OFFICIAL USER GUIDE · VERSION 3.0.0

Cyber Forensics By Umami Solutions

Simple Step-by-Step User Manual

This manual is public and can be read or downloaded without signing in.

Authorised use only. Use the product only for evidence, systems, accounts, providers and targets you are legally authorised to examine. The tool preserves facts and provenance; it does not turn guesses into evidence.

60-SECOND START

The whole workflow in nine steps

1 Sign in -> 2 Activate -> 3 Create case -> 4 Add evidence -> 5 Review ->
6 Verify -> 7 Findings -> 8 Report -> 9 Archive

1. Create an account or sign in.
2. If paid access is not active, enter the one-time 6-digit code issued for your email.
3. Click **Start investigation** and record the case/reference details.
4. Open the case and click **Add evidence**. Choose the closest evidence type and record truthful source/acquisition details.
5. Review Evidence, Timeline, Connections, Findings, Analysis runs, Hash matches and Archives.
6. Use **Verify** on important evidence before reporting or transfer.
7. Record important observations as Findings, keeping fact, interpretation and limitations separate.
8. Open Report setup, save report metadata, run integrity preflight and fix every blocker before final release.
9. Create and verify a case Archive when an approved preservation/transfer package is needed.

BUILT-IN HELP

Whenever you are unsure, click the ?

The interface includes contextual **Simple Help**. A page Help button explains the current area. Each forensic-domain card has its own question-mark button, and key case actions such as Add evidence, Search, Report, Archive, Findings, Verify, Details and Transfer have their own help.

Every help panel answers the same questions

- What is this?
- When do I use it?
- What do I give it?
- What do I get back?
- What must I be careful about?
- What are the exact steps?

Beginner words

The **Beginner words** switch simplifies labels and explanations. Turning it on does not change forensic processing, evidence, hashes or reports - only the language used in the interface.

Account, sign-in and activation

Create account

Enter your name, email and a strong password. You can sign in before paid activation, but forensic tools remain locked until activation.

Activate paid access

After payment, Umami Solutions issues a one-time 6-digit code tied to your account email. Open **Access & Licence**, enter it once, and the account becomes licensed.

Password reset

Use Forgot password on the sign-in screen. Follow the reset link delivered through the configured support/mail workflow.

Super Admin MFA

The owner account supports TOTP authenticator verification and one-time recovery codes. Store recovery codes securely when MFA is enrolled.

Start and manage an investigation

1. Click **+ New investigation**.
2. Enter the official case/reference number when available.
3. Add a short title that a reviewer can understand quickly.
4. Record the investigating officer and authority/permission reference.
5. Use the correct case time zone. Ambiguous source times may depend on this when their own zone is missing.
6. Open the case workspace. All evidence, custody, analysis, findings, report releases and archives remain tied to that case.

Add evidence and preserve provenance

Rule: Preserve first, analyse second. The platform records SHA-256 and SHA-512, preserves the original evidence, and uses a verified working copy for supported analysis.

1. Click **+ Add evidence**.
2. Give the evidence an exhibit/evidence number.
3. Select the closest forensic domain.
4. Record where it came from: source/device ID, location, make/model, serial/IMEI, state and exhibit tag where applicable.

5 Record how it was acquired: method, tool/process and version, time zone, start/end time, write protection and known errors.

6 Select the evidence file or authorised export.

7 Click **Preserve, hash & analyse working copy**.

8 If descriptive provenance later needs correction, use **Details**. The evidence bytes and integrity hashes are not editable there.

9 Whenever possession/responsibility changes, use **Transfer** to add a chain-of-custody event.

Understand the seven case tabs

Evidence

Preserved files, provenance, SHA-256/SHA-512 and Verify/Details/Transfer actions.

Timeline

Timestamped events normalized for review while keeping source-time provenance.

Connections

Entities and identifiers correlated across source records.

Findings

Investigator observations, interpretations and explicit limitations.

Analysis runs

Which deterministic/import engine ran, its version, status and time.

