Understanding Your FRE 902(13) Certificate

A section-by-section guide to the self-authenticating certificate FileSworn generates for your digital evidence.

1. Certificate Sections Explained

File Identification

The certificate begins by identifying the digital file: original filename, file size in bytes, MIME type (e.g., video/mp4, image/jpeg), and the FileSworn asset ID. This section establishes which specific file the certificate covers.

SHA-256 Hash

A SHA-256 cryptographic fingerprint is computed the moment the file is uploaded. This hash conforms to the NIST FIPS 180-4 standard. The certificate records both the full hash value and the timestamp of computation. If even one bit of the file changes, the hash will be completely different, proving the file has not been modified since upload.

Upload and Storage Record

Records when the file was uploaded, its storage mode (temporary access or preserved evidence), any expiration settings, and whether a litigation hold is active. This establishes the chain of events from the moment the file entered the system.

Access Audit Trail

A summary of every recorded access event: viewer email address, timestamp, IP address, user agent (browser and device), and the action taken (e.g., viewed, downloaded receipt). This section documents who accessed the evidence and when.

Viewer Attribution Methodology (Section 5)

This section documents the four-step process FileSworn uses to link a specific viewer to each access event. Most attorneys will encounter this for the first time. The four steps:

1. **Verification:** the recipient's email address is verified before any access is granted to the file
2. **Rendering:** a viewer identity watermark containing the verified email is applied in real time during viewing
3. **Persistence:** the watermark remains visible throughout the entire viewing session and cannot be dismissed

4. **Log Correlation:** the watermark identity matches the access audit trail entry, creating a verifiable link between the viewer and their viewing session

The watermark detail level is selected when creating each share link: **Standard** (viewer email), **Detailed** (email + timestamp), or **Full** (email + timestamp + IP hash). All three levels follow the same four-step methodology. The certificate documents whichever level was applied.

NTP Timestamp Authority

All timestamps in the certificate are synchronized to Network Time Protocol sources and stored as immutable records. This ensures timestamps are accurate and defensible.

Independent Verification

The certificate includes instructions for any party to verify file integrity independently. Anyone with a copy of the original file can recompute the SHA-256 hash using standard tools:

- **macOS / Linux:** `sha256sum filename.mp4`
- **Windows:** `certutil -hashfile filename.mp4 SHA256`

If the computed hash matches the hash on the certificate, the file is identical to the original.

Declaration Under Penalty of Perjury

The certificate concludes with a declaration under 28 U.S.C. Section 1746, which carries the same legal weight as a sworn affidavit. This declaration attests that the information in the certificate is true and correct.

2. How to Present the Certificate in Court

Follow these steps to use the FRE 902(13) certificate when introducing digital evidence at trial:

1. **File with pre-trial disclosures.** Include the certificate as an exhibit attachment with your pre-trial submissions or exhibit list.
2. **Provide written notice to opposing counsel.** FRE 902(13) requires written notice at least 14 days before trial. The notice must include a copy of the certificate and make the underlying digital file available for inspection.
3. **List both the certificate and the file.** Your exhibit list should include the certificate as a companion exhibit alongside the digital evidence it authenticates.
4. **Offer the certificate at trial.** When presenting the digital evidence, offer the certificate as the authentication foundation. Move for admission of both the certificate and the underlying file.
5. **Respond to challenges without live testimony.** If opposing counsel objects, the certificate provides the authentication foundation without requiring live testimony from a custodian of records. The self-authenticating nature of FRE 902(13) means the electronic process speaks for itself.

Important: Check your jurisdiction's local rules for variations in the notice period. Some courts require more than 14 days or have specific formatting requirements for self-authenticating exhibits.

3. The Legal Basis

Applicable Rules and Statutes

Citation	What It Covers
FRE 902(13)	Self-authenticating certified records generated by an electronic process or system
FRE 902(14)	Self-authenticating certified data copied from an electronic device, storage medium, or file
FRE 901	General authentication requirement: evidence must be sufficient to support a finding that the item is what the proponent claims
28 U.S.C. 1746	Unsworn declarations under penalty of perjury may substitute for sworn affidavits

What SHA-256 Proves

- **Integrity:** the file has not been modified since the hash was computed
- **Identity:** the hash is a unique fingerprint for this specific file
- **Timestamp:** the file existed in this exact form at the recorded upload time

SHA-256 is approved by NIST under FIPS 180-4 and is used by the US government, financial institutions, and forensic professionals worldwide.

How Opposing Counsel Can Verify

1. Obtain a copy of the digital file
2. Compute the SHA-256 hash using standard tools
3. Compare the computed hash to the hash printed on the certificate
4. If the hashes match, the file is identical to the original

Verification commands:

- **macOS / Linux:** `sha256sum filename.mp4`
- **Windows:** `certutil -hashfile filename.mp4 SHA256`

For questions about using FileSworn certificates in your practice, contact anthony@filesworn.com or schedule a walkthrough at calendly.com/anthony-kulick/filesworn-demo.