IMF for Content Provenance

Using Immutable File Containers to Prove What's Real

Benjamin Toso • v1.0 • February 2026

Summary

Photos used to be evidence. That's changing fast. Google, Samsung, and Apple now ship AI editing tools that alter images before you even look at them. Courtrooms are struggling with it. Journalists are struggling with it. Regular people sharing insurance photos or documenting property damage are going to struggle with it.

The industry's answer is C2PA—a consortium-backed standard that embeds provenance data at capture time. It's good work, but it only runs on a few high-end cameras, it depends on certificate authorities that charge annual fees, and the metadata gets stripped the moment you upload to social media or send through a messaging app.

IMF (Immutable File Container) takes a different angle. Instead of requiring special hardware, IMF lets you seal any files—from any camera, phone, or computer—into a cryptographically signed, blockchain-timestamped container after capture. It doesn't replace C2PA. It fills the gap for the billions of devices and photos that C2PA doesn't cover.

The Problem

Photos Are No Longer Trustworthy by Default

Google's Magic Eraser ships on every Pixel. Samsung's generative editing is a headline feature. Apple's Clean Up tool launched with iOS 18. These aren't Photoshop—they're one-tap alterations available to anyone, and they don't leave obvious traces.

The legal system hasn't caught up. The American Bar Association flagged AI-manipulated imagery as a problem for evidence authentication in 2024. Their concern: the rules of evidence were written when altering a photo required skill and left artifacts. That's no longer true. The International Criminal Court raised similar concerns about authenticating digital evidence in conflict zones.

C2PA: Right Idea, Slow Rollout

C2PA is backed by Adobe, Microsoft, Google, Sony, and others. The standard is sound. But the practical reality as of early 2026:

- Only Sony (Alpha 1, A9 III, A7S III, A7 IV), Leica (M11-P, SL3), and Nikon (Z6 III, planned) support in-camera signing. Zero consumer smartphones ship with C2PA capture.
- Upload a C2PA-signed image to Reddit, WhatsApp, or any image converter—the provenance metadata is gone. Take a screenshot—gone.

- The trust model runs on X.509 certificates from certificate authorities. Annual cost: $50–$500. If the CA is compromised or the cert expires, trust breaks.
- Cameras working offline (common in field journalism) can't reach a Time Stamp Authority. They fall back to the device clock, which is trivial to manipulate.
- C2PA allows metadata from EXIF and other formats to be ported into manifests. A bad actor can backdate a Photoshop DateCreated tag, import it into a C2PA manifest, and argue prior ownership in court. The spec explicitly permits this.

None of this makes C2PA bad. It makes it incomplete. Billions of photos are taken daily on devices with no provenance story at all.

How IMF Works

IMF is a sealed archive format. You put files in, seal the container, and what comes out is cryptographically locked: signed by your key, hashed for tamper detection, and optionally timestamped on the Bitcoin blockchain.

What's Inside

- Ed25519 signatures—ties the container to a specific person's identity
- SHA-256 hash of every file—any modification, even a single bit, is detectable
- AES-256-GCM encryption (optional)—for content that needs to stay private
- Bitcoin blockchain timestamp via OpenTimestamps—a decentralized proof of when the container was sealed, independent of any company or certificate authority
- Zero external dependencies—the tool is a single binary written in Go with no third-party libraries. Verification works offline.

The Workflow

1. Capture photos with whatever you have—phone, DSLR, drone, body cam, doesn't matter
2. Import and seal into an IMF container as soon as practical—ideally minutes after capture
3. Anchor the sealed container's hash to Bitcoin via OpenTimestamps (requires internet once; confirmation takes hours)
4. Share the .imf file. The recipient opens it in IMF Viewer, sees the signature, file hashes, and blockchain timestamp

The sealed container is the artifact. It doesn't depend on metadata that can be stripped.
The .imf file IS the proof.

