

Verdict

Sealed and intact

Files unchanged since they were sealed on 2026-09-20 16:14:56 UTC.

Capture signals: strong

What this dossier establishes

That the files described were sealed by Evidiq on 2026-09-20 16:14:56 UTC and have not changed since: their fingerprints show it, and the chronology says where each date comes from.

What it does not establish

That the scene is real or not staged, nor who made the capture. A photograph of a screen is still a real capture of a false scene.

Sealed on 2026-09-20 16:14:56 UTC	Area near Argenteuil	Location 49.0, 2.2 (deliberately coarse, ~11 km)
Signer Evidiq Production Signing · ECDSA P-256 certificate, issued by Evidiq Production Root CA	Capture Evidiq app (Android) · attested device (Google Play Integrity)	Rubric Evidiq standard rubric.
Sealed index 100 (a value included in the anchored fingerprint, needed to recompute the inclusion)		

Checks

Device and app	Were the device and the app intact and unmodified at the time of capture?	Verified
File integrity	Is the file identical to what the app captured and signed?	Verified
Sealing date	Is there a public record, independent of Evidiq, that this proof existed at a given date?	Verified

**Verify this dossier online**

<https://evidiq.io/verify/7Kv2F28XSE6CdBia9pxgxw.Vzsy2jMuT0R6QYouDZocww>

Authenticity of this document

This document carries no electronic signature. The attachments can be verified independently, and would still verify even if this PDF had been altered: compare the fingerprints in this dossier with those of your own files.

Dossier content · SHA-256

d6f4 f195 4f96 c783 4fec da38 8858 aa69
fa68 5028 5eb3 b19b 77ce 4d06 3a77 3b00

Sealed exhibits

Each exhibit is identified by its SHA-256 fingerprint: a value computed over the exact file. If a single pixel changes, the fingerprint changes entirely.



Reduced preview for printing, without metadata. Only the original is authoritative: the fingerprint opposite is computed over it.

Exhibit 1 / 1

Photograph

Format
JPEG · 2.8 MB

Declared date and time
2026-09-20 16:14:33 UTC · by the file

Provenance
C2PA manifest not attached: this share link does not transmit originals

Original file
Not attached: this share link does not transmit originals

SHA-256 fingerprint of the original
67ed 565b c423 0566
84d3 b3fd d186 b1a1
0be0 9372 03ab f560
e7d7 f7ef d2cb ad10

Recapture analysis

Partial analysis. Some of the measurements are not available on the device that took this photo. The measurements available found nothing.

Comparing a fingerprint. Compute the SHA-256 of your copy of the file and compare the 64 characters, grouped by four. A single difference means your copy is not the sealed file.

Checks

Each check is measured at capture and has only three possible results. A point not measured cannot be added afterwards: a sealed proof no longer changes.

Verified measured at capture and passed **Failed** measured and failed **Not measured** not collected, reason given

Device and app

Verified

Were the device and the app intact and unmodified at the time of capture?

The device and the app were attested at capture time.

File integrity

Verified

Is the file identical to what the app captured and signed?

Every file carries an intact content signature, checked just now, and matches its sealed fingerprint.

 Signer **Evidiq Production Signing** Algorithm **ECDSA P-256** Issued by **Evidiq Production Root CA**

Sealing date

Verified

Is there a public record, independent of Evidiq, that this proof existed at a given date?

The timestamp is written into the Bitcoin blockchain. It verifies publicly, without Evidiq.

 Block **967859** Block time **2026-09-20 16:48:56 UTC** Batch root **d17e9829...8feab3**

Checks executed when this dossier was downloaded, on 11 October 2026 at 10:37 UTC.

Chronology and retention

Each date says where it comes from. Sources are not equal: a phone's clock is a declaration, a Bitcoin block is a fact anyone can check.

Date and time	Event	Source of the time	Checked with
2026-09-20 16:14:33 UTC 18:14:33, Paris time	Capture of exhibit 1 Time written in the file's metadata.	Declared by the file	—
2026-09-20 16:14:56 UTC 18:14:56, Paris time	Proof sealed Checks executed, result frozen.	Evidiq server	Online page
2026-09-20 16:48:56 UTC 18:48:56, Paris time	Proof recorded in block 967859 The proof existed no later than this instant.	Public blockchain	Online page
2026-09-20 17:05:58 UTC 19:05:58, Paris time	Dossier issued, version 2 Content signed by Evidiq.	Evidiq server	Content signature dossier.sig
2026-09-20 17:08:08 UTC 19:08:08, Paris time	Dossier submitted to OpenTimestamps Dossier fingerprint included in a batch, root sent to the public calendars.	Evidiq server	—
2026-09-20 17:28:30 UTC 19:28:30, Paris time	Dossier recorded in block 967867 The dossier existed no later than this instant.	Public blockchain	OpenTimestamps proof dossier.ots
2026-10-11 10:37:37 UTC 12:37:37, Paris time	This copy downloaded Affects neither the content, nor the fingerprints, nor the signatures.	Evidiq server	—

What each source of time is worth

Declared: a declaration, sealed with the exhibit. A clock can be wrong, an integrator can be mistaken.

Evidiq server: Evidiq's synchronised clock. It commits Evidiq, not a third party.

Third-party timestamp: an independent authority attests the date with a signed token.

Public blockchain: depends on no authority. Accurate to about two hours, a property of the Bitcoin protocol.

Retention

Live capture only: the app imports no file from the gallery.

