



Eviquire

Full User Manual — Version 6

DESKTOP USER MANUAL • OCTOBER 2026

Target release: Eviquire 6.0.6110.18

Illustrated interface: Eviquire 6.0.6110.16

For investigators, forensic examiners, law enforcement, compliance teams, and legal reviewers

This manual explains capture and case-management workflows; it is not legal advice. Investigators remain responsible for lawful authority, evidence handling, and admissibility requirements.

EVIQUIRE IS A PRODUCT OF RICTA TECHNOLOGIES SRL



www.ricta.io | www.eviquire.com

Technical support: support@ricta.io

© 2026 Ricta Technologies Srl. All rights reserved.

Table of Contents

1. [Introduction](#)
 2. [System Requirements](#)
 3. [Installation Guide](#)
 4. [Getting Started](#)
 5. [Core Concepts](#)
 6. [Case Management](#)
 7. [Acquisition Workflow](#)
 8. [Evidence Capture Types](#)
 9. [Chain of Custody](#)
 10. [Integrity and Verification](#)
 11. [Reports](#)
 12. [Reviewing Evidence and the Acquisition Review Tool](#)
 13. [Exporting and Deliverables](#)
 14. [Advanced Features](#)
 15. [Security and Privacy](#)
 16. [Troubleshooting](#)
 17. [Best Practices](#)
 18. [FAQ](#)
 19. [Glossary](#)
 20. [Appendices](#)
 21. [Version 6 Interface Reference](#)
 22. [Release Evolution and Further Help](#)
-

1. Introduction

1.1 What Is Eviquire

Eviquire is a forensic evidence acquisition platform designed to help investigators collect, preserve, verify, package, and review digital evidence. This manual documents the Eviquire 6 generation and follows the current **Case → Acquisition → Evidence** interface. It provides a controlled acquisition environment for web, mail, mobile, file download, network, and session-based evidence. The platform is intended for situations where an investigator must be able to show not only what was collected, but also how it was collected, when it was collected, who collected it, which system collected it, and whether the exported material still matches the original capture. Eviquire treats an acquisition as a structured forensic event. A user does not simply take a screenshot or save a web page. Instead, Eviquire creates a case context, starts an acquisition session, records chain-of-custody events, creates evidence identifiers, hashes captured files, writes summaries, produces reports, timestamps integrity records, and packages evidence into archives that can later be reviewed or transferred. The platform is especially useful when live digital content must be collected from environments that can change quickly, such as web pages, authenticated portals, social media, online marketplaces, messaging interfaces, webmail, downloadable files, or content reached through specific browser, proxy, DNS, or session settings. Eviquire is also useful for internal compliance and corporate investigations where a repeatable workflow and documented handling process are required.

1.1.1 Scope of This Manual

This guide covers the Desktop Case Manager and forensic-browser workflows, including web, Android Mobile Live (beta), and Mail (beta) acquisition. It incorporates documented functionality in 6.0.6110.18, released 16 October 2026. The interface illustrations were captured from the 6.0.6110.16 build of the same release generation. Cloud editions and licensed configurations may present different options.

A case is an investigation container, an acquisition is one collection session, and an evidence item is one recorded capture or event. These three levels are displayed together in the Case Manager. For clarity, screen-level guidance uses the exact text of controls wherever the supplied interface screenshots expose it.

Forensic scope: Hashes, timestamp responses, blockchain transaction references, and activity records substantiate preservation and integrity; they do not independently prove the truth, authorship, or legal admissibility of source material.

1.1.2 Publisher and Product Ownership

Eviquire is a software product developed and published by **Ricta Technologies Srl**. Ricta Technologies Srl provides product information at www.ricta.io, while Eviquire product information is available at www.eviquire.com.

For product assistance, use the Support function within Eviquire, consult help.eviquire.com, or contact support@ricta.io. When sharing screenshots, logs, or other diagnostic materials, follow your organization's evidence-handling and data-protection requirements.

Manual coverage: Eviquire Desktop 6.0.6110.18 (16 October 2026 release). Screenshots show build 6.0.6110.16. Feature availability depends on the installed platform, licensing, configuration, and acquisition type. Always record the actual running application version in investigative records.

1.2 Purpose Of The Platform

The purpose of Eviquire is to make digital evidence collection more defensible. A defensible collection workflow requires more than saving files. It requires a documented procedure, stable identifiers, traceable timestamps, integrity verification, reviewable metadata, and packaging that protects context. Eviquire supports that purpose by combining acquisition tools with forensic recordkeeping. The platform records activity logs, creates evidence packages, stores acquisition metadata, captures network and browser artifacts when configured, and creates reports at evidence, acquisition, and case level. This layered design allows an investigator to explain a single evidence item in detail while still preserving the broader session and case context. Eviquire is not a replacement for investigator judgment, legal authorization, or organizational evidence-handling policy. It is a technical platform that helps apply those requirements consistently.

Important: Eviquire can collect sensitive information, including browser session data, cookies, downloaded files, mail evidence, network traffic, TLS key logs, and investigator credentials if they are transmitted during capture. Operate the platform according to applicable law, warrant scope, consent requirements, organizational policy, and data protection obligations.

1.3 Key Capabilities

Eviquire provides the following key capabilities:

- Case management for organizing one or more acquisition sessions.
- Web acquisition using a controlled forensic browser environment.
- Screenshot and full-page visual capture.
- Page source and full-page source capture.
- Combined visual and source capture.
- File download capture.
- Mail evidence acquisition.
- Video recording of acquisition sessions.
- Network capture using PCAPNG output where TShark is available and enabled.
- Browser profile preservation, including cache, cookies, and persistent storage.
- Chain-of-custody logging with UTC timestamps.
- Evidence, acquisition, and case reporting in PDF and JSON formats.
- File hashing using MD5, SHA2-256, and SHA3-256.
- Evidence hash lists and packaging-time hash comparisons.
- Timestamp Authority request and response files.
- Blockchain anchoring of summary hashes where enabled.
- Case closure and final case ZIP package creation.
- Review workflows for packaged evidence and acquisition data.
- Optional proxy, Tor, DNS-over-HTTPS, automation, and batch collection features.

1.4 Who Should Use Eviquire

Eviquire is designed for professionals who need reliable digital evidence collection and documentation:

- Law enforcement investigators collecting online evidence.
- Digital forensic examiners preserving web, mail, and session-based material.
- Corporate investigators documenting internal or external web evidence.
- Compliance teams preserving regulatory or policy-related evidence.
- Legal professionals preparing evidentiary material for disclosure or review.
- Incident response teams collecting web-based indicators, downloads, and network traces.
- Fraud teams documenting marketplace listings, phishing pages, or account activity.
- Technical reviewers validating integrity of exported evidence packages.

Beginners can use Eviquire through its guided case and acquisition workflow. Advanced users can enable additional forensic options such as network capture, deep collection, browser profile preservation, proxy routing, DNS-over-HTTPS, and batch acquisition.

1.5 Core Forensic Principles

Eviquire is designed around five forensic principles: integrity, chain of custody, repeatability, defensibility, and separation of scope. Integrity means that evidence files are hashed and summarized so later reviewers can determine whether the material changed. Eviquire records MD5, SHA2-256, and SHA3-256 values for files and packages. SHA2-256 and SHA3-256 are the primary modern integrity indicators; MD5 is included primarily for compatibility with legacy review environments. Chain of

custody means that Eviquire records what happened during the acquisition. Events include timestamps, descriptions, URLs, files, hashes, and investigator/session context. The chain-of-custody record helps explain the path from live source to forensic package. Repeatability means that investigators can use consistent workflows across cases. Eviquire provides standard acquisition settings, predictable identifiers, structured folders, and consistent reports. Defensibility means the final package can be explained. An investigator should be able to describe the case, acquisition, evidence item, capture method, timestamps, hashes, reports, and exported files in a clear and technically coherent way. Separation of scope means that Eviquire preserves evidence at multiple levels. A single evidence item is its own package. A full acquisition is a session package containing all evidence and session artifacts. A case is the outer investigative package containing one or more acquisitions.

2. System Requirements

2.1 Supported Operating Systems

Supported operating systems depend on the Eviquire edition and installer. Current packaging and deployment workflows support Windows and Linux/Ubuntu release targets. Recommended operating systems:

- Microsoft Windows 10 or Windows 11, 64-bit.
- Ubuntu Linux 22.04, 64-bit (identified in the 2026 desktop release notes).
- macOS beta builds were introduced with version 5.0.6110.13; platform availability and capture permissions depend on the distributed build.
- For other Linux versions, use only a build explicitly supplied for that distribution.

Investigator Tip: Use a dedicated acquisition workstation or virtual machine. Avoid running unrelated applications during capture, especially when network capture is enabled, because system-wide traffic may be included in the PCAP file.

2.2 Hardware Requirements

Minimum hardware depends on the size and complexity of evidence. For basic web screenshots and page source captures, Eviquire can run on a modern workstation. For video recording, full-page capture, network capture, batch acquisitions, and large exports, higher specifications are strongly recommended. Minimum recommended hardware:

- 64-bit processor with 4 cores.
- 8 GB RAM.
- 20 GB free disk space for small cases.
- Display resolution of 1366 x 768 or higher.
- Stable network connection.

Recommended forensic workstation:

- 6 or more CPU cores.
- 16 GB RAM or more.
- Dedicated SSD storage with substantial free space.
- Separate evidence storage volume.
- Hardware encryption or encrypted evidence volume.
- Reliable backup destination.
- Trusted time synchronization.
- Appropriate permissions for installation, evidence folders, and any packet-capture components. A portable application build may run without administrator rights, but operating-system packet capture components can still require separate installation or elevated permissions.

2.3 Disk Space

Disk space is one of the most important operational requirements. Eviquire can generate many artifacts:

- Screenshots and full-page images.
- PDF reports.
- JSON reports.
- Raw evidence archives.
- Final evidence ZIP files.
- Acquisition archives.
- Case archives.
- Browser profiles.
- Network PCAPNG files.
- TLS key logs.
- Video recordings.
- Database files.

Large web pages, long videos, full network captures, and batch collections can grow quickly. Before starting an acquisition, estimate how much content will be captured and confirm that the destination drive has adequate free space. As a practical rule, maintain free space at least three times larger than the expected raw acquisition size. This is because Eviquire may temporarily hold raw files, archive files, reports, summaries, and final packages at the same time during finalization. Eviquire has a specific feature to safely stop and close an acquisition if the space is running low.

Caution: Low disk space can cause incomplete capture, missing files, failed report generation, hash mismatches, or corrupted packages. Always confirm available disk space before a high-volume acquisition.

2.4 RAM

RAM usage depends on browser workload, page complexity, screenshots, full-page capture, video recording, and network processing. A minimum of 8 GB RAM is acceptable for small acquisitions. For production forensic use, 16 GB should be considered the practical minimum, and 32 GB or more is preferred. Full-page capture can consume significant memory because the browser, image buffers, page source, scripts, and generated image/PDF artifacts may exist simultaneously. Batch capture and deep collection further increase memory use.

2.5 Network Requirements

Eviquire requires network access for acquisitions involving live online content. Optional features may require additional network access:

- Proxy exit-node checks.
- Tor routing.
- DNS-over-HTTPS servers.
- WHOIS lookup services.
- Online evidence report storage.
- Timestamp Authority requests.
- Blockchain Timestamp anchoring.
- Software updates.
- License validation or telemetry, depending on edition.

If your organization operates in a restricted network, allowlist the required vendor, timestamp, blockchain, proxy, and update endpoints according to your deployment guidance.

2.6 Permissions

Some features require elevated permissions or supporting tools:

- Some installation methods may require administrator rights; portable distribution can avoid an application-installation step where supported.
- Network capture may require TShark/dumpcap permissions, regardless of whether Eviquire itself runs as a standard user.
- Packet capture drivers may be required on Windows.
- Writing to protected folders may require elevated privileges.
- Browser profile, case package, and export folders must be writable.
- Linux network capture may require capture capabilities or root-level configuration.

Warning: Do not run Eviquire with unnecessary elevated privileges during routine evidence collection unless required by policy or a specific feature. Use the least privilege that permits the intended acquisition.

2.7 Optional Forensic Workstation Recommendations

For high-assurance work, prepare a dedicated workstation or VM profile:

- Install only required acquisition tools.
 - Disable unrelated background applications.
 - Use a clean browser profile generated by Eviquire.
 - Synchronize system time with a trusted source.
 - Record workstation identity and operator identity.
 - Use encrypted storage for evidence output.
 - Keep software versions documented.
 - Validate TShark and packet capture availability before operational use.
 - Test report generation and export on a non-evidentiary sample case.
-

3. Installation Guide

3.1 Downloading The Installer

Download Eviquire only from the approved vendor portal (www.eviquire.com). Verify that the installer version matches your deployment instructions. Before installation:

1. Confirm the operating system is supported.
2. Confirm sufficient disk space.
3. Confirm required permissions.
4. Confirm any antivirus, endpoint protection, or application control policies permit installation.

Investigator Tip: Record the installer version and installation date in your lab or workstation documentation. Software version information may be relevant when explaining how evidence was acquired.

3.2 Installing On Windows

To install Eviquire on Windows:

1. Obtain the appropriate Windows installer or portable application distribution from the official Eviquire download channel. If using a portable edition, place the supplied program files on the approved local or removable storage location and start the designated executable. For an installer-based edition, continue with the installation steps below.
2. Download the install software from www.eviquire.com.
3. For an installer-based edition, run the Eviquire Windows installer and follow the installation wizard.
4. Accept license terms when prompted and choose the installation directory where applicable.
5. Complete installation and launch Eviquire (or launch the portable executable for a portable distribution).

6. Sign in using the credentials registered in the Eviquire portal (www.eviquire.com).

If network capture is required, confirm that Wireshark/TShark and packet capture support are installed and accessible. Eviquire can detect whether network capture support is available and may disable network capture options if the required tool is not present.

3.2.1 Windows Portable ZIP (Version 6)

Version 6 is available as a **Windows portable ZIP** in addition to installation-based distribution. The archive includes required application runtimes, including app-local Visual C++ libraries. Portable application execution is useful on investigation workstations where installing the application is restricted.

1. Download the approved Windows portable distribution from Eviquire and extract it to a writable location, such as an approved local folder or USB drive.
2. Launch Eviquire using the executable provided in the extracted package. Sign in or activate according to your license.
3. Select the evidence storage destination and confirm sufficient available space before creating a case.
4. If packet capture is required, separately ensure that the **host** has compatible packet capture components and privileges; bundling the Eviquire runtime does not install TShark or grant dumpcap permissions.

Portable-operation precaution: An application can run from removable media, but forensic acquisition requires reliable, writable evidence storage. Avoid unplugging removable drives while collecting, recording, finalizing, or verifying evidence.

3.3 Installing On Linux

To install Eviquire on Linux where a Linux build is provided:

1. Confirm the distribution and version are supported by your release.
2. Ensure required runtime dependencies are installed.
3. Make the installer executable if needed.
4. Run the installer using the method documented for your deployment.
5. Confirm the application can write to the configured data directory.
6. Confirm browser, multimedia, and network capture dependencies are present.

Network capture on Linux may require additional permissions. If TShark cannot capture packets, configure capture capabilities according to your organization's security policy.

3.3.1 Ubuntu Appliance (Version 6)

The Ubuntu Appliance provides a portable Linux distribution containing its required application runtime, including FFmpeg media tools and Firebird. Use it on a compatible Linux environment with **X11 or XWayland** support. Packet capture still relies on host-installed TShark and properly configured dumpcap permissions.

1. Obtain the official Appliance; save it in an approved writable directory.
2. Grant execute permission when required, then launch the Appliance.
3. Complete user sign-in, check multimedia features, and test the intended evidence capture and export workflow.

Platform note: macOS remains a beta platform. Always test video, application-audio capture, screen permissions, and file access on the specific OS release used for an investigation.

3.4 macOS Beta Availability

A macOS beta was introduced with the August 2026 release. These instructions apply when your organization has received a compatible macOS beta build. For a supported macOS build:

1. Open the signed installer or application package.
2. Follow macOS security prompts.
3. Grant required permissions such as file access, screen recording, or network capture only as instructed.

4. Launch Eviquire.
5. Complete activation.

Caution: macOS privacy controls may block screen recording, browser automation, or file access until permissions are granted. Validate all capture features before operational use.

3.5 First Launch

On first launch, Eviquire initializes user configuration, data folders, interface settings, and licensing status. Depending on edition, the application may display a welcome screen, license prompt, update prompt, or guided setup flow. Confirm the following:

- Your investigator name and user profile are correct.
- The data folder is appropriate for evidence storage.
- The application version is correct.
- Network capture tools are detected if needed.
- Proxy/Tor settings are disabled unless required.
- Report branding settings are correct if your organization uses custom reports.

3.6 Licensing And Activation

Eviquire editions may enable different feature sets. Community or limited editions may restrict certain acquisition modes or advanced features. Professional or enterprise editions may enable online reports, blockchain anchoring, WHOIS, automation, or advanced collection options. To activate:

1. Open the licensing or activation section.
2. Enter the license key or sign in using your organization-approved method.
3. Confirm the activated edition.
4. Restart Eviquire if prompted.

If your organization uses centralized deployment, license information may be preconfigured.

3.7 Updating Software

Eviquire may include a maintenance or update tool. To check for updates:

1. Open the update function from the application or maintenance tool.
2. Check for available versions.
3. Review release notes and compatibility guidance.
4. Install the update.
5. Restart Eviquire.
6. Run a test acquisition before operational use.

Warning: Avoid updating Eviquire in the middle of an active acquisition. Document any software version changes between acquisitions. If version changes occur between acquisitions, note the version change in the case documentation.

4. Getting Started

4.1 Overview Of The Interface

Eviquire is organized around the investigative workflow:

1. Create or open a case.
2. Start an acquisition.

3. Capture evidence.
4. Review evidence.
5. Finalize the acquisition.
6. Close and export the case.

The interface presents case records, acquisition records, evidence records, reports, and configuration settings. The application separates the case manager from the forensic browser. The manager organizes cases and starts acquisitions. The browser performs the live acquisition and records session artifacts.

4.2 Case Manager Dashboard — Three-Level Layout

The **Case Manager** is the primary desktop workspace. The current interface presents the investigation hierarchy on the left and a context-sensitive **Details** pane on the right. Selecting an item changes the details shown on the right without switching away from the Case Manager.

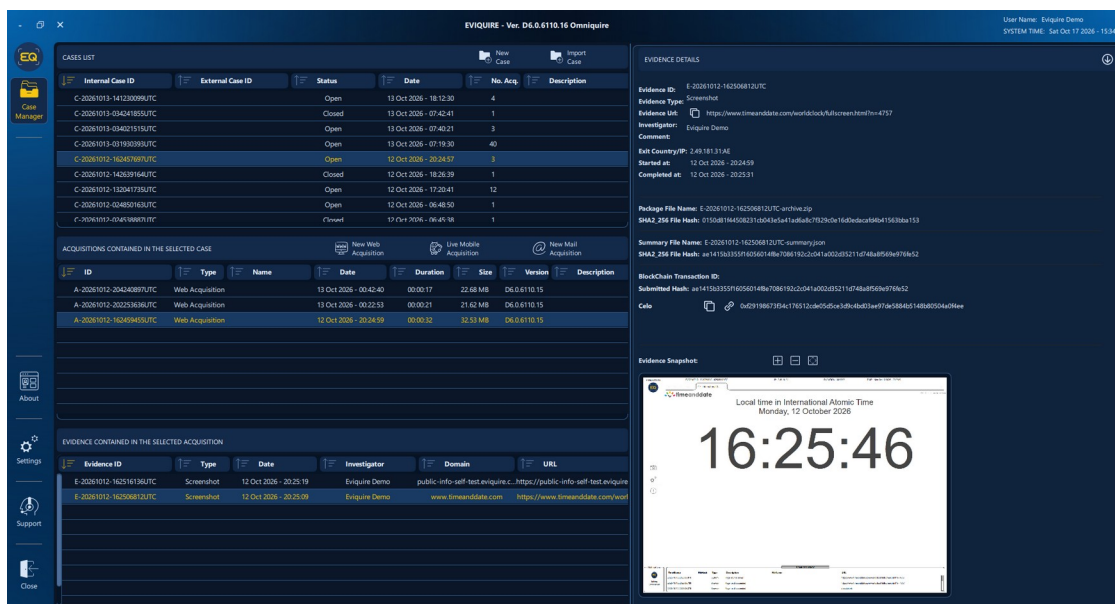


Figure 1. Case Manager, illustrated using Eviquire 6.0.6110.16.

The left-side workspace has three lists:

1. **CASES LIST** — all cases, with columns **Internal Case ID**, **External Case ID**, **Status**, **Date**, **No. Acq.**, and **Description**.
2. **ACQUISITIONS CONTAINED IN THE SELECTED CASE** — acquisitions associated with the selected case, showing **ID**, **Type**, **Name**, **Date**, **Duration**, **Size**, **Version**, and **Description**. This band also provides **New Web Acquisition**, **Live Mobile Acquisition**, and **New Mail Acquisition** actions.
3. **EVIDENCE CONTAINED IN THE SELECTED ACQUISITION** — individual evidence records, with **Evidence ID**, **Type**, **Date**, **Investigator**, **Domain**, and **URL**.

The right panel changes according to whether a case, acquisition, or evidence item is selected. See the dedicated sections below for each detail view. Typical dashboard tasks include:

- Creating a new case.
- Selecting an existing case.
- Reviewing acquisitions in a case.
- Opening an acquisition for review.
- Starting a new acquisition.
- Closing a case.
- Importing or exporting case packages.
- Adjusting application settings.

4.3 Left Navigation Sidebar

The icon rail is displayed on the left side of the Case Manager. The screenshots show **Case Manager**, **About**, **Settings**, **Support**, and **Close**. The **Case Manager** entry opens the three-level investigation workspace. **About** provides product information, **Settings** opens application configuration, **Support** opens the support workflow, and **Close** exits the application.

At the top of the Case Manager, the application displays its version. The upper-right corner shows **User Name** and **SYSTEM TIME**. Distinguish that displayed system time from UTC-formatted case, acquisition, and evidence identifiers and chain-of-custody records.

Case list controls: **New Case** and **Import Case** appear above the case table. Action icons also appear inside the details pane for the selected object. Use the icon tooltip and confirmation dialog before performing destructive or irreversible operations.

4.3.1 Working Through the Lists

To reach a captured item, first select a **case**, then select one of its **acquisitions**, and finally select an **evidence** row. A selected row is highlighted; related information is refreshed in the adjacent tables and on the right. Sort controls are visible in table headers. Some tables can be scrolled horizontally when the window is narrow.

Example: Select a case with three acquisitions, choose a web acquisition from the middle list, then choose a screenshot in the lower list. The Evidence Details panel then displays its evidence ID, source URL, timestamps, integrity fields, and preview.

Do not confuse selection with export: Clicking a row shows metadata. Download, review, and export actions are separate operations shown through toolbar icons and detail views.

4.4 Cases

Cases are the highest-level investigative units. A case should represent a matter, investigation, incident, legal request, or compliance review. A case may contain one acquisition or many acquisitions. Use one case when the evidence belongs to the same matter and should be exported together. Use separate cases when legal authority, subject matter, retention requirement, or disclosure scope differs.

4.5 Acquisitions

An acquisition is one collection session. It has a start time, end time, acquisition type, investigator, options, browser/network context, and evidence list. Use separate acquisitions when:

- Evidence is collected at different times.
- Different proxy, Tor, DNS, or network settings are used.
- Different investigators perform collection.
- Different target systems or accounts are involved.
- A clean separation is required for legal or reporting purposes.

4.6 Evidence Viewer

The evidence viewer allows users to inspect captured evidence. Depending on the evidence type, the viewer may show screenshots, reports, source files, downloads, mail content, logs, metadata, and package information. The viewer is designed for review and validation. It should not be treated as a substitute for the original evidence package. The package and its hashes remain the authoritative forensic deliverable.

4.7 Reports

Eviquire produces reports at three levels:

- Evidence reports describe one evidence item.
- Acquisition reports describe one acquisition session.
- Case reports describe the whole case.

PDF reports are intended for human review. JSON reports are intended for structured validation, ingestion, or technical review.

4.8 Settings

Settings control data location, capture behavior, proxy settings, Tor, DNS-over-HTTPS, video recording, network capture, logging, report branding, language, update behavior, and automation where available.

Investigator Tip: Review settings before each operational acquisition. A prior case may have used a proxy, Tor, DNS-over-HTTPS, or batch capture configuration that should not be reused unintentionally.

5. Core Concepts

5.1 Case

A case is the outer container for an investigation. It holds acquisition sessions and ultimately becomes the final case package. A case provides organizational, legal, and reporting scope. Case data can include:

- Case identifier.
- Description.
- Owner or investigator.
- Last edit date.
- Closure date.
- Case state.
- Acquisition list.
- Case archive.
- Case report.
- Case summary.
- Case timestamp and blockchain metadata.

The forensic value of the case is context. It explains why acquisitions are grouped together and provides a final deliverable for the matter.

5.2 Acquisition

An acquisition is a collection session inside a case. It is the operational unit that records the live capture process. An acquisition starts when the investigator launches the acquisition browser and ends when the session is closed and packaged. Acquisition data can include:

- Acquisition ID.
- Acquisition name.
- Acquisition type.
- Investigator.
- Start and end time.
- Duration.
- Version.
- Public IP and country.
- Proxy IP.
- Tor state.
- DNS-over-HTTPS configuration.
- User agent.

- Mail or mobile parameters where applicable.
- Video recording state.
- Network capture state.
- WHOIS, system info, certificate, and deep collection settings.
- Evidence list.
- Acquisition archive, report, summary, timestamp, and blockchain metadata.

The forensic value of the acquisition is procedural. It documents the session in which evidence was collected.

5.3 Evidence Item

An evidence item is one captured object or capture action. It may be a screenshot, page source, full-page capture, file download, mail message, video, or combined capture. Each evidence item receives an evidence ID and is associated with:

- Case ID.
- Acquisition ID.
- Acquisition type.
- Investigator identity.
- URL/domain or device/mail context.
- Chain-of-custody events.
- Raw evidence files.
- Evidence archive.
- Evidence report.
- Evidence summary.
- Timestamp files.
- Blockchain metadata where enabled.

The forensic value of the evidence item is precision. It isolates one captured thing so it can be reviewed and verified independently.

5.4 Evidence Package

An evidence package is the final ZIP for one evidence item. It normally contains the raw evidence archive, evidence report, JSON report, summary JSON, timestamp files, and blockchain metadata. The evidence package is useful when a reviewer needs one item without the entire acquisition. It is also useful for targeted disclosure, technical validation, or exhibit preparation.

5.5 Acquisition Package

An acquisition package is the sealed package for an entire session. It contains the evidence packages and session artifacts needed to explain the collection environment. Acquisition artifacts can include:

- Acquisition database.
- Chain-of-custody logs.
- Browser profile.
- Network logs.
- PCAPNG.
- TLS key log.
- Video recordings.
- System info.
- Certificates.
- Evidence packages.

- Acquisition report.
- Acquisition summary.
- Timestamp and blockchain metadata.

The acquisition package is useful when the complete session must be reviewed.

5.6 Case Package

A case package is the final export for the whole investigation. It can contain one or more acquisitions, case reports, summaries, timestamp files, blockchain metadata, and optionally a viewer package. The case package is the most complete deliverable. It is appropriate for archiving, disclosure, handoff to legal teams, or long-term preservation.

5.7 Session IDs

Eviquire uses IDs to bind files and records together:

- C-...UTC identifies a case.
- A-...UTC identifies an acquisition.
- E-...UTC identifies an evidence item.

These identifiers appear in folder names, package names, reports, summary JSON, database records, and chain-of-custody entries. This makes it easier to correlate artifacts during review.

5.8 Hashes

Hashes are cryptographic fingerprints of files. Eviquire records MD5, SHA2-256, and SHA3-256 values. If a file changes, its hash changes. Eviquire uses hashes to:

- Identify evidence files.
- Validate packages.
- Detect mismatches between capture-time and packaging-time file states.
- Populate reports and summaries.
- Support timestamp and blockchain anchoring.