IMF vs. C2PA

	C2PA	IMF
Signs at capture	Yes, if hardware supports it	No. Seals post-capture.
Works with	Sony, Leica, Nikon (few models)	Any camera or device
Timestamp	TSA server (centralized)	Bitcoin blockchain

Survives sharing	No. Metadata stripped by platforms.	Yes. Container is the file.
Trust model	X.509 PKI ($50–$500/yr)	Ed25519 keys (free, self-managed)
Verify offline	Partial—needs CA check	Yes. Signature + hash only.
File types	Images, video, audio, docs	Anything
Proves device origin	Yes (hardware attestation)	No. Proves who sealed and when.
Dependencies	CA infrastructure, TSA servers	None. Bitcoin anchor is optional.

These aren't competing standards. C2PA is strong at capture-time attestation when you have the right hardware. IMF is strong as a post-capture seal that works with everything. A photo shot on a Sony with C2PA, then sealed into IMF with a blockchain anchor, has both device attestation and independent timestamp—that's a hard combination to challenge in court.

Where This Matters

Conflict Journalism

A photographer in a war zone shoots on whatever camera they can get. They don't have a Sony Alpha 1. At the end of the day, they seal the raw files into an IMF container on a laptop, sign with their key, and anchor to Bitcoin when they get connectivity. Months later, when someone claims the photos were fabricated, the blockchain timestamp proves they existed in that exact form on that date.

Crime Scene Documentation

A forensic tech photographs a scene and seals everything into an IMF container before leaving. The SHA-256 hashes, Ed25519 signature, and Bitcoin anchor create a verifiable chain of custody. Federal Rules of Evidence 902(13)–14 allow self-authenticating electronic evidence from reliable systems. IMF's cryptographic chain fits.

Insurance Claims

A property inspector documents storm damage and seals the photos immediately. When the claim is disputed three months later, the sealed container proves the documentation existed before any repair work started. No he-said-she-said about when photos were taken or whether they were edited.

IP and Creative Work

A designer seals work-in-progress files at milestones. Each sealed container is a timestamped proof of creation. If someone later claims the work as theirs, the blockchain anchor establishes priority—cheaper and faster than formal registration.

Whistleblowing

Sensitive documents go into an encrypted IMF container. The encryption keeps them private. The signature proves the source when the whistleblower is ready to identify themselves. The blockchain anchor proves the documents existed before any investigation began—which matters when the other side claims they were fabricated after the fact.

Next Step: IMF Seal (Mobile App)

The biggest practical gap in the IMF workflow is the time between capture and sealing. On a laptop, it's minutes. With a mobile app, it could be seconds.

What It Does

IMF Seal is a mobile app (iOS and Android) that seals photos and files into IMF containers on the phone. Capture a photo in the app or import from the camera roll, tap Seal, and you have a signed .imf container with a pending blockchain anchor.

Key Features

- Capture or import from camera roll
- One-tap seal—creates a signed IMF container on-device
- Automatic Bitcoin anchoring when online
- Keys stored in the device's secure enclave (iOS Keychain / Android Keystore)—private keys never leave the hardware
- Share .imf files via any channel—AirDrop, email, cloud storage
- Batch mode for sealing a full shoot in one container

Technical Notes

The IMF core is written in Go with zero external dependencies. Go compiles to mobile via gomobile or as a C library called through FFI. Ed25519 signing and SHA-256 hashing are fast—even older phones handle them without noticeable delay. The heavy work (blockchain confirmation) happens asynchronously after the seal.

Future: Bridging C2PA and IMF

If a photo arrives with C2PA Content Credentials—from a Sony or Leica—IMF can preserve that manifest inside the sealed container. This adds a blockchain timestamp that doesn't expire when the X.509 certificate does, and bundles the C2PA original with any derivatives in a single tamper-proof archive.

C2PA proves the camera. IMF proves custody and time. For archival purposes, having both in one container is as close to airtight provenance as you can get with current technology.

Status

IMF is open source (Apache 2.0) and available at github.com/btoso/immutable-container. The macOS desktop viewer (IMF Viewer) is signed, notarized, and supports double-click opening of .imf files. The CLI supports container creation, sealing, extraction, and Bitcoin anchoring via OpenTimestamps.

The mobile app is the next phase. The core library is portable. The UI and platform integration need to be built.

Contact: Benjamin Toso • github.com/btoso/immutable-container