ProofSnap

Digital Evidence

TEST CAPTURE, NOT FOR LEGAL USE

Domain	getproofsnap.com
Captured	2026-11-07T16:22:43.420Z
Timestamp	Bitcoin OpenTimestamps: submitted, Bitcoin confirmation pending at sealing
Content Credentials	C2PA Content Credentials embedded

Page & transport

Source URL	https://getproofsnap.com/samples/lakeside-insurance-auto.html
Page title	Auto Insurance | Lakeside Insurance Agency (fictional sample)
HTTP status	200
Capture method	Full-page rendered screenshot via Playwright Chromium
User agent sent to the site	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/153.0.0.0 Safari/537.36 ProofSnapAPI/2.0
Client Hints sent	sec-ch-ua: "Chromium";v="153", "Not_A Brand";v="8"; sec-ch-ua-platform: "Linux"; sec-ch-ua-mobile: ?0

The browser ran headless on Linux. The identity it sent to the site (user agent and any Client Hints) presents it as Chromium without a headless marker (recorded in metadata.json, browser_identity).

Viewport	Desktop
HTML size	4,461 bytes
Cookies present	0
Captured by	ProofSnap API · dashboard session
Capture engine	Chromium 153.0.8010.0 / Playwright 1.63.0 · ProofSnap API 2.0.0+60f66ed41097
Capture region	eu-central-1
Capture window	2026-11-07T16:22:38.800Z to 2026-11-07T16:22:52.123Z (13,323 ms)
Scroll before the screenshot	The page was scrolled to its end once, so that content that loads on scrolling was loaded.
Test watermark	A repeated TEST watermark was drawn over the screenshot image because this is a test capture.
Collapsed content	Opening collapsed sections was requested; the capture software recognized none that could be opened safely, so the page was captured as displayed.

TLS / SSL

Protocol	TLS 1.3
Issuer	Amazon (Amazon RSA 2048 M01)
Subject	getproofsnap.com
Valid from	2026-09-20T00:00:00.000Z
Valid to	2027-04-05T23:59:59.000Z
SHA-256 fingerprint	`454744cdb1275a9e9419379656de0d07de5f04a295c16bdfcc3d563974f085ee`

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

DNS resolution

Hostname	getproofsnap.com
Resolved IPs	18.173.205.49, 18.173.205.94, 18.173.205.33, 18.173.205.118
Connected address	18.173.205.94
Independent resolvers	dns.google: 18.173.205.33, 18.173.205.49, 18.173.205.118, 18.173.205.94, 2600:9000:2724:5c00:8:b88c:9c00:93a1, 2600:9000:2724:e800:8:b88c:9c00:93a1, 2600:9000:2724:4800:8:b88c:9c00:93a1, 2600:9000:2724:1000:8:b88c:9c00:93a1, 2600:9000:2724:aa00:8:b88c:9c00:93a1, 2600:9000:2724:fc00:8:b88c:9c00:93a1, 2600:9000:2724:c000:8:b88c:9c00:93a1, 2600:9000:2724:5600:8:b88c:9c00:93a1; cloudflare-dns.com: 18.173.205.118, 18.173.205.94, 18.173.205.33, 18.173.205.49, 2600:9000:2724:9600:8:b88c:9c00:93a1, 2600:9000:2724:2e00:8:b88c:9c00:93a1, 2600:9000:2724:4400:8:b88c:9c00:93a1, 2600:9000:2724:6e00:8:b88c:9c00:93a1, 2600:9000:2724:2800:8:b88c:9c00:93a1, 2600:9000:2724:7000:8:b88c:9c00:93a1, 2600:9000:2724:6200:8:b88c:9c00:93a1, 2600:9000:2724:c800:8:b88c:9c00:93a1
DNS check	dns.google and cloudflare-dns.com returned the address 18.173.205.94 for getproofsnap.com.

HTTP response headers (selection)

server	AmazonS3
content-type	text/html
date	Sat, 07 Nov 2026 16:22:41 GMT
x-cache	Miss from cloudfront
strict-transport-security	max-age=31536000; includeSubDomains; preload
content-security-policy	self
x-frame-options	DENY
etag	W/"90ce65cc38b5a09c2037ce73cf5f06d5"

Full header set preserved in metadata.json.