5.9 Timestamping

Timestamping creates external proof that a specific summary file existed at a particular time. Eviquire uses timestamp request and response files:

- .tsq: timestamp query/request.
- .tsr: timestamp response.

The timestamp is applied to the summary JSON, not necessarily every raw file individually. Because the summary contains hashes of the archive and report, timestamping the summary effectively timestamps the integrity statement for the package.

5.10 Blockchain Verification

Where enabled, Eviquire submits summary hashes for blockchain anchoring. This provides an additional external integrity reference. Blockchain metadata is stored with the package so reviewers can inspect anchoring information. Blockchain anchoring does not replace traditional forensic verification. It supplements hashes, timestamp authority files, chain-of-custody records, and reports.

5.11 Chain Of Custody

Chain of custody is the documented history of evidence handling. Eviquire records chain-of-custody events during acquisition. These events help explain what happened, when, by whom, and which file was produced. Eviquire logs include:

- UTC timestamp.
- Event type.
- Event description.
- URL.
- File path or relative file name.
- SHA2-256 file hash where applicable.

The chain-of-custody record is central to defensible review.

6. Case Management

6.1 Creating A Case

Create a case before collecting evidence. A case should represent one investigative matter or legal scope. Procedure:

1. Open Eviquire.
2. Navigate to the case manager.
3. Select New Case.
4. Enter case metadata such as description, owner, investigator, matter name, or internal reference.
5. Confirm the case details.
6. Save the case.

Eviquire creates the case folder and case database as needed. The case receives a stable case ID, normally beginning with C-.

Investigator Tip: Use a case name or description that is meaningful but does not expose unnecessary sensitive information if the package name or folder path is later viewed by third parties.

Figure 2. NEW CASE CREATION: internal and external metadata with Advanced / Bulk Pageshot options.

The **NEW CASE CREATION** dialog separates **Internal Information**, **External Information**, and **Advanced** batch-capture controls. The Internal Case ID and default case name are generated by Eviquire. The Case Owner field identifies the current owner account; Description holds the investigation context.

Where applicable, **External Case ID** and **External Case Name** allow Eviquire to be linked to the reference scheme used by the investigating organization, court, or evidence-management system. These references do not replace Eviquire's internal case identifier.

The **Advanced** area includes **Bulk Pageshot Acquisition**, optional **Dump Images** and **Download Video** selections, and a field for multiple target URLs. Enter only investigation-authorized targets; automated collection must remain within the applicable collection scope.

Tip: Populate meaningful external references before the first acquisition, and verify every URL supplied to a bulk operation. A long URL list can increase storage requirements and collection time considerably.

6.1.1 Internal and External Case IDs

Eviquire assigns an **Internal Case ID**, normally beginning with C- and ending in UTC. The **External Case ID** is a separate field used to associate the Eviquire record with the organization's investigation, incident, or matter tracking system. These identifiers may be identical in a demonstration case, but they serve different purposes. Where available, enter a meaningful external reference without changing the generated internal identifier.

The **Status** field identifies whether a case is open or closed. The **No. Acq.** field displays how many acquisition records belong to that case. The **Date** and **Description** columns make the case recognizable in the list.

6.2 Editing Case Metadata

Case metadata may include description, owner, state, notes, or workflow fields depending on edition. Update metadata when the scope or administrative details change. Procedure:

1. Select the case.
2. Open the case details view.
3. Edit the relevant fields.
4. Save changes.
5. Confirm the updated case information.

Changes to case metadata should be consistent with internal evidence-handling policy. If a change affects legal scope or collection authority, document that separately.

6.2.1 Case Details Panel

Select a case in the **CASES LIST** to display **CASE DETAILS** in the right panel. The illustrated panel separates **External Case Details** and **Internal Case Details**, followed by **Description** and **Attached Files**. The case-level toolbar contains edit, document/report, add, file, download/export, and delete-style icons; action availability can depend on case state. Read the tooltip and application confirmation before selecting an icon.

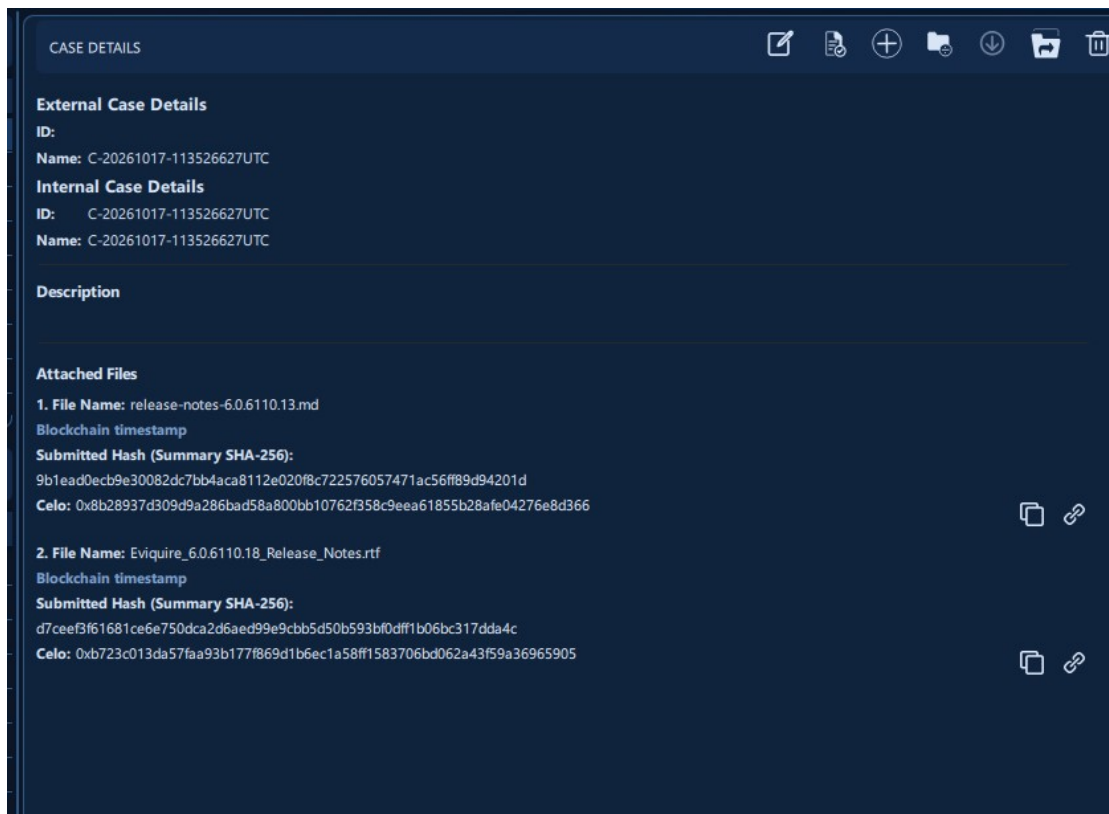


Figure 3. The case-level Details pane lists attached files and their blockchain timestamp information.

6.3 Assigning Investigators

Investigator identity may be set in the user profile, case, or acquisition form depending on workflow. The investigator name is included in evidence summaries and chain-of-custody context. Before starting an acquisition:

1. Confirm the active user profile.
2. Confirm investigator name and surname.
3. Confirm license or account identity if applicable.
4. Confirm the correct case is selected.

If multiple investigators work on a case, use separate acquisitions for each investigator or document role changes carefully.

6.3.1 Adding Supporting Files to a Case

Version 6 provides a dedicated **FILES** tab within the **EDIT CASE** dialog. It permits investigators to attach relevant supporting documents to the case, such as authorization records, investigator notes, scope documentation, or third-party references. These attachments are distinct from evidence captured during an acquisition.

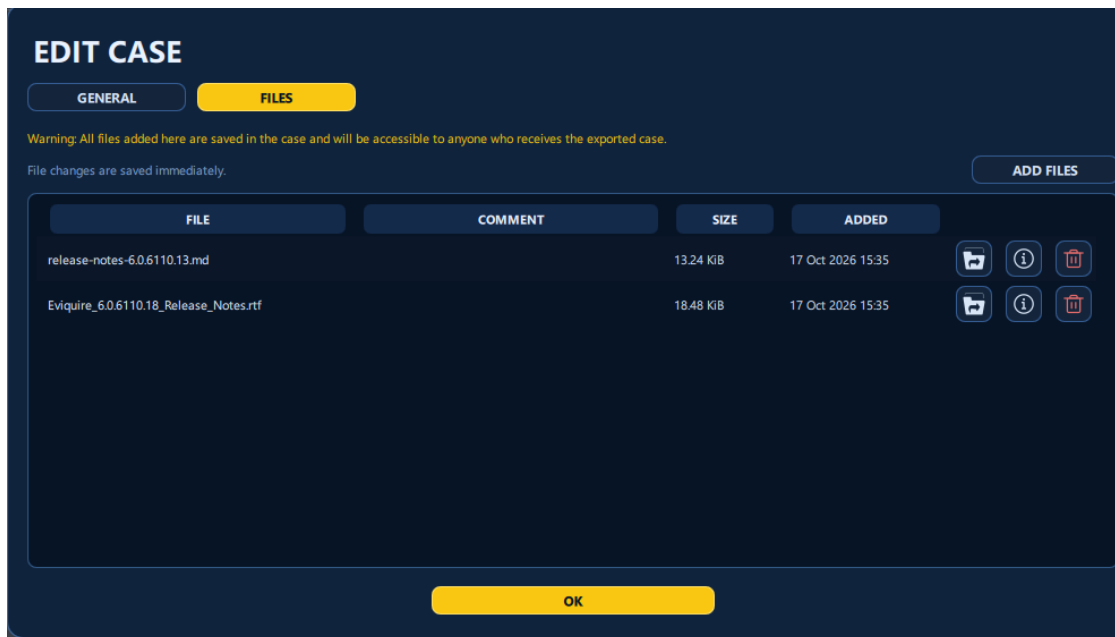


Figure 4. The Files tab lists filename, optional comment, size, and date added.

Procedure — attach a file to a case

1. Select the open case in **CASES LIST**.
2. Open the case editing action from the **CASE DETAILS** toolbar.
3. Choose the **FILES** tab, then select **ADD FILES**.
4. Select the intended local file or files. Review the filename, size, and addition time in the list.
5. Use the available file-row controls to access the attachment, view information, or remove it where permitted. Add an explanatory comment where supported.
6. Select **OK** to leave the dialog.
7. Return to **CASE DETAILS** and review the **Attached Files** section.

Important information displayed by the product: *File changes are saved immediately.* The dialog warns that **all files added here are saved in the case and will be accessible to anyone who receives the exported case.** Do not attach privileged or unrelated material without assessing export and disclosure scope.

For each file, the case Details pane can display a **Blockchain timestamp** section containing a **Submitted Hash (Summary SHA-256)** and a **Celo** transaction identifier. Copy and link icons provide a way to reference the recorded transaction. These integrity fields relate to the attachment's recorded summary and anchoring; they do not mean that the full attachment content is publicly stored on the blockchain.

Attachment versus evidence: A case attachment is contextual material introduced by the investigator. An evidence item is an acquisition output with its own evidence ID and capture record. Keep these categories distinct in reports and disclosures.

6.4 Notes

Use notes to document investigative context that is not automatically captured:

- Legal authority or consent reference.
- Target account or URL list.
- Time-sensitive conditions.
- Authentication steps performed before capture.
- Known limitations.
- External tools used.
- Deviations from standard procedure.

Notes do not replace Eviquire's chain-of-custody logs. They complement them.

6.5 Case Classification (Where Available)

Some deployments may expose classification fields or tags. If available in your edition, use them to classify cases and evidence. Example tags include:

- Fraud.
- Phishing.
- Marketplace.
- Internal investigation.
- Regulatory.
- Urgent.
- Privileged.
- Contains PII.

Tags improve triage and review but should not be used as the only description of evidence.

6.5.1 Case Context Menu

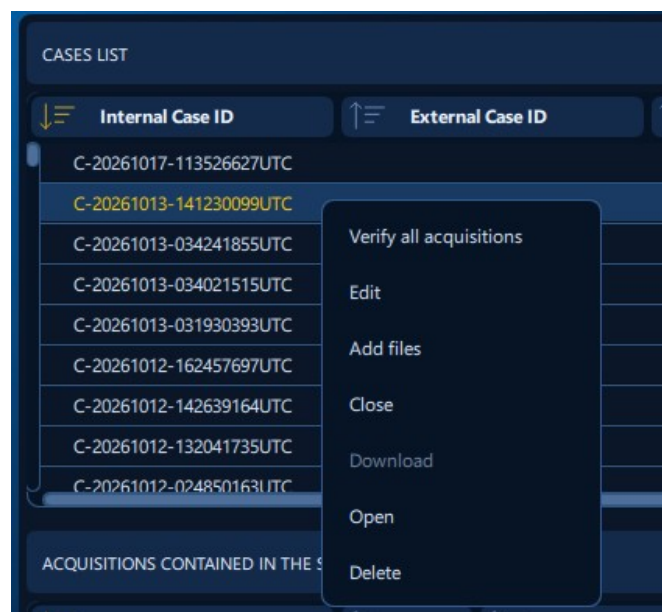


Figure 5. Case list context menu, including Verify all acquisitions, Edit, Add files, Close, Open, and Delete.

Right-click a case row to access available case actions. **Verify all acquisitions** launches the integrity-verification interface; **Edit** opens case metadata; **Add files** attaches supporting material; **Close** opens final case packaging; **Open** displays or enters the selected case. **Download** may be unavailable until the case has an appropriate finalized package.

Caution: Deletion removes access to case records according to the application workflow; follow retention, legal-hold, and authorization rules before using a destructive action.

6.6 Closing A Case

Close a case when collection and review are complete and the case is ready for final packaging. Procedure:

1. Select the case.
2. Confirm all acquisitions are finalized.
3. Confirm all evidence items are present.
4. Confirm reports are generated.
5. Select Close Case.

6. Choose whether to add a viewer package, if supported.
7. Enter an export password if required.
8. Start closure.
9. Wait for hashing, compression, reporting, timestamping, and final packaging to complete.
10. Confirm the final case ZIP was created.

Closing a case creates a case archive, case report, case summary, timestamp files, blockchain metadata where enabled, and final case ZIP.

Warning: Treat case closure as a formal evidence-handling action. Do not close a case until you have confirmed the collection scope and export requirements.

Figure 6. CLOSE THE CASE: password, optional online report, and included-viewer controls.

The **CLOSE THE CASE** dialog displays the Internal Case ID and Internal Case Name. Enter a **Password** when using the available protected-export workflow, and select optional **Save Report Online** or **Add Viewer** settings only when they are appropriate for the matter.

Select **CLOSE THE CASE** to start final packaging. Allow report generation, file inventory, hashing, timestamping, and archive finalization to complete. Do not modify the case folder or interrupt storage during this operation. A successfully closed case is not intended to be reopened or edited; additional evidence should be documented in a supplemental case or permitted follow-up workflow.

Disclosure reminder: A case package can contain browser state, TLS secrets, attachments, and other sensitive session material. Review its handling classification and deliver its password through a separate secure channel.

6.7 Exporting A Case

A closed case can be exported as a final ZIP package. If a password is used, communicate it through a separate secure channel. Recommended export practices:

- Store the original export in a secure evidence repository.
- Generate transfer copies from the original.
- Record the exported file hash.
- Use encrypted transfer methods.
- Keep password and package separate.
- Document recipient, date, transfer method, and hash verification.

6.8 Closed Cases and Supplemental Work

Closed Eviquire cases cannot be reopened for editing. This protects the integrity of the original closed case package. When additional collection is required after closure, preserve the original export unchanged and create a separate case or supplemental acquisition under a new open case, documenting the link to the original matter.

Do not attempt to modify the closed archive or its included metadata. If information must be provided to a reviewer, create a separate explanatory note or derivative disclosure package and preserve its relationship to the original.

7. Acquisition Workflow

7.1 Starting A New Acquisition

An acquisition starts from a selected case. Procedure:

1. Select an open case in **CASES LIST**.
2. In **ACQUISITIONS CONTAINED IN THE SELECTED CASE**, choose **New Web Acquisition**, **Live Mobile Acquisition**, or **New Mail Acquisition** according to the planned collection.
3. Complete the acquisition metadata fields, especially **Acquisition Name** and **Description**.
4. Check the displayed **Investigator** and the automatically assigned **Acquisition ID**.
5. Configure the **Browser user agent**, **Proxy**, **TOR Proxy**, **Content Language**, and **DoH Settings** as needed for web collection.
6. Review all checkboxes within **Acquisition options**, including any active video, network, report, resource, and timestamp settings.
7. Confirm the configuration is appropriate for the legal scope, capture objectives, data protection requirements, and expected storage.
8. Select **START NEW ACQUISITION** and wait for the appropriate acquisition window.
9. When the session is finished, close it using the application workflow and allow packaging to finish.

Eviquire launches the forensic browser. During the live session, the browser records events and captures selected artifacts. When the session closes, the manager finalizes the acquisition package.

7.1.1 New Acquisition Dialog (Version 6)

Figure 7. The Version 6 New Acquisition dialog organizes settings into session metadata (left) and acquisition options (right).

The following fields appear on the web **NEW ACQUISITION** form:

Field	Purpose / investigator action
Acquisition ID	Generated identifier for this session (starts with A- and ends in UTC). Preserve it unchanged.
Investigator	Identity of the investigator recorded for this session. Verify it matches the actual operator.
Acquisition Name	A short human-readable name for the collection session.
Description	Narrative purpose, collection boundaries, and other relevant context.
Browser user agent	Browser identification preset or value presented to target websites.
Proxy	Selected routing profile; No proxy is available.
TOR Proxy	Enable Tor routing when it is required by scope and available in the build.
Content Language	Preferred content or localization setting (for example en-US).
DoH Settings	Open the DNS-over-HTTPS configuration dialog.

Buttons: **CANCEL** closes the form without starting the new session; **START NEW ACQUISITION** begins the configured session. Changes in routing, user agent, and language may affect which version of a web page the website presents, so they belong in forensic documentation.

7.2 Selecting Acquisition Type

Eviquire supports multiple acquisition types:

- Web Acquisition: browser-based capture of web pages, downloads, screenshots, source, network, and context artifacts.
- Mobile Acquisition: capture from a connected or configured mobile device workflow.
- Mail Acquisition: capture of email messages and mail-related screenshots.

The acquisition type determines which fields and capture tools are available. For example, mobile acquisition requires device information, while mail acquisition requires mail server, port, protocol, username, and password.

7.2.1 Acquisition Options Explained

The right side of the Version 6 form groups available web acquisition controls into four categories. The presence of a control does not mean it is active: inspect its checkbox state. The values below describe the on-screen labels and their intended acquisition context.

Group	Option	Meaning / effect
Core options	Video Recording	Record the visual acquisition session to provide interaction and timing context.
Core options	Network Traffic	Capture packet-level network activity where the required components and permissions are available.
Core options	Application Network Acquisition (HAR)	Capture application-layer HTTP requests and responses as a HAR artifact.
Core options	Chromium Network Audit (NetLog)	Record detailed Chromium browser network diagnostic events.
Evidence options	Realtime Evidence Timestamp	Request an external timestamp for the relevant evidence integrity record during finalization.
Evidence options	Save each Evidence Report Online	Publish or store individual evidence reports using the enabled online reporting service. Check disclosure policy before activation.
Domain & System Artifacts collection	Automatic Tests	Run the configured automatic checks associated with acquisition.
Domain & System Artifacts collection	Fetch WHOIS Data	Collect domain-registration context where retrievable.
Domain & System Artifacts collection	Save System Info	Preserve operating system and workstation context.
Domain & System Artifacts collection	Save Certificates	Preserve certificate/trust-environment information according to the implementation.
Browser & Web Artifacts	Advanced Resources Collection	Preserve additional browser/web resources beyond the visible page.
Browser & Web Artifacts	Advanced Cookies Collection	Capture a richer collection of cookie-related artifacts; handle as sensitive session material.
Browser & Web Artifacts	Automatic Cookie Consent	Allow the configured consent handling behavior. Its action selector is a separate control.

The screenshot shows **Video Recording**, **Network Traffic**, **Realtime Evidence Timestamp**, and **Advanced Resources Collection** selected in the illustrated session. This is an example configuration, not a universal recommendation or a statement of defaults for all licenses.

Automatic Cookie Consent Selection

The **Automatic Cookie Consent** checkbox enables the function; the adjacent drop-down specifies the desired response, such as **Reject all** in the illustrated dialog. A selection visible in the drop-down does not mean a website’s banner was actually processed; verify the checkbox state and acquisition records. Cookie preferences can affect which page resources load, and site behavior can differ between services. For forensic repeatability, document whether the tool interacted with a consent banner, what response was requested, and whether the operation succeeded.

For capture integrity, do not automatically accept cookies when the collection objective or legal scope requires avoiding such consent. Consider starting another independent acquisition if a different consent response must be compared.

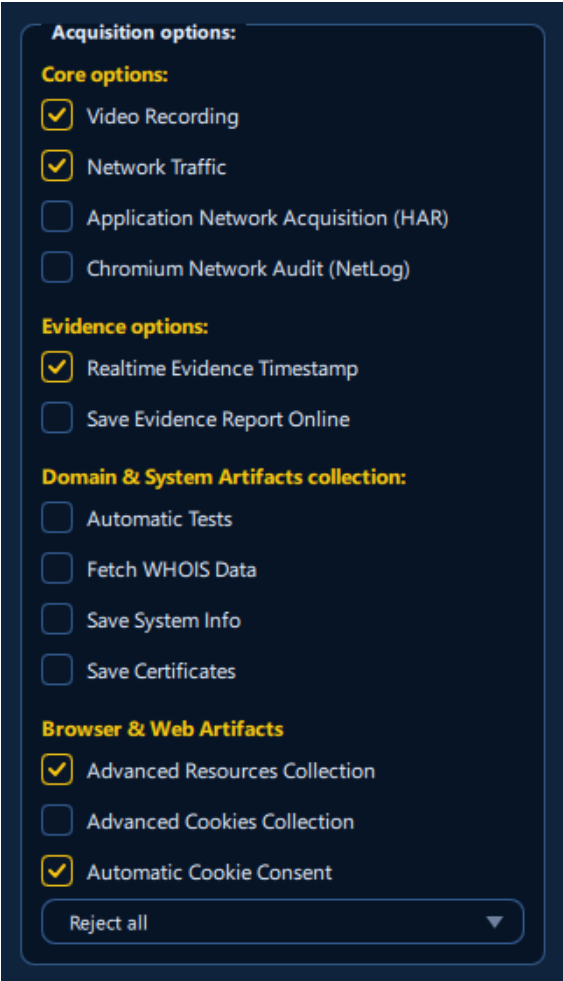


Figure 8. Version 6 web acquisition options, grouped by Core, Evidence, Domain & System, and Browser & Web artifacts.

7.2.2 Core, Evidence, and Artifact Options

The web acquisition dialog groups individual collection settings by purpose. Each enabled option influences captured material, the session metadata, and potentially the final acquisition archive size. Disabled controls should not be interpreted as proof that the underlying information never existed: they indicate a feature was not selected for the session.

Control	Effect and recommended use
Video Recording	Record investigator interaction with the acquisition browser, when supported.
Network Traffic	Collect packet-level traffic (PCAPNG) using supported host capture components.

Application Network Acquisition (HAR)	Collect browser-observed HTTP request/response artifacts; distinct from host PCAP.
Chromium Network Audit (NetLog)	Record Chromium network diagnostic events and timing information.
Realtime Evidence Timestamp	Request external timestamps for individual finalized evidence summaries.
Save Evidence Report Online	Publish eligible evidence reports to the configured online service, subject to policy.
Automatic Tests / Fetch WHOIS	Collect enabled diagnostic or registration-related technical context.
Save System Info / Save Certificates	Record system context or certificate environment artifacts.
Advanced Resources Collection	Preserve additional observed web resources when supported.
Advanced Cookies Collection	Collect detailed cookie metadata and lifecycle observations.
Automatic Cookie Consent	Attempt supported Accept all / Reject all actions and log actual clicks.

Important distinction: Evidence reports may be generated locally even if **Save Evidence Report Online** is disabled. Online saving is a separate option. Realtime timestamping is configured separately from acquisition finalization timestamping.

7.2.3 Mail Acquisition (Beta): POP3 and IMAP

Figure 9. NEW MAIL ACQUISITION (BETA): POP3/IMAP selection, server, port, credentials, and connection check.

Select **New Mail Acquisition** from the selected case. In the mail dialog, confirm the generated Acquisition ID and Investigator, enter a meaningful Acquisition Name and Description, then choose **POP3** or **IMAP**. Supply the authorized **Server**, **Port**, **User Name**, and **Password**; use **CHECK** to validate connectivity or account details before starting the acquisition.

The illustrated example selects POP3 and shows port 995. The actual port and encryption requirements depend on the mail server. Mail acquisitions provide optional **Video Recording**, **Save each Evidence Report Online**, and **Realtime Evidence Timestamp** settings. Protect mailbox credentials and scope collection to the authorized account and messages.

7.2.4 Android Mobile Live Acquisition (Beta)

Figure 10. Android Mobile Live Acquisition (BETA): connected-device selector and USB connection instructions.

Select **Live Mobile Acquisition** and verify the case context, generated Acquisition ID, investigator, name, and description. On the Android device, enable Developer Options (commonly by tapping **Build Number** seven times), then enable **USB Debugging**. Connect the phone to the workstation using USB and accept the device's debugging authorization prompt.

Choose the phone in **Compatible mobile device**. Use the device refresh control if it is not listed. This beta workflow provides **Video Recording**, **Save each Evidence Report Online**, and **Realtime Evidence Timestamp**. Device compatibility, operating-system permissions, and USB debugging policies can differ between devices; test the supported capture path before live casework.

Mobile safety: Enabling USB debugging changes device trust and access settings. Record authorization and device identifiers and restore device settings according to your approved operating procedure after acquisition.

7.3 Investigator Metadata

Before capture, confirm:

- Investigator name.
- Acquisition name.
- Acquisition comment.
- Case ID.
- Acquisition type.
- Expected target URLs or accounts.
- Language or content settings.

This metadata appears in reports and summary files. Accurate metadata supports later review and testimony.

7.4 Browser Launch

When the acquisition begins, Eviquire launches the forensic browser process and passes session information through environment variables. The browser initializes storage, database, chain-of-custody logging, profile paths, network logging, SSL key logging, request interception, and acquisition UI. The browser is isolated from the manager process so the live acquisition can run as a dedicated session. When the browser exits, the manager packages the results.

V D6.06110.16 EVIDENCE ID: E-20261017-170437899UTC IP: 249.181.31 DURATION: 00:06:26 TIME: Sat Oct 17 2026 - 21:04:39

TimeStamp	FileHash	Type	Description	FileName	URL
2026-10-17 21:04:39.010		System	User agent changed	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	https://r3--sn-xupn5a5u5x-4wged.googlevideo.com/videoplayback?expire=1792278215&ei=ZqrTapPvH...
2026-10-17 21:04:38.763	58c9..19bc	System	Evidence summary saved (JSON)	/Evidences/E-20261017-170437899UTC/E-20261017-170437899UTC...	https://www.youtube.com/watch?v=9yXZuRfALS
2026-10-17 21:04:38.751	d047..19e6	System	Page source saved	/Evidences/E-20261017-170437899UTC/E-20261017-170437899UTC...	https://www.youtube.com/watch?v=9yXZuRfALS

Figure 11. Live forensic browser during a YouTube capture; the footer displays real-time Chain of Custody and acquisition notifications.

The forensic browser displays **software version**, **Acquisition ID or Evidence ID**, **public exit IP**, **elapsed duration**, and a **time display** across the top. Use the acquisition tools on the left and the expandable Chain of Custody footer to follow evidence production, navigation, download activity, and operational messages.

The example shows a downloaded-video notification in the acquisition workspace. The visible page and session recording provide context, while the evidence package and logs remain the authoritative preserved files. Displayed times may follow an investigator-selected GMT offset; UTC records are retained for the forensic event timeline.

