

Can File Timestamps Be Trusted

File timestamps are records, not facts. This guide details the different timestamp families, common causes of innocent rewrites, and how manipulation leaves traces. It covers trustworthiness in practice, common mistakes, and when to involve a digital forensic expert.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
<https://e-discovery.uk/library/can-file-timestamps-be-trusted>

TIMESTAMPRELIABILITY · A GUIDE FOR UK LAWYERS Can File Timestamps Be Trusted?
What Each Timestamp Measures, When It Lies, and How to Tell COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
MANIPULATION DETECTION 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 timestamp is a record, not a fact 03 The timestamp families: file system, document, platform and transmission 04 Innocent rewrites: copies, moves, migrations, sync and time zones 05 Clocks: drift, misconfiguration, time zones and calibration 06 Manipulation: how timestamps are changed, and the traces it leaves 07 Trustworthiness in practice: corroboration, grading and pleading dates 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:
ATIMESTAMPISTRUSTWORTHYWHENYOUKNOWWHICH SYSTEMWROTEIT,
WHATEVENTITRECORDS, THATTHECLOCKWASRIGHT, ANDTHAT
INDEPENDENTRECORDSAGREE: ANDUNTRUSTWORTHY, ORATLEASTUNPROVEN,
WHENEVERANYOFTHOSEISUNKNOWN

§ 02 · FIRST PRINCIPLES The problem in plain English: a timestamp is a record, not a fact

§ 03 · THEFAMILIES The timestamp families: file system, document, platform and transmission

§ 04 · INNOCENTREWRITES Innocent rewrites: copies, moves, migrations, sync and time zones

§ 05 · CLOCKS Clocks: drift, misconfiguration, time zones and calibration

§ 06 · MANIPULATION Manipulation: how timestamps are changed, and the traces it leaves

§ 07 · TRUSTWORTHINESSINPRACTICE Trustworthiness in practice: corroboration, grading and pleading dates

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION
SYSTEM INTERNAL COUNTERPART + CLOCK FILE- DOCUMENT- BACKUPS + SYSTEM
STAMPS STAMPS COPIES LOGS PLATFORM TRANSMISSION RECORDS RECORDS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THE CREATED DATE THAT WAS A COPY
EXAMPLE2 · THECLOCKTHATWASSETBACK, ANDTHELOGTHATNOTICED EXAMPLE3 ·
THETIMESTAMPSTHATDISAGREEDANDTHEONETHATWASRIGHT

§ 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 · INSTRUCTION FOR TIME S TA MPRELIABILITYEXAMINATION

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

§ 13 · COMMON QUESTIONS Frequently asked questions The file says it was created after it
was last modified. Is that proof of tampering? Which timestamps are most reliable? Can
timestamps really be faked? Our device's clock was wrong. Are its timestamps useless? The
other side's chronology rests on file dates. How do we test it? Does opening a file change its
timestamps?

§ 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

The file says it was created after it was last modified. Is that proof of tampering?

Almost never: it is the signature of a copy, a cross-volume move, an extraction or a restore, which give the new file-system entry a fresh created date while preserving the content's modified date (§4): Example 1's leaver- process move. It becomes a question only when the copy cannot be traced and the other families disagree with the claimed history.

Which timestamps are most reliable?

Server-side stamps from synchronised platforms (version rungs, audit events, email server hops), corroborated by each other (§3, §7): they are written by clocks the user does not control and stored where the user cannot edit. Local file-system and document-internal stamps are indicative: useful, editable, and graded accordingly.

Can timestamps really be faked?

Yes, trivially, with free tools or a clock rollback: and the faking leaves traces: NTFS's second timestamp set, the journal's order in g, the logged clock change, the application build that postdates the claimed date, and the platform or transmission record that disagrees (§6): Example 2's resolution was exposed by all four. The forger controls the value, not the context.

Our device's clock was wrong. Are its timestamps useless?

No: a systematically wrong clock is calibrated against reference events (a received email, a server-logged sync, a dated photograph) to establish the offset, and the stamps corrected within stated bounds (§5, guide 96 §4). What is useless is a wrong clock nobody knew about; a known offset is just arithmetic.

The other side's chronology rests on file dates. How do we test it?

With §7's checklist in reverse: which family is each date from, which clock wrote it, what corroborates it, what innocent o per at i on might explain any anomaly, and do §6's traces exist: then §11's requests for the platform, journal and clock records that answer. Chronologies built on single local stamps rarely survive the questions (guide 96 Example 3).

Does opening a file change its timestamps?

It can change the accessed stamp (where access-time updating is enabled), and some applications rewrite modified stamps or internal fields on open and auto-save: which is why evidence is imaged write-blocked before anyone reads it (§7), and why the "quick look" before instruction is the error guide 97 §3 warns against. The stamps as found are the evidence; handling rewrites them. 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 Page 15 of 17

Source: <https://e-discovery.uk/library/can-file-timestamps-be-trusted>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.