ProofSnap
Digital Evidence

TEST CAPTURE, NOT FOR LEGAL USE

PROVENANCE CERTIFICATE

Source Acquisition Record

Evidence ID	cap_ro373lGfHiCmP5Jm
Page title	Auto Insurance | Lakeside Insurance Agency (fictional sample)
Captured (UTC)	2026-11-07T16:22:43.420Z
SHA-256 (screenshot)	`1e5340fcf91d1d88bc902c02d24e23354515dfbe8b8aa58304e185fbef06a550`
Capture software	ProofSnap API 2.0.0+60f66ed41097
Capture server region	eu-central-1
Captured by	ProofSnap API · dashboard session

URL: https://getproofsnap.com/samples/lakeside-insurance-auto.html

The ProofSnap API loaded the page from its web address over a secured (TLS) connection. It was not uploaded from a file. Every file in this package except manifest.json, manifest.sig, publickey.pem and manifest.json.ots is hashed (SHA-256 and SHA-512) in manifest.json, which is signed with a 4096-bit RSA key.

ACQUISITION DETAIL

Protocol	TLS 1.3
Issuer	Amazon (Amazon RSA 2048 M01)
Subject	getproofsnap.com
Validity	2026-09-20T00:00:00.000Z to 2027-04-05T23:59:59.000Z
SHA-256 fingerprint	`454744cdb1275a9e9419379656de0d07de5f04a295c16bdfcc3d563974f085ee`
Resolved IP addresses	18.173.205.49, 18.173.205.94, 18.173.205.33, 18.173.205.118
Connected address	18.173.205.94

The issuer name, the fingerprint and certificate_chain.pem come from a separate TLS connection to the same address, made after the page loaded.

ACQUISITION AND INTEGRITY CHECKS

Status at the time this record was generated; this document is not updated afterwards.

Retrieval from the web address	HTTP 200 over TLS 1.3
Origin server TLS certificate	recorded
DNS resolution	confirmed by dns.google and cloudflare-dns.com
Clock check against time servers (SNTP)	+1 ms ± 5 ms at start, +1 ms ± 5 ms at sealing (against time.google.com and time.cloudflare.com)
Content Credentials (C2PA)	signed on screenshot
OpenTimestamps proof	submitted, confirmation pending at sealing
eIDAS qualified electronic time stamp	not included

How the source was acquired

This capture was performed by ProofSnap's server-side API, which loaded the page itself from its web address. The page was not supplied as a file by the requester. An independent DNS lookup of getproofsnap.com (dns.google and cloudflare-dns.com) returned the address the page was loaded from (18.173.205.94). The capture server's clock was compared with the time reported by time.google.com and time.cloudflare.com. The package was then sealed: manifest.json records the hash of each file it lists and is signed with a private key created only for this package. The signature does not identify a signatory; a change to a file listed in the manifest is revealed by a mismatch of its hash.

Before the screenshot was taken, the following changes were made to the rendered page or to how it was captured: page scrolled down once. The capture shows the page as it was after these changes. Each change and its outcome are recorded in forensic_log.json (page_modifications).

This certificate documents how the capture was acquired and sealed. It does not determine whether images or other content within the page are authentic or AI-generated, and it does not replace the court's assessment of the evidence.

The package can also be verified at https://getproofsnap.com/verify/index.html or with the scripts in the verification/ folder. The full technical record is in chain_of_custody.json and metadata.json in this package.