7.5 Capture Settings

Capture settings determine which artifacts are collected. Common settings include:

- Video recording.
- Network traffic capture.
- Application Network Acquisition (HAR).
- Chromium Network Audit (NetLog).
- Realtime Evidence Timestamp.
- Save each evidence report online.
- Automatic cookie consent handling and browser cookie collection.
- Automatic tests.
- WHOIS lookup.
- System information.
- Certificates.
- Deep collection.
- Content language.

- DNS-over-HTTPS settings.
- Proxy or Tor routing.

Use the minimum settings that satisfy the investigative requirement. Extra artifacts can improve context, but they can also increase package size and sensitivity.

7.6 Network Logging

Network logging captures traffic generated during the session into a PCAPNG file where supported. This can be valuable for showing server connections, redirects, downloads, requests, and related communication. Before enabling network capture:

1. Confirm TShark is installed and detected.
2. Confirm permissions are sufficient.
3. Close unrelated applications.
4. Consider using a dedicated VM.
5. Warn investigators that credentials may appear in traffic or decrypted logs.

Warning: Network capture may include traffic from the entire host, not only the Eviquire browser. If other applications are open, their traffic may be included. This can introduce privacy, privilege, and scope issues.

7.6.1 Choosing PCAPNG, HAR, and Chromium NetLog

These options serve different forensic purposes and are not interchangeable:

Artifact	Capture level	Especially useful for	Important limitations
Network Traffic (PCAPNG)	Packets seen at the capture interface	Endpoints, timings, network flows, packet-level examination	Can include unrelated system traffic; HTTPS content may remain encrypted unless suitable keys exist.
Application Network Acquisition (HAR)	Browser HTTP request/response transactions	Headers, methods, status, redirects, requested resources, and timing	HAR is not packet capture and does not ordinarily provide comprehensive DNS-resolution telemetry. Sensitive headers and tokens may be present.
Chromium Network Audit (NetLog)	Chromium internal network event log	Browser networking behavior, DNS/resolver events when logged, proxy behavior, connection diagnostics	Browser-specific diagnostic format; event coverage depends on configuration and browser version.

Capture more than one format when technically justified. Record which options were enabled and verify that the expected files are present after closure. If DNS visibility is a principal objective, evaluate the actual resolver and browser log outputs; do not assume DNS transactions will appear in a HAR file.

7.6.2 HAR and Chromium NetLog (Version 6)

HAR captures browser-observed HTTP requests, responses, timing, headers, and supported response bodies, with a dedicated viewer offering filters, sorting, and raw-response downloads. It is especially useful for analyzing dynamic web applications and API calls without requiring the investigator to inspect packet-level traffic.

Chromium NetLog captures the browser networking stack's diagnostic events. It can help explain network connection, DNS, cache, proxy, and timing behavior. NetLog is not an interchangeable substitute for full HAR bodies or host packet capture; evidence contents depend on the enabled capture mode.

Output	Primary perspective	Principal handling consideration
PCAPNG	Packets observed by the host capture engine	May include unrelated system traffic; depends on host tools/permissions.
HAR	Application-level HTTP	May include authenticated headers,

	request/response context	cookies, tokens, and response bodies.
NetLog	Chromium network diagnostics and browser internals	May expose URL, DNS, proxy, and sensitive network metadata.

Privacy: Enable these outputs selectively. HAR, NetLog, PCAPNG, TLS key logs, and advanced cookies can each expose session data or credentials.

7.7 Proxy And Tor Settings

Proxy and Tor settings route acquisition traffic through a configured network path. This can be useful for geographic testing, anonymity requirements, or controlled routing. Before using a proxy or Tor:

- Confirm legal authority permits the routing method.
- Confirm exit country and public IP.
- Record the proxy configuration.
- Verify the target content is reachable.
- Understand that different routing can change page content.

Eviquire records exit country and public IP events when available, and acquisition metadata includes public IP, country, and proxy IP.

7.8 DNS Over HTTPS

DNS-over-HTTPS settings control how the forensic browser resolves domain names. Available modes may include system DNS, secure-only, or secure-with-fallback, depending on platform support. DNS settings matter because DNS resolution can influence what content is reached. If non-default DNS-over-HTTPS is used, document the mode and server templates.

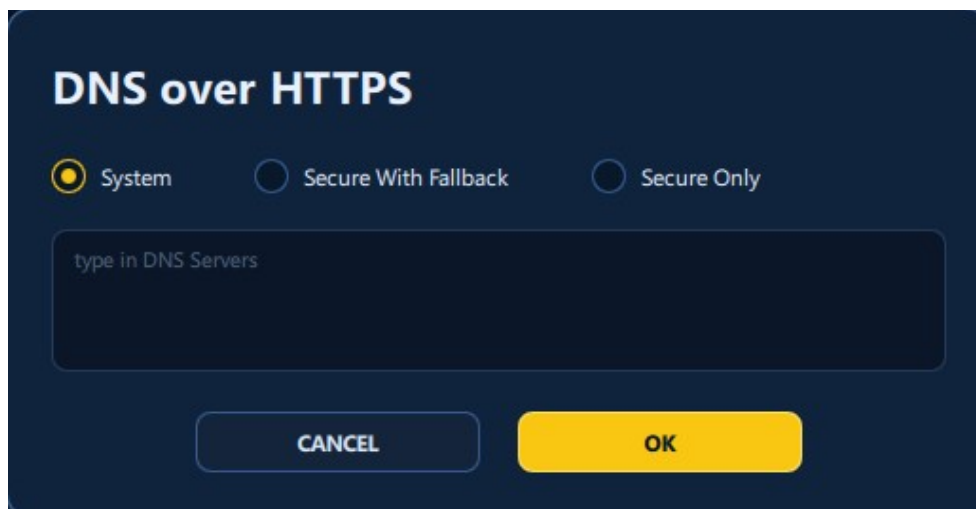


Figure 12. DNS OVER HTTPS: System, Secure With Fallback, Secure Only, and DNS server configuration.

Click **DoH Settings** from the New Acquisition dialog to choose how the browser resolves names. **System** uses the configured system-resolution behavior; **Secure With Fallback** prefers configured secure DNS with a fallback path; **Secure Only** requires secure resolution, which may cause sites to fail to load if the chosen resolver is unavailable.

Enter the DNS server details appropriate to the selected secure mode. Preserve the chosen DNS settings as acquisition context and test resolution before collecting time-sensitive evidence, particularly when routing through a proxy or Tor.

7.9 Video Recording

Video recording captures the acquisition session visually. This can help show investigator actions, page interactions, menus, scrolling, downloads, and evidence capture timing. When enabled, Eviquire starts a recorder and logs recording start and end events. Video duration is stored in acquisition metadata. On some Linux desktop environments, video capture may require X11 rather than Wayland.

Caution: Video recording may capture sensitive information visible on screen, including credentials, unrelated windows, notifications, or personal data. Prepare the workstation before capture.

7.10 Automatic Screenshots

Automatic screenshots may be available as part of acquisition or testing flows. Use them when the workflow requires regular visual preservation without manual intervention. Confirm the resulting image count and disk usage during long sessions.

7.11 Deep Collection Mode

Deep collection is intended to collect additional technical artifacts, such as request/response data or expanded page material, depending on configuration. It can improve technical analysis but can also increase case size and sensitivity. Use deep collection when:

- You need request/response context.
 - You expect dynamic content.
 - You need more than a static screenshot.
 - You are prepared to review larger technical artifacts.
-

8. Evidence Capture Types

8.1 Screenshot Capture

Screenshot capture records the visible state of the browser or acquisition interface. It is useful for preserving a specific page, form, message, listing, file download state, account view, or other visual evidence. Procedure:

1. Navigate to the target content.
2. Confirm the URL and page title are correct.
3. Confirm the user agent and routing settings are correct.
4. Select Screenshot.
5. Wait for Eviquire to save the screenshot.
6. Review the evidence entry after capture.

Artifacts typically include:

- PNG screenshot.
- PDF rendering for standard screenshot captures.
- Evidence summary JSON.
- Chain-of-custody events.
- Evidence report after finalization.
- Evidence archive and final evidence ZIP.

Forensic significance: the screenshot shows what the investigator observed at capture time. The associated metadata and hashes document when it was captured and whether the file later changed.

8.1.1 Reviewing a Screenshot from the Case Manager

Once the acquisition has been finalized, return to **Case Manager**, select the case and acquisition, and click the screenshot record in **EVIDENCE CONTAINED IN THE SELECTED ACQUISITION**. The right **EVIDENCE DETAILS** panel provides the evidence ID, type, URL, investigator, comment, exit network information, start/completion times, archive and summary filenames with SHA2-256 hashes, and available blockchain transaction information. A visual **Evidence Snapshot** appears below these integrity details. Use its zoom controls to inspect the preview. For formal review, inspect the underlying evidence package rather than relying only on the thumbnail.

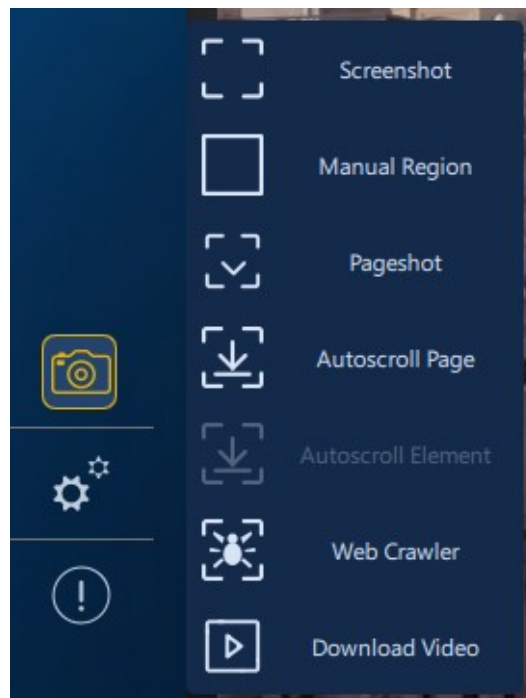


Figure 13. Forensic browser capture menu: Screenshot, Manual Region, PAGESHOT, Autoscroll Page/Element, Web Crawler, and Download Video.

8.1.2 Choosing a Capture Tool

Open the capture menu using the **camera** icon in the browser. Choose **Screenshot** for the current viewport, **Manual Region** for a selected area, **PAGESHOT** for a long-page image sequence, or **Autoscroll Page** for guided full-page traversal. **Autoscroll Element** targets a suitable scrollable page region, such as a comments panel; the control may be disabled when no eligible region is detected.

Web Crawler is available for crawl-oriented capture tasks. **Download Video** launches a media-download workflow for supported online sources. The tool used, target URL, and produced artifacts should be checked in the acquisition record. A region screenshot is intentionally narrower than a complete-page capture; provide surrounding context as appropriate.

8.2 Full-Page Capture

Full-page capture, or pageshot, records a page beyond the currently visible viewport. Eviquire can scroll and capture long pages in segments, then create PDF material from pageshots. Procedure:

1. Navigate to the target page.
2. Wait for content to fully load.
3. Expand dynamic sections if required.
4. Select Full Page or Pageshot.
5. Wait for scrolling and capture to complete.
6. Review generated pageshot images and PDF output.

Artifacts may include:

- Multiple Pageshot PNG files.
- A4 PDF pageshot output.
- Page source if combined with source capture.
- Hash list.
- Evidence archive.
- Evidence report.

Forensic significance: full-page capture preserves content that may not fit on a single screen. It is useful for long social feeds, terms pages, search results, listings, or long-form articles.

Investigator Tip: Avoid interacting with the page during automatic scrolling. Dynamic content can change while capture is in progress.

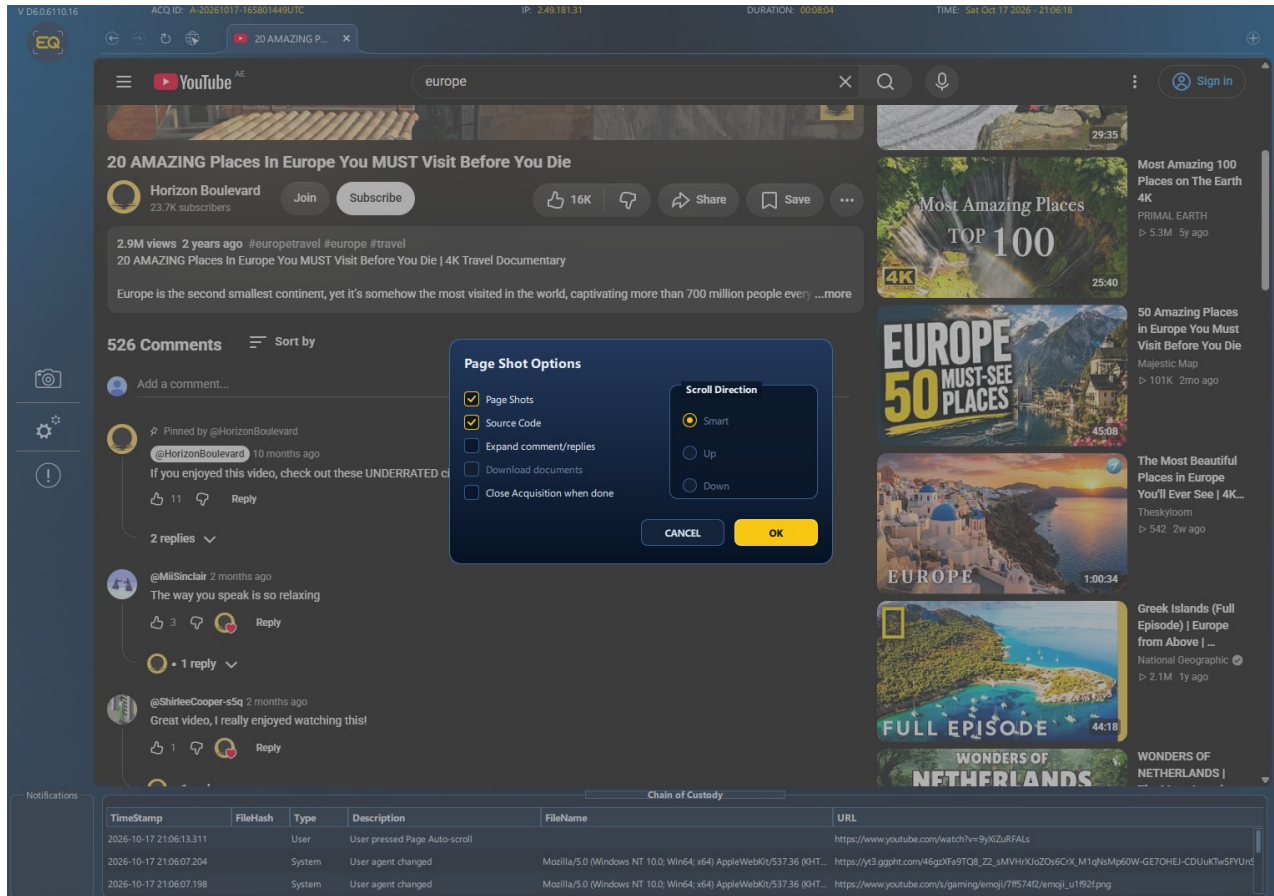


Figure 14. Page Shot Options displayed over a live comments section during an autoscroll workflow.

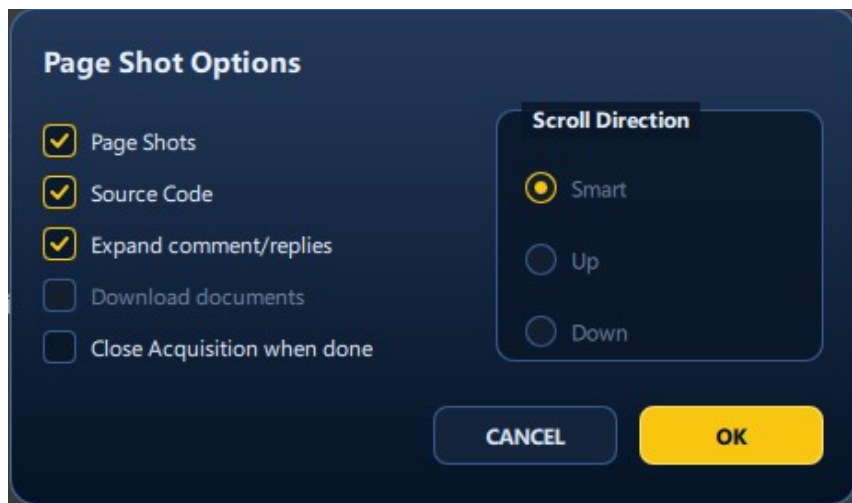


Figure 15. Page Shot Options: visual frames, source, comment/reply expansion, optional downloads, and scroll direction.

8.2.1 Page Shot and Autoscroll Options

Select **Page Shots** to preserve visual segments of the scrolling page, and **Source Code** to preserve associated source material. **Expand comment/replies** attempts supported comment and nested-reply expansion before and during collection; site layouts may affect the outcome. **Download documents** is offered where supported and may be disabled for the selected target.

Under **Scroll Direction**, select **Smart** for automatic directional selection, or **Up / Down** for a defined traversal direction. **Close Acquisition when done** can be selected for an operation that should finish the acquisition automatically after capture. Use this only when no other capture tasks remain.

Version 6 freezes the initial screenshot and supported social metadata before scrolling changes the observed page. Scrollable regions are detected passively, and nested or initially non-overflowing comment containers can be eligible for selection. The browser guards against interrupted operations, target changes, and scroll-response timeouts while preserving successfully captured frames.

Evidence interpretation: Comment counts, replies, recommendations, and feeds can change during capture. Treat the source's behavior and the Chain of Custody as part of the evidence context; automatic expansion does not guarantee exhaustive retrieval of all comments on a changing website.

8.3 Page Source Capture

Page source capture saves HTML or extracted page source text. It provides technical context behind the visual page.

Procedure:

1. Navigate to the target page.
2. Confirm the desired state is loaded.
3. Select Page Source.
4. Wait for source capture to complete.
5. Review the source artifact and summary.

Artifacts may include:

- Page source text file.
- Summary JSON.
- Chain-of-custody event.
- Evidence report.
- Evidence package.

Forensic significance: source capture can show links, metadata, embedded scripts, hidden content, references, and markup not visible in screenshots.

8.4 Combined Visual And Source Capture

Combined capture preserves both what the page looked like and what source or full-page data was available. This is often the strongest web evidence workflow because it combines human-readable visual evidence with technical context. Procedure:

1. Navigate to the page.
2. Confirm content loaded.
3. Select combined visual and source capture or configure full-page capture to include source.
4. Wait for screenshots, source extraction, finalization, and packaging.
5. Review both visual and source artifacts.

Forensic significance: combined capture reduces the risk that a screenshot alone will be challenged as incomplete or that source alone will be difficult for non-technical reviewers to understand.

8.5 File Download Capture

File download capture records files downloaded during acquisition. A user-initiated download becomes an evidence item. Eviquire can also collect files downloaded as part of another evidence item. Procedure:

1. Navigate to the download source.
2. Confirm URL, page context, and file identity.
3. Initiate the download.

4. Allow Eviquire to save the file in the evidence directory.
5. Wait for the download event and summary.
6. Review the evidence package.

Artifacts may include:

- Downloaded file.
- Screenshot of download context.
- Page source around the download workflow.
- Summary JSON.
- Evidence report.
- Evidence ZIP.

Forensic significance: downloaded files are hashed and linked to the URL and acquisition context. The screenshot helps show the circumstances under which the file was obtained.

8.5.1 Downloading Online Video

The **Download Video** action shown in the browser capture menu can collect supported online media as an evidence item. Version 6 records richer companion metadata where available, including the video title, description, subtitle information, original filename, and hashes. These metadata fields are included only when available from the observed source and the chosen download workflow.

Wait for the download process and evidence packaging to complete. The notification area and Chain of Custody provide progress and completion context. Video and subtitle files are separate artifacts: preserve both their original bytes and their recorded hashes, and never substitute a converted review copy for original evidence.

8.6 Email Acquisition

Mail acquisition captures email evidence from configured mail accounts or servers. It can preserve message files and mail interface screenshots. Procedure:

1. Create a mail acquisition.
2. Enter server, port, protocol, user, and password.
3. Confirm collection scope.
4. Start the acquisition.
5. Select or search mail items.
6. Capture selected messages.
7. Review message evidence and reports.

Artifacts may include:

- .eml files.
- HTML mail renderings where generated.
- Mail screenshots.
- Sender, subject, server ID, and email timestamp in event descriptions.
- Evidence summaries.
- Evidence reports.
- Evidence packages.

Forensic significance: email acquisition preserves message content and server-related identifiers while linking messages to the case and acquisition.

Warning: Mailboxes can contain privileged, private, or out-of-scope messages. Confirm legal scope before acquiring mail evidence.

8.7 Mobile Evidence Acquisition

Mobile acquisition workflows preserve evidence associated with a connected or configured mobile device. Depending on deployment, this may include screenshots, device display capture, or mobile-specific evidence packages. Procedure:

1. Connect or select the mobile device.
2. Confirm device ID.
3. Start a mobile acquisition.
4. Capture screenshots or supported artifacts.
5. Review mobile evidence packages.

Artifacts may include:

- Mobile screenshots.
- Device video recording where enabled.
- Device ID metadata.
- Evidence summaries.
- Chain-of-custody events.

Forensic significance: mobile acquisition associates evidence with a device identifier and preserves visual state from the mobile source.

8.8 Video Capture

Video capture records the acquisition session or device display. It is primarily a contextual artifact, not a replacement for individual evidence packages. Procedure:

1. Enable video recording before starting acquisition.
2. Start the acquisition.
3. Wait for recording started confirmation.
4. Perform capture actions.
5. End the session.
6. Confirm recording ended and duration was recorded.

Artifacts may include:

- MP4 recording files.
- Video log.
- Video duration metadata.
- Recording start and end chain-of-custody events.

Forensic significance: video helps explain the workflow, user actions, and timing of events.

8.9 WHOIS Capture

WHOIS capture records registration information for a domain involved in web evidence. It is typically collected during web evidence finalization when enabled. Artifacts include:

- WHOIS text file.
- Chain-of-custody event.
- Summary and package inclusion when part of evidence.

Forensic significance: WHOIS can help identify domain registration context, although WHOIS data may be privacy-protected, incomplete, or changed over time.

8.10 Robots.txt Capture

Eviquire can request and save `/robots.txt` from the target host. Forensic significance: robots.txt can show crawling preferences and site structure hints at capture time. It is not proof of content authenticity, but it provides context about the host.

8.11 Sitemap Capture

Eviquire can request and save `/sitemap.xml` from the target host. Forensic significance: sitemap data can show declared site structure, important URLs, and update hints. It can assist later analysis of how a page fits within a site.

8.12 Certificates Capture

Certificate capture records trusted root certificate information from the acquisition environment. On Windows this uses the system root certificate store. On Linux it can extract certificate subject and email details from the CA certificate bundle. Forensic significance: certificate data helps document the trust environment used during browsing. This can matter when reviewing HTTPS interception, enterprise trust roots, or certificate-related disputes.

8.13 System Info Capture

System info capture records information about the acquisition workstation. On Windows it uses `systeminfo`. On Linux it records operating system, kernel, host, CPU, memory, block devices, PCI/USB devices, IP addresses, and disk usage. Forensic significance: system information documents the acquisition environment. It helps explain the tool context and can support repeatability.

9. Chain Of Custody

9.1 What Gets Logged

Eviquire logs events that explain acquisition activity. Events include:

- Session welcome and version.
- Acquisition ID, name, and type.
- Investigator identity.
- Tor and proxy information.
- Start time.
- Video recording state.
- Network traffic state.
- Automatic tests state.
- WHOIS/system/certificate/deep collection state.
- DNS-over-HTTPS settings.
- User navigation.
- Browser page-load events.
- Screenshots.
- Page source saves.
- Downloads.
- Evidence summary saves.
- Evidence archive saves.
- Report saves.
- Timestamp events.

- Recording start and end.
- Session closed.
- Errors or cancellation events.

Each event can include a file and hash when a file is produced.

9.2 UTC Timestamps

Events use UTC timestamps. UTC is important because it avoids ambiguity across time zones, daylight saving changes, and geographically distributed teams. When presenting evidence, explain whether displayed times are UTC or local time. Eviquire chain-of-custody records should be treated as UTC unless otherwise noted.

9.3 Investigator Identity

Investigator identity appears in session metadata, reports, summaries, and chain-of-custody context. Before starting an acquisition, verify that the correct operator identity is configured. For multi-operator investigations, use separate acquisitions or clearly document handoffs.

9.4 URLs And Page Context

For web events, Eviquire records URLs, domain information, page title, and user agent where available. This helps reviewers understand what page was captured and under what browser identity. For split-view captures, Eviquire can record left and right URL/user-agent/page-title context.

9.5 Hashes In Chain Of Custody

When an event creates or references a file, the log can include the file's SHA2-256 hash. This hash supports later verification. If a reviewer extracts a file and computes SHA2-256, the value should match the recorded value unless the file was altered.

9.6 Reports In Chain Of Custody

Report creation is also logged. This matters because reports are generated artifacts and should be traceable. Evidence PDF and JSON reports, acquisition reports, and case reports are all part of the final deliverable structure.

9.7 How Logs Are Used In Court Or Formal Review

Chain-of-custody logs can help answer common evidentiary questions:

- Who performed the acquisition?
- When did the session start and end?
- What was captured?
- What URL was visited?
- Was the page loaded successfully?
- Was the evidence file hashed?
- Were reports generated?
- Did the session close normally?
- Were there errors?
- Were proxy, Tor, video, network, or DNS settings active?

Logs do not by themselves prove truth of web content. They document the tool's actions and handling process. They are strongest when combined with reports, hashes, timestamps, source files, screenshots, and investigator notes.

9.8 Best Practices

- Confirm investigator identity before capture.
- Use descriptive acquisition names.
- Keep acquisition comments factual.

- Avoid unrelated browsing during acquisition.
 - Do not manually move or rename files inside active acquisition folders.
 - Review logs after capture.
 - Preserve original packages.
 - Export copies for review rather than modifying originals.
-

10. Integrity And Verification

10.1 MD5

MD5 is a legacy hash algorithm. Eviquire records MD5 for compatibility with tools and workflows that still display or compare MD5. MD5 should not be relied on alone for modern forensic integrity decisions because collision attacks are known. Use MD5 as a secondary identifier only.

10.2 SHA2-256

SHA2-256 is a modern cryptographic hash and the primary integrity value used in many forensic workflows. Eviquire displays SHA2-256 in reports, summaries, chain-of-custody logs, and hash lists. When verifying exported files, SHA2-256 should be the primary comparison value.

10.3 SHA3-256

SHA3-256 is another modern cryptographic hash algorithm. Eviquire records SHA3-256 alongside SHA2-256. Having both values provides additional assurance and compatibility with different verification policies.

10.4 Hash Comparisons

Eviquire performs hash comparisons at evidence packaging time. It compares files in the evidence directory against the file hashes recorded in the database when the evidence was created. If the SHA2-256 value matches, the hash list records matching status. If it differs, the hash list records a mismatch. Hash mismatch can indicate:

- File modification after capture.
- Incomplete write before hashing.
- Packaging race condition.
- Manual file tampering.
- Tool or filesystem error.

Treat hash mismatches seriously. Review logs, source files, timestamps, and file modification dates.

10.5 Evidence Hash Lists

Evidence hash lists are tab-separated text files. They record:

- Path and filename.
- Created time UTC.
- Last modified time UTC.
- File size.
- Integrity check result.
- Acquisition hash timestamp UTC.
- SHA2-256 at acquisition time.
- SHA3-256 at acquisition time.
- MD5 at acquisition time.
- Packaging hash timestamp UTC.

- SHA2-256 at packaging.
- SHA3-256 at packaging.
- MD5 at packaging.

These files are valuable for technical reviewers because they show both file metadata and integrity comparison state.

10.6 Acquisition And Case Hash Lists

Acquisition and case hash lists record file trees and hashes at broader scope. They provide a manifest of the package contents before archiving and finalization. Use acquisition and case hash lists when verifying:

- All expected evidence packages are present.
- Reports and summaries exist.
- Database files are included.
- File sizes and timestamps are consistent.
- No unexpected files appear.

10.7 Timestamp Authority Files

Eviquire creates timestamp request and response files:

- `.tsq`: timestamp request.
- `.tsr`: timestamp response.

