VERUM OMNIS

AI FORENSICS FOR TRUTH

DOCUMENT SEALING & FORENSIC VERIFICATION

A briefing for law enforcement and legal practitioners

Evidence that proves its own integrity —
without a server, an account, or trust in us.

SHA-512	BITCOIN	ON-DEVICE	NO ACCOUNT
cryptographic fingerprint	independent time anchor	the file never leaves you	anyone verifies, free

verumglobal.foundation

Free to use now | No download required | Verification free for everyone, forever

What this service is

Verum Omnis is a document sealing and forensic verification service. It does two distinct things, and it is worth separating them clearly, because they answer two different questions a court asks about a document.

1. Sealing — “is this the same document, and did it exist then?”

Sealing takes a document and produces a sealed copy that carries its own proof of integrity: a SHA-512 cryptographic fingerprint computed from the file's exact contents, a verification QR code, and a timestamp anchored to the Bitcoin blockchain through OpenTimestamps. Change a single character anywhere in the file — one digit in an amount, one letter in a name — and the fingerprint changes completely, and verification fails.

2. Forensic analysis — “does this bundle contradict itself?”

The forensic engine reads the document and reports contradictions in it: the same event dated two different ways, an amount that changes between pages, a signature block that never signed, a clause invoked on a condition the record itself contradicts, a company registration number that does not check out. It works from a fixed set of 46 contradiction types across 40 detectors, and it quotes the text and cites the page for every single finding.

THE DISTINCTION THAT MATTERS IN COURT

The seal proves the document has not changed since a fixed moment in time. The analysis reports what the document says about itself. They are kept deliberately separate: no forensic conclusion is ever stamped onto the original document. The sealed original stays pristine — the findings live in a separate sealed report.

What it never does

- It never states a verdict. The report will tell you that a termination date is stated as 7 March in one place and 13 March in another, and cite both pages. It will not tell you who lied. That determination belongs to the court, and a report that made it would be inadmissible opinion rather than evidence.
- It never hedges. A finding is stated as fact and anchored to quoted text, or it is not stated at all. There are no probability scores, no confidence percentages, and no risk bands to argue about under cross-examination.
- It never uploads your document. The analysis runs inside your own browser, on your own device.

How to use it

There is nothing to install and no account to create. Open verumglobal.foundation on a phone or a computer, choose a file, and seal it.

1 **Choose what you need**

Seal Only produces the sealed original and a seal certificate. Forensic Analysis adds an on-device scan of the document and a separate sealed forensic report.

2 **Seal the document**

The fingerprint is computed in your browser, the timestamp is submitted to the Bitcoin blockchain, and you receive the sealed file. The Bitcoin anchor typically confirms within one to two hours; the seal is valid immediately and the confirmation strengthens it.

3 **Hand it over**

Share the sealed bundle straight to email or a messaging app, or save it. Optional password protection means the recipient must contact you for the password before they can open it — which gives you a delivery receipt in their own words.

4 **Anyone verifies it, at any time**

Scanning the QR code, or visiting the verification page, recomputes the fingerprint and checks the blockchain anchor. No account, no permission, no fee — including for the other side, the defence, and the court.

For investigators

- Seal an exhibit at the moment it comes into your possession. The blockchain anchor establishes that the file existed in exactly that form at that time, independently of your evidence management system.
- Optional sender identity (name, ID number, address) is written into your private seal certificate for affidavit pre-fill and chain of custody — never into the public QR code unless you explicitly choose that.
- Sealing a bundle at intake and again at hand-over produces two anchored points in the chain, and the fingerprints prove nothing changed between them.
- The forensic report gives a triaged reading list: the most serious contradictions first, each with the page to open and a concrete next step to verify it.

For attorneys

- Seal your client's bundle before it is served or filed. If the document is later disputed, the fingerprint and the blockchain anchor answer the authenticity question without an expert witness.
- Run discovery bundles through the forensic analysis. The engine reads several hundred pages in minutes and returns contradictions with page citations — the mechanical part of the work you would otherwise pay a junior to do over days.
- Every finding is anchored to a quote and a page, so it can be checked directly against the original before you rely on it.
- The report cites candidate statutory provisions for the jurisdictions the documents themselves point to — starting points for counsel to confirm, expressly not legal conclusions.
- A plain-language version is produced alongside the technical report, written for a client, an investigating officer,

or a magistrate reading it cold.