Hash matches

Exact-byte matches against enabled reference/known-file hash sets.

Archives

Verifiable case ZIPs with manifest and fixity hashes.

Write findings correctly

A good forensic finding separates three things:

Observation = what the evidence shows

Example: "The supplied browser database contains a visit to example.test at the recorded timestamp."

Interpretation = what it may mean

Example: "This may indicate browser activity associated with that URL."

Limitations = what it does not prove

Example: "This record alone does not prove who physically used the device."

Severity

Use severity to prioritize review, not to exaggerate certainty.

Reporting, preflight and final release

1. Open **Report setup**
2. Record requester, organisation, request date, report authorizer, case time zone, purpose/scope and evidence disposition.
3. Save the metadata.
4. Run **integrity preflight**. The platform re-checks evidence/chains and required release conditions.
5. If an external forensic engine requires a validation record, final release stays blocked until a matching Pass or Conditional validation record exists.
6. Release a Draft for review when appropriate.
7. Release Final only when authorised and all blockers are resolved.
8. Use Print report for the readable/printable case view.

Create and verify a case archive

A forensic archive is a self-contained ZIP containing the case snapshot, preserved evidence and a manifest with integrity information.

1. Click

Archive case

2. Add retention date/notes if required by policy.
3. Create the archive.
4. Open the Archives tab and click **Verify**.
5. Only after verification, download/copy it to approved secure storage.

SPECIAL WORKFLOWS

Security, Hash Sets, Research, Integrations and Desktop Apps

Security Check

Use only for a target you are authorised to assess. Record the host/IP, written authority/reference and scope. The desktop performs non-exploitative service/version discovery after receiving a short-lived signed scan ticket.

Hash Sets

Import SHA-256 reference lists or supported NIST NSRL RDSv3 data. An exact hash match means identical bytes; it does not prove who used the file or why.

Research Lab

Use it for unfamiliar artefacts or research ideas. Its output is exploratory only and must be confirmed by deterministic evidence before it is relied upon.

Integrations

Provider and specialist connectors remain boundaries until authorised access/API data is provided. A connector never substitutes for legal authority.

Desktop applications

Licensed users open Download Apps and choose the official macOS Apple Silicon, macOS Intel or Windows x64 build. The private catalogue verifies the package release hash before delivery.

Tool validation ledger

Supervisors/admins can record the exact external engine/tool version, platform, test reference, result and validated scope. A ledger entry records actual validation evidence; it does not automatically certify a tool.

Super Admin and customer access

The Super Admin console is owner-only. It can issue one-time 6-digit activation codes, review licences/devices, revoke a licence, revoke a single device, restore a device, void an unused code or reissue a replacement code.

Security: Customer codes are email-bound and single-use. The full code is intended to be shown only when generated/reissued. Keep the Super Admin account protected with MFA.

Audit & Integrity

Audit & Integrity verifies the cryptographic activity chain and shows recorded actions. If it reports an invalid chain, investigate before final reporting. A valid chain confirms internal consistency of the recorded history; it does not by itself judge whether every investigative conclusion is correct.

COMPLETE FORENSIC COVERAGE REFERENCE

34 forensic domains

The cards below come from the same capability catalogue used by the live Forensic Lab. Each card tells you what the domain is for, what it accepts, how it is processed and the important boundary you must understand.

01

Evidence Collection & Intake

Document authority, scene/source state, identifiers, provenance, preservation and custody before examination.

Typical inputs

- physical/digital evidence
- provider productions
- exports
- forensic images

Processing path

BUILT_IN

- built-in evidence register
- dual-hash preservation
- custody/audit chains

Important limit

Physical safety, seizure authority, packaging, Faraday isolation and organizational SOPs remain examiner responsibilities.

02

Computer & Disk Forensics

Preserve and examine Windows, macOS and Linux computer evidence with built-in artefact parsing plus established-engine imports/connectors.

