TimeBinder.io

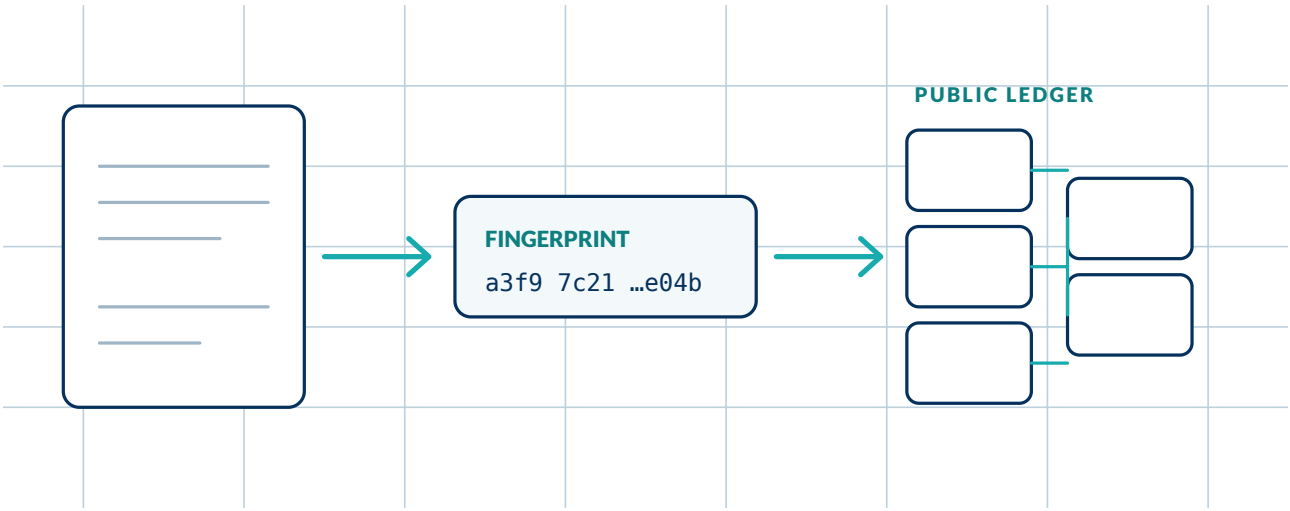
FREE GUIDE FOR LAWYERS · NOT LEGAL ADVICE

Evidence AI Can't Backdate

Cryptographic Timestamps for Lawyers

How an independent, verifiable timestamp shows a file existed by a date, and why that matters when deepfakes and AI edits are everywhere

What a timestamp can and can't establish, how the check works, where the rules point in the US, EU, UK and Australia, and a practical routine for preserving files.



START HERE

The short version

An independent, verifiable timestamp shows that an exact file existed no later than a recorded time, and that it still matches its fingerprint. It does not show who made the file, that the content is genuine, or that a court will admit it.

WHAT IT SUPPORTS

No one can create a valid record for a time that has already passed, and any edit to the file changes its fingerprint, so an altered copy no longer matches. That is a narrow but useful anchor when files can be generated or edited cheaply.

WHAT IT DOES NOT ESTABLISH

Authorship, ownership, copyright status, that the content is authentic or human-made, or how any tribunal will treat it. A deepfake made today can be timestamped today. The timestamp shows when that exact file existed, not where it came from.

Inside

1 How an independent timestamp works 3
2 What it can and can't say, claim by claim 4
3 Where the rules point: US, EU, UK, Australia 5
4 A practical routine: preserve, fingerprint, keep, authenticate 6
5 Alternatives and when to use them 7
6 Sources, and start free 8

This guide is general information for legal professionals. It is not legal advice and does not guarantee that any record will be admitted or given weight. Rules differ by jurisdiction and change. Check current law for your matter.

