Website Web Server And Application Logs

Website and application logs record every request, enabling reconstruction of user activity. This guide details how these layered logs prove page state and attribution, outlining collection, preservation, and common pitfalls for UK litigators.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/website-web-server-and-application-logs

WEB & APPLICATIONLOGS · A GUIDE FOR UK LAWYERS Website, Web Server and Application Logs Request Trails, User Journeys and Proving What Happened on a Website COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM USER-JOURNEY RECONSTRUCTION CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: LAYEREDLOGSRECONSTRUCTWHATAUSERDID; PAGE - STATE PROOFANDATTRIBUTIONDECIDEWHATITMEANS

§ 02 · FIRST PRINCIPLES The problem in plain English: the site remembers every request

§ 03 · THEESTATE The log estate: servers, applications, CDNs and analytics

§ 04 · THEJOURNEY Reconstructing journeys: sessions, clicks and transactions

§ 05 · THESCREEN Proving page state: what the site showed and when

§ 06 · WHO Attribution: IP, account, device, human

§ 07 · BEFOREROTATION Retention, collection and the preservation race

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE BROWSER / SERVER WAF DATABASE IDENTIT Y RECOVERABLE USER'S DEVICE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THESURCHARGETHECHECKOUTNEVERSERVED EXAMPLE2 · THEREVIEWCAMPAIGNWITHONEFINGERPRINT EXAMPLE3 · THETAKEOVERDEFENCE, TESTEDANDUPHELD

§ 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 · WEB - LOGLIMBFORTHEPRESER VAT I ON LETTER

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

§ 13 · COMMON QUESTIONS Frequently asked questions How long do websites keep their logs? Can logs prove someone read the terms and conditions? We only have an IP address for the wrongdoer. Is that enough? The defendant says their account was hacked. Now what? Is a Wayback Machine capture admissible to show what a page said? Can we get the other side's server logs in disclosure?

§ 14 · REFERENCE Glossary CDN CGNAT WAF 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

How long do websites keep their logs?

By default, briefly: server rotations of days to weeks, platform and CDN retention per plan, analytics per configuration: and almost never with litigation in mind. Treat every web matter as a guide 77-style race: census the layers, ask each one's retention, and send the §11 letter inside the shortest answer.

Can logs prove someone read the terms and conditions?

They prove service: the terms URL requested and returned 200 in the session, the checkbox posted, the version live that day (from the §5 history): which is what online-contract law generally needs: reasonable notice and incorporation, not telepathy. What no log proves is reading: plead the served-and-accepted sequence, and let Example 1 remind you to verify the serving before relying on it.

We only have an IP address for the wrongdoer. Is that enough?

It is a start: an IP plus a precise UTC timestamp supports subscriber disclosure from the ISP (Norwich Pharmacal being the usual route), and the account, device and fingerprint layers usually thicken the ladder before and after: Example 2's fourteen accounts fell to exactly that stack. An IP alone, pleaded as a person, is the mistake; an IP used as the first rung is the method.

The defendant says their account was hacked. Now what?

Test it: the take over defence has a signature either way: login geography and device history, resets and recovery-detail changes, the platform's own anomaly flags, and the counterpart-device question (was the accused's machine active, and did it touch the site?). Example 3 shows the defence surviving honest exam in at i on; fabricated versions rarely do, because take over s leave their own trail and its absence is loud.

Is a Wayback Machine capture admissible to show what a page said?

Routinely received, sensibly weighed: it is a dated third-party snapshot, strong for static public pages at its capture moments, silent between them and for personalised content. Use it as one voice beside deployment history, CMS records and the counterpart browser: the §5 chorus: rather than as the soloist.

Can we get the other side's server logs in disclosure?

Yes, where relevant and proportionate: they are documents within control like any other, and PD 57AD's models reach them: the craft is asking per §11: named layers, defined sessions and periods, raw formats, retention stated: so the request is cheap to comply with and expensive to resist. Expect the proportionality conversation, and win it by narrowness. cflab. u k · e-disc ove r y. u k