Why this is, in our view, the most secure design available

That is a strong claim, so here is the argument in full, and the reasoning is architectural rather than promotional. Most secure document services ask you to trust a company. This one is built so that you do not have to — including not having to trust us.

There is no server holding your documents

Your document is never uploaded. The analysis runs client-side, in your browser. There is no uploads bucket, no user database, no login backend, and no central store of documents or findings anywhere in the system. This is not a policy that could be changed next quarter; it is the architecture, and it is documented as a hard constraint of the platform.

WHY THIS MATTERS MORE THAN ENCRYPTION

A service that stores your evidence encrypted still holds your evidence — and can be breached, subpoenaed, sold, or shut down. Data that was never collected cannot be leaked, seized from us, or lost when a company fails. For privileged material and live investigations, that difference is the whole point.

The proof does not depend on us being here

Verification recomputes the SHA-512 fingerprint and checks the OpenTimestamps anchor on the Bitcoin blockchain. It is not a lookup in our database — there is no such database. If this organisation disappeared tomorrow, every document ever sealed would remain verifiable by anyone with the file and the public blockchain, because the proof lives in the file and in a public ledger that no one, including us, can edit.

The seal cannot be forged by the people who built it

We cannot backdate a seal. The Bitcoin blockchain fixes when the fingerprint existed, and neither we nor anyone else can rewrite it. We cannot alter a sealed document and re-seal it silently either, because the altered file produces a different fingerprint and fails verification against the original anchor. The system is designed so that its operator has no special powers over the evidence.

The analysis is deterministic, which is what makes it testifiable

The forensic engine contains no randomness and no wall-clock time in its analysis path. The same document produces exactly the same findings, in the same order, in the same words, every time it is run — by you, by the other side, by an expert appointed by the court. That is a property a generative AI cannot offer, and it is the difference between an instrument and an opinion.

Every finding is anchored, and gaps are disclosed

- Each finding quotes the text it is based on and cites the page it came from, so it can be checked against the original in seconds.
- If pages could not be read — a poor scan, a photograph, a page beyond the analysis limit — the report names those pages, states why, and instructs that they be reviewed by a person. Silence about unread pages would be a false clean bill of health.
- When an optional AI review is used, it is labelled as advisory and kept separate from the verified findings; the

deterministic engine's output is never mixed with it.

What the seal proves, and what it does not

A tool used in court should be as clear about its limits as its strengths, and these limits are stated in the reports themselves.

The seal proves

- That this exact file existed in this exact form at or before the anchored moment.
- That it has not been altered by so much as one character since.
- That anyone can confirm both of those facts independently, without asking us and without an account.

The seal does not prove

- That the contents of the document are true. Sealing a false statement produces a perfectly verifiable false statement — what it establishes is that the statement was made, in those words, by that time.
- Who wrote the document, unless the sender chose to record their identity in the certificate.
- That a person is guilty of anything. The engine reports contradictions in the record; the verdict is the court's.

A NOTE ON THE FORENSIC FINDINGS

The engine is deliberately conservative. Its guards exist because each one was earned on a real evidence bundle where an unguarded rule produced a false statement under seal. A missed contradiction is a cost; a false one stated as fact in a sealed report is a much greater one.

Cost

Everything on this website — sealing, forensic analysis and verification — is free to use for the duration of the Constitutional Court proceedings. There is no trial period to register for and no payment details to enter.

Beyond that period, use remains free for private citizens and for law enforcement agencies, anywhere in the world. Commercial use, including by legal practices, is governed by the Constitution's revenue statutes: the same terms for everyone, agreed at installation rather than negotiated.

Verification is free for everyone, permanently and without exception — including the party disputing a document, and the court. That is not generosity; a proof only one side can afford to check would be worth nothing.

In one sentence

Verum Omnis produces evidence that carries its own proof — mathematically verifiable by anyone, anchored to a public ledger no one controls, analysed by a deterministic engine that states facts and reserves every verdict for the court.