list of domains routinely misrepresents ordinary browsing as intent.

EXAMPLE 2 · THE CLEARED HISTORY THE ACCOUNT REMEMBERED

An employee suspected of misappropriating confidential material had, on the afternoon he resigned, cleared his browser history, and the local device showed almost nothing for the relevant period, a §7 concealment step. But the §8 estate held the record: his browser was signed into an account that synced history to the cloud, and the synced copy, preserved and collected through the account, held the deliberate searches and the downloads he had cleared locally, including searches for the material and visits to the systems he had exfiltrated from. The §5 recovery also carved fragments of the deleted local history that matched. The clearing itself, dated to the afternoon of resignation and after the duty to preserve had arisen, became a §10 point in its own right. The lesson is §8's: clearing local history does not clear the synced account, and the cloud copy, with recovered local fragments, routinely defeats the deletion.

EXAMPLE 3 · THE SHARED COMPUTER AND THE WRONG PROFILE

In a matter turning on who had researched a particular subject, the prosecution attributed browser searches to the defendant on a household computer. The §6 attribution discipline told a different story: the computer had several browser profiles and several users, and the relevant searches sat in a profile that was not the defendant's and had been active, per the session and login artefacts, at times the defendant was demonstrably elsewhere (guide 105). The transition data confirmed the searches were deliberate, but by someone else. Attribution, tested rather than presumed, shifted the searches away from the defendant. The lesson is §6's: browser activity belongs to a profile on a device, not automatically to the assumed person, and on shared machines the profile, session and timing must be examined before any search or visit is laid at a particular door.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Reading every URL as a visit:** the fundamental error, counting auto-loaded adverts, trackers and redirects as deliberate visits (Example 1, §4).
- **Ignoring transition data:** the history read as a flat list, without the transition type that distinguishes typed and clicked from automatic (§4).
- **Presuming attribution:** activity laid at the assumed person without checking profile, session and timing on a shared device (Example 3, §6).
- **Trusting the timestamp blindly:** browser times read without conversion or clock reconciliation, misplacing visits in the day (§6).
- **Missing the sync account:** a cleared local history taken as the whole story, the cloud copy never sought (Example 2, §8).
- **Over-reading private mode:** a sparse private-browsing trace treated as proof of nothing, or its remnants over-interpreted (§5).
- **Counting rather than weighing:** a large number of domains presented as significant without regard to how each arose (§4).
- **Treating deletion as guilt automatically:** routine history clearing read as concealment without dating it against any duty (§7).

Technical limitations

- **History does not equal intent:** the presence of a URL, especially an auto-loaded one, is not proof of a deliberate act: the core limit (§4).
- **Attribution is separate:** the browser records a profile's activity, not a person's, without corroboration (§6).
- **Private mode limits the record:** private browsing leaves sparse traces, so absence there is not absence of activity (§5).
- **Recovered fragments lack context:** a carved URL may survive without its transition or timing, limiting how much can be said of it (§5).
- **Sync and retention vary:** whether history synced, and how long the cloud keeps it, varies by account and setting, and is established, not assumed (§8).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which browsers, profiles and accounts were in use, and was the device shared, so attribution and sync are addressed from the outset?
- What is the precise browsing question, which searches, sites or downloads, and over what window, so the analysis is scoped?
- Was history cleared, private mode used, or any clean-up tool run around the relevant time?

Ask your opponent

- Please preserve and disclose the browser artefacts (history, searches, downloads, cache, cookies, autofill) for [device/profile] for [period], including any synced browser or platform account history, and confirm the browsers and profiles present.
- For any browsing relied on, please provide the transition type and context of each URL, so deliberate visits can be distinguished from automatic loads, redirects and prefetch.
- Please confirm whether history was cleared, private mode used, or any clean-up software run, and when.

Ask your eDiscovery / forensic provider

- For each URL relied on, was it typed, clicked, redirected or auto-loaded, and what is its honest weight?
- Whose profile and session was active, and does the timing corroborate attribution to the person?
- Does the synced account or recovered deleted history add or contradict anything the live device shows?

SUGGESTED WORDING · INSTRUCTION FOR A BROWSER-ARTEFACT EXAMINATION

> "We instruct you to examine the browser and internet artefacts on the device(s) at Schedule 1 for the period stated. Please: (1) collect, preserving integrity, the history, search, download, cache, cookie and autofill artefacts across every browser and profile present, and recover deleted browsing records where possible; (2) obtain, through the relevant account, any synced browser or platform history, noting whether local history was cleared; (3) for each URL, search and download relied on, determine and state the transition type and context, distinguishing deliberate user action (typed, clicked, searched, downloaded) from automatic activity (adverts, trackers, redirects, prefetch, background sync); (4) establish attribution by profile, login state, session and timing, testing rather than presuming which user was responsible on any shared device, and reconcile timestamps to a common clock; and (5) state the honest weight of each artefact, expressing findings at the level the evidence supports and flagging any material relied on by another party that is in fact automatic rather than deliberate. Note any history clearing, private-mode use or clean-up tools and their timing."

§ 12 · QUICK CONTROL

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

The browser-artefact checklist

- ☐ All browsers and profiles on the device identified
- ☐ History, searches, downloads, cache, cookies and autofill collected and hashed
- ☐ Deleted browsing records recovered where possible
- ☐ Synced browser or platform account history obtained
- ☐ Transition type established for each URL relied on
- ☐ Deliberate action distinguished from automatic activity
- ☐ Attribution tested by profile, session and timing, not presumed
- ☐ Timestamps converted and reconciled to a common clock
- ☐ History clearing, private mode and clean-up tools noted and dated
- ☐ Each artefact stated at its honest weight

Red flags

- A list of domains presented as deliberate visits with no transition analysis: Example 1.
- Browser activity attributed to a person on a shared device without profile checks: Example 3.
- A cleared local history treated as the whole record: Example 2.
- Timestamps relied on with no time-zone or clock reconciliation.
- Automatic loads, redirects and prefetch counted as chosen visits.
- Routine history clearing asserted as concealment without dating.
- Private-mode gaps over-read in either direction.