Typical inputs

- preserved files
- browser SQLite
- EVTX/log exports
- TSK/Autopsy/KAPE/Zimmerman/Plaso exports
- E01/raw via validated engine

Processing path

HYBRID

- built-in hash/metadata/browser
- TSK/Autopsy import
- KAPE/Zimmerman import
- Plaso import

Important limit

Raw/E01 filesystem traversal, unallocated-space recovery and carving use validated external engines rather than unvalidated PHP reimplementations.

03

Filesystem, Imaging & Recovery

Track forensic images, partitions, filesystems, deleted-file recovery, carving, keyword/string searches and write-protection validation.

Typical inputs

- E01/Ex01/raw images
- TSK/libewf exports
- carving/recovery exports
- CFTT/Federated test reports

Processing path

EXTERNAL_ENGINE

- libewf/TSK boundary
- PhotoRec/tsk_recover/bulk_extractor imports

Important limit

Block-device imaging and hardware write blocking require validated acquisition tools/hardware and are not emulated by the web app.

04

Remote Endpoint Collection

Normalise focused collections from authorised remote-response tools while preserving collection scope and provenance.

Typical inputs

- Velociraptor collections
- osquery results
- EDR/exported triage bundles
- KAPE remote collections

Processing path

IMPORT

- Velociraptor/osquery/KAPE adapters

Important limit

Remote execution requires the organization’s authorised endpoint tooling and credentials; this product does not deploy covert agents.

05

Damaged Media & Data-Recovery Casework

Record condition, recovery attempts and specialist imaging/recovery outputs for damaged HDD/SSD/NVMe/NAND media.

Typical inputs

- ddrescue maps/logs
- specialist recovery manifests
- partial images

Processing path

SPECIALIST_BOUNDARY

- recovery-log adapter
- specialist-lab connector boundary

Important limit

Clean-room repair, chip transplant, NAND reconstruction and invasive hardware recovery require a qualified specialist laboratory.

06

Android, iPhone & Mobile App Forensics

Preserve lawfully accessible mobile data and analyse trusted backups, exports and forensic reports including communications, payments, app usage, Wi-Fi, location, health/fitness and social artefacts.

Typical inputs

- trusted iOS backups
- Android shared/exported data
- ALEAPP/iLEAPP
- vendor forensic reports
- UICC/SIM exports

Processing path

HYBRID

- desktop trusted acquisition
- ALEAPP/iLEAPP import
- vendor-report adapter

Important limit

No passcode bypass, exploit acquisition, Secure Enclave bypass or proprietary full-filesystem extraction is included.

07

Memory / RAM Forensics

Normalise captured-memory results for processes, network connections, injected-code indicators, handles and related volatile artefacts.

Typical inputs

- Volatility 3 JSON/CSV
- memory acquisition manifests

Processing path

EXTERNAL_ENGINE

- Volatility 3 import

Important limit

Memory acquisition and plugin parsing remain validated external-engine functions.

08

Network / Packet Forensics

Reconstruct network activity from packet, flow, DNS, HTTP, TLS and IDS/NSM records.

Typical inputs

- tshark/Wireshark exports
- Zeek logs
- Suricata EVE
- PCAP/PCAPNG via desktop engine

Processing path

HYBRID

- tshark
- Zeek
- Suricata adapters

Important limit

Deep protocol dissection and stream reconstruction require installed packet-analysis tooling.

09

Wi-Fi, Bluetooth & Wireless Evidence

Correlate supplied wireless scan, association, Bluetooth and device-network records.

Typical inputs

- Wi-Fi history exports
- pcap metadata
- Bluetooth logs
- mobile/OS wireless artefacts

Processing path

IMPORT

- generic wireless-event adapter
- mobile/endpoint imports

Important limit

Active RF interception, spectrum capture and protected wireless decryption require lawful specialist equipment/workflows.

10

Malware Triage & Reverse-Engineering Imports

Triage suspicious files without executing them and import results from rule engines, antivirus, sandboxes and reverse-engineering tools.