These files are generated for summary JSON files. A timestamp response can be validated using compatible timestamp verification tools and the relevant TSA certificate chain. The timestamp proves that a specific summary hash existed at the timestamping time. Because the summary describes the archive and report hashes, it acts as the package integrity statement.

10.8 Blockchain Anchoring

Blockchain anchoring submits a summary hash to an external blockchain-related service or workflow. The resulting metadata is stored with the package. Use blockchain anchoring as an additional proof layer. It should be interpreted together with:

- Summary JSON.
- Hash values.
- Timestamp authority response.
- Chain-of-custody logs.
- Reports.
- Original package file.

10.8.1 Understanding the Celo Reference in the Details Pane

In the illustrated Version 6 interface, the **BlockChain Transaction ID** field contains a **Submitted Hash** and a **Celo** hexadecimal transaction identifier with copy and external-link controls. The submitted hash refers to the recorded integrity summary; the hexadecimal string identifies the blockchain transaction carrying the anchoring reference. Use the displayed copy control when documenting the transaction rather than retyping a long value.

Interpretation: A blockchain transaction establishes an external reference for an anchored hash. It does not directly certify who authored a page, whether a page's claim is correct, or whether a court will admit the evidence. For complete validation, verify the archive and summary hashes, the signed TSA response when present, and the transaction metadata together.

10.9 Verifying Exported Evidence

To verify an evidence package:

1. Preserve the original ZIP.
2. Work on a copy.

3. Extract the evidence ZIP.
4. Locate the summary JSON.
5. Read the file information section.
6. Compute SHA2-256 of the evidence archive and report.
7. Compare values to the summary JSON.
8. Validate .tsq and .tsr if timestamp verification is required.
9. Review blockchain raw metadata if present.
10. Extract the raw evidence archive if file-level review is needed.
11. Review the evidence hash list.
12. Compare file-level hashes where required.

Investigator Tip: Always record the hash of the exported ZIP before transferring it. That export hash is separate from the internal evidence hashes and helps prove the transferred container was not altered.

10.10 Graphical Acquisition and Case Integrity Verification

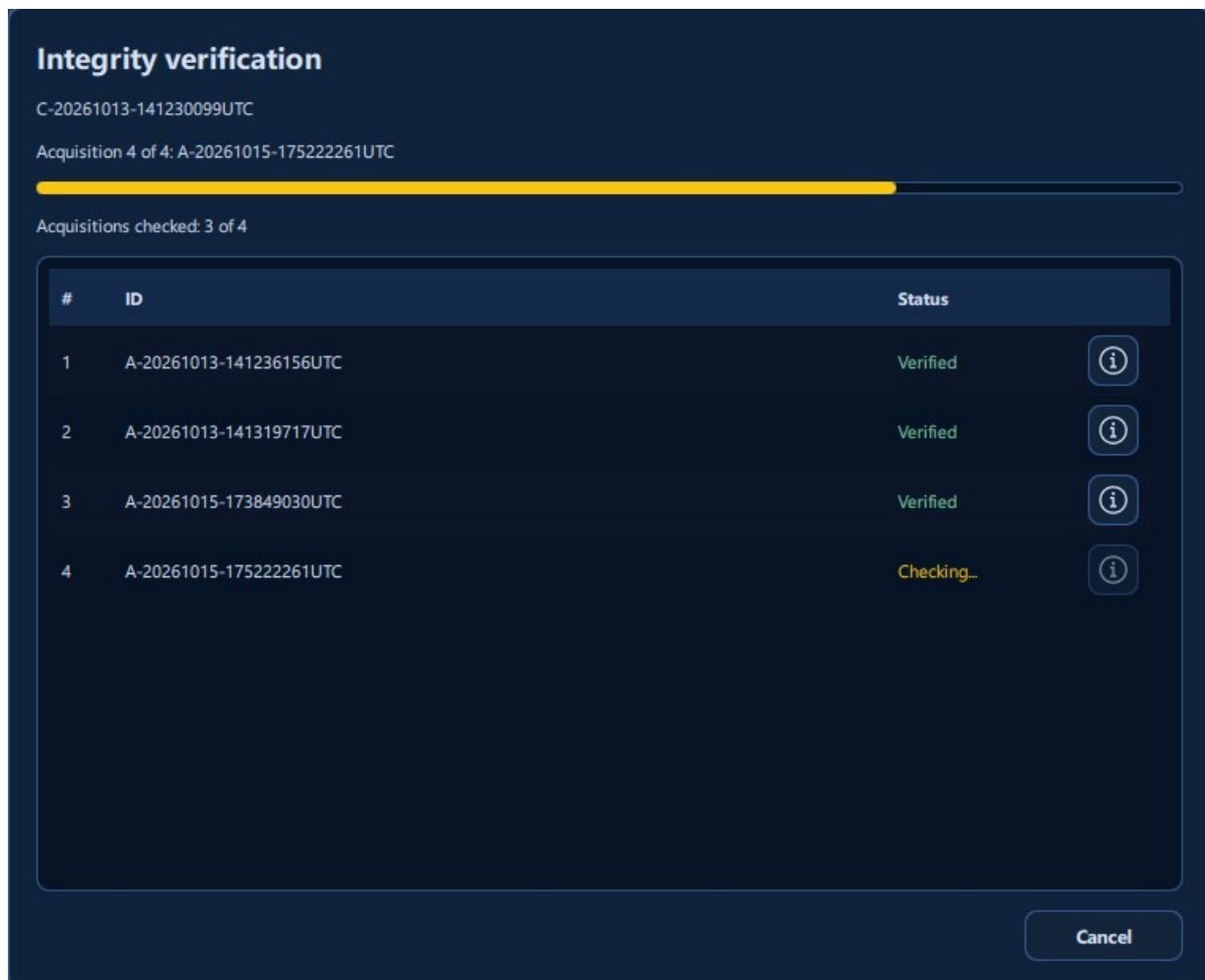


Figure 16. Case-wide integrity verification checks each acquisition and records its status.

From the Case Manager case context menu, select **Verify all acquisitions**. Eviquire displays the case identifier, acquisition-by-acquisition progress, and results such as **Verified** and **Checking....** The information button beside a row opens the corresponding detailed acquisition verification result.

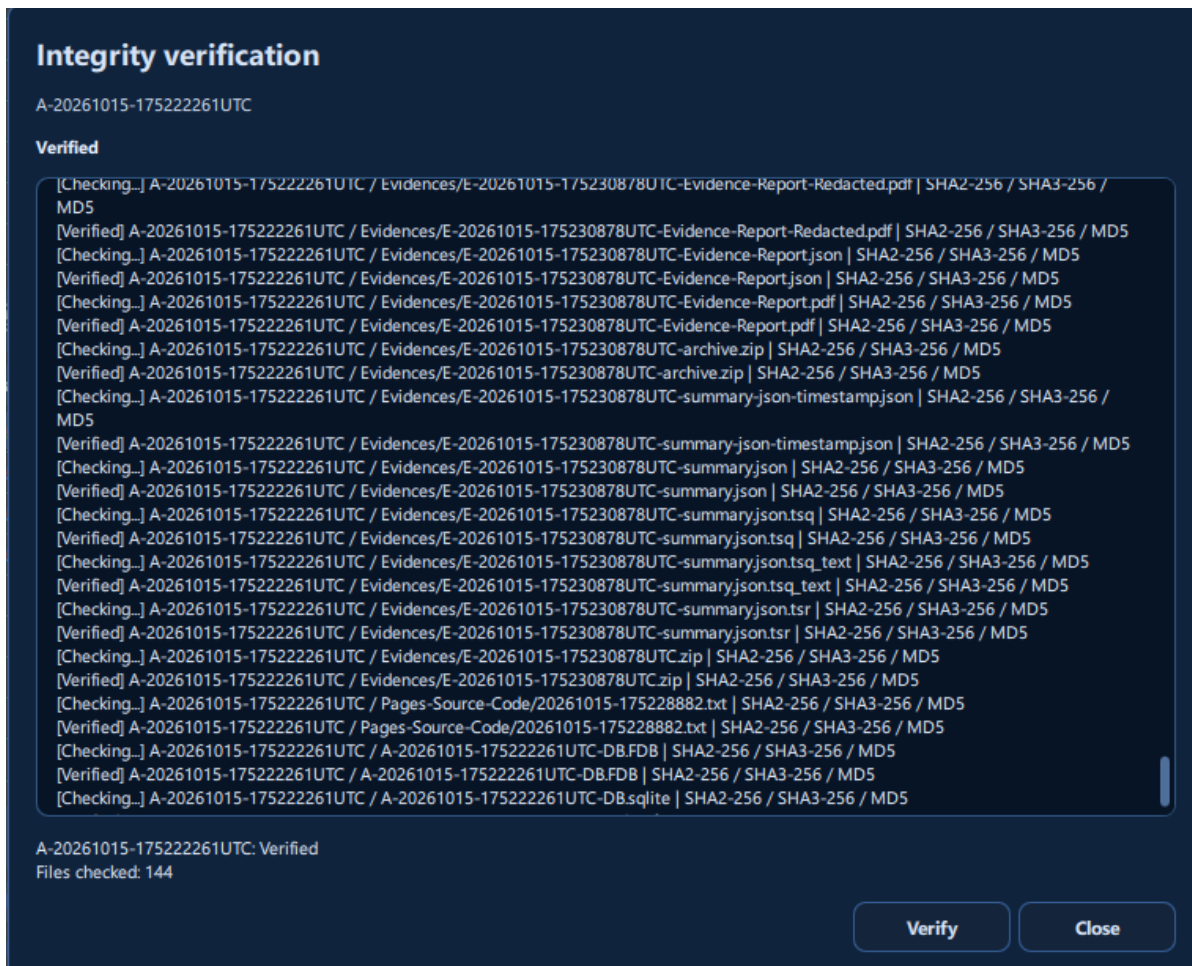


Figure 17. Acquisition integrity verification: file-by-file hashes, result lines, and files checked.

Acquisition verification compares original file inventory and recorded **SHA2-256**, **SHA3-256**, and **MD5** values as applicable. The result view shows file paths, per-file states, and a count of files checked. In the illustrated example, an acquisition is marked **Verified** after 144 files were checked. These figures describe only the illustrated sample acquisition.

1. Select the case or acquisition to verify. Run the verification operation appropriate to the review scope.
2. Monitor the progress display, then inspect any non-verified, unreadable, or missing-file result before relying on the package.
3. Open detailed findings and record the verification result in the investigative review record.
4. Preserve the original case or acquisition files unchanged. Any analysis, extraction, or retry should use approved review procedures.

Verification meaning: A successful hash comparison indicates that the verified files match their recorded digest values. It does not establish the truth of third-party web content or resolve questions of collection authority or evidential weight.

11. Reports

11.1 Evidence Reports

Evidence reports describe a single evidence item. They are created during evidence finalization and usually include:

- Evidence ID.
- Acquisition ID.
- Case ID.
- Evidence type.

- Capture URL or device/mail context.
- Investigator identity.
- File information.
- Hash information.
- Archive details.
- Report details.
- Timestamp or blockchain references where available.

Evidence reports are useful for exhibit-level review. They allow a reviewer to understand one item without reading the entire acquisition package.

11.2 Acquisition Reports

Acquisition reports describe a full acquisition session. They include session metadata, acquisition options, evidence lists, archive information, and relevant technical context. Acquisition reports are useful when explaining the entire collection event. They connect individual evidence items to the session in which they were captured.

11.3 Case Reports

Case reports summarize the entire case. They may include case metadata, acquisition list, closure information, package information, and integrity metadata. Case reports are useful for handoff to legal teams, compliance teams, supervisors, or external reviewers.

11.4 PDF Reports

PDF reports are intended for human reading, printing, and disclosure. They are suitable for:

- Investigator review.
- Attorney review.
- Court exhibits.
- Compliance documentation.
- Executive summaries.

PDF reports should be preserved with their hashes and summary JSON.

11.5 JSON Reports

JSON reports are structured machine-readable reports. They are suitable for:

- Automated validation.
- Ingestion into review platforms.
- Technical analysis.
- Audit workflows.
- Long-term archival with metadata.

Do not discard JSON reports simply because a PDF exists. The JSON report may contain structure that is easier to validate programmatically.

11.6 Executive Summaries

An executive summary should explain the acquisition in plain language:

- What matter the evidence relates to.
- When collection occurred.
- Who performed collection.
- What was collected.

- Which major settings were used.
- Whether acquisition completed successfully.
- Where the final package is stored.

Eviquire reports provide technical data. Investigators may still need to prepare a separate case narrative for legal or management audiences.

11.7 Technical Appendices

Technical appendices should preserve details that may be too detailed for an executive summary:

- Hash lists.
- Network capture metadata.
- Browser profile notes.
- TShark version and hash.
- TLS key log references.
- Timestamp validation results.
- Blockchain anchoring results.
- Known errors or limitations.

11.8 Local Evidence Reports and Branding (Version 6)

Version 6 creates **local PDF and JSON evidence reports** that capture available evidence context, investigator identity, comments, filenames, file hashes, and supported visual previews. This is independent of the optional **Save each Evidence Report Online** selection, which governs online availability for eligible reports.

Configure local evidence report branding separately from acquisition report branding where supported. You can preview reports inside Eviquire, save a preview, or open it in an external PDF viewer. The local evidence report footer includes page counts and evidence/acquisition identifiers; redacted report versions omit those identifiers.

Preserve original PDF and JSON report files, the associated summary, and their hashes. A locally created PDF report is explanatory documentation; it should be reviewed together with the raw evidence rather than treated as a replacement for source artifacts.

12. Reviewing Evidence and the Acquisition Review Tool

12.1 Opening Packages

Review workflows depend on whether you are opening an evidence, acquisition, or case package. General procedure:

1. Work on a copy of the package.
2. Verify the ZIP hash before extraction.
3. Extract to a controlled review folder.
4. Locate the summary JSON.
5. Locate the PDF report.
6. Review chain-of-custody logs.
7. Extract raw archives only when needed.
8. Preserve original package unchanged.

12.1.1 Using Acquisition Details in the Manager

Select an acquisition row in the middle table. The **ACQUISITION DETAILS** pane appears on the right; it exposes identifiers, session context, captured artifact integrity data, and a record of the enabled acquisition settings.

Import Case

Description

Description

ACQUISITION DETAILS

Acquisition ID: A-20261012-162459455UTC
Acquisition Name:
Acquisition Type: Web Acquisition
Investigator: Eviquire Demo
Exit Country: 2.49.181.31:AE
TOR: Disabled
Started at: 12 Oct 2026 - 20:24:59
Completed at: 12 Oct 2026 - 20:25:31
User Agent:
DNS Over HTTPS: System

Package File Name: A-20261012-162459455UTC-archive.zip
SHA2_256 File Hash: 25400fc7c4595014ac7f6b906fa3c414d291503a8a26d40198b68a5380b3129d

Summary File Name: A-20261012-162459455UTC-summary.json
SHA2_256 File Hash: ffb6534539b3916ccfd77534ae57233039e70b3a615f340bc76b0e58e7bd6aa3

BlockChain Transaction ID:
Submitted Hash: ffb6534539b3916ccfd77534ae57233039e70b3a615f340bc76b0e58e7bd6aa3
Celo   0x6508688d1c06579105a860a686bd1676c9cc770ee035c020e102ffd337259ec1

Video Recording: True
System Network Traffic Dump (PCAP): True
Application Network Traffic Dump (HAR): False
Chromium Network Audit (NetLog): False
Save each Evidence Report Online: False
Realtime Evidence Timestamp: True
Automatic Tests: True
Fetch WHOIS Data: False
Save System Info: False
Save Certificates: False
Advanced Resources Collection: True
Advanced Cookies Collection: False
Automatic Cookie Consent: Disabled
Content Language: en-US

Description:

Figure 18. An acquisition's details include the user agent, proxy/Tor context, start/end times, report/archive hashes, blockchain reference, and acquisition options.

The panel shown includes **Acquisition ID**, **Acquisition Name**, **Acquisition Type**, **Investigator**, **Exit Country/IP**, **TOR**, **Started at**, **Completed at**, **User Agent**, and **DNS Over HTTPS**. Beneath this, the manager displays **Package File Name**, **SHA2_256 File Hash**, **Summary File Name**, and the summary hash. It also lists the **BlockChain Transaction ID** information (including **Submitted Hash** and **Celo**) and enumerates the session's options with True/False or named values. Example options visible include Video Recording, PCAP, HAR, NetLog, realtime timestamps, WHOIS, advanced resources, cookie collection, automatic consent, and content language.

This makes the manager useful for confirming that the actual session settings match the procedure used. For technical evidence review, open the reports and package data alongside this summary.

12.1.2 Using Evidence Details in the Manager

EVIDENCE DETAILS

Evidence ID: E-20261012-162506812UTC
Evidence Type: Screenshot
Evidence Url: https://www.timeanddate.com/worldclock/fullscreen.html?n=4757
Investigator: Eviquire Demo
Comment:
Exit Country/IP: 2.49.181.31:AE
Started at: 12 Oct 2026 - 20:24:59
Completed at: 12 Oct 2026 - 20:25:31

Package File Name: E-20261012-162506812UTC-archive.zip
SHA2_256 File Hash: 0150d81f44508231cb043e5a41ad6a8c7f329c0e16d0edacaf4b41563bba153

Summary File Name: E-20261012-162506812UTC-summary.json
SHA2_256 File Hash: ae1415b3355f16056014f8e7086192c2c041a002d35211d748a8f569e976fe52

BlockChain Transaction ID:
Submitted Hash: ae1415b3355f16056014f8e7086192c2c041a002d35211d748a8f569e976fe52

Celo 0xf29198673f34c176512cde05d5ce3d9c4bd03ae97de5884b5148b80504a0f4ee

Evidence Snapshot:

Evidence Snapshot Preview:

Figure 19. Evidence Details presents the selected evidence item's identity, integrity fields, blockchain information, and screenshot preview.

Select an evidence row in the lower table. The right-side panel updates to **EVIDENCE DETAILS** and displays **Evidence ID**, **Evidence Type**, **Evidence Url**, **Investigator**, **Comment**, **Exit Country/IP**, **Started at**, and **Completed at**. It also shows the evidence package name and hash, the summary file name and hash, blockchain anchoring information when present, and **Evidence Snapshot**. The snapshot toolbar contains zoom and fit-style controls.

The **Evidence URL** may be long; use the displayed copy icon when available. A preview is for rapid identification. Evidence integrity should be evaluated against the original exported files, their recorded hashes, and the generated report.

12.2 Viewing Screenshots

Screenshots may be viewed directly as PNG files or through PDF reports. When reviewing screenshots:

- Confirm the evidence ID.

- Confirm the URL or device context.
- Confirm timestamp.
- Confirm file hash.
- Confirm screenshot dimensions and visible content.
- Review related page source if available.

If a screenshot is used as an exhibit, include the report and summary hash references.

12.2.1 Evidence Comments and Review Downloads

Evidence comments were introduced in the Version 5 review workflows and are included in acquisition reporting. Use factual, precise comments to document observations and limitations, keeping interpretations separate from the captured content. Version 5 also introduced screenshot download controls in **Acquisition Review**. Use these tools to obtain working copies for review; maintain the archived original as the evidentiary source.

12.3 Reviewing Page Source

Page source files are text files. Review them with a text editor that does not modify files automatically. Avoid tools that rewrite line endings, reformat HTML, or save metadata. When reviewing source:

- Confirm file hash first.
- Use read-only mode where possible.
- Search for URLs, scripts, metadata, and hidden fields.
- Compare with screenshot where relevant.
- Document any analysis performed.

12.4 Checking Downloads

Downloaded files should be reviewed carefully:

- Verify file hash.
- Confirm download URL.
- Confirm file name and size.
- Scan in a controlled malware-safe environment if needed.
- Do not open suspicious executables on a production workstation.
- Preserve the original downloaded file.

If the download is malware or suspected malware, use isolated forensic malware-handling procedures.

12.5 Reading Logs

Review logs in this order:

1. Chain-of-custody text log.
2. Chain-of-custody HTML log.
3. Acquisition database records if technical review is required.
4. Browser net log for web/network issues.
5. TShark log for packet capture issues.
6. Application debug logs for troubleshooting.

Logs tell the procedural story. Reports summarize it. Hashes verify it.

12.6 Validating Hashes

To validate a file:

1. Locate the expected SHA2-256 value in the summary, report, or hash list.

2. Compute SHA2-256 of the file using a trusted tool.
3. Compare values exactly.
4. Record the validation tool, version, date, and result.

If values differ, stop and investigate. Do not continue treating the file as verified until the discrepancy is explained.

12.7 Viewing Metadata

Metadata appears in several places:

- Summary JSON.
- Evidence report JSON.
- Acquisition report JSON.
- Case report JSON.
- Database.
- Hash lists.
- File system timestamps.

Summary JSON is the primary metadata record for package integrity. Reports provide human-readable and structured context. Hash lists provide file-tree-level integrity information.

12.8 Opening the Acquisition Review Tool

The Acquisition Review Tool is the read-only examination workspace for a completed acquisition. It brings together the session package, captured evidence, video, reports, Chain of Custody, downloads, browser resources, cookie events and TLS certificate observations. It is designed to let reviewers follow an acquisition from its recorded environment to the individual artifacts without altering the originals.

1. Open Case Manager and select the case containing the acquisition.
2. Select the acquisition in the middle ACQUISITIONS CONTAINED IN THE SELECTED CASE table.
3. In ACQUISITION DETAILS, use the review/view control (eye icon) to open the Acquisition Review Tool.
4. Confirm the Acquisition ID, acquisition time range and user displayed in the header before examining artifacts.
5. Choose a top navigation tab. Select items within a tab to display their previews or technical details.

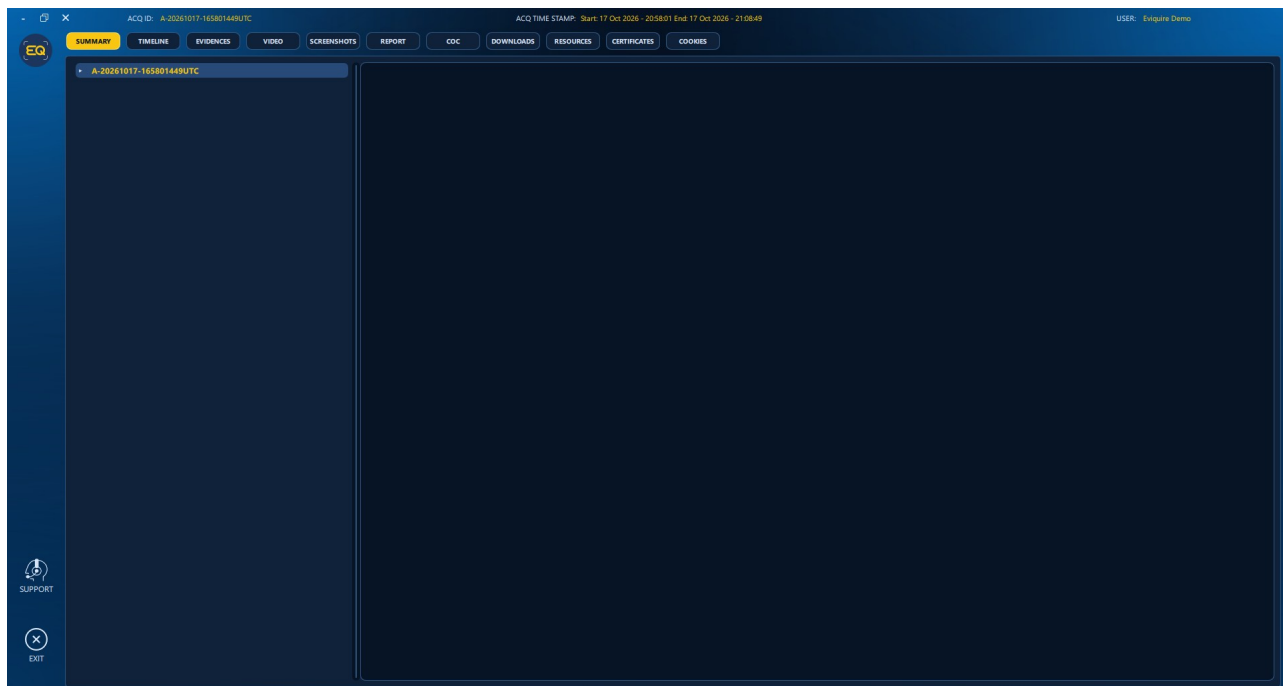


Figure 23. The Acquisition Review Tool opens with the acquisition header, tab navigation, file tree and preview workspace.

The active tab is highlighted in yellow. The header identifies the acquisition and investigator, and shows its start/end timestamps. The left sidebar provides Support and Exit. Displayed session times may reflect the configured time zone; raw Chain of Custody and timeline event timestamps retain UTC references.

Review principle: A visual preview is a convenience for inspection; the original archived artifact, corresponding file hashes, reports and custody records remain the evidence of record.

12.9 Review Workspace: Tab Reference

The review window provides the following primary areas. The content visible in a specific acquisition depends on the evidence captured and the options enabled during that acquisition.

Tab	Primary purpose
SUMMARY	Browse the acquisition archive file tree and inspect included files.
TIMELINE	Explore time-correlated cookie, TLS, evidence and video events.
EVIDENCES	Select an evidence item, review its file inventory and preview supported formats.
VIDEO	Play the acquisition-session recording when captured.
SCREENSHOTS	Browse screenshot, region-shot and pageshot images.
REPORT	View the acquisition report PDF.
COC	Read the acquisition Chain of Custody as a structured log.
DOWNLOADS	Review collected download media and accompanying metadata.
RESOURCES	Examine browser resource requests and application HAR data.
CERTIFICATES	Review observed TLS certificates and connection context.
COOKIES	Review detailed browser cookies and lifecycle events when collected.

12.10 SUMMARY: Acquisition File Explorer

SUMMARY presents an expandable tree rooted at the acquisition ID. Folders and files reflect actual contents of the acquisition archive; a reviewer can expand a folder and select an included file to inspect the supported preview on the right.

The Artifacts-Network branch may contain Application-HAR data (HAR file and companion JSON summaries), Local-TShark captures (PCAPNG, logs and summaries), and a PCAPNG TLS key log when captured. Application HAR is browser-observed HTTP evidence and is distinct from host packet capture. Files should not be inferred to exist merely because a branch is shown in an example screenshot.

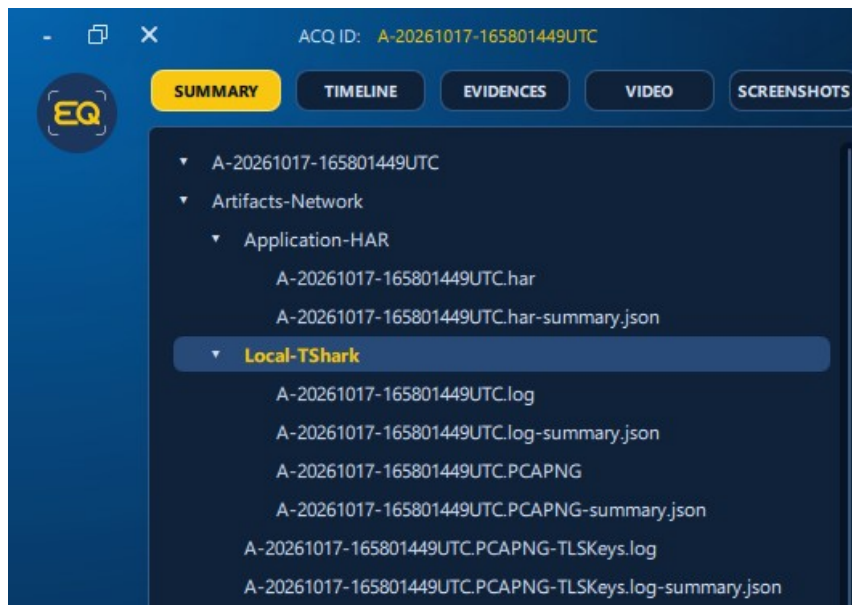


Figure 24. The SUMMARY network branch distinguishes Application-HAR, Local-TShark PCAPNG/logs, and TLS key material.

