Domain DNS And Hosting Records

This guide details how to investigate domain, DNS, and hosting records to uncover website ownership and infrastructure history. It covers unmasking registrants, reconstructing domain activity, and addressing email authentication issues, providing practical guidance for UK litigators.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/domain-dns-and-hosting-records

DOMAIN & HOSTING EVIDENCE · A GUIDE FOR UK LAWYERS Domain, DNS and Hosting Records Who Is Behind a Website, and How Its Infrastructure History Is Proved COMPUTER FORENSICS LAB

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

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: PUBLICINFRASTRUCTURERECORDSNARROWTHEFIELD; REGISTRARANDHOSTDISCLOSURENAMESTHEHAND: ANDTHEHISTORYISARCHIVED EVENWHENTHESITEISGONE

§ 02 · FIRST PRINCIPLES The problem in plain English: the address book of the internet

§ 03 · THELAYERS The record layers: registration, DNS, hosting and certificates

§ 04 · THESEQUENCE Unmasking: from redacted WHOIS to a named registrant

§ 05 · THEPAST Reconstructing history: what the domain did and when

§ 06 · THEMAILQUESTION Email authentication: SPF, DKIM, DMARC and spoofing disputes

§ 07 · GETTINGITSTOPPED, GETTINGITNAMED Remedies and process: registrars, hosts, Nominet and the courts

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE RECORDS HOST PUBLIC REGISTRAR / (LIVE) ACCOUNTS THIRD-PART Y PAYMENT VICTIM-SIDE DELETED / ARCHIVES LAYER RECORDS RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THESUPPLIERELEVENDAYSOLD

EXAMPLE2 · THE " COMPETITOR " REVIEW SITE EXAMPLE3 · THEDOMAINTHATCHANGEDHANDSMID - DISPUTE

§ 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 · INFRASTRUCTURELIMBFORTHEPRESER VAT I ON LETTER

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

§ 13 · COMMON QUESTIONS Frequently asked questions WHOIS shows the registrant as "REDACTED FOR PRIVACY". Dead end? The fraudulent site has already been taken down. Have we lost the evidence? Can we find every domain a wrongdoer operates? An email claims to be from our client's domain. How do we prove it was not? Is a Norwich Pharmacal order really available against a registrar or payment process or? Should our client publish DMARC even if it is the victim here?

§ 14 · REFERENCE Glossary DMARC DKIM RDAP SPF UDRP 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

WHOIS shows the registrant as "REDACTED FOR PRIVACY". Dead end?

Starting line: the residue (registrar, dates, nameservers) plus fingerprint cluster in g, archives and content identifiers usually narrows sharply, and the registrar holds the actual identity for disclosure by request or order:

The fraudulent site has already been taken down. Have we lost the evidence?

Mostly no: registration and DNS history, certificate logs and content archives were recording all along, the registrar and host retain account records, and the payment layer retains the money's path: §8's map is the recovery plan. What take d own does cost is anything never archived: which is why on live matters capture always precedes the abuse report.

Can we find every domain a wrongdoer operates?

Often most of them: certificate transparency, shared fingerprints, nameserver and registration patterns, and same-account disclosure from registrars map estates well: Example 1's o per at or ran to five cousins, Example 2's to two. "Every" is unprovable: findings say "the following linked domains", with the linking evidence per domain, and stay open to additions.

An email claims to be from our client's domain. How do we prove it was not?

From the receipt evidence: the message's Authentication-Results and full headers show whether SPF/DKIM/ DMARC passed at delivery and which infrastructure actually sent it; the client's published records at the date (from DNS history) show what should have passed; and the sending domain's own §3 profile (cousin spelling, creation date, MX) usually completes the story. Where everything passed cleanly from the genuine domain, the inquiry pivots honestly to compromise or insider: guide 79 §6's fork.

Is a Norwich Pharmacal order really available against a registrar or payment process or?

In principle yes, on the standard mixed-up-in-wrongdoing basis, and process or s are often the most productive target because payment instruments resist fabrication: the practical constraints are jurisdiction and drafting precision (exact domains, accounts, dates, in the respondent's own vocabulary). The §4 package is what persuades the court the order will actually identify someone.

Should our client publish DMARC even if it is the victim here?

Immediately: a reject-policy DMARC record (rolled out carefully) makes the client's domain hard to spoof and generates reports of attempts: prospectively protective, and retrospectively relevant, since the absent policy at the material time is increasingly raised in loss-allocation arguments after payment frauds, as Example 1's bank correspondence shows. It is the rare remediation that is also good evidence hygiene. cflab. u k · e-disc ove r y. u k