

Metadata For Lawyers What It Can And Cannot Prove

Metadata records specific technical events. Understanding these events, corroborating across sources, and pleading exactly that is crucial. This guide explains metadata families, innocent rewrites, manipulation signatures, and safe reading techniques for UK lawyers.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.

<https://e-discovery.uk/library/metadata-for-lawyers-what-it-can-and-cannot-prove>

METADATA · A GUIDE FOR UK LAWYERS Metadata for Lawyers: What It Can and Cannot Prove Reading the Data About the Data Without Being Misled by It COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
MANIPULATION EXAM IN AT I ON CPR PART 35 EXPERT REPORT S FULL
CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the data about the data 03 The metadata families: file system, application, communication and media 04 What rewrites metadata innocently: copies, migrations and sync 05 Reading fields safely: corroboration before conclusion 06 Metadata as manipulation evidence: backdating and its signatures 07 Preserving and producing metadata: collection to load file 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:
EVERYMETADATAFIELDRECORDSASPECIFICTECHNICALEVENT: KNOWWHICHEVENT,
CORROBORATEACROSSSSOURCES, ANDPLEAEXACTLYTHAT

§ 02 · FIRST PRINCIPLES The problem in plain English: the data about the data

§ 03 · THEFAMILIES The metadata families: file system, application, communication and media

§ 04 · THEINNOCENTREWRITES What rewrites metadata innocently: copies, migrations and sync

§ 05 · SAFEREADING Reading fields safely: corroboration before conclusion

§ 06 · THEMANIPULATIONSIGNATURES Metadata as manipulation evidence: backdating and its signatures

§ 07 · CUSTODY OF THE FIELDS Preserving and producing metadata: collection to load file

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION CLOUD
FILE'S OWN COMMUNICATION COUNTERPART DEVICE BACKUPS / FIELDS RECORD
COPIES ARTEFACTS ARCHIVES DMS / PLATFORMS

§ 09 · IN THE WILD Worked examples EXAMPLE1 ·
THEANOMALYTHATWASALAPTOPREFRESH EXAMPLE2 ·
THE2019AGREEMENTWRITTENBY2022SOFTWARE EXAMPLE3 ·
THEPHOTOTHATPLACEDTHEPHOTOGRAPHER

§ 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 · META DATA PARAGRAPHFORTHEDISCLOSUREPROTOCOL

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

§ 13 · COMMON QUESTIONS Frequently asked questions Can metadata prove when a
document was really created? The author field names our opponent. Is that proof they wrote
it? A key document's dates look wrong. Manipulation? Does email in g or copying a document
really destroy metadata? Our documents were produced as PDFs and the other side now
questions their dates. Are we stuck? Is metadata admissible, and how much weight does it get?

§ 14 · REFERENCE Glossary EXIF XMP 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

Can metadata prove when a document was really created?

Often, but never from one field: authorship dating rests on the lattice: embedded internals, platform version ladders, first transmission, presence in period backups: agreeing. A file-system created date alone dates a copy event; Example 2 shows what real dating evidence looks like, and Example 1 shows why the single field misleads.

The author field names our opponent. Is that proof they wrote it?

It is proof a profile bearing that name was configured in the author in g application: templates, shared machines and IT-imaged laptops write other people's names daily. Treat it as the ladder's first rung and corroborate: platform saves under their account, drafting sessions on their device, the document travelling from their mailbox: per §5's rung discipline.

A key document's dates look wrong. Manipulation?

Statistically, probably a copy or migration: §4's innocent rewrites explain most anomalies, which is why the baseline and the IT history are read first: Example 1's sequence. What survives that filter: internal contradictions, impossible sequences, lattice silence: is §6's territory, and worth the full exam in at i on.

Does email in g or copying a document really destroy metadata?

It rewrites the file-system family (new dates, new paths) while embedded internals usually survive: "destroy" overstates it, but every handling event overwrites part of the record and adds noise the exam in at i on must later subtract. The practical rule stands: preserve first, then investigate: and tell the client's helpful IT team today.

Our documents were produced as PDFs and the other side now questions their dates. Are we stuck?

No: the natives still exist (production copies are derivatives), and the dating case runs from the §8 lattice regardless: DMS ladders, transmissions, backups: which no flattening touched. Produce the natives with provenance under the protocol, and let the lattice answer: it is usually stronger than the fields anyway.

Is metadata admissible, and how much weight does it get?

Routinely admissible as real evidence, with weight tracking exactly the disciplines in this guide: preserved provenance, stated events, excluded innocents, corroborating lattice: the difference between a finding a court adopts and a field an opposing expert re-explains. Weight is built at collection time, which is the quiet moral of the whole guide. cflab. u k · e-discove r y. u k

©2026 Computer Forensics Lab Ltd · cflab.uk · e-discovery.uk · info@cflab.uk · +44 (0)20 7164 6915 Page 15 of 17

Source: <https://e-discovery.uk/library/metadata-for-lawyers-what-it-can-and-cannot-prove>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.