The Browser-Profile branch may contain Cache, IndexedDB, Local Storage, Service Worker, Session Storage, Cookies, History, Trust Tokens and other Chromium state. Treat profile files as sensitive session artifacts; they can contain authentication-related data and should be inspected in a controlled environment.

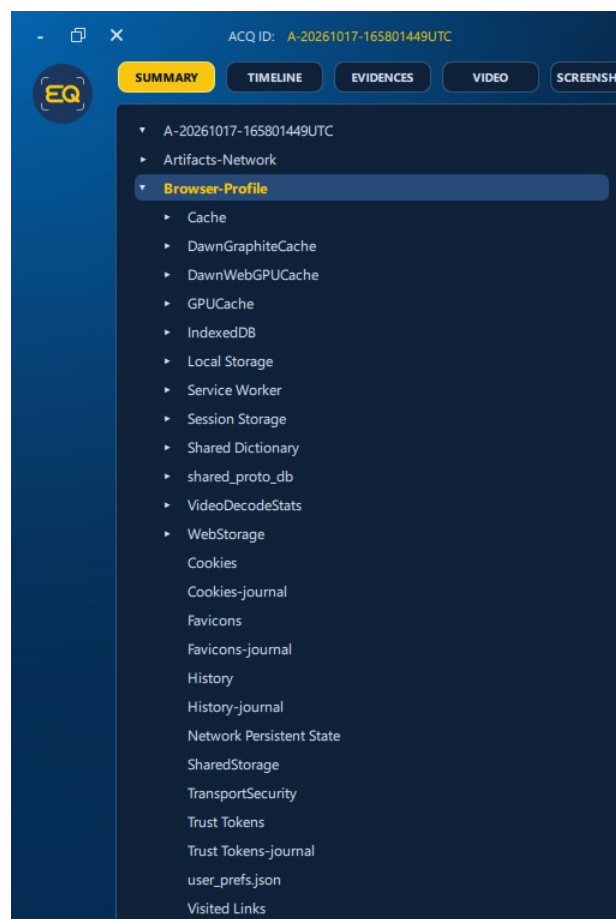


Figure 25. The archived Chromium browser profile preserves browser storage and state folders for technical review.

Additional top-level entries can include Browser-Profile-split, Chain of Custody, Evidences, Pages-Source-Code, JSON cookie/TLS observation timelines, certificate and cookie databases, an acquisition database, hash lists, reports, summary JSON, TSA files, video, system information and certificates. Some SQLite and Firebird-related files visible in the archive are application evidence records; use non-destructive tools and review copies if database analysis is required.

12.11 SUMMARY: Reading Archived Files

Selecting a file in SUMMARY opens an appropriate supported preview. This is useful for correlating a report or evidence item with the actual artifact path and for assessing what the archive contains before exporting or conducting independent verification.

12.11.1 Chain of Custody Files in the Archive

The Chain of Custody directory contains a human-readable HTML activity log and a plain-text User-Activity log. The HTML view presents labeled timestamp, event type and description columns; the text view is suited to independent parsing, search and forensic workflows. These are alternative renderings of custody data rather than separate acquisition sessions.

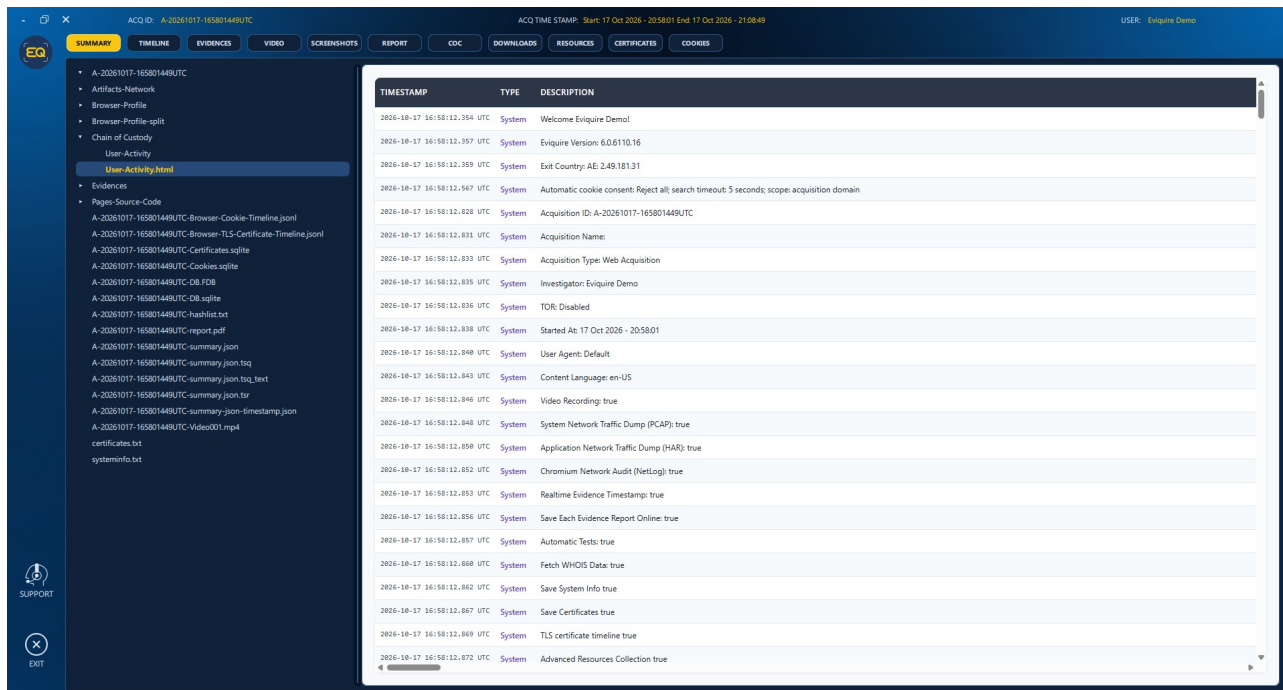


Figure 26. An archived User-Activity.html log displayed in the SUMMARY file viewer.

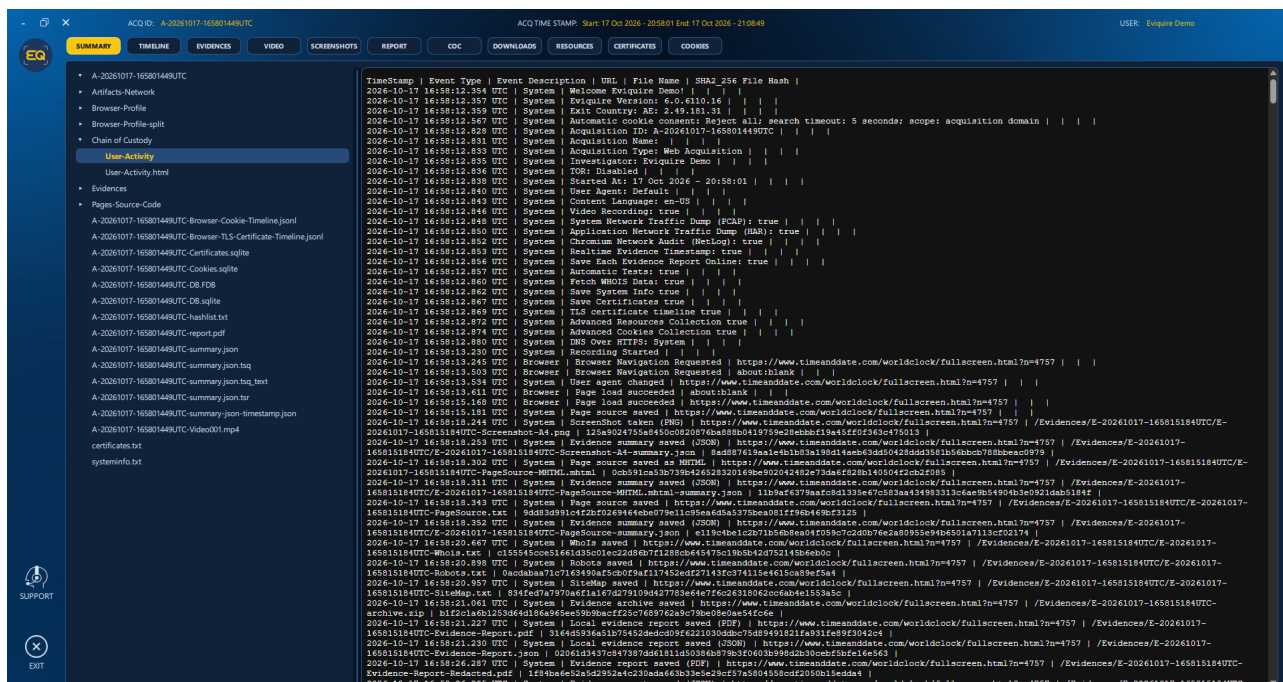


Figure 27. The text User-Activity log preserves timestamped event rows with URL, filename and file-hash columns.

12.11.2 PDF Evidence and Acquisition Reports

Evidence packages may contain local evidence report PDFs as well as JSON, redacted report variants, summaries and timestamp receipts. Select a report PDF to use the integrated PDF viewer with page thumbnails, page navigation, zoom, save and print controls. The report identifies its case/acquisition lineage, evidence details, capture context and recorded integrity values.

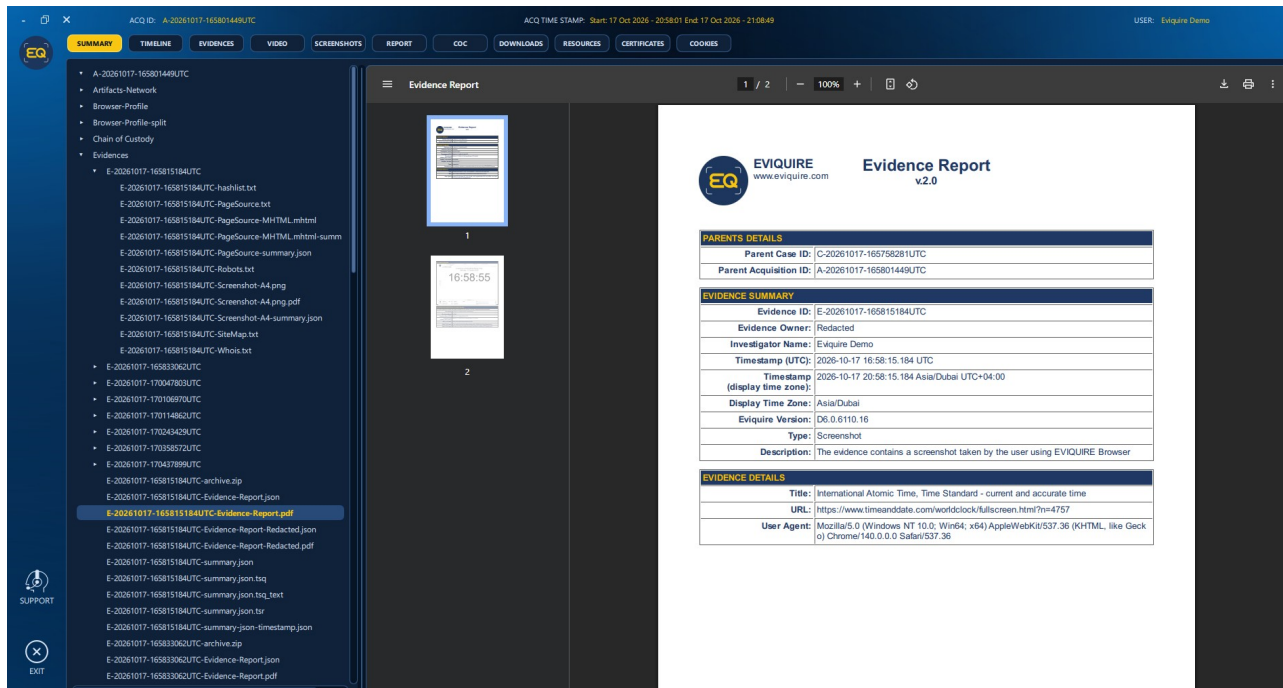


Figure 28. An Evidence Report PDF opened from the evidence-file inventory, with related package files visible in the tree.

Acquisition-level reports can also be selected from the SUMMARY root, allowing the reviewer to verify session settings and the acquisition package information directly in the same workspace.

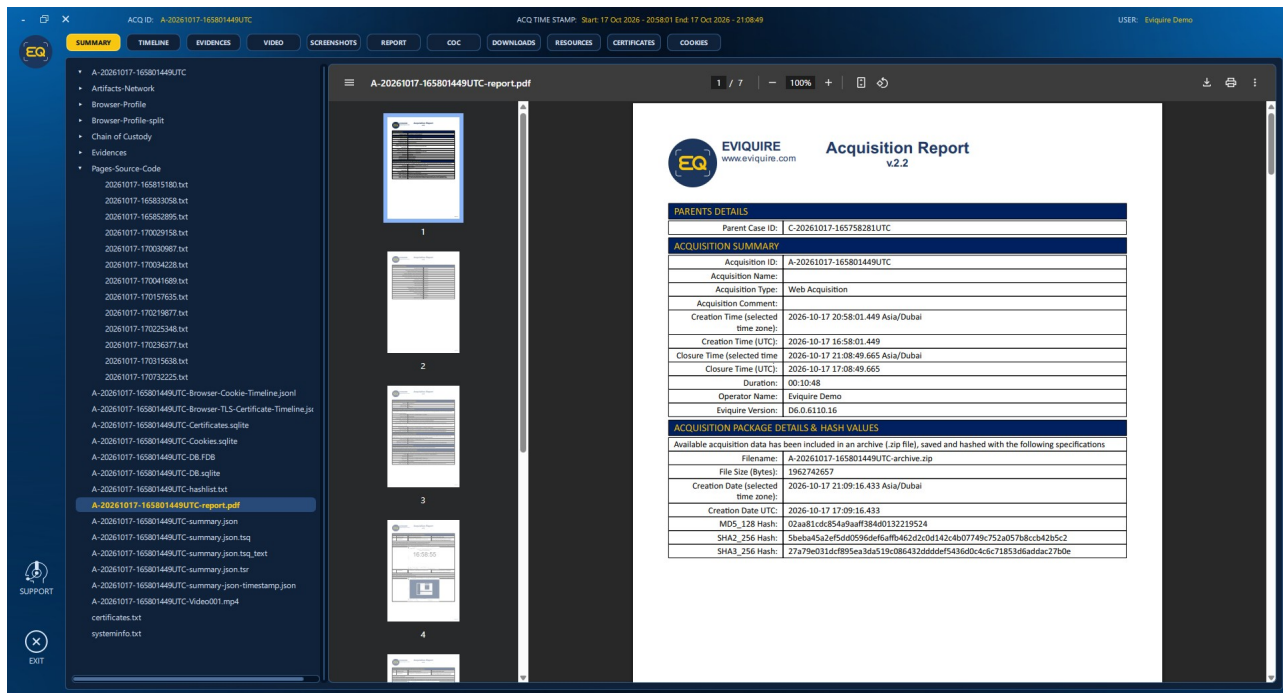


Figure 29. The acquisition-level PDF report opened as an archived file in SUMMARY.

12.11.3 Page Source and Structured Metadata

Text and MHTML source captures should be interpreted in the context of the corresponding captured page and timestamp. The browser rendering, raw source, DOM-related material and resource traces can differ because modern pages update after loading. In the viewer, source files are readable without changing the underlying archive.

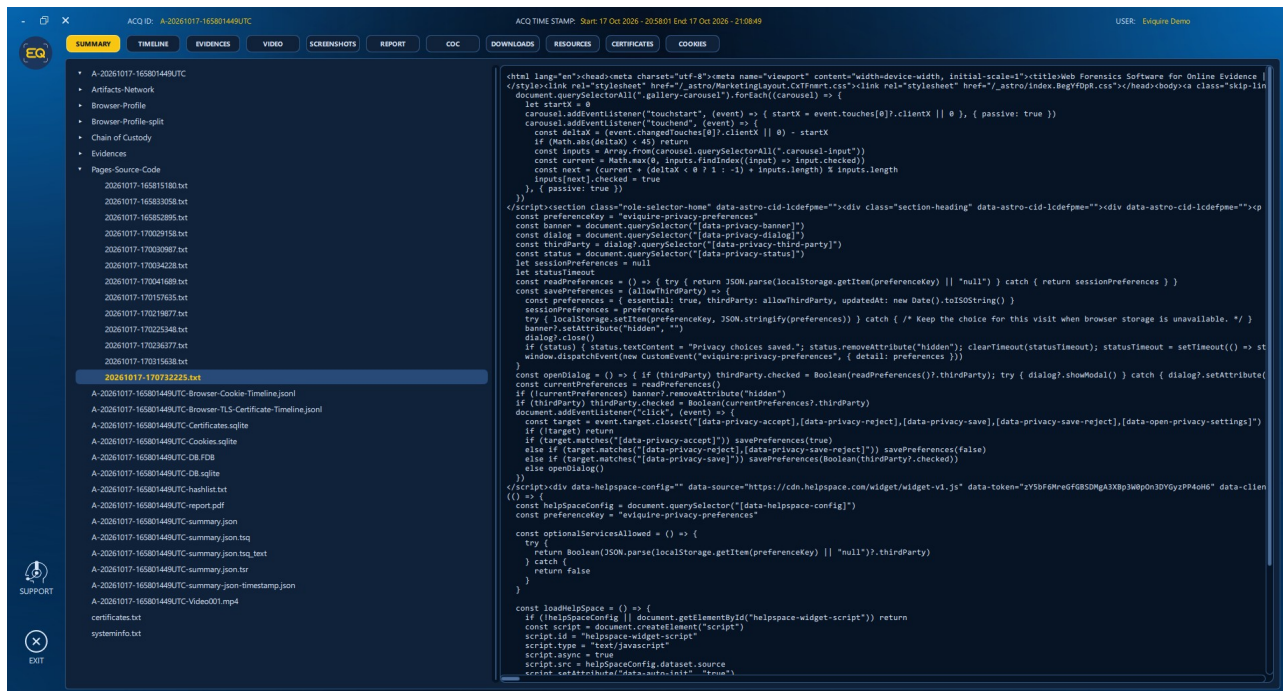


Figure 30. Plain-text page-source artifact shown in the SUMMARY viewer.

JSON files preserve structured technical details, including downloaded media summaries, identifiers, original filenames, URLs, timestamps, hash values and collection diagnostics where recorded. The preview can truncate large files for usability: the visible warning “Preview limited to the first 1 MiB. The original file is unchanged” refers only to the preview, not to acquisition truncation.

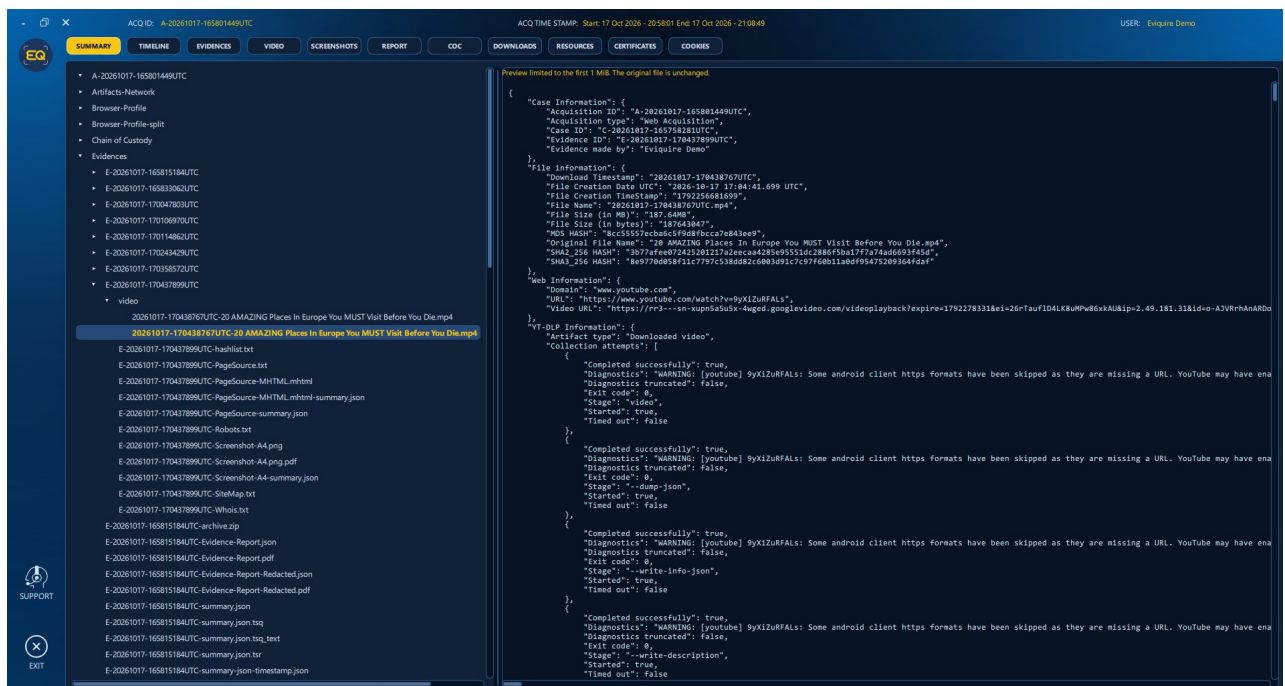


Figure 31. JSON metadata preview; the 1 MiB display limit does not truncate or alter the original file.

12.11.4 Hash Lists and File Inventories

An acquisition hash list provides a file-by-file integrity manifest, including stored paths, timestamps, sizes and recorded hashes. It helps explain which files belong to the acquisition and supports independent integrity validation. The screenshot shows acquisition-time hashes and related metadata; use the full file and verification tool for a definitive comparison.

Full Path & Filename	Created Time UTC	Last Modified Time UTC	File Size Bytes	Acquisition Hash Timestamp UTC	SHA2-256 At the Time of Acquisition (from DB)	SHA3-256 At the Time of Acq.
Artifacts-Network/Application-HAR/A-20261017-165801449UTC-Har	2026-10-17 17:08:41.773	2026-10-17 17:08:41.773	234586576	2026-10-17 17:08:41.773	9762a5fe3a38e4e0	4884a
Artifacts-Network/Application-HAR/A-20261017-165801449UTC-Har-summary.json	2026-10-17 17:08:41.773	2026-10-17 17:08:41.773	234586576	2026-10-17 17:08:41.773	9762a5fe3a38e4e0	4884a
Artifacts-Network/Local-TShare/A-20261017-165801449UTC-PCAPNG	2026-10-17 16:58:18.817	2026-10-17 17:08:48.946	347802288	2026-10-17 17:08:48.946	181054071a88970	01280d
Artifacts-Network/Local-TShare/A-20261017-165801449UTC-PCAPNG-summary.json	2026-10-17 17:08:53.007	2026-10-17 17:08:53.007	574	2026-10-17 17:08:53.007	01280d	01280d
Artifacts-Network/Local-TShare/A-20261017-165801449UTC-log	2026-10-17 16:58:18.908	2026-10-17 16:58:18.908	0	2026-10-17 16:58:18.908	0380ca4294fc1c148	0380ca4294fc1c148
Artifacts-Network/Local-TShare/A-20261017-165801449UTC-log-summary.json	2026-10-17 17:08:53.009	2026-10-17 17:08:53.009	561	2026-10-17 17:08:53.009	0380ca4294fc1c148	0380ca4294fc1c148
Artifacts-Network/A-20261017-165801449UTC-PCAPNG-TLSKeys.log	2026-10-17 16:58:12.909	2026-10-17 17:08:28.349	23378	2026-10-17 17:08:28.349	0380ca4294fc1c148	0380ca4294fc1c148
Artifacts-Network/A-20261017-165801449UTC-PCAPNG-TLSKeys.log-summary.json	2026-10-17 17:08:54.884	2026-10-17 17:08:54.884	581	2026-10-17 17:08:54.884	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/0	2026-10-17 16:58:13.563	2026-10-17 17:08:51.642	4086	2026-10-17 17:08:51.642	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/1	2026-10-17 16:58:13.562	2026-10-17 17:08:49.790	532480	2026-10-17 17:08:49.790	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/2	2026-10-17 16:58:13.563	2026-10-17 17:08:51.642	1855768	2026-10-17 17:08:51.642	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/3	2026-10-17 16:58:13.564	2026-10-17 17:08:51.642	8306480	2026-10-17 17:08:51.642	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000001	2026-10-17 16:58:15.115	2026-10-17 16:58:15.115	18920	2026-10-17 17:09:04.384	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000002	2026-10-17 16:58:12.412	2026-10-17 16:58:12.412	6915	2026-10-17 17:09:04.385	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000003	2026-10-17 16:58:12.478	2026-10-17 16:58:12.478	109122	2026-10-17 17:09:04.386	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000004	2026-10-17 16:58:12.499	2026-10-17 16:58:12.499	104095	2026-10-17 17:09:04.387	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000005	2026-10-17 16:58:12.508	2026-10-17 16:58:12.508	108126	2026-10-17 17:09:04.388	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000006	2026-10-17 16:58:12.652	2026-10-17 16:58:12.652	19057	2026-10-17 17:09:04.389	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000007	2026-10-17 16:58:12.655	2026-10-17 16:58:12.655	17187	2026-10-17 17:09:04.390	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000008	2026-10-17 16:58:12.674	2026-10-17 16:58:12.674	108184	2026-10-17 17:09:04.391	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000009	2026-10-17 16:58:12.676	2026-10-17 16:58:12.676	29276	2026-10-17 17:09:04.392	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000010	2026-10-17 16:58:12.706	2026-10-17 16:58:12.706	20784	2026-10-17 17:09:04.393	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000011	2026-10-17 16:58:12.737	2026-10-17 16:58:12.737	81529	2026-10-17 17:09:04.394	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000012	2026-10-17 16:58:12.736	2026-10-17 16:58:12.736	189722	2026-10-17 17:09:04.395	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000013	2026-10-17 16:58:12.955	2026-10-17 16:58:12.955	146687	2026-10-17 17:09:04.396	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000014	2026-10-17 16:58:13.235	2026-10-17 16:58:13.235	2899	2026-10-17 17:09:04.397	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000015	2026-10-17 16:58:13.170	2026-10-17 16:58:13.170	24262	2026-10-17 17:09:04.398	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000016	2026-10-17 16:58:13.174	2026-10-17 16:58:13.174	36196	2026-10-17 17:09:04.399	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000017	2026-10-17 16:58:13.189	2026-10-17 16:58:13.189	62133	2026-10-17 17:09:04.400	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000018	2026-10-17 16:58:13.252	2026-10-17 16:58:13.252	136138	2026-10-17 17:09:04.401	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000019	2026-10-17 16:58:13.272	2026-10-17 16:58:13.272	18788	2026-10-17 17:09:04.402	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000020	2026-10-17 16:58:13.272	2026-10-17 16:58:13.272	21697	2026-10-17 17:09:04.403	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000021	2026-10-17 17:08:28.122	2026-10-17 17:08:28.122	36185	2026-10-17 17:09:04.404	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000022	2026-10-17 17:08:28.124	2026-10-17 17:08:28.124	45067	2026-10-17 17:09:04.405	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000023	2026-10-17 17:08:28.207	2026-10-17 17:08:28.207	189122	2026-10-17 17:09:04.406	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000024	2026-10-17 17:08:28.216	2026-10-17 17:08:28.216	74322	2026-10-17 17:09:04.407	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000025	2026-10-17 17:08:28.227	2026-10-17 17:08:28.227	109722	2026-10-17 17:09:04.408	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000026	2026-10-17 17:08:28.235	2026-10-17 17:08:28.235	209165	2026-10-17 17:09:04.409	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000027	2026-10-17 17:08:28.251	2026-10-17 17:08:28.251	45858	2026-10-17 17:09:04.410	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000028	2026-10-17 17:08:28.260	2026-10-17 17:08:28.260	65332	2026-10-17 17:09:04.411	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000029	2026-10-17 17:08:28.276	2026-10-17 17:08:28.276	41193	2026-10-17 17:09:04.412	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000030	2026-10-17 17:08:28.336	2026-10-17 17:08:28.336	97119	2026-10-17 17:09:04.413	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000031	2026-10-17 17:08:28.357	2026-10-17 17:08:28.357	284423	2026-10-17 17:09:04.414	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000032	2026-10-17 17:08:28.389	2026-10-17 17:08:28.389	153933	2026-10-17 17:09:04.415	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000033	2026-10-17 17:08:28.407	2026-10-17 17:08:28.407	389955	2026-10-17 17:09:04.416	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000034	2026-10-17 17:08:28.409	2026-10-17 17:08:28.409	177426	2026-10-17 17:09:04.417	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000035	2026-10-17 17:08:28.782	2026-10-17 17:08:28.782	61385	2026-10-17 17:09:04.418	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000036	2026-10-17 17:08:28.780	2026-10-17 17:08:28.780	29084	2026-10-17 17:09:04.419	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000037	2026-10-17 17:08:28.800	2026-10-17 17:08:28.800	108184	2026-10-17 17:09:04.420	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000038	2026-10-17 17:08:28.824	2026-10-17 17:08:28.824	69320	2026-10-17 17:09:04.421	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000039	2026-10-17 17:08:28.834	2026-10-17 17:08:28.834	108126	2026-10-17 17:09:04.422	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000040	2026-10-17 17:08:30.814	2026-10-17 17:08:30.814	29258	2026-10-17 17:09:04.423	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000041	2026-10-17 17:08:30.925	2026-10-17 17:08:30.925	18178	2026-10-17 17:09:04.424	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000042	2026-10-17 17:08:31.617	2026-10-17 17:08:31.617	95808	2026-10-17 17:09:04.425	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000043	2026-10-17 17:08:31.728	2026-10-17 17:08:31.728	23324	2026-10-17 17:09:04.426	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000044	2026-10-17 17:08:31.744	2026-10-17 17:08:31.744	22157	2026-10-17 17:09:04.427	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000045	2026-10-17 17:08:31.791	2026-10-17 17:08:31.791	44892	2026-10-17 17:09:04.428	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000046	2026-10-17 17:08:31.908	2026-10-17 17:08:31.908	19816	2026-10-17 17:09:04.429	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000047	2026-10-17 17:08:31.922	2026-10-17 17:08:31.922	28238	2026-10-17 17:09:04.430	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000048	2026-10-17 17:08:31.927	2026-10-17 17:08:31.927	17488	2026-10-17 17:09:04.431	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000049	2026-10-17 17:08:31.952	2026-10-17 17:08:31.952	58776	2026-10-17 17:09:04.432	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000050	2026-10-17 17:08:34.164	2026-10-17 17:08:34.164	13322	2026-10-17 17:09:04.433	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000051	2026-10-17 17:08:34.147	2026-10-17 17:08:34.147	194589	2026-10-17 17:09:04.434	0380ca4294fc1c148	0380ca4294fc1c148
Browser-Profile/Cache/Cache_Data/f/000052	2026-10-17 17:08:34.147	2026-10-17 17:08:34.147	27508	2026-10-17 17:09:04.435	0380ca4294fc1c148	0380ca4294fc1c148

Figure 32. An acquisition hash list displayed as original text in SUMMARY, showing file paths and recorded integrity metadata.