Uploaded originals are kept by Evidiq, hosted in France (OVHcloud), under its retention policy.

Deleting an original at Evidiq invalidates neither this dossier nor its attachments.

Any change of content issues a new numbered version; earlier versions stay unchanged.

Verify independently

Everything below can be checked without Evidiq, with free tools: OpenSSL 3 and the OpenTimestamps client, on Linux or macOS (Windows: WSL or Git Bash). The files named are attached to this PDF: open your reader's "Attachments" panel, save them into one folder and run the commands from there. Some readers built into web browsers do not show attachments.

Dossier v2, issued 2026-09-20 17:05:58 UTC. Its content is signed by Evidiq: the signature covers the dossier's data, not this PDF file.

This dossier's date is sealed in Bitcoin (block 967867): its digest is a leaf of the anchored batch, and that date depends on no authority, not even a TSA.

1 The dossier's content is what Evidiq signed

DSSE envelope, Ed25519 signature over dossier.json. The first two commands rebuild the exact bytes that were signed.

```
printf 'DSSEv1 35 application/vnd.evidiq.dossier+json %s ' "$(wc -c < dossier.json | tr -d ' ')" > pae.bin
cat dossier.json >> pae.bin
openssl pkeyutl -verify -pubin -inkey evidiq-dossier-key.pem -rawin -in pae.bin -sigfile dossier.sig
```

Expected output

```
Signature Verified Successfully
```

2 The verification key is the one Evidiq publishes

A key attached to the PDF could have been replaced along with the signature. Only the key published at the address below is authoritative: the command must print the fingerprint that appears in its name.

<https://api.evidiq.io/.well-known/evidiq-keys/13da89066183efca45850dee1aa813e3384e7a2e58ba00417bea343a85635e47.pem>

```
openssl pkey -pubin -in evidiq-dossier-key.pem -outform DER | sha256sum
```

Expected output

```
13da89066183efca45850dee1aa813e3384e7a2e58ba00417bea343a85635e47 -
```

3 The dossier existed before Bitcoin block 967867

The OpenTimestamps proof starts from the fingerprint of dossier.json and leads to block 967867. ots info prints that fingerprint, then the block's Merkle root: compare it with the root of block 967867 in the block explorer of your choice. With a local Bitcoin node, the OpenTimestamps client makes that comparison itself.

```
sha256sum dossier.json
ots info dossier.ots
```

Expected output

```
20a16c678ed50d02ef884946f3ceec7d3d37e6def89ad0c351eac7863673d62 dossier.json
File sha256 hash: 20a16c678ed50d02ef884946f3ceec7d3d37e6def89ad0c351eac7863673d62
verify BitcoinBlockHeaderAttestation(967867)
```

Attachments

File	Content	Size
dossier.json	Dossier content, version 2: what this PDF lays out, and what the signature, the timestamp and the anchor protect	4 kB
dossier.sig	Ed25519 signature of the content (DSSE envelope)	64 B
evidiq-dossier-key.pem	Public key that verifies the signature	113 B
dossier.ots	OpenTimestamps (Bitcoin) proof of the content	3 kB
README.txt	This procedure as plain text, for offline use	2 kB

Scope, method and framework

Nature of the document

Technical report produced automatically by Evidiq from the data recorded at capture and at sealing. It is neither a forensic expert report nor a bailiff's statement. It characterises neither the scene nor the person who made the capture.

Method, in brief

The files are sent to Evidiq, which computes their fingerprints, runs the checks and freezes the result. Evidiq signs the dossier's content, has it timestamped by a third party when an authority is configured, and records its fingerprint in the Bitcoin blockchain through OpenTimestamps. Data is hosted in France (OVHcloud).

Probative value

Under French law, a fact may be proven by any means (Civil Code, art. 1358). This dossier is one element, weighed by the court or the person receiving it.

Evidiq is not a qualified trust service provider within the meaning of Regulation (EU) No 910/2014 (eIDAS), and this dossier claims no legal presumption for itself.

The Bitcoin anchor establishes that the data existed before the block was recorded; it belongs to no qualified register.

Where stronger probative force is needed, a French bailiff (commissaire de justice) can record the verification of this dossier from its attachments.

Privacy

The printed position is deliberately rounded (about 11 km). This dossier contains neither the identity of the person who captured, nor their device identifier, nor their exact position.

Glossary

Fingerprint (SHA-256)

A 64-character value computed over a file. It changes entirely if a single byte changes.

Sealing

The moment Evidiq freezes the result of a proof's checks. Nothing changes it afterwards.

C2PA

Open content-provenance standard: a signed manifest ties the file to its origin.

RFC 3161 timestamp

A token signed by a timestamping authority, attesting that a fingerprint existed at a date.

Bitcoin anchor

The recording of a fingerprint in the Bitcoin blockchain, through OpenTimestamps, checkable by anyone.

DSSE / Ed25519

Envelope format and algorithm of the signature Evidiq places on the dossier's content.

Sealed index

The sum of the points of the checks measured at capture. It does not say the scene is real.

Not measured

A check not collected at capture. Final for this proof; the reason is given.



Evidiq SASU · SIREN 107 992 760 · RCS Paris · registered office: 47 rue Vivienne, 75002 Paris, France · data hosted in France (OVHcloud)

This document is your archive copy: the fingerprints, timestamps and attachments it contains can be verified independently of Evidiq, with standard tools.

Generated on 2026-10-11 10:37:37 UTC · evidiq.io · contact@evidiq.io

End of dossier