When to involve a digital forensic expert

Whenever browsing is relied on for intent, knowledge or presence, because the interpretive traps are exactly where cases are won and lost: the expert separates the deliberate visit from the automatic load using transition data and the redirect chain, so a list of domains is not mistaken for a list of choices (Example 1, §4); at attribution, where profile, session and timing are tested rather than presumed on shared devices (Example 3, §6); at recovery, where cleared history is reconstructed from the sync account and carved fragments (Example 2, §5, §8); at timing, where timestamps are converted and reconciled; and at deployment, where each artefact is presented at its honest weight under CPR Part 35 or CrimPR Part 19, and an opponent's over-read history is rebutted. Through **cflab.uk** and **e-discovery.uk**, browser analysis turns raw history into honest evidence by asking not just what URL is present but how it got there and who was at the keyboard: because a browser is a powerful witness only when its record is read for what the user did, not merely what the machine visited.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Does a website in the browser history mean our client went there?

Not necessarily, and this is the crux (§4, Example 1). A page loads adverts, trackers, images and redirects from many other domains automatically, and prefetch and background sync add more, so the history and cache routinely contain URLs the user never chose. The browser records how each URL was reached, typed, clicked, redirected, prefetched, and that transition data, not the bare presence of the address, tells you what was a deliberate visit.

Our client cleared their history. Is it gone?

Usually not entirely: deleted browsing records are often recoverable from unallocated space, database free pages and cache remnants (§5), and, importantly, if the browser was signed into a syncing account, the history was copied to the cloud and survives the local clearing (§8, Example 2). Clearing the device does not clear the account. The clearing itself, if done after a duty to preserve arose, may also be a point in its own right (§7).

Can we tell who was actually using the browser?

Only with care: the browser records a profile's activity on a device, not certainly a person's (§6, Example 3). On a shared computer or one with several profiles, the history may belong to someone else, so attribution is tested through the profile, the login state, the session artefacts and the timing against known presence, and corroborated. A search or visit is laid at a particular person's door only when that evidence supports it, not on the assumption that the device is theirs.

What about private or incognito browsing?

It leaves a sparser trace, but not always nothing: private modes avoid saving normal history, yet remnants can survive in memory, DNS cache and related system artefacts (§5), and the destinations and network may still hold records (§8). So private browsing limits the local record without guaranteeing invisibility, and its gaps are stated honestly rather than read, in either direction, as proof.

Are searches stronger evidence than visits?

Generally yes: a typed search term is a deliberate, articulated act that shows what the user actively sought, and it is among the most probative browser artefacts (§3). A page visit may be deliberate or automatic; a download is a deliberate acquisition. The weight follows the deliberateness, so searches and downloads, read with their transition and context, carry more than a bare auto-loaded URL, and the analysis says so honestly.

The other side is relying on a long list of sites. How do we respond?

Have the list examined artefact by artefact (§4, Example 1). Very often a long, alarming list dissolves under transition analysis into a few deliberate visits and a mass of automatic loads, redirects and pop-up domains generated by ordinary browsing. The reconstruction of what the user actually chose, versus what the pages loaded on their own, and the profile and timing behind it, frequently reduces an over-read list to something far narrower and fairer.

§ 14 · REFERENCE

Glossary

Browser history
The record of visited URLs with times and visit counts.

Transition type
How a URL was reached: typed, clicked, redirected, prefetched.

Cache
Stored page resources, largely created automatically.

Cookie
A small site record showing interaction with that site.

Prefetch
Pages pre-loaded by the browser before the user opens them.

Redirect chain
A sequence of domains passed through from one click.

Profile
A separate browser identity; history belongs to a profile.

Sync account
The account that copies history to the cloud and other devices.

Private mode
Browsing that avoids saving normal history.

Autofill
Saved form data and credentials, evidencing account use.

Sources and authoritative references

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

- cflab.uk, digital forensics services (browser and internet-artefact analysis, deleted-history recovery, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 04 · Collection and Phase 06 · Analysis (browser collection and interpretation as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Forensic Science Regulator, Code of Practice v2 (interpretation and its limits): gov.uk, FSR Code · ISO/IEC 27037: iso.org, 27037
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response (artefact analysis): csrc.nist.gov, SP 800-86 · Attorney General's Guidelines on Disclosure 2024 (interpretation and fair presentation of digital material): gov.uk, AG Guidelines
- PD 57AD and CPR Part 31: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Browser work at the laboratory begins from the principle that a URL is not an intention. The history, searches, downloads, cache, cookies and autofill are collected across every browser and profile with integrity preserved, deleted records are recovered from unallocated space and caches, and the synced account is reached so a cleared local history does not end the enquiry (Example 2). The interpretive core is the separation of deliberate action from automatic activity: for every URL relied on, the transition type and the redirect chain are established, so adverts, trackers, redirects and prefetch are not mistaken for chosen visits, and an opponent's alarming list of domains is reduced to what the user actually did (Example 1). Attribution is tested, not presumed, through profile, session and timing on shared devices, and timestamps are reconciled to a common clock (Example 3). Each artefact is then presented at its honest weight, a typed search as strong, an auto-loaded domain as almost nothing, so the evidence survives cross-examination. Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding question throughout is not merely what URL is present, but how it got there and who was at the keyboard.

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