Important: The file viewer is not a substitute for integrity verification. Compare the original exported file against the corresponding recorded SHA2-256 and SHA3-256 values using an approved independent tool.

12.12 TIMELINE: Unified Chronological Review

TIMELINE places distinct acquisition events on a shared UTC-oriented axis. The controls shown include Cookies, TLS certificates, Evidence and Video. Event markers can represent groups of nearby events, and the timeline supports mouse-wheel zoom and drag-to-pan. A selected marker displays the event list; selecting an eligible individual event opens its details and linked technical context.

1. Open TIMELINE and confirm the displayed acquisition time range.
2. Use the category controls to focus on cookies, TLS certificates, evidence, or video activity.
3. Zoom into a period of interest and pan to the desired capture interval.
4. Select an event cluster, then a specific event, to inspect its observed UTC time, type and linked artifact.
5. Correlate selected events with the COC log and original source records before drawing conclusions.

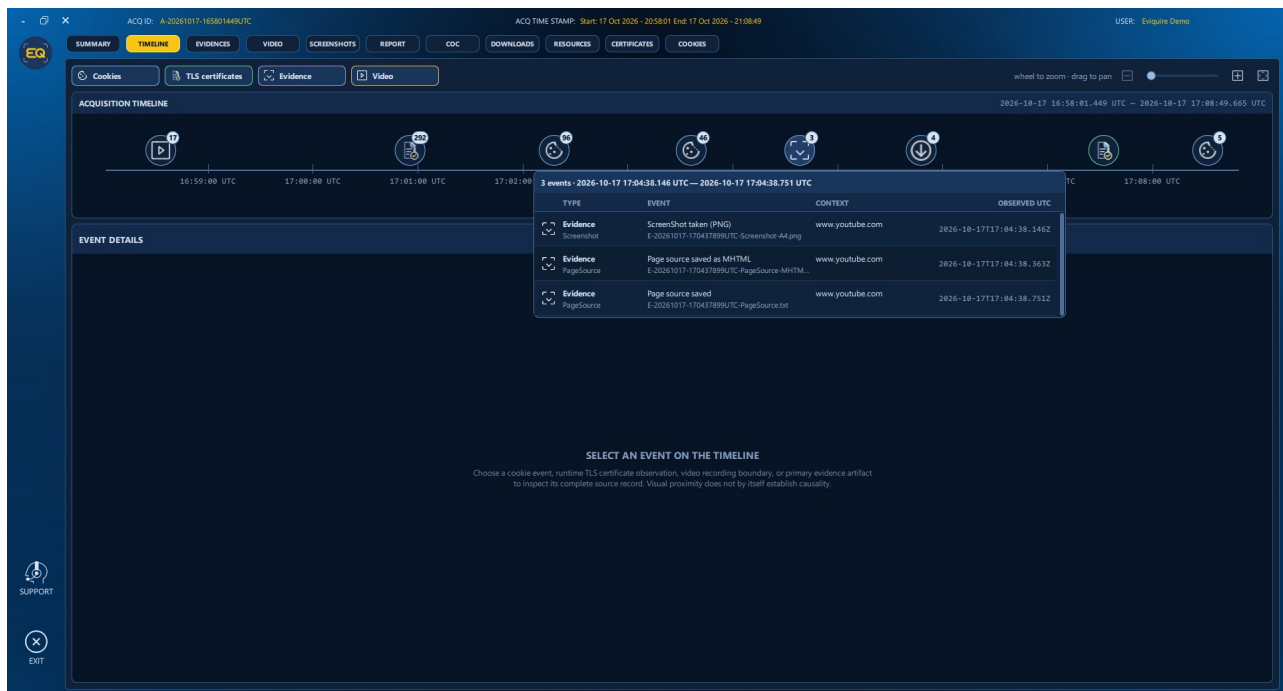


Figure 33. Unified TIMELINE with event clusters, category selectors, UTC ticks and event-list overlay.

Nearby timeline markers establish temporal proximity only. For example, a TLS observation close to an evidence screenshot does not, by itself, prove the page originated from the certificate holder. Interpret sequence and causality using the full recorded context.

12.13 EVIDENCES: Individual Evidence Review

The EVIDENCES tab lists captured evidence records with their evidence IDs, timestamps, types and target domains. When a record is selected, the FILES panel displays its constituent files, types and sizes. Selecting a supported file produces a read-only preview and may expose zoom/fit or file download controls.

1. Open EVIDENCES and select an evidence ID matching the item under review.
2. Confirm its capture time, evidence type and recorded URL or domain.
3. Review the FILES list; distinguish the raw archive, report, summary, source, screenshot and timestamp artifacts.
4. Open the visual capture or report for interpretation, then validate required file hashes against the actual package.

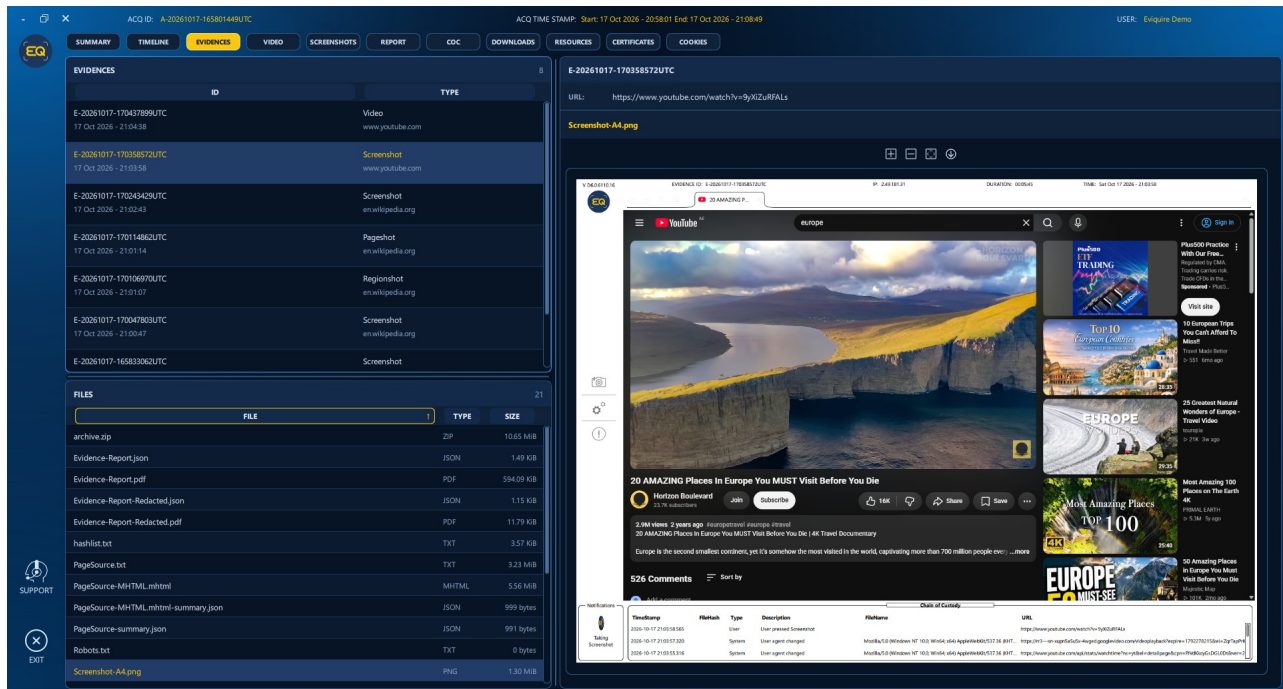


Figure 34. The EVIDENCES tab combines an evidence inventory, per-item file list and screenshot preview.

A single evidence item can include both visual and technical material, such as a screenshot and its source, WHOIS data, robots.txt, sitemap or summary JSON. A visual preview shows the recorded page state; it should not be mistaken for a live re-visit to the original website.

12.14 VIDEO: Session Recording

VIDEO displays the recorded acquisition session when Video Recording was enabled. Its playback controls allow pause/play, scrubbing through the recording, elapsed/total time inspection and volume adjustment. The recording may show Eviquire controls, visible user actions, page interactions and the acquisition Chain of Custody footer.

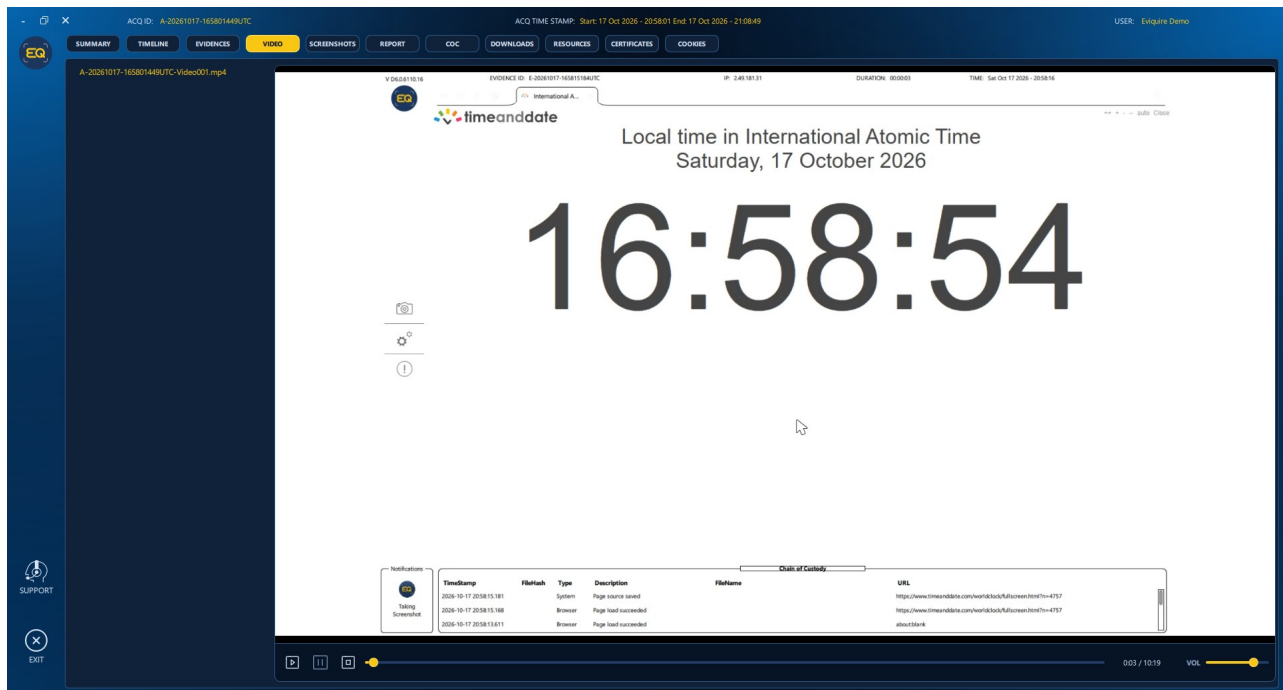


Figure 35. Session video review with seek bar, playback controls, elapsed time and volume.

Session video is distinct from an externally downloaded website video. The session recording documents operator actions over time; downloaded media is a separately collected artifact with its own source information, filename and hashes. The viewer supports direct playback of supported AV1 and HEVC media without rewriting the original evidence file.

12.15 SCREENSHOTS: Visual Evidence Gallery

SCREENSHOTS lists still-image artifacts, including standard screenshots, region shots and the sequential PageShot frames that form a longer-page capture. Select an entry to display the image, then use the available controls to zoom, fit the image, or save the original file for controlled examination.

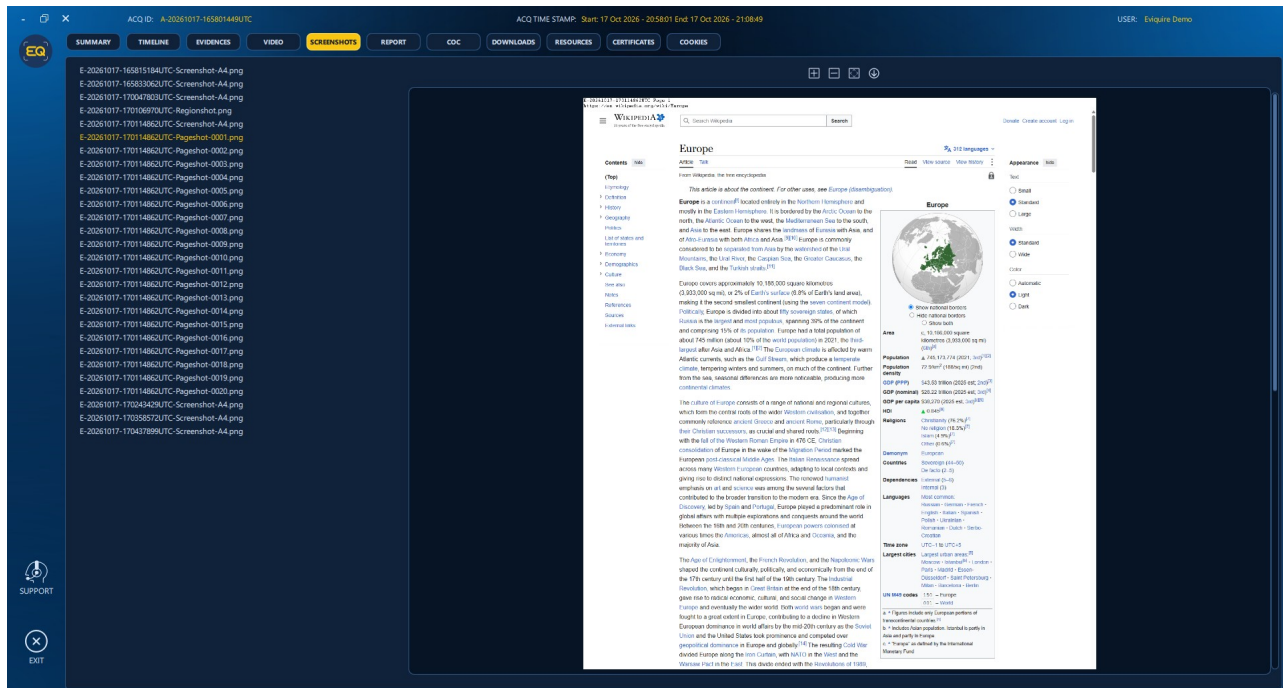


Figure 36. The SCREENSHOTS tab lists source image files, including successful PageShot frame numbers.

Sequential PageShot images document different positions of a longer web page; they are not necessarily interchangeable with the final compiled PDF. Verify that the sequence is complete when continuity matters, and document any browser content that changed during automatic scrolling.

12.16 REPORT: Acquisition-Level Documentation

REPORT opens the generated acquisition PDF report in the integrated viewer. Typical entries include the parent case ID, acquisition ID, operator, acquisition type, session times (with UTC and selected display time zone), software version, archive filename, package size and cryptographic hashes. Use the page navigator, zoom, save or print tools as needed.

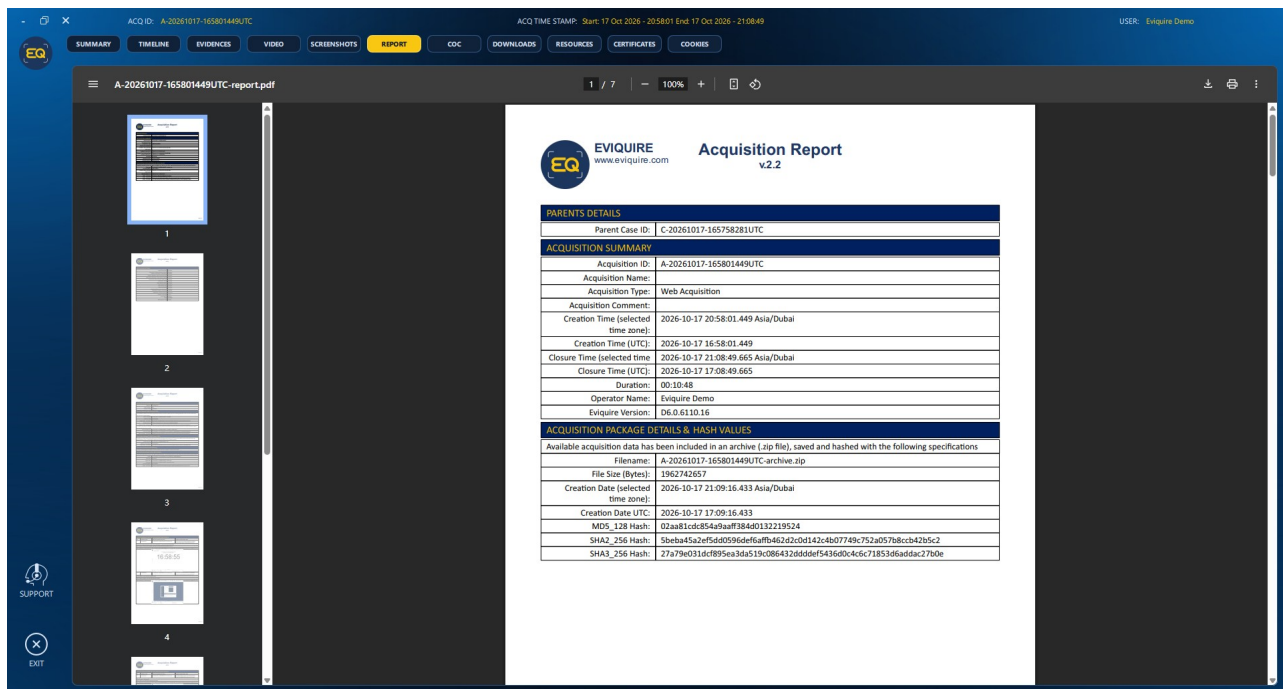


Figure 37. The REPORT tab displays the acquisition PDF report, with its parent case, session summary and archive integrity values.

Evidence reports and acquisition reports serve different scopes. Use the evidence report to describe a particular capture; use the acquisition report to describe the full session and technical conditions under which evidence was acquired. Preserve both the PDF and its structured JSON and summary records when exporting.

12.17 COC: Chain of Custody

COC presents a structured activity record with UTC timestamp, event type, description and file information. It includes session initialization and selected options, navigation, evidence creation, file saves, downloads, timestamp operations, recording and closure events. The displayed log is valuable for reconstructing what the software observed and what the operator did.

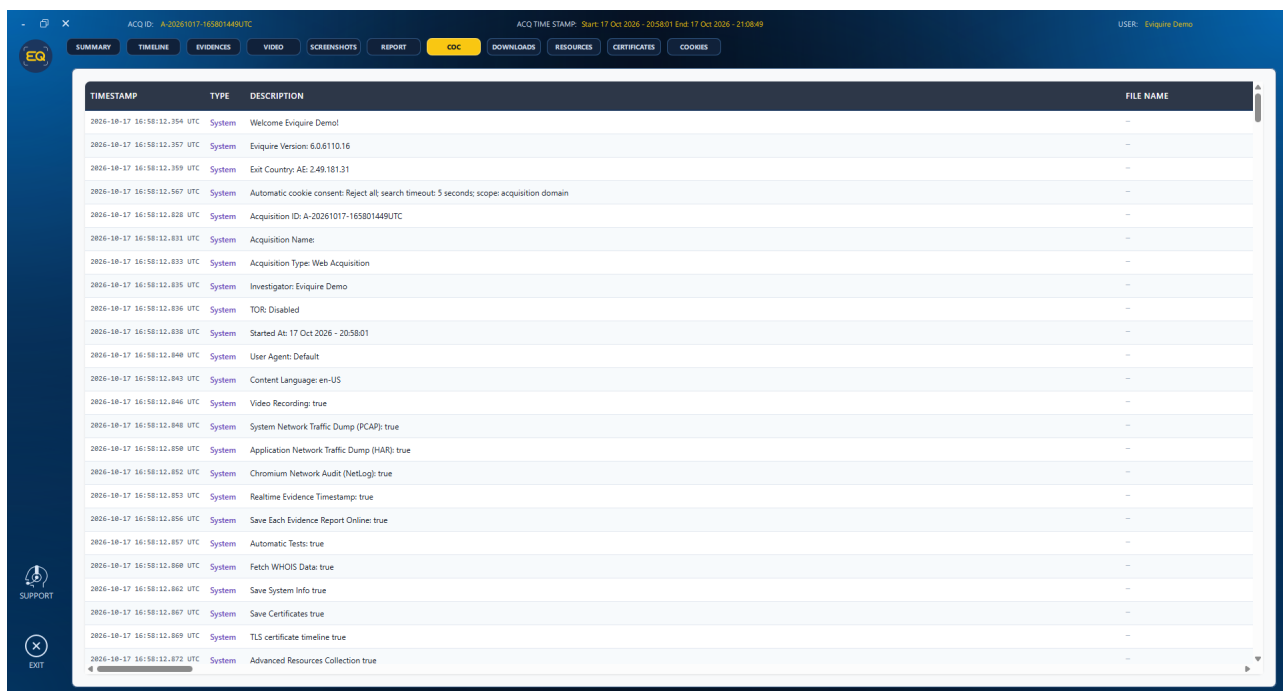


Figure 38. The dedicated COC tab displays timestamped application, browser and investigator events.

Where a file-hash field is populated, correlate it with the exact file described by that event. Use the original User-Activity file and summary/hash manifests for machine-readable or formal validation. A custody log records actions and handling; it does not independently prove that statements displayed on a website are true.

12.18 DOWNLOADS: Downloaded Media and Companion Metadata

DOWNLOADS focuses on downloaded files. In the illustrated example, a downloaded website video appears in the file list, with a media player above a structured JSON metadata panel. Metadata may include the source URL, original media filename, download time, size, hash values, collection status and available titles/descriptions or diagnostic messages.

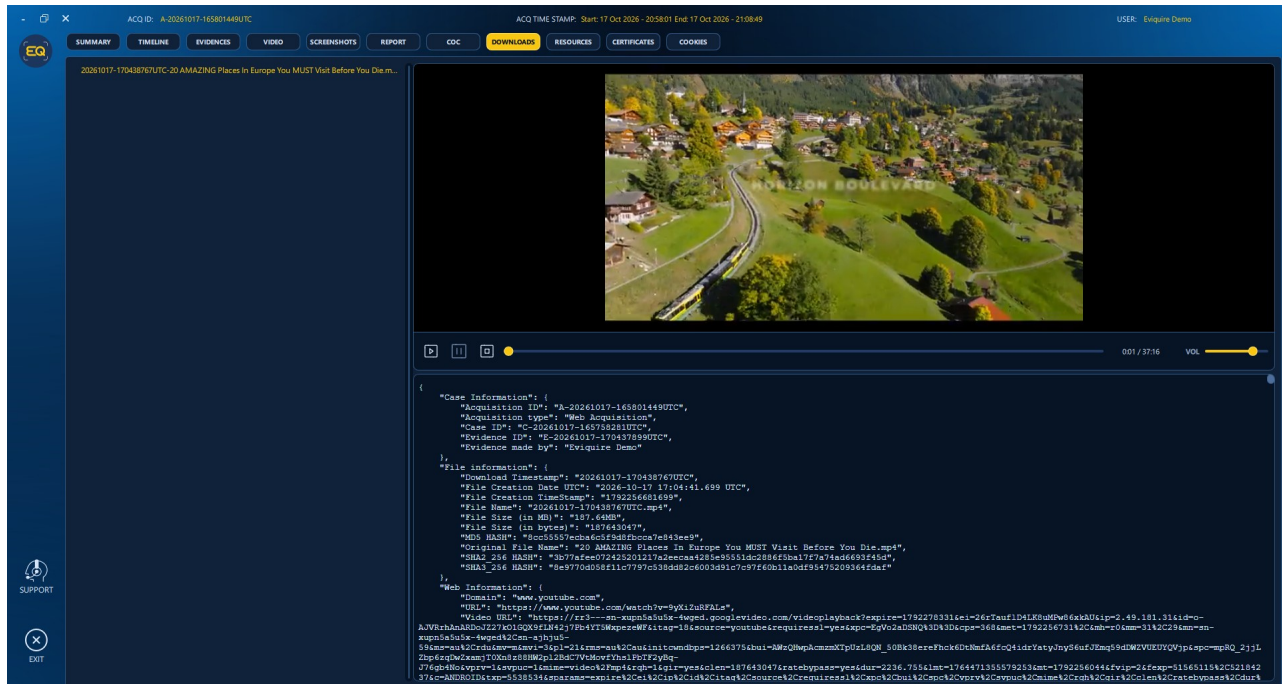


Figure 39. The DOWNLOADS tab plays acquired media and displays its structured download metadata.

The same downloaded video and its JSON companion may also be inspected from the evidence folder in SUMMARY. Confirm that the media being reviewed belongs to the selected evidence item and distinguish any download warnings from successful collection results.