Domain registration (WHOIS / RDAP)

Registrar	NameCheap, Inc.
Created	2025-10-19
Expires	2027-10-19
Updated	2026-10-02
Nameservers	dns1.registrar-servers.com, dns2.registrar-servers.com
DNSSEC	not signed
Source	WHOIS

Time check (SNTP)

Capture server clock offset	+1 ms ± 5 ms at start, +1 ms ± 5 ms at sealing (against time.google.com and time.cloudflare.com)

Cryptographic chain

Bitcoin OpenTimestamps: manifest hash submitted to OpenTimestamps calendars (manifest.json.ots). Once it is confirmed in a Bitcoin block, usually within hours, the upgraded proof shows that manifest.json existed no later than that block's time.

RSA-4096 signature (integrity check only, key created only for this package): public key in publickey.pem (manifest.sig)

C2PA Content Credentials: embedded in screenshot.jpeg and stored in the c2pa.json sidecar file

SHA-256 (screenshot) `1e5340fcf91d1d88bc902c02d24e23354515dfbe8b8aa58304e185fbef06a550`

Independent verification

Verification does not depend on ProofSnap's continued operation. Any party can:

1. Validate manifest.sig against publickey.pem (both inside this ZIP)

2. Verify manifest.json.ots, or the upgraded proof once issued, with an OpenTimestamps client
3. Inspect Content Credentials at contentcredentials.org (image integrity; the issuer is ProofSnap itself)

Captured page text

The text of the captured page, as rendered by the browser (document.body.innerText), is preserved in domtextcontent.txt inside this evidence package. Its SHA-256 hash is listed in manifest.json and is covered by the manifest signature, so any alteration of the text is detectable.

Network records in this package, hashed into the manifest: network.har and network.original.har.

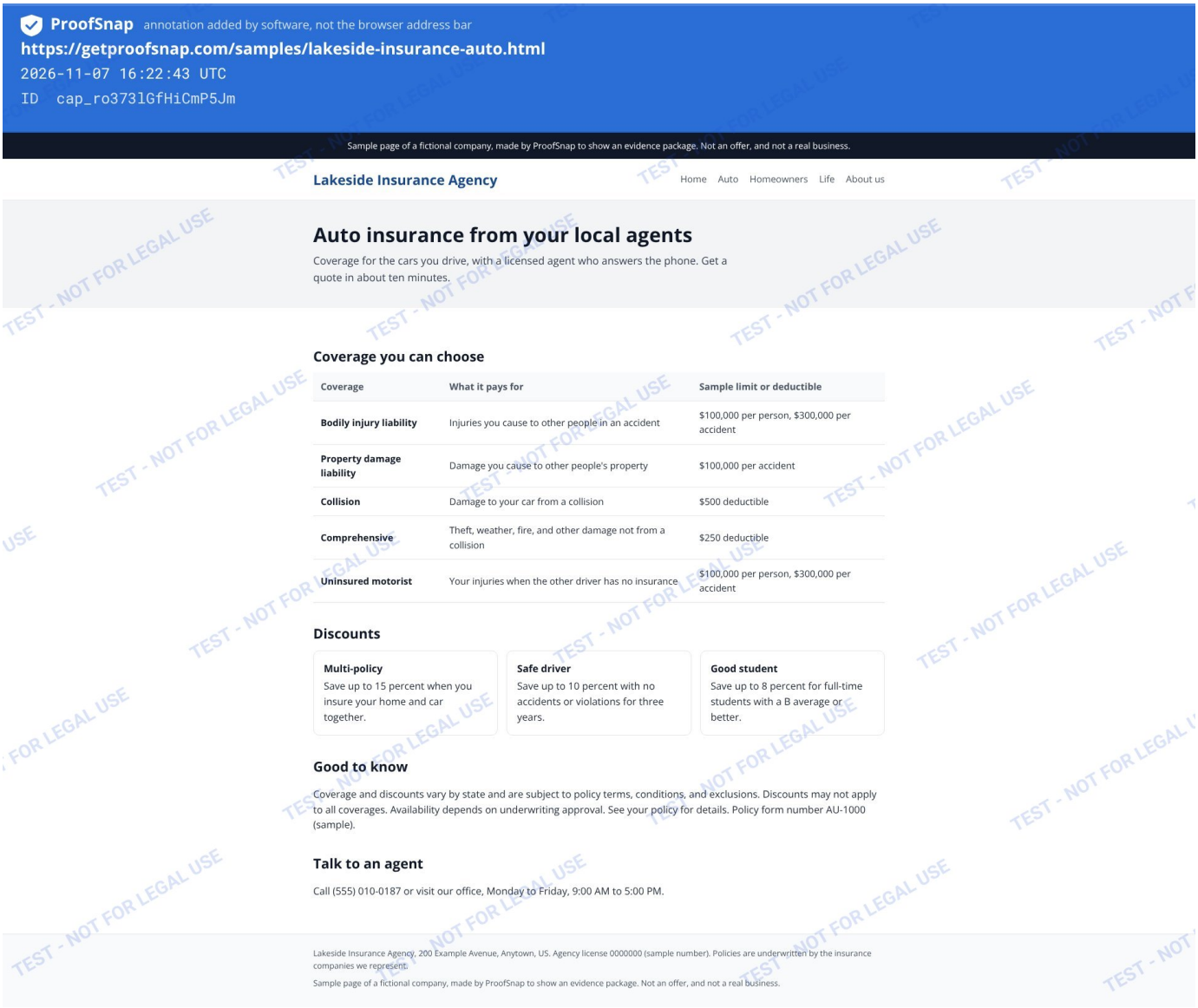
Cookie values in network.har and network.original.har are replaced with "[redacted]".