1 · MECHANICS

How an independent timestamp works



In plain words

1. **The fingerprint.** A SHA-256 hash is calculated from the file's exact bytes. Change one byte and the hash changes completely. TimeBinder calculates it in your browser, and the file stays on your device.
2. **The record.** The fingerprint, not the file, is recorded on the Bitcoin blockchain, a public ledger copied across many independent computers. The time comes from the block that holds the transaction. No single party, including TimeBinder, can alter an entry afterwards. You do not need to hold or use cryptocurrency, and the ledger holds only the fingerprint.
3. **The certificate.** You receive a Proof of Time Certificate (a PDF with a QR code and the transaction details).
4. **The check.** Later, anyone can fingerprint the file again and compare. A match means it is the same file. A mismatch means it is not.

> **POOLED OR ASAP**
>
> A **Pooled** TimeBind groups your fingerprint with others in one shared entry. It is usually recorded within 24 to 48 hours, often sooner, and is checked through TimeBinder. An **ASAP** TimeBind gets its own transaction, sent straight away, and can be checked independently from the certificate and the public ledger.

The same idea elsewhere

The open-source OpenTimestamps project uses the same approach. Its client documentation says verifying a timestamp needs a local Bitcoin Core node (a pruned node is fine) and calls the software "production software that has been in use for many years".

2 · LIMITS

What it can and can't say

The "AI can't backdate" point is narrow. It is about *when* an exact file existed, not about what the file shows.

Proposition	Supported?	Why
The file existed no later than the recorded time	**Yes**	That is what the record shows, if the file still matches
The file is unchanged since then	**Yes, for an exact match**	Any edit gives a different fingerprint
The time can be altered afterwards	**No**	The time is held on a public ledger outside the parties' control
Someone created a record for an earlier time	**No**	A valid record can't be made for a time that has already passed
Who made the file	**No**	Nothing in the record identifies an author
Who owns it, or copyright status	**No**	Not a registration of any right
The content is genuine, human-made or true	**No**	A generated or edited file made today can be timestamped today
A court will admit it or give it weight	**Not guaranteed**	Depends on the rules, the facts and the other evidence

> **DON'T OVERSTATE IT**
>
> Avoid describing a TimeBind as proof of authorship, originality, authenticity or "court-ready" evidence. Describe it as a third-party record of when an exact file existed and whether a file still matches.

Why the narrow claim still matters

Metadata is written by the device or program and can often be edited. Generative tools can produce plausible documents, images and audio. An external record made at the time gives the court or the other side one fixed point that doesn't depend on either party's system clock. It works best alongside witness evidence and other records.

3 · JURISDICTIONS

Where the rules point

An outline only. None of these provisions says a public-ledger timestamp will be admitted or given any particular weight. Check current law and local practice.

Jurisdiction	What the source says	Source
United States (federal)	Authentication requires evidence sufficient to support a finding that the item is what the proponent claims (Rule 901(a)). Examples include a witness with knowledge and evidence about a process or system showing it produces an accurate result (901(b)(1), (9)). Rule 902(13) and (14) allow certain electronic records, and data copied from a device or file identified by a process such as hash value, to be authenticated by a qualified person's certification, with notice. The 2017 committee notes say this goes to authenticity only; other objections remain.	FRE 901, 902 (law.cornell.edu/rules/fre)
European Union	eIDAS Art 41(1): an electronic time stamp shall not be denied legal effect and admissibility as evidence solely because it is electronic or is not a qualified time stamp. Art 41(2): a *qualified* electronic time stamp enjoys a presumption of the accuracy of the date and time and the integrity of the data. A public-ledger timestamp is not a qualified time stamp.	Regulation (EU) 910/2014, Arts 41–42 (eur-lex.europa.eu)
England and Wales	CPR 32.19: a party is deemed to admit the authenticity of a disclosed document unless it serves notice to prove it at trial. Civil Evidence Act 1995 s 8 deals with how statements in documents are proved.	legislation.gov.uk (CPR r 32.19; CEA 1995 s 8)
Australia (Commonwealth)	Evidence Act 1995 s 146: where it is reasonably open to find that a process or device, if properly used, ordinarily produces the asserted outcome, it is presumed that it did so on the occasion in question, unless evidence sufficient to raise doubt is adduced. State and territory law may differ.	Evidence Act 1995 (Cth) s 146 (austlii.edu.au)

Reading across

- Admissibility and weight are separate questions. A court may admit a record and still give it little weight.
- Foundation matters. Someone usually has to explain how the file was kept, how the TimeBind was made and how it was checked.
- For EU matters where the presumption of accuracy is wanted, a qualified electronic time stamp is the instrument the Regulation addresses.