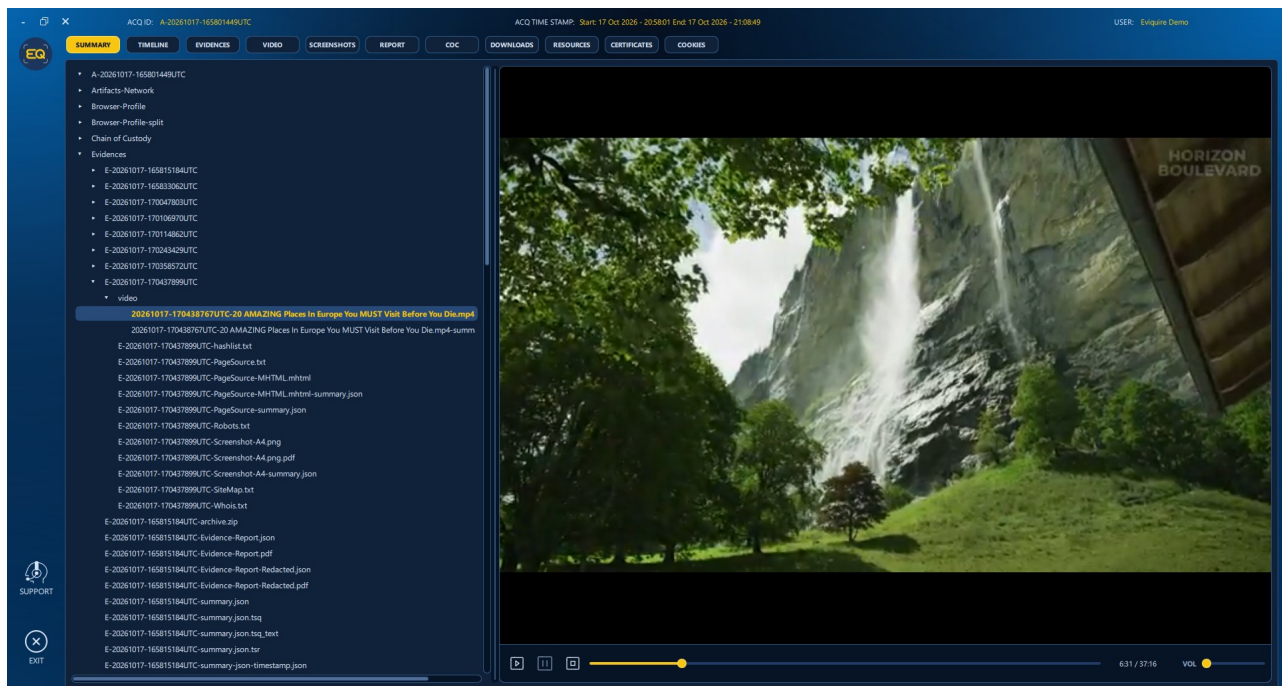


Figure 40. A downloaded MP4 selected in the SUMMARY file tree and played without modifying the original media.

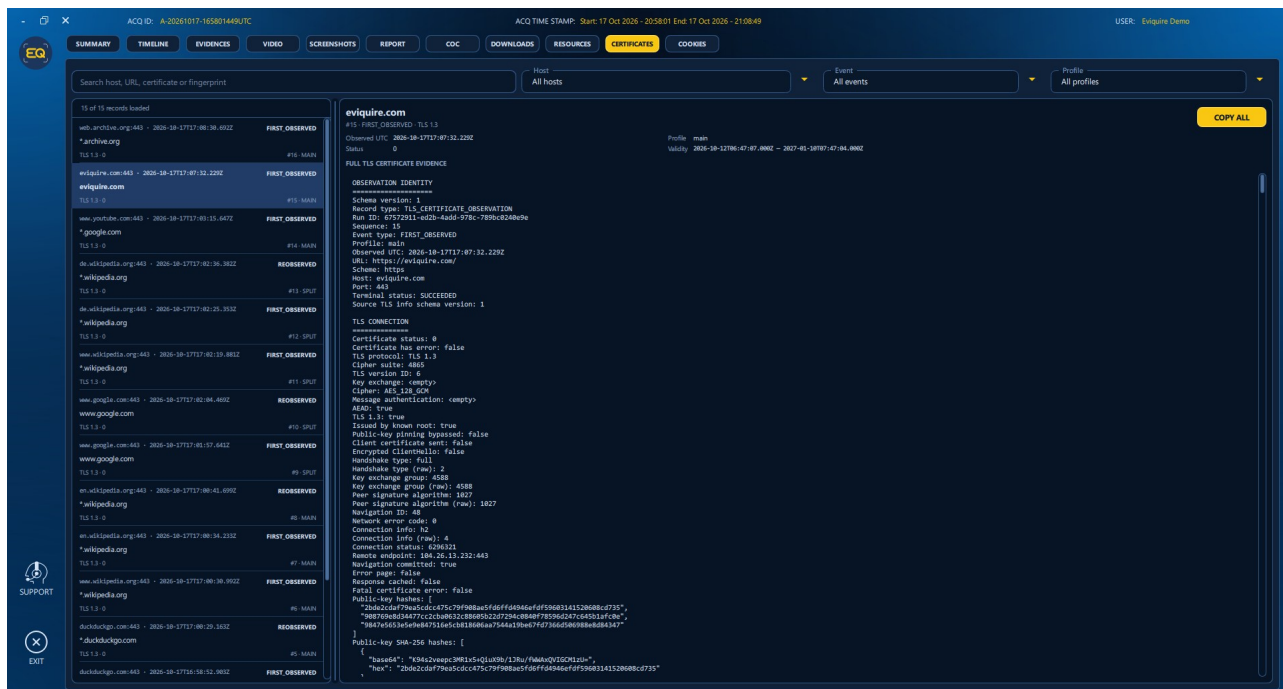


Figure 42. The CERTIFICATES tab includes searchable host observations, event/profile filters and detailed TLS certificate evidence.

The COPY ALL action copies the displayed technical record for analysis. Use the observed time, host, SNI or URL and certificate context together. A certificate record proves what the browser observed during a connection; it does not itself establish the reliability or truth of webpage content.

12.21 COOKIES: Browser Cookie Evidence

When Advanced Cookies Collection was enabled for the acquisition, the COOKIES review tab provides access to preserved cookie information and lifecycle events. Records can be examined in connection with domain context and the acquisition timeline. Automatic Cookie Consent configuration and consent-click events, if present, should be compared with the COC to distinguish automatic browser behavior from operator interaction.

1. Open COOKIES for an acquisition that used detailed cookie collection.
2. Locate the target domain and relevant cookie entries or lifecycle events.
3. Compare observation timestamps with the TIMELINE and COC tabs.
4. Document any cookie values or session identifiers separately under the investigation's privacy and access controls.

Sensitive information: Cookie stores and HTTP resources may contain active session tokens or account information. Handle their exports under the same controls as other sensitive evidence.

12.22 Cross-Checking Integrity and Provenance

Acquisition review is strongest when the displayed records agree across independent views. The SUMMARY tree identifies the actual artifact; EVIDENCES links it to a capture ID; COC documents actions at recorded times; TIMELINE provides chronological context; REPORT summarizes the session; and the package summary/hash list provides file-integrity data. Where timestamping or blockchain anchoring was enabled, verify receipts against the submitted summary hash rather than assuming that a transaction reference verifies every underlying file independently.

For a downloaded media file, for example, inspect its evidence record, original filename, video playback, source URL and JSON summary, and then independently compute its digest on a copy. For a screenshot, compare the captured image with its evidence report and underlying source/context, check COC timestamps and file paths, and verify its reported SHA2-256 value.

12.23 Recommended End-to-End Acquisition Review

1. Identify the correct case, acquisition ID, investigator and session dates in Case Manager and the review header.
2. Open SUMMARY and inspect the top-level artifact inventory; confirm which HAR, PCAPNG, browser-profile, custody and report files actually exist.

3. Open REPORT to establish the recorded acquisition configuration and package identifiers.
4. Open COC to reconstruct the operator and system events, including any errors, retries or warnings.
5. Use TIMELINE to correlate visual captures, downloads, video, certificate and cookie events at relevant UTC times.
6. Use EVIDENCES, SCREENSHOTS and VIDEO to evaluate the content of the selected evidence items.
7. Use DOWNLOADS, RESOURCES, CERTIFICATES and COOKIES when those artifacts are relevant to the investigative question.
8. Examine each selected file's associated summary, recorded digest and package lineage; carry out independent integrity verification on review copies.
9. Preserve the original acquisition archive, record findings and export only the permitted scope through an approved process.

Display times: The example screens show a Dubai display time zone (UTC+04:00) while the COC activity rows use UTC. State which time basis is used in any report, timeline exhibit or witness explanation.

13. Exporting And Deliverables

13.1 Export Evidence ZIP

Export an evidence ZIP when a single evidence item must be provided or reviewed independently. Use cases:

- Exhibit preparation.
- Targeted legal disclosure.
- Technical validation of one capture.
- Sharing one item with a subject matter expert.

Before delivery:

1. Compute the evidence ZIP hash.
2. Confirm the package opens.
3. Confirm the report and summary are present.
4. Transfer securely.
5. Record recipient and transfer method.

13.1.1 Download an Individual Evidence Package (Version 6)

In the **Case Manager**, select an evidence item and use the **download button** in **EVIDENCE DETAILS**, or open the evidence-table context menu and choose the evidence download action. This saves the **original evidence ZIP** rather than only a screenshot or preview.

Version 6 can retrieve evidence packages from active acquisition archives and closed cases, including password-protected case packages when the required access credentials are provided. The original archive and its contents are not modified by retrieval.

1. Select the correct case, acquisition, and evidence ID.
2. Download the individual original evidence ZIP to an approved review or transfer location.
3. Record its resulting filename and SHA2-256 digest; verify expected summary, timestamp and report contents before delivery.

Handling distinction: A preview-image download is not the same deliverable as the complete evidence ZIP. Use the complete package when proof of integrity and provenance is required.

13.2 Export Acquisition ZIP

Export an acquisition ZIP when the full session must be reviewed. Use cases:

- Legal review of complete collection session.

- Technical validation of all evidence in an acquisition.
- Review of browser profile, network capture, or logs.
- Demonstration of investigator workflow.

The acquisition ZIP has more context than individual evidence packages and may contain sensitive session artifacts.

13.3 Export Case ZIP

Export the case ZIP when the entire investigation must be delivered or archived. Use cases:

- Final case closure.
- Handoff to legal team.
- Disclosure production.
- Long-term evidence archive.
- Transfer to another forensic examiner.

The case ZIP is the most complete and sensitive deliverable.

13.4 Password Protection

If password protection is available, use it for exported case packages containing sensitive evidence. Follow these rules:

- Use strong passwords.
- Do not send the password with the ZIP.
- Store passwords in an approved secrets system.
- Record who received the password.
- Follow organizational encryption policy.

Caution: Password protection does not replace secure storage, access control, or transfer procedures.

13.5 Secure Transfer Recommendations

Use secure transfer methods:

- Encrypted evidence portal.
- Approved secure file transfer platform.
- Encrypted external media with chain-of-custody documentation.
- Internal evidence repository.
- Legal discovery platform with access logging.

Avoid:

- Consumer file sharing.
- Unencrypted email attachments.
- Personal cloud accounts.
- Informal messaging channels.

13.6 Delivering To Legal Teams

When delivering to legal teams, include:

- Final ZIP package.
- Export hash.
- Brief package description.
- Case report PDF.
- Verification instructions.
- Known limitations.

- Password delivery instructions, if applicable.

Legal teams may not need every technical artifact immediately, but the package should preserve them.

14. Advanced Features

14.1 Browser Profiles

Eviquire uses a browser profile during acquisition. The profile can preserve cookies, cache, persistent storage, and related browser data. This is important when evidence depends on session state. Forensic value:

- Shows browser context.
- Preserves authentication-related state.
- Supports review of how content was accessed.
- Helps reproduce session behavior in some circumstances.

Risk:

- May contain sensitive cookies or tokens.
- May include private browsing artifacts.
- May create disclosure concerns.

Handle browser profiles as sensitive evidence.

14.2 Cookies And Session Persistence

Eviquire maintains browser state within an acquisition to support navigation and, when authorized, authenticated content collection. Advanced Cookies Collection can preserve cookie observations and lifecycle events. The investigator should not assume cookies or site consent decisions carry across new, isolated acquisitions.

- Use dedicated accounts when possible.
- Avoid personal investigator accounts unless authorized.
- Document login steps.
- Capture logout state if relevant.
- Understand that cookies can be sensitive credentials.

14.2.1 Automatic Cookie Consent Handling

The Version 6 acquisition form provides an **Automatic Cookie Consent** checkbox and response selection. Use it only when the acquisition protocol specifies a deliberate cookie-banner action. For instance, a public-page investigation that requires minimal interaction can leave the option disabled. If the protocol instead requires a rejected-consent state, enable the option and select **Reject all** where offered.

Cookie banners and consent frameworks differ between websites. Rules-based handling can reduce manual work but cannot guarantee every banner is detected. A consent response may affect cookies, third-party calls, page appearance, and the evidence collected. Record and review actual consent interaction events; do not infer a successful rejection or acceptance merely from selecting a setting. Automated handling does not authorize unrelated account or data access.

The **Advanced Cookies Collection** option is separate: it governs cookie artifact collection and should not be confused with automated interaction with the banner.

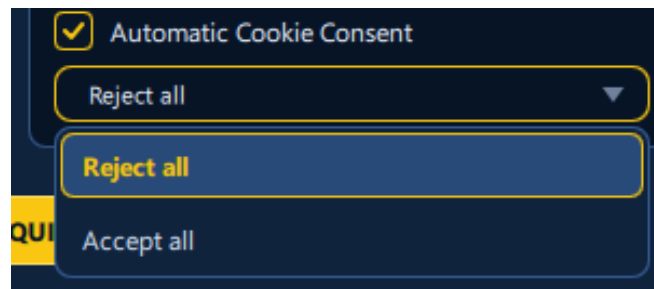


Figure 20. Automatic Cookie Consent offers Reject all and Accept all choices when enabled.

Select **Automatic Cookie Consent** in the New Acquisition form, then choose **Reject all** or **Accept all** from the dropdown. The application attempts the corresponding action only on supported consent dialogs; an unsupported site or modified banner may require user review. Actual automated consent clicks are recorded in Chain of Custody.

Supported-site handling includes major services such as Google, Facebook, Instagram, YouTube, TikTok, and Reddit, subject to site changes. Choosing Reject all does not prove that every optional cookie was refused: verify the visible dialog outcome and captured cookie events where that distinction matters.

14.3 Proxy Routing

Proxy routing can be used to control the apparent network origin of browser traffic. Eviquire records public IP and country information where available. Use proxy routing when the investigation requires:

- Geographic testing.
- Controlled egress.
- Enterprise network routing.
- Separation from investigator workstation IP.

Document all proxy settings.

14.4 Tor Mode

Tor mode routes traffic through Tor where supported. It can affect content, speed, access, and legal interpretation. Use Tor mode only when authorized and appropriate. Record why Tor was used and what exit information was observed.

14.5 PCAP Network Capture

PCAP network capture records packet-level session traffic. Eviquire writes PCAPNG files and TShark logs when configured and supported. Forensic value:

- Supports network timeline analysis.
- Shows domains, IPs, connections, and transfers.
- Helps validate downloads.
- Can support incident response analysis.

Risks:

- May capture unrelated host traffic.
- May contain credentials.
- May contain personal data.
- Can create very large files.

14.6 TLS Key Logs

TLS key logs can support decryption of browser TLS traffic in tools that support key log import. Eviquire writes the SSL key log path into the browser environment. Forensic value:

- Can help analyze encrypted traffic.

- Supports technical validation of browser communication.

Risks:

- Highly sensitive.
- Can expose decrypted session contents.
- Must be protected like credentials or privileged evidence.

14.7 Automation

Automation can create cases, configure acquisition options, launch acquisitions, and close cases according to provided configuration. It is useful for cloud, batch, or repeatable collection workflows. Before using automation:

- Validate the configuration on test targets.
- Confirm case naming and metadata.
- Confirm evidence options.
- Confirm export settings.
- Confirm legal scope for every target.

14.7.1 Recording Engine and Multi-Monitor Considerations

The August 2026 release introduced an FFmpeg-based recording engine, with improvements for targeted window capture and application-focused audio. Visual recording is contextual evidence and should be validated alongside discrete captured artifacts. If multiple monitors are used, maintain consistent display scaling across monitors to avoid recording alignment problems or inaccurate visual interaction markers. Use a short test recording after changing display or audio configuration.

14.7.2 Media Recording and Review

The FFmpeg-based recorder supports application/window-scoped capture and process-scoped audio on supported systems. Recorded click indicators help relate mouse actions to visual events. Multi-monitor use is supported, but **consistent display scaling across monitors** is recommended to minimize click-coordinate and capture-alignment issues.

Windows builds request protection against routine sign-out, shutdown, restart, and automatic idle sleep while an acquisition is running or finalizing. Operating-system policy and forced shutdown can override these requests. Screen lock and manual Sleep/Hibernate may still occur. Plan for reliable power and storage; protection requests do not make an acquisition immune to interruption.

14.8 Batch Captures

Batch capture lets investigators process multiple URLs or targets. It can optionally cycle through proxies depending on configuration. Best practices:

- Test with a small batch.
- Use clear acquisition names.
- Monitor disk space.
- Review failures promptly.
- Preserve the original URL list.
- Mark processed URLs.

14.9 Historical Website Search and Comparison

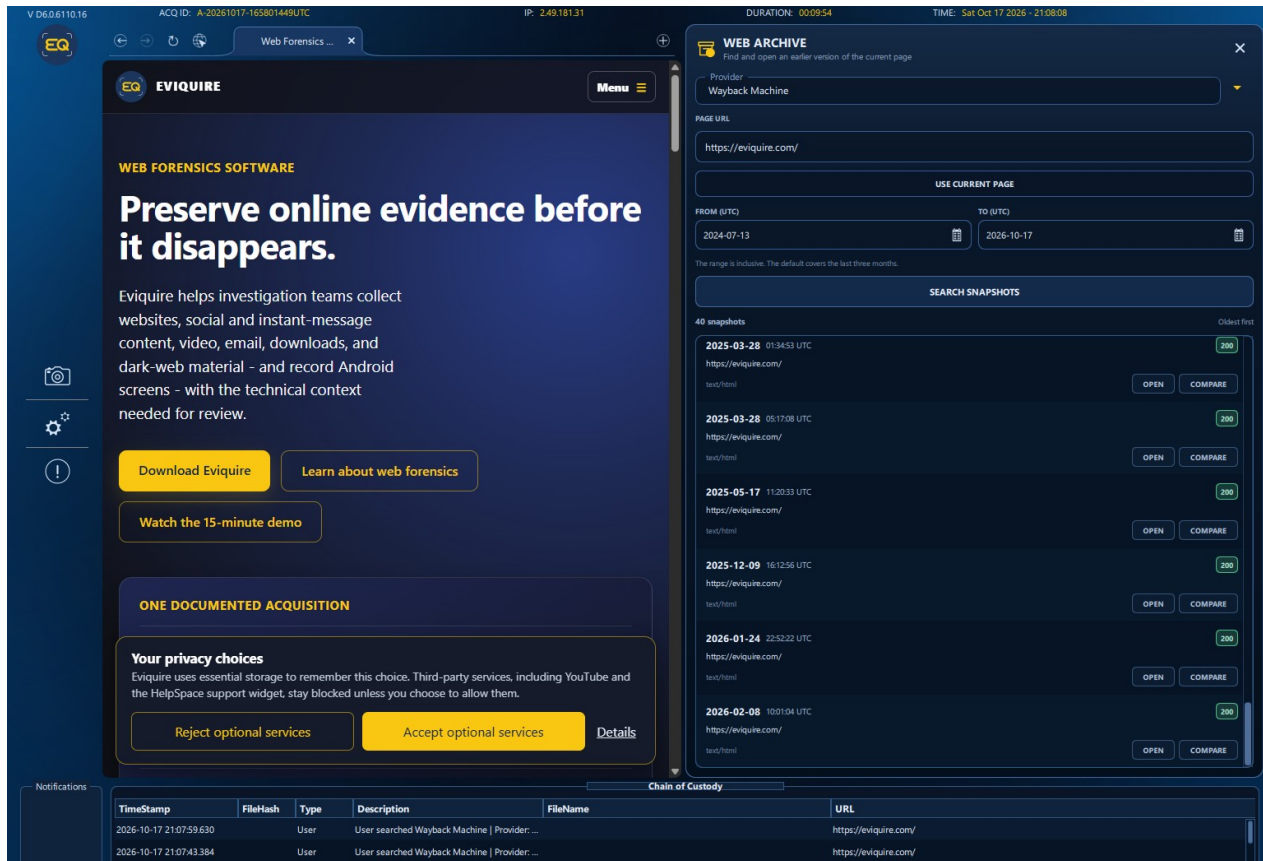


Figure 21. WEB ARCHIVE: snapshot search by URL and UTC date range, with Open and Compare actions.

The **WEB ARCHIVE** panel provides access to historical snapshots from **Wayback Machine** and **Arquivo.pt**, subject to provider availability. Open the tool while viewing a target web page; select the archive provider, enter a URL or use **USE CURRENT PAGE**, and choose the **FROM (UTC)** and **TO (UTC)** range.

1. Choose the archive provider and the target page URL. Confirm that URL normalization has not changed the intended resource.
2. Choose an inclusive date range and press **SEARCH SNAPSHOTS**.
3. Review returned timestamps, archived URLs, resource types, and available response-status indicators.
4. Select **OPEN** to view a historical snapshot or **COMPARE** to examine historical and current versions side by side.

Archived views can be incomplete or affected by missing resources, crawler exclusions, access limits, or website changes. Record the archive provider and snapshot timestamp alongside the current-page acquisition. Historical content should be preserved using the normal evidence capture workflow if required for the case.

14.10 Acquisition Information and Live Storage Monitoring

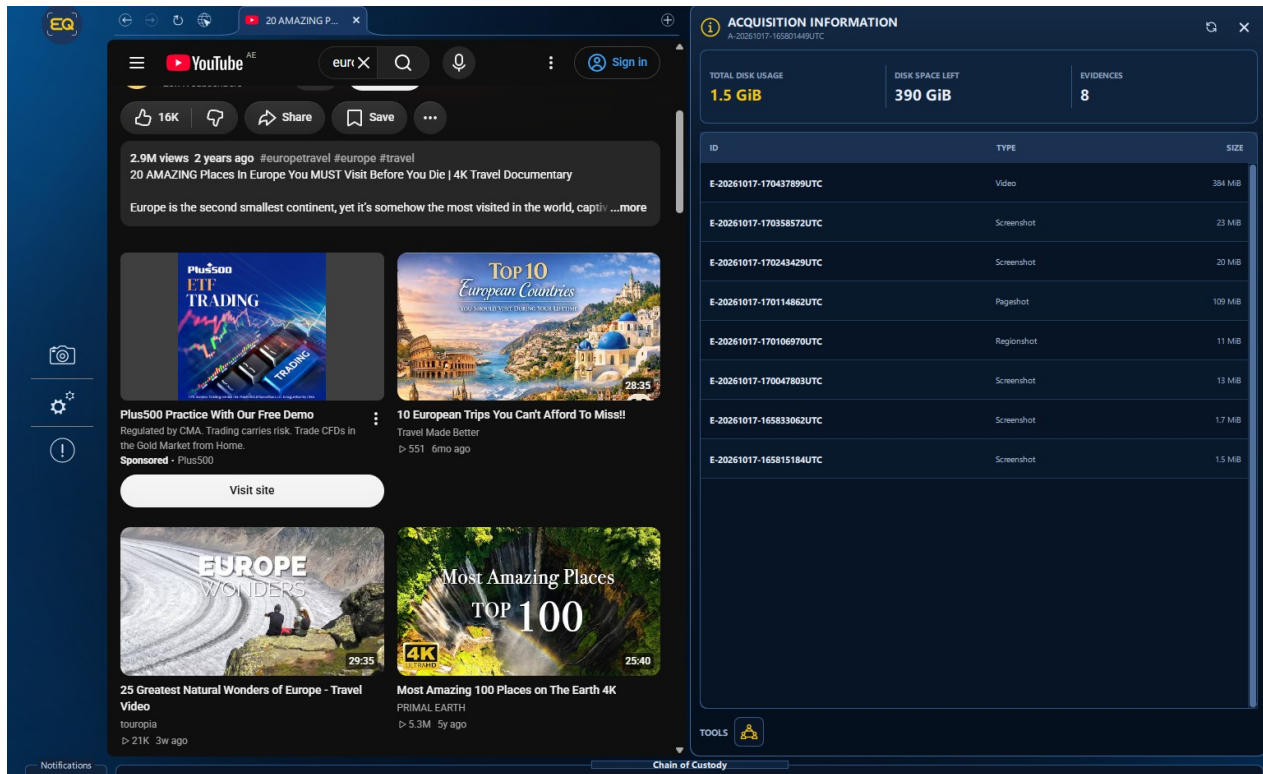


Figure 22. ACQUISITION INFORMATION: evidence list, total disk usage, and available storage during the live session.

Open the **ACQUISITION INFORMATION** panel during a live capture to review the acquisition identifier, evidence count, **TOTAL DISK USAGE**, **DISK SPACE LEFT**, and the collected evidence list with individual types and sizes. This helps the investigator identify unusually large captures and avoid storage exhaustion during lengthy videos, pageshots, or network collections.

The example shows eight evidence entries, including video, screenshots, a pageshot, and a regionshot. Values represent the illustrated session only. Refresh or reopen the panel when operational decisions depend on current storage status.

14.11 Resilience, Recovery, and Timestamp Handling

Version 6 performs FreeTSA and blockchain timestamp operations in parallel with bounded waits and explicit failure handling. Timestamping problems or interrupted finalization no longer automatically prevent recovery-oriented packaging of collected material. Reports and logs distinguish completed processing from operations that did not finish.

If an acquisition terminates unexpectedly, preserve the partial evidence and diagnostics and use the application's recovery workflow. Video, Pageshot, and browser shutdown paths have improved timeouts and error handling. Windows diagnostic packages may include relevant crash dumps, logs, and version information; those diagnostics are separate from evidence and are not uploaded automatically.

Important: A recovered or partially finalized acquisition must still be verified. Document any unavailable timestamps, incomplete exports, cancelled operations, or missing artifacts rather than treating recovery as proof that every planned collection task succeeded.

15. Security And Privacy

15.1 Handling Sensitive Evidence

Eviquire evidence may contain:

- Personal data.
- Credentials.

- Cookies.
- Session tokens.
- Mail messages.
- Attachments.
- Network traffic.
- TLS keys.
- Business confidential data.
- Privileged legal material.
- Malware or suspicious downloads.

Treat all Eviquire packages as sensitive unless classified otherwise.

15.2 Encryption Recommendations

Use encryption for:

- Evidence storage volumes.
- Exported ZIP files where supported.
- External drives.
- Backups.
- Long-term archives.
- Transfers.

Encryption should be paired with key management. A lost password may make evidence inaccessible.

15.3 Access Controls

Restrict access according to role:

- Investigators collect evidence.
- Forensic examiners validate packages.
- Legal teams review reports.
- Administrators manage software and licensing.
- Auditors review logs and controls.

Use least privilege and maintain access logs where possible.

15.4 Storage Best Practices

- Store evidence on approved encrypted storage.
- Avoid local desktop folders for long-term storage.
- Use evidence repositories with access logging.
- Back up original packages.
- Maintain immutable or write-protected copies where policy requires.
- Record hashes at transfer and archive points.

15.5 Retention Policies

Retention depends on legal, regulatory, organizational, and case requirements. Define:

- How long original packages are retained.
- Who can authorize deletion.
- How deletion is recorded.
- How backups are handled.

- How sensitive data is minimized.
- How privileged data is segregated.

Warning: Do not delete evidence packages unless authorized by policy, legal hold status, and case disposition.

15.6 Sensitive v6 Artifacts and Sharing

HAR, Chromium NetLog, advanced cookie records, browser profiles, TLS key logs, and system packet captures may include authentication data or information beyond the target page. When exporting an acquisition, apply the organization's access-control, redaction, secure-sharing, and retention requirements to each of these components.

Case attachments are **included in exported cases**. The Files tab warns that recipients of the case package can access those files. Do not attach workpapers or privileged communications unless their inclusion in the export is authorized and deliberate.

16. Troubleshooting

16.1 Browser Not Launching

Possible causes:

- Missing browser executable.
- Installation incomplete.
- Insufficient permissions.
- Antivirus blocking execution.
- Corrupt configuration.
- Unsupported operating system.

