v1.0.0 · last reviewed 2026-05-30

technical briefing for counsel, opposing experts, and dfir leadership

catalog scope (live at generation time)

- 5,194 tools site-wide across 17 categories
- 4,004 forensic tools in the public catalog
- 52 case-type playbooks · 55 reference proof investigations
- forensic grade distribution - A: 3,454 · B: 550 · C: 0 · D: 0
- production build sha (when deployed): dev

what it is / what it is not

fatcousin forensics is a local-first browser toolbox for analysis-phase digital incident response. investigators load vendor exports and artifacts on a machine they control; processing runs in JavaScript and Web Workers; structured output and custody events stay on the device unless the investigator chooses to export them.

this is not collection-stage chain-of-custody software, not a SIEM, not an EDR, and not a managed IR service. it ships hash-anchored analysis-phase session custody log infrastructure - sha-256 on inputs and outputs, append-only custody events, .fc-case export with manifest.sha256 sidecar, optional ed25519 signing, and client-side interop exports - designed to support examiner testimony and counsel review. upstream acquisition, independent verification, and qualified legal advice remain required.

analysis-phase custody infrastructure

- case sessions in localStorage - tool slug, version, build sha, timestamps, input filenames, sha-256 of inputs, optional sha-256 of outputs, structured findings, notes
- append-only custody log - corrections are new events, not edits to prior rows (not a per-event hash chain)
- .fc-case zip - manifest.json, custody log, manifest.sha256 sidecar, optional signature.json, optional timestamp.json (rfc 3161 opt-in), optional embedded bytes
- optional ed25519 signing - device-local key via Web Crypto; covers custody log payload and manifest bytes independently
- offline verification - npm run forensics:verify-fc-case and browser import at /forensics/sessions
- interop exports from sessions - universal csv, magnet axiom csv, stix 2.1 bundle, misp event json, autopsy 4.x ingest module
- investigation package - .fc-case plus exhibit html, reproducibility report, and examiner declaration draft (four separate downloads)

local-first architecture

no server route ingests user evidence. open DevTools -> Network before running a tool: you should see static assets only, not POST requests carrying file bytes. proof and methodology pages include a VERIFY panel that flags outbound requests outside an allowlist after load.

- browser-only processing - no accounts, no evidence upload endpoint
- heavy parsers (ffmpeg, onnx, wasm) load from static origin or /public/workers/ and still execute locally
- tool pages stamp build sha and manifest version when available - correlate a captured run with the deployed site

catalog quality and grading

every available forensic tool carries an auto-grade from the public rubric at /forensics/rubric. ship bar: B minimum for new forensic tools, A target. grades are regenerated in CI from forensics-audit.csv.

- A - production-ready: fixtures, honest boundaries, stackable where eligible, export paths
- B - shippable: core engine works; may lack full fixture depth or stack wiring
- C / D - not shipped to the public catalog

validation and replay

- 370/370 flagship golden replay - engineering gate (not exposed as public source checkout)
- synthetic proof investigations at /forensics/proof - evidence packs, per-engine goldens, replayable binders
- replay in browser - download evidence from a proof page and compare output digests to the published receipt
- validation methodology at /forensics/validation-methodology - determinism, discrepancy reproduction, build identity

how to verify (summary)

- browser: drag .fc-case onto /forensics/sessions - review manifest.sha256 match, signature status, warnings
- offline: email labs@fatcousin.com for qualified-reviewer verification tooling (not shipped on the public site)
- network: DevTools -> Network while running a tool - confirm no evidence upload
- replay: open /forensics/proof/bec-sterling (or any flagship) and compare digests to the published receipt

full step-by-step instructions at /forensics/verify

where to read more (web)

the whitepaper, scope, standards, and rubric pages carry the long-form detail this brief summarizes. use the links on the web version of this page; the pdf lists paths only.

claims we do not make

- court compliant, admissible, or certified for litigation
- chain-of-custody software (unqualified - collection stage is upstream)
- guaranteed for litigation or regulatory filing
- expert conclusions or legal findings - outputs are aids to human judgment

document identity

brief version: 1.0.0
last reviewed: 2026-05-30
canonical web URL: https://fatcousin.com/forensics/reviewer-kit#brief
site build sha at generation: dev

verify this PDF: compare SHA-256 of the downloaded file against the digest published at the canonical URL above. do not rely on an unversioned copy.

operated by FatCousin Labs Inc. · labs@fatcousin.com ·
https://fatcousin.com/forensics/reviewer-kit