4 · ROUTINE

Preserve, fingerprint, keep, authenticate

Before or at the time

- [ ] Save the exact file. Do not open and re-save it.
- [ ] Work on copies. Keep the original untouched.
- [ ] Make a TimeBind of up to 10 files. Choose ASAP when independent checking or a precise date matters.
- [ ] Store the certificate with the original files.
- [ ] Note who did it, when, on which device.

If a dispute starts

- [ ] Preserve and do not edit. Keep a custody log of who held the files.
- [ ] Re-fingerprint the preserved file and compare it with the certificate.
- [ ] Consider whether an expert is needed for the wider history of the device or file.
- [ ] Plan authentication: who can speak to creating and checking the TimeBind.
- [ ] Take advice on disclosure, privilege and the local evidence rules.

Points a witness statement might cover

An outline for discussion with the lawyer instructing the witness, not a form.

- What the file is and how it came to be held.
- How and when the TimeBind was made, and on what device.
- That the fingerprint of the file as now held matches the certificate, and how that was checked.
- What the witness does not claim: authorship, content truth, or anything about who else had the file.

> **KEEP WITH THE CERTIFICATE**
>
> The exact original file, the certificate PDF, the date you made it, any notes on the device and software, and a copy of the check you ran later.

Technical reference: NIST SP 800-86 recommends preserving file times when collecting data, verifying copies with message digests and keeping a record of custody.

5 · CHOOSING

Alternatives and when to use them

Tool	Good for	Not for
Independent timestamp (TimeBind)	Showing an exact file existed by a time and still matches. Low cost, quick, file stays on device.	Authorship, content truth, identity, presumptions of accuracy under EU law.
Qualified electronic time stamp (EU)	Where the eIDAS presumption of accuracy of date, time and integrity is wanted.	Not a public-ledger record. Provided by qualified trust service providers.
Notary or witnessed copy	Identity, signatures, certified copies.	Showing a digital file's state at a time by itself.
Forensic examiner	The history of a device or file, and how it got there. Expert opinion.	Cheap, quick checks. Dates not independent of the device.
Platform or business records	Activity inside a system, workflow, who did what in that system.	Independence from the platform and its administrators.

Often best together

A TimeBind taken when a file is finalised, platform logs for context, a witness who can explain both, and an examiner only if the history is contested. See the longer comparisons at timebinder.io/compare.

Not suitable if

- You need to show who wrote or owns something. Use contracts, registers and testimony.
- The file must remain secret even as a fingerprint. Consider whether the fingerprint alone is acceptable for your matter.
- You need advice. This guide is not legal advice.

6 · NEXT STEPS

Start free

Make your first TimeBind free. No credit card required. The file stays on your device and the fingerprint is made in your browser.

Start free →

https://app.timebinder.io/?utm_source=pdf&utm_medium=guide&utm_campaign=legal-guide

Pricing: first Pooled TimeBind free. Further Pooled TimeBinds from US$5. ASAP TimeBind US$15. Each TimeBind holds up to 10 files and includes a Proof of Time Certificate. Checking is free.

Sources (checked 10 November 2026)

1. US Federal Rules of Evidence 901 and 902, with advisory committee notes: https://www.law.cornell.edu/rules/fre/rule_901 and /rule_902
2. Regulation (EU) No 910/2014 (eIDAS), Arts 41 and 42: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910
3. Civil Procedure Rules (England and Wales) r 32.19: https://www.legislation.gov.uk/uksi/1998/3132/rule/32.19
4. Civil Evidence Act 1995 s 8: https://www.legislation.gov.uk/ukpga/1995/38/section/8
5. Evidence Act 1995 (Cth) s 146: https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ea199580/s146.html
6. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf
7. OpenTimestamps client README: https://github.com/opentimestamps/opentimestamps-client

Questions: support@timebinder.io · TimeBinder.io is operated from Australia. General information only. Not legal advice. A TimeBind shows that an exact file existed no later than a recorded time and still matches its fingerprint; it does not show authorship, ownership or any outcome.