Typical inputs

- files
- YARA
- ClamAV
- sandbox reports
- static-analysis exports

Processing path

HYBRID

- hash sets
- YARA/ClamAV
- sandbox/reverse-engineering adapters

Important limit

Dynamic execution belongs in an isolated malware laboratory; imported detections are indicators, not attribution or intent conclusions.

11

Browser & Web Artefacts

Analyse histories, downloads, searches, bookmarks, cache/export metadata and browser databases from supported acquisitions.

Typical inputs

- Chromium History
- Safari History.db
- Firefox Places exports
- browser forensic exports

Processing path

BUILT_IN

- built-in SQLite browser parsing
- Firefox/export adapters

Important limit

Encrypted credentials/session secrets are not extracted for account takeover.

12

Email & Messaging Evidence

Read message headers/routes and normalise authorised mailbox/message exports.

Typical inputs

- EML
- MBOX/provider exports
- message-trace exports

Processing path

BUILT_IN

- built-in RFC822 parser
- mail export normaliser

Important limit

Deleted/restricted provider-side data requires an authorised provider export/connector.

13

Cloud & SaaS Forensics

Preserve collection manifests and normalise authorised cloud audit, storage and SaaS exports.

Typical inputs

- AWS
- Azure/Entra
- Google Cloud
- Microsoft 365
- SaaS provider exports
- cloud collection manifests

Processing path

HYBRID

- cloud audit normaliser
- provider connector boundary

Important limit

Private provider-side acquisition requires legitimate credentials, legal process or provider tooling.

14

Telecom / CDR / BTS

Normalise calls, messages and tower/site records supplied by an authorised source.

Typical inputs

- CDR CSV
- BTS/site tables
- provider productions
- authorised telecom connector

Processing path

HYBRID

- CDR/BTS normaliser
- provider plug-in boundary

Important limit

Subscriber data and provider-side live/historical network location require authorised operator access. CDR/site records do not by themselves identify who used a device or pinpoint an exact handset position.

15

Historical Cell-Site & RF Analysis

Correlate supplied CDR/site/sector records and RF survey measurements without overstating location precision.

Typical inputs

- CDR/BTS
- sector/azimuth tables
- drive-test/RF survey CSV
- mapping exports

Processing path

HYBRID

- HCSA/RF deterministic import
- telecom-provider boundary

Important limit

RF propagation and historical cell-site interpretation require trained experts, validated measurements and jurisdiction-appropriate methodology; the system does not perform live covert tracking.

16

Financial & Transaction Tracing

Follow supplied bank, card, UPI, gateway and wallet transaction records and correlate references/times/accounts.

Typical inputs

- bank/UPI CSV
- gateway exports
- mobile-payment artefact exports

Processing path

BUILT_IN

- transaction normaliser
- entity correlation

Important limit

Private financial data requires a lawful source export or authorised connector.

17

Cryptocurrency & Blockchain Analysis

Follow supplied/public-chain transactions, addresses, timestamps and transaction identifiers without guessing ownership.

Typical inputs

- transaction CSV/JSON
- wallet/address lists
- public explorer exports

Processing path

IMPORT

- chain-export normaliser
- entity correlation

Important limit

Address ownership/attribution is never inferred solely from an address or transaction graph.

18

Photo / Video / Document Metadata

Preserve media/documents and extract or import available metadata, hashes, codec/container properties and GPS fields.

Typical inputs

- photos
- video
- audio
- documents
- ExifTool
- ffprobe

Processing path

HYBRID

- hash/metadata
- ExifTool/ffprobe adapters

Important limit

Metadata can be absent, transformed or manipulated and must be corroborated.

19

Forensic Image Analysis & Authentication

Manage integrity, enhancement provenance and specialist image-authentication/content-analysis results.

Typical inputs

- image files
- camera/scanner test records
- authentication/enhancement reports

Processing path

HYBRID

- metadata/fixity
- specialist report adapter

Important limit

Source-camera attribution, manipulation/deepfake conclusions and photogrammetric interpretation require validated specialist methods and human review.