image_inventory.json lists 0 displayed images; the folder images/ holds 0 copies, one for each unique hash.

Page screenshot

Full-page capture: the screenshot shows the full page.

Preview: full-resolution screenshot in screenshot.jpeg.



Capture Process Record

TEST CAPTURE, NOT FOR LEGAL USE

Description of the process

The data described below was captured by an automated, documented forensic process: a headless Chromium browser navigated to the target URL and rendered the page. Artifacts captured: full-page screenshot, HTML, single-file MHTML snapshot, DOM text and network log (network.har, network.original.har). Each artifact was hashed (SHA-256 and SHA-512) and listed in a manifest (manifest.json). The screenshot was signed with C2PA Content Credentials. The manifest was signed with a freshly generated RSA-4096 key pair (the private key is not stored; the public key is in publickey.pem), and the manifest hash was submitted to OpenTimestamps; the proof was pending at sealing. Verification does not depend on ProofSnap retaining any key. Once confirmed in a Bitcoin block, the OpenTimestamps proof shows that the manifest existed no later than the time of that block. This captured evidence copy can be independently verified by any party from the artifacts in the package; re-acquisition of the live source is not guaranteed, as a web page may change, be removed, or vary by region and time.

Capture metadata

Capture ID: cap_ro373lGfHiCmP5Jm

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

Captured (ISO 8601, UTC): 2026-11-07T16:22:43.420Z

Changes made to the page, or to how it was imaged, before capture: page scrolled down once.

Files in this package: screenshot.jpeg, metadata.json, page.html, page.mhtml, network.har, network.original.har, domtextcontent.txt, text_layout.json, image_inventory.json, forensic_log.json, chain_of_custody.json, c2pa.json, certificate_chain.pem, verification/verify.sh, verification/verify.ps1, verification/VERIFICATION_GUIDE.txt, provenance_certificate.pdf, evidence.pdf, manifest.json, manifest.sig, publickey.pem, manifest.json.ots.

The hash of this report (evidence.pdf) is listed in manifest.json; manifest.json is signed (manifest.sig) and its hash was submitted to OpenTimestamps (manifest.json.ots).

Scope and limitations

This record reflects the page as captured at the stated time. Dynamic, personalized, geolocated, or login-gated content may differ for other viewers or at other times.

Archived network resources are those fetched during this capture; cached, lazy-loaded, or consent-gated resources may be absent (see network.har).

Limitations and disclaimer

Whether and how the record is used as evidence is for the court to decide. ProofSnap gives no assurance of how a court will assess it in a particular proceeding.