Browser History And Internet Artefacts

Browser history and internet artefacts record visits, searches, and downloads. This guide for UK lawyers details what browsers record, how to interpret these artefacts, and the limits of their evidential value, including distinguishing deliberate actions from automatic activity.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/browser-history-and-internet-artefacts

BROWSER & INTERNETARTEFACTS · A GUIDE FOR UK LAWYERS Browser History and Internet Artefacts What the Browser Records, What It Means, and What It Does Not Prove COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES MULTI-BROWSER ARTEFACT ANALYSIS DELETED-HISTORY RECOVERY CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: a URL is not an in ten t i on 03 What the browser records, and where 04 Deliberate action versus automatic activity 05 Collecting and recovering browser artefacts 06 Interpretation, attribution and honest limits 07 Deployment: knowledge, intent, research and concealment 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary The headline point: a browser records visits, searches, downloads and much more with great clarity, but a deliberate user action from automatic background activity and stating each artefact at its honest weight.

§ 02 · FIRST PRINCIPLES The problem in plain English: a URL is not an in ten t i on

§ 03 · WHATTHEBROWSERRECORDS What the browser records, and where HISTORY SEARCHES DOWNLOADS CACHE / COOKIES ACCOUNTS / SYNC

§ 04 · ACTIONVERSUSAUTOMATION Deliberate action versus automatic activity

§ 05 · COLLECTINGANDRECOVERING Collecting and recovering browser artefacts

§ 06 · INTERPRETATIONANDHONESTLIMITS Interpretation, attribution and honest limits

§ 07 · DEPLOYMENT Deployment: knowledge, intent, research and concealment

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE ACCOUNT SIGNED-IN DEVICE OS / SYSTEM NETWORK / DELETED / BROWSER ARTEFACTS DESTINATION RECOVERABLE SYNCED OTHER (CLOUD) DEVICES

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEADVERTDOMAINSMISTAKENFORDELIBERATEVISITS EXAMPLE2 · THECLEAREDHISTORYTHEACCOUNTREMEMBERED EXAMPLE3 ·

THESHAREDCOMPUTERANDTHEWRONGPROFILE

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTIONFORABROWSER - ARTE FAC TEXAMIN AT ION

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The browser-artefact checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Does a website in the browser history mean our client went there? Our client cleared their history. Is it gone? Can we tell who was actually using the browser? What about private or incognito browsing? Are searches stronger evidence than visits? The other side is relying on a long list of sites. How do we respond?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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 d own load 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. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

Source: https://e-discovery.uk/library/browser-history-and-internet-artefacts. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.