20

Forensic Video & DVR Evidence

Preserve video/DVR exports, normalise codec/timing metadata and import forensic video-analysis results with transformation provenance.

Typical inputs

- video files
- DVR exports
- ffprobe/FFmpeg reports
- video-analysis reports

Processing path

HYBRID

- ffprobe/FFmpeg metadata import
- DVR/specialist report adapter

Important limit

Proprietary DVR extraction, frame-accurate interpretation and authenticity opinions may require specialist hardware/software and examiner review.

21

Forensic Audio Evidence

Preserve audio, record processing provenance and import codec/waveform/enhancement/specialist results.

Typical inputs

- audio files
- ffprobe/FFmpeg/SoX reports
- forensic-audio reports

Processing path

HYBRID

- audio metadata adapter
- specialist report adapter

Important limit

Speaker comparison, intelligibility enhancement conclusions and authenticity opinions require qualified forensic-audio methods and review.

22

Online Content Preservation

Preserve public-facing web content captures and normalise HAR/WARC/screenshot/export provenance.

Typical inputs

- HAR
- WARC metadata
- web capture manifests
- screenshots/PDF exports

Processing path

BUILT_IN

- HAR/WARC adapter
- fixity/provenance

Important limit

Collection must respect applicable authority, terms, privacy and platform constraints; private-account bypass is not performed.

23

OSINT & Threat Intelligence

Correlate public or lawfully supplied indicators and STIX objects.

Typical inputs

- STIX 2 JSON
- IOC lists
- public research exports

Processing path

IMPORT

- STIX/IOC normaliser
- entity correlation

Important limit

The core does not access private accounts, bypass platform controls or make identity attribution solely from public indicators.

24

Server, Web, Application & Service Logs

Normalise server/application/security records to reconstruct incidents.

Typical inputs

- Apache/Nginx
- auth/system logs
- application logs
- SIEM exports

Processing path

BUILT_IN

- generic event normalisers

Important limit

Conclusions are bounded by source log completeness, clock accuracy and retention.

25

Identity, Authentication & Access Forensics

Rebuild sign-ins, MFA, account changes, VPN/SSO and access events from authorised audit logs.

Typical inputs

- AD/Entra
- Okta/Auth0
- VPN/RADIUS
- SSO exports

Processing path

IMPORT

- identity-event normaliser

Important limit

Requires authorised identity-provider audit exports/connectors.

26

Database & SQLite Forensics

Review preserved SQLite databases and imported database audit/query/transaction records.

Typical inputs

- SQLite copies
- audit/query logs
- specialist recovery exports

Processing path

HYBRID

- read-only SQLite metadata
- database audit adapters

Important limit

Proprietary transaction-log/page recovery requires engine-specific specialist tooling.

27

Virtual Machine, Hypervisor & Container Forensics

Analyse supplied VM snapshots, hypervisor records, container events and Kubernetes audit data.

Typical inputs

- VM exports
- Docker/Podman events
- Kubernetes audit
- hypervisor logs

Processing path

IMPORT

- Kubernetes/container normalisers

Important limit

Guest filesystem examination follows the endpoint/filesystem engine boundary.

28

IoT, Wearable & Embedded Evidence

Preserve and normalise lawfully acquired smart-home, router, wearable and embedded-device logs/exports.

Typical inputs

- device logs
- firmware images
- router exports
- wearable exports

Processing path

HYBRID

- hash/metadata
- IoT export adapters

Important limit

Chip-off/JTAG/ISP, proprietary firmware decoding and destructive hardware methods require qualified specialist tooling.

29

Vehicle Infotainment & Telematics

Normalise authorised vehicle/infotainment exports including paired devices, navigation destinations, events and telematics records.

Typical inputs

- vehicle forensic reports
- infotainment exports
- telematics CSV/JSON

Processing path

HYBRID

- vehicle-export adapter
- vendor/specialist boundary

Important limit

Physical acquisition and proprietary decoding are vehicle/vendor specific and may require specialist tools.

30

Drone / UAS Forensics

Normalise aircraft/controller/app flight logs, GPS paths, launch/landing points, telemetry and device identifiers.

Typical inputs

- flight logs
- controller exports
- mobile app reports
- vendor forensic exports

Processing path

HYBRID

- drone-flight adapter
- vendor/specialist boundary

Important limit

Damaged aircraft, chip-level extraction, proprietary decoding and RF countermeasure analysis require specialist handling.

31

Encryption & Protected Evidence

Track encryption state, supplied keys/recovery material and outputs from authorised specialist decryption workflows.

Typical inputs

- encryption metadata
- recovery-key records
- decrypted forensic copies
- specialist reports

Processing path

SPECIALIST_BOUNDARY

- provenance/fixity
- specialist boundary

Important limit

No online credential attacks, credential theft, covert key capture or authentication bypass is provided.

32 Super Timeline & Relationship Graph

Combine normalised records into time-ordered and linked-entity views with source-time provenance.

Typical inputs

- all normalised case records
- Plaso/Timesketch exports

Processing path

BUILT_IN

- built-in timeline/entities
- Plaso/Timesketch import

Important limit

Timeline quality is bounded by source timestamp quality, clock drift and timezone context.

33 Archiving, Retention & Fixity

Create self-contained case archives and verify retained evidence/report fixity over time.

Typical inputs

- case evidence
- case snapshot
- retention metadata

Processing path

BUILT_IN

- built-in archive/fixity ledger

Important limit

Organizational redundancy, off-site storage, legal holds and retention policy remain administrative responsibilities.

34

Authorised Security Assessment

Check approved systems for exposed services and import vulnerability/web-assessment results to recommend remediation.

Typical inputs

- authorised target
- Nmap
- Nessus/OpenVAS
- ZAP/Burp reports

Processing path

HYBRID

- signed-ticket safe Nmap
- scanner imports

Important limit

No exploit delivery, password attack, persistence, stealth, destructive testing or unauthorized access is included.

Troubleshooting - quick answers

I can sign in but tools are locked

Open Access & Licence and enter the one-time 6-digit activation code issued for the same email account.

My evidence Verify check fails

Stop. Do not report, transfer or rely on that item until the discrepancy is investigated. A failed hash means the current bytes do not match the recorded integrity value.

Final report release is blocked

Run report preflight and read every requirement. Missing provenance, failed integrity or a required external-tool validation record can intentionally block final release.

I do not know which evidence type to choose

Open Forensic Lab and click the ? beside likely domains. Read Typical inputs and Important limit before uploading.

A provider/private system has the data

Use the relevant integration/provider boundary only when you have lawful access or an authorised export. The application does not bypass provider controls.

The Research Lab suggested something

Treat it as a hypothesis, not a fact. Confirm it with deterministic evidence, an established forensic method or qualified specialist review.

Plain-English glossary

SHA-256 / SHA-512

Cryptographic fingerprints used to check whether file bytes are still exactly the same.

Provenance

The documented story of where evidence came from and how it was acquired/handled.

Chain of custody

A record of who had responsibility/possession of evidence, when and why.

Deterministic

The same input and method should produce reproducible results, rather than an AI guess.

Finding

A documented observation plus, where appropriate, interpretation and stated limitations.

Validation record

Evidence that a specific external tool/version was tested for a stated scope using a known method/dataset.

Forensic archive

A packaged copy of the case/evidence with a manifest and fixity hashes for later verification.

Connector boundary

A place where an authorised external provider/tool can plug in; the application does not claim access until that connector/data is actually available.

What the tool deliberately does not do

- It does not create legal authority or provider permission.
- It does not perform covert account access, credential theft, password bypass or authentication bypass.
- It does not claim that AI/research suggestions are evidence.
- It does not pretend specialist hardware methods such as chip-off, clean-room repair or proprietary exploit acquisition are built into a PHP web application.
- It does not treat a hash match, IP, address, CDR row or public-chain address as automatic proof of identity, intent or ownership.