Recommended actions:

1. Restart Eviquire.
2. Confirm installation path.
3. Check application logs.
4. Confirm license status.
5. Run a test acquisition.
6. Contact support if the browser process exits immediately.

16.1.1 File Attachments or Detail Fields Not Visible

If a case file or integrity field is not visible, first confirm that the correct case is selected and inspect the right-side **CASE DETAILS** panel. Case attachments are administered in **EDIT CASE → FILES**, while acquired evidence appears in the lower **EVIDENCE** list. Scroll the right pane when its content exceeds the window height, and ensure the window is large enough to display the relevant fields. The exact icons may vary with the installed maintenance build.

16.2 Capture Failed

Possible causes:

- Page changed during capture.
- Disk space exhausted.
- Browser rendering issue.
- Network connection failed.
- Script-heavy page did not stabilize.
- Full-page capture exceeded resources.

Recommended actions:

1. Review chain-of-custody logs.
2. Check error messages.
3. Confirm disk space.
4. Try a smaller capture.
5. Capture screenshot and source separately.
6. Record the limitation in notes.

16.3 Downloads Missing

Possible causes:

- Download was blocked.
- File already existed and duplicate handling cancelled part of a workflow.
- Browser download did not complete.
- Target required authentication.
- Disk path was unavailable.

Recommended actions:

1. Review download events.
2. Check evidence Downloads folder.
3. Check browser/network logs.
4. Repeat download in a new acquisition if legally permitted.
5. Confirm file hash and size.

16.4 Hash Mismatch

Possible causes:

- File changed after initial hash.
- File was incomplete when first recorded.
- Manual alteration.
- Packaging issue.
- Filesystem or tool error.

Recommended actions:

1. Preserve the package as-is.
2. Review evidence hash list.
3. Compare database hash and packaging hash.
4. Check timestamps.
5. Review chain-of-custody entries.
6. Document findings.
7. Reacquire if necessary and permitted.

16.5 Network Capture Unavailable

Possible causes:

- TShark not installed.
- Capture driver missing.
- Insufficient permissions.
- Tool path incorrect.

- Endpoint protection blocked capture.

Recommended actions:

1. Install or repair Wireshark/TShark.
2. Confirm dumpcap availability.
3. Run Eviquire with required permissions if policy permits.
4. Validate with a test acquisition.
5. Disable network capture if not required.

16.6 License Issue

Possible causes:

- License expired.
- Offline activation not completed.
- Network validation unavailable.
- Incorrect key.
- Edition does not include requested feature.

Recommended actions:

1. Check license status.
2. Re-enter license key.
3. Confirm network access to licensing service.
4. Contact administrator.
5. Confirm edition entitlements.

16.7 Slow Performance

Possible causes:

- Large page.
- Full-page capture.
- Video recording.
- Network capture.
- Deep collection.
- Low RAM.
- Slow disk.
- Proxy or Tor latency.

Recommended actions:

1. Close unrelated applications.
2. Disable unnecessary options.
3. Use SSD storage.
4. Increase RAM.
5. Split capture into smaller acquisitions.
6. Avoid Tor unless required.

16.8 Large Case Exports

Possible causes:

- PCAP files.
- Video recordings.

- Browser profiles.
- Large downloads.
- Batch captures.
- Full-page screenshots.

Recommended actions:

1. Estimate size before export.
 2. Use high-capacity storage.
 3. Confirm free space is at least three times expected export size.
 4. Use secure transfer designed for large files.
 5. Preserve export hash.
-

16.9 Automatic Consent or Social Expansion Does Not Work

Cookie consent automation and social-media comment expansion depend on supported website structures. If a banner is not handled or comments fail to expand, first confirm the applicable option is enabled, whether the target changed layout, and what Chain of Custody recorded. Attempt an authorized manual action if permitted, or preserve the partially collected page with explanatory notes.

16.10 HAR, NetLog, or Cookie Records Are Missing

Review the acquisition details to confirm **Application Network Acquisition (HAR)**, **Chromium Network Audit (NetLog)**, or **Advanced Cookies Collection** was enabled. A setting may not create a substantial artifact if no eligible activity occurred. Check browser logs and finalization results before concluding that a collection failed.

16.11 Interrupted Pageshot or Recovery Operation

If capture ends early because of a timeout, target-page change, browser close, or cancelled operation, Eviquire is designed to preserve completed frames where possible. Verify the pageshot sequence and PDF against the captured scope. Preserve incomplete output, identify the stopping point, and make a new authorized acquisition when further collection is required.

16.12 Portable Startup, Video Playback, and Linux Permissions

For portable Windows operation, confirm full extraction, writable application folders, and endpoint-policy compatibility. For Ubuntu Applmage operation, confirm a compatible runtime with X11/XWayland. If packet capture is unavailable, check host TShark/dumpcap rather than the Applmage's bundled multimedia tools. AV1/HEVC playback depends on the matching multimedia runtime; do not change the evidence files to make a viewer work.

16.13 Getting Technical Support

If a problem cannot be resolved by the procedures in this chapter, open the in-application Support option or contact support@ricta.io. The online help center is available at help.eviquire.com. Include sufficient detail to reproduce the behavior while protecting case information.

Prepare the following information, where relevant:

Eviquire build/version, operating system and edition or deployment type (Windows installed/portable, Ubuntu Applmage, macOS beta).

Affected function, expected result, actual result, reproducible steps and the exact on-screen error message.

Date and time of the incident, including the displayed time zone; acquisition and case identifiers only when authorized to disclose them.

Relevant redacted screenshots, harmless configuration details and diagnostic logs. Do not send license keys, passwords, tokens, cookies or TLS key logs.

Whether the original evidence/archive remains intact and whether acquisition finalization or integrity verification reported a problem.

Evidence safety: Preserve original acquisition and case packages unchanged. Do not transmit sensitive evidence or diagnostic archives containing case data unless authorized and instructed to use an approved secure transfer method.

17. Best Practices

17.1 Defensible Evidence Collection

Use a consistent workflow:

1. Prepare workstation.
2. Confirm time synchronization.
3. Confirm case and investigator metadata.
4. Configure acquisition options.
5. Record legal authority or scope externally.
6. Capture evidence.
7. Review logs and reports.
8. Verify hashes.
9. Export securely.

17.2 Repeatable Workflows

Repeatability improves credibility. Use templates or standard operating procedures for common collection types:

- Web page screenshot and source.
- Authenticated web session.
- File download.
- Mail capture.
- Network capture.
- Batch URL capture.

Document deviations.

17.3 Minimizing Contamination

To reduce contamination:

- Use a clean VM or workstation.
- Close unrelated applications.
- Use dedicated accounts.
- Avoid personal browser sessions.
- Use Eviquire's controlled browser profile.
- Do not browse unrelated sites during acquisition.
- Do not manually modify evidence folders.

17.4 Proper Documentation

Eviquire documents technical events automatically, but investigators should still document:

- Legal authority.
- Scope.
- Target identifiers.

- Authentication steps.
- Search terms.
- Observed behavior.
- Limitations.
- External tools.
- Transfer and storage actions.

17.5 Audit Readiness

For audit readiness:

- Preserve original packages.
 - Store hashes in case notes.
 - Keep reports with packages.
 - Maintain access logs.
 - Verify timestamp files when needed.
 - Document software versions.
 - Record any errors or warnings.
-

18. FAQ

18.1 What is the difference between a case and an acquisition?

A case is the overall investigation container. An acquisition is one collection session inside a case. A case can contain multiple acquisitions.

18.2 What is an evidence item?

An evidence item is one captured object or action, such as a screenshot, page source, file download, email message, or full-page capture.

18.3 What is an evidence package?

An evidence package is the final ZIP for one evidence item. It contains the raw evidence archive, report, summary, timestamp files, and blockchain metadata where available.

18.4 What is an acquisition package?

An acquisition package preserves the full collection session, including evidence packages, logs, database, browser profile, network artifacts, video, reports, and summaries.

18.5 What is a case package?

A case package is the final export for the whole investigation. It contains one or more acquisitions and case-level reports, summaries, timestamps, and integrity metadata.

18.6 Why does Eviquire use UTC?

UTC avoids ambiguity caused by time zones and daylight saving changes. It supports consistent review across jurisdictions.

18.7 Which hash should I rely on?

Use SHA2-256 as the primary integrity hash. SHA3-256 is also strong. MD5 is included for compatibility and should not be used alone.

18.8 Does Eviquire prove that online content was true?

No. Eviquire preserves what was observed and collected under documented conditions. It supports authenticity and integrity of the capture, not the truthfulness of the content itself.

18.9 Can Eviquire capture authenticated pages?

Yes, when the investigator has lawful access and uses the forensic browser session. Browser profile and cookies may preserve authenticated state.

18.10 Are credentials captured?

They can be, especially in network captures, browser profiles, cookies, TLS key logs, screenshots, or video. Use caution and follow legal scope.

18.11 What happens if network capture is disabled?

The acquisition can still collect screenshots, source, downloads, reports, and logs. The PCAPNG artifact will not be created.

18.12 Why is TShark required?

TShark is used for packet capture. Without it, Eviquire cannot create TShark PCAPNG network captures.

18.13 What is the TLS key log?

The TLS key log stores secrets that can help decrypt browser TLS traffic in compatible analysis tools. It is sensitive and must be protected.

18.14 What is a timestamp request file?

The .tsq file is a timestamp request generated for a summary JSON file.

18.15 What is a timestamp response file?

The .tsr file is the timestamp authority response proving the summary existed in a particular hashed form at timestamping time.

18.16 What does blockchain anchoring do?

It submits a summary hash to an external blockchain-related anchoring workflow. This provides an additional external integrity reference.

18.17 Can I edit evidence after capture?

Do not edit evidence files. Work on copies for analysis. Editing original evidence will change hashes and may compromise defensibility.

18.18 Why does Eviquire create JSON reports?

JSON reports provide structured metadata for technical review, validation, automation, and long-term archival.

18.19 Why does Eviquire create PDF reports?

PDF reports provide human-readable summaries suitable for review, printing, disclosure, and legal presentation.

18.20 Can I use Eviquire in a virtual machine?

Yes, and it is often recommended. Confirm video recording, network capture, display scaling, and storage access before operational use.

18.21 Why should I close unrelated applications before network capture?

Network capture may record host-level traffic. Closing unrelated applications reduces irrelevant or private traffic in the PCAP.

18.22 What if a hash mismatch occurs?

Preserve the package, review the hash list, check logs and timestamps, document the mismatch, and reacquire if required and permitted.

18.23 Can I send evidence by email?

Avoid sending evidence packages by ordinary email. Use approved secure transfer methods and encryption.

18.24 Can I password-protect exports?

Case export workflows may support password protection. Use strong passwords and send them separately from the package.

18.25 What should I deliver to legal reviewers?

Provide the final package, export hash, case report, verification instructions, known limitations, and password transfer details if applicable.

18.26 Does Eviquire preserve browser cookies?

The acquisition browser uses persistent profile storage, so cookies and session state may be preserved in the browser profile artifacts.

18.27 What is deep collection?

Deep collection enables additional technical capture such as request/response or richer page-related data depending on configuration.

18.28 Should I enable every option?

No. Enable options required by the investigation. More artifacts can improve context but also increase sensitivity, size, and review burden.

18.29 Can I reopen a closed case?

No, reopen a case is not possible to Preserve the integrity of the original closed package.

18.29.1 Can I add documents directly to a case?

Yes. Use the **FILES** tab in **EDIT CASE** to attach supporting files. Those attachments become part of the case, and the interface warns that recipients of the exported case will be able to access them. Keep attachments separate from independently acquired evidence items.

18.29.2 What is the difference between PCAPNG, HAR, and NetLog?

PCAPNG records packet-level traffic, HAR records browser-level HTTP exchanges, and Chromium NetLog records browser network diagnostic events. Enable the outputs that correspond to the investigation's questions; none is a complete replacement for the others.

18.29.3 Does selecting Reject all automatically reject cookies?

Not by itself. **Automatic Cookie Consent** must also be enabled, and actual results depend on the target website and handling rules. Review the session logs and the rendered page to establish what occurred.

18.30 How should I verify a final case ZIP?

Compute the ZIP hash, extract a copy, review the case summary, compare archive/report hashes, validate timestamp files if required, and review blockchain metadata where present.

18.31 What is the difference between automatic consent and advanced cookie collection?

Automatic Cookie Consent attempts supported Accept all or Reject all actions and logs the clicks it performs. **Advanced Cookies Collection** records detailed browser cookie metadata and lifecycle events. Either option can be used independently when available.

18.32 Does case integrity verification change my evidence?

The graphical integrity-verification workflow is designed to compare file inventory and cryptographic hashes **without modifying original evidence**. Preserve the original files and record the verification results.

18.33 Does Save Evidence Report Online control local evidence reporting?

No. Version 6 supports local evidence reports; the online-report option is a separate publication or storage choice for eligible reports.

18.34 Can I compare a historical web archive to the live page?

Yes. The WEB ARCHIVE tool supports supported Wayback Machine and Arquivo.pt snapshot searches, opening historical captures, and comparison with the current page. Preserve any relevant comparison as evidence according to case scope.

18.35 Are recovered acquisitions automatically complete?

No. Recovery preserves available materials and records incomplete processing when appropriate. Review the Chain of Custody, file inventory, and cryptographic verification results before accepting the acquisition as complete.

19. Glossary

Acquisition

A time-bounded evidence collection session inside a case.

Acquisition Archive

The archive containing the acquisition session directory and artifacts.

Acquisition Package

The finalized acquisition deliverable, including archive, reports, summaries, timestamps, and metadata.

Browser Net Log

A browser-generated network activity log, usually stored as JSON.

Browser Profile

The browser storage area containing cookies, cache, persistent storage, and related session state.

Case

The outer investigation container holding one or more acquisitions.

Case Package

The final case ZIP containing the whole investigation deliverable.

Chain Of Custody

The documented record of evidence handling events.

DNS Over HTTPS

DNS resolution over HTTPS. It can affect how domain names are resolved during acquisition.

Evidence Archive

The compressed raw evidence files for one evidence item.

Evidence Item

A single captured object or capture action.

Evidence Package

The final ZIP for one evidence item.

Hash

A cryptographic fingerprint of a file.

MD5

A legacy hash algorithm included for compatibility.

PCAPNG

A packet capture file format used for network traffic evidence.

SHA2-256

A modern cryptographic hash algorithm used as a primary integrity value.

SHA3-256

A modern cryptographic hash algorithm recorded as an additional integrity value.

Summary JSON

A structured file containing package integrity metadata, hashes, timestamps, and case/acquisition/evidence linkage.

Timestamp Authority

A service that provides timestamp proof for a submitted hash or file representation.

TSQ

A timestamp request file.

TSR

A timestamp response file.

TLS Key Log

A file containing TLS secrets that may allow decryption of browser TLS traffic in compatible tools.

Tor

An anonymity network that routes traffic through relay nodes. Use must be authorized and documented.

User Agent

The browser identity string presented to websites.

WHOIS

Domain registration information, subject to availability and privacy protections.

20. Appendices

Appendix A: Example Folder Structure

```
<data-root>/
  <hashed-user-email>/
    C-20260429-101010000UTC/
      C-20260429-101010000UTC-DB.sqlite
    A-20260429-101500000UTC/
      A-20260429-101500000UTC-DB.sqlite
    Chain of Custody/
      User-Activity
      User-Activity.html
    Browser-Profile/
    Pages-Source-Code/
    Artifacts-Network/
      Browser-NetLogs.json
      A-20260429-101500000UTC.PCAPNG-TLSKeys.log
    Local-TShark/
      A-20260429-101500000UTC.PCAPNG
      A-20260429-101500000UTC.log
    Evidences/
      E-20260429-101700000UTC/
        E-20260429-101700000UTC-Screenshot-A4.png
        E-20260429-101700000UTC-Screenshot-A4.png.pdf
        E-20260429-101700000UTC-summary.json
        E-20260429-101700000UTC-hashlist.txt
        E-20260429-101700000UTC-archive.zip
        E-20260429-101700000UTC-report.pdf
        E-20260429-101700000UTC-report.json
        E-20260429-101700000UTC.zip
      systeminfo.txt
      certificates.txt
      A-20260429-101500000UTC-hashlist.txt
      A-20260429-101500000UTC-archive.zip
```

A-20260429-101500000UTC-report.pdf
 A-20260429-101500000UTC-report.json
 A-20260429-101500000UTC-summary.json
 C-20260429-101010000UTC-archive.zip
 C-20260429-101010000UTC-report.pdf
 C-20260429-101010000UTC-report.json
 C-20260429-101010000UTC-summary.json

Appendix B: Sample Evidence Package Contents

E-20260429-101700000UTC.zip
 E-20260429-101700000UTC-archive.zip
 E-20260429-101700000UTC-report.pdf
 E-20260429-101700000UTC-report.json
 E-20260429-101700000UTC-summary.json
 E-20260429-101700000UTC-summary.json.tsq
 E-20260429-101700000UTC-summary.json.tsr
 E-20260429-101700000UTC-summary.json.tsq_text
 <blockchain raw metadata file, when present>

The archive inside the package may contain:

E-20260429-101700000UTC-Screenshot-A4.png
 E-20260429-101700000UTC-Screenshot-A4.png.pdf
 E-20260429-101700000UTC-PageSource.txt
 E-20260429-101700000UTC-Whois.txt
 E-20260429-101700000UTC-Robots.txt
 E-20260429-101700000UTC-SiteMap.txt
 E-20260429-101700000UTC-hashlist.txt
 Downloads/
 downloaded-file.ext
 PDF/
 E-20260429-101700000UTC-Pageshots-A4-0-50.pdf

Appendix C: Sample Acquisition Package Contents

A-20260429-101500000UTC-archive.zip
 A-20260429-101500000UTC-report.pdf
 A-20260429-101500000UTC-report.json
 A-20260429-101500000UTC-summary.json
 A-20260429-101500000UTC-summary.json.tsq
 A-20260429-101500000UTC-summary.json.tsr
 <blockchain raw metadata file, when present>

The acquisition archive may contain:

A-20260429-101500000UTC-DB.sqlite
 Chain of Custody/User-Activity
 Chain of Custody/User-Activity.html
 Browser-Profile/
 Pages-Source-Code/
 Artifacts-Network/Browser-NetLogs.json
 Artifacts-Network/A-20260429-101500000UTC.PCAPNG-TLSKeys.log

Artifacts-Network/Local-TShark/A-20260429-101500000UTC.PCAPNG
 Artifacts-Network/Local-TShark/A-20260429-101500000UTC.log
 Evidences/E-20260429-101700000UTC.zip
 systeminfo.txt
 certificates.txt
 A-20260429-101500000UTC-hashlist.txt

Appendix D: Sample Chain-Of-Custody Log

TimeStamp	Event Type	Event Description	URL	File Name	SHA2_256 File Hash
2026-04-29 10:15:00.000 UTC	System	Welcome Jane Investigator!			
2026-04-29 10:15:01.000 UTC	System	Eviquire Version: D[Version]			
2026-04-29 10:15:04.000 UTC	System	Acquisition ID: A-20260429-101500000UTC			
2026-04-29 10:15:06.000 UTC	Browser	Browser Navigation Requested	https://example.test		
2026-04-29 10:15:09.000 UTC	Browser	Page load succeeded	https://example.test		
2026-04-29 10:16:20.000 UTC	System	ScreenShot taken (PNG)	https://example.test	/Evidences/E-20260429-101620000UTC/E-20260429-101620000UTC-Screenshot-A4.png	<sha2-256>
2026-04-29 10:16:21.000 UTC	System	Evidence summary saved (JSON)	https://example.test	/Evidences/E-20260429-101620000UTC/E-20260429-101620000UTC-summary.json	<sha2-256>
2026-04-29 10:16:30.000 UTC	System	Evidence archive saved	https://example.test	/Evidences/E-20260429-101620000UTC-archive.zip	<sha2-256>
2026-04-29 10:16:35.000 UTC	System	Evidence report saved (PDF)	https://example.test	/Evidences/E-20260429-101620000UTC-report.pdf	<sha2-256>
2026-04-29 10:16:42.000 UTC	System	Evidence timestamped	https://example.test	/Evidences/E-20260429-101620000UTC-summary.json.tsr	<sha2-256>
2026-04-29 10:20:00.000 UTC	System	Session Closed			

Appendix E: Sample Verification Workflow

Use this workflow to validate a delivered evidence package.

1. Copy the delivered evidence ZIP to a review workstation.
2. Compute SHA2-256 of the delivered ZIP and record it.
3. Extract the ZIP into a review folder.
4. Locate the summary JSON.
5. Open the summary JSON in read-only mode.
6. Identify the expected hash of the raw evidence archive.
7. Compute SHA2-256 of the raw evidence archive.
8. Compare the computed hash to the summary value.
9. Identify the expected hash of the PDF report.
10. Compute SHA2-256 of the PDF report.
11. Compare the computed hash to the summary value.
12. Validate the .tsq and .tsr files using an approved timestamp validation process.
13. Review blockchain metadata if present.
14. Extract the raw evidence archive only if file-level inspection is required.
15. Review the evidence hash list.
16. Compare file-level hashes for any files used in analysis or presentation.

17. Record verification results in the review notes.

Appendix F: Sample Acquisition Review Checklist

Before accepting an acquisition as complete, confirm:

- Acquisition ID is correct.
- Case ID is correct.
- Investigator identity is correct.
- Acquisition start and end times are present.
- Evidence list is complete.
- Chain-of-custody logs are present.
- Acquisition database is present.
- Reports are present.
- Summary JSON is present.
- Hash list is present.
- Network artifacts are present if network capture was enabled.
- Video artifacts are present if video recording was enabled.
- System info is present if enabled.
- Certificates are present if enabled.
- Evidence packages open successfully.
- No unexpected hash mismatch is present.
- Known errors are documented.

Appendix G: Sample Case Closure Checklist

Before closing a case, confirm:

- All acquisitions are complete.
- All evidence packages are finalized.
- Reports have been generated.
- Errors have been reviewed.
- Legal scope has been satisfied.
- Sensitive material has been identified.
- Export location has sufficient space.
- Password protection requirements are known.
- Viewer package requirement is known.
- Case package hash will be recorded.
- Transfer method is approved.

Appendix H: Artifact Reference

Artifact	Purpose
Evidence PNG	Visual capture of observed content
Evidence PDF	Stable human-readable visual rendering
Page source TXT	Technical source or markup capture
Mail EML	Preserved email message file
Downloaded file	File obtained during acquisition
WHOIS TXT	Domain registration context
Robots TXT	Host robots.txt context

Sitemap XML/TXT	Host sitemap context
Evidence hash list	File-level integrity manifest
Evidence archive ZIP	Raw evidence container
Evidence report PDF	Human-readable evidence report
Evidence report JSON	Structured evidence report
Evidence summary JSON	Integrity metadata for package
TSQ	Timestamp request
TSR	Timestamp response
Blockchain raw metadata	External anchoring metadata
Acquisition DB SQLite	Session records, events, evidence, metadata
User-Activity	Text chain-of-custody log
User-Activity.html	HTML chain-of-custody log
Browser profile	Browser cookies, cache, storage, profile data
Browser-NetLogs.json	Browser network activity log
PCAPNG	Packet capture
TShark log	Packet capture tool log
TLS key log	TLS decryption support data
Video MP4	Session or device recording
systeminfo.txt	Acquisition workstation details
certificates.txt	Trusted certificate context
Acquisition report PDF/JSON	Session-level report
Case report PDF/JSON	Case-level report

Appendix I: Detailed Package Internals

This appendix explains the expected structure and meaning of the three major package layers: the evidence package, the acquisition package, and the case package. These layers are intentionally redundant in some areas. Redundancy is useful in forensic work because the same fact can be confirmed from more than one place: a report, a summary JSON, a hash list, a database record, a chain-of-custody event, and the file system. When reviewing any Eviquire deliverable, begin by identifying the scope of the package. Do not assume that a ZIP file represents the whole case. An evidence ZIP may contain only one capture item. An acquisition archive may contain a full session but not necessarily every acquisition in the case. A final case ZIP is the broadest deliverable and should be treated as the primary long-term export for a completed investigation.

I.1 Evidence Package Internals

An evidence package is designed to answer a focused question: what exactly was captured for this evidence item, what files make up the evidence, what context was known at capture time, and how can the reviewer verify that the captured material has not changed? The final evidence package is normally named:

<evidence-id>.zip

Inside it, the reviewer should expect several categories of files. The raw evidence archive is normally named:

<evidence-id>-archive.zip

This archive contains the actual captured material. For a screenshot, it contains image files and possibly screenshot PDFs. For page source, it contains source text. For a download, it contains the downloaded file and any contextual screenshot/source material. For mail, it contains the mail file and related evidence. For a full-page capture, it can contain many pageshot images and generated PDF files. The evidence PDF report is normally named:

<evidence-id>-report.pdf

The PDF report is the human-readable evidence report. It is useful for investigators, attorneys, managers, and reviewers who need a clear description of the evidence without manually examining every technical artifact. The PDF should be treated as a report about the evidence, not as a replacement for the raw evidence archive. The evidence JSON report is normally named:

<evidence-id>-report.json

The JSON report is the structured counterpart to the PDF. It is intended for technical review, automated validation, or ingestion into another system. If a discrepancy appears between a PDF report and a JSON report, preserve both and perform a technical review before relying on either alone. The evidence summary JSON is normally named:

<evidence-id>-summary.json

The summary JSON is one of the most important files in the package. It is the integrity statement for the evidence package. It records file information for the evidence archive and, where applicable, the report. It can include file name, file size, file creation date UTC, file creation timestamp, MD5, SHA2-256, SHA3-256, URL, domain, device ID, evidence ID, acquisition ID, acquisition type, case ID, and investigator identity. The timestamp files are normally named:

<evidence-id>-summary.json.tsq

<evidence-id>-summary.json.tsr

The .tsq file is the timestamp request. The .tsr file is the timestamp response. The response should be validated using an approved timestamp verification process if formal timestamp validation is required. These files are important because they establish that the summary existed in a particular form at or before the timestamp response time. Blockchain raw metadata may also be present. The exact file name depends on the blockchain metadata suffix used by the application. This file records blockchain anchoring information for the submitted summary hash. Blockchain anchoring should be treated as an additional proof layer, not as the only integrity mechanism. The evidence package may contain a timestamp request text rendering:

<evidence-id>-summary.json.tsq_text

This file can help reviewers understand the timestamp request in a more readable form, depending on configuration. When a reviewer extracts the raw evidence archive, they may find an evidence hash list:

<evidence-id>-hashlist.txt

This file is a file-level integrity manifest. It is especially important because it compares hashes stored at acquisition time with hashes calculated at packaging time. A matching result supports the conclusion that files remained stable between creation and final packaging. A mismatch requires investigation and documentation. The evidence package is therefore made of three functional groups:

- Captured material: screenshots, source, downloads, mail, WHOIS, robots.txt, sitemap.xml, generated PDFs, or other evidence files.
- Interpretation material: PDF and JSON evidence reports.
- Verification material: summary JSON, hash list, timestamp files, blockchain metadata, and recorded hashes.

Forensic reviewers should keep these groups conceptually separate. A screenshot is what was captured. A report explains it. A summary and hash list help verify it.

1.2 Acquisition Package Internals

An acquisition package is designed to answer a broader question: what happened during the collection session, what settings were active, what evidence was produced, and what environmental artifacts support the collection? The acquisition archive is normally named:

<acquisition-id>-archive.zip

This archive contains the acquisition working directory after evidence packages have been created and acquisition-level artifacts have been generated. It may contain the acquisition SQLite database, chain-of-custody logs, browser profile, network artifacts, video artifacts, system information, certificates, evidence package references, and acquisition hash list. The acquisition database is normally named:

<acquisition-id>-DB.sqlite

This database is a key technical artifact. It stores structured information about chain-of-custody events, evidence records, navigation history, request/response data where enabled, acquisition metadata, evidence comments, and video duration.

The database allows Eviquire to reconstruct the acquisition for review. Technical users may inspect it only using approved forensic methods and should avoid modifying it. The chain-of-custody folder normally contains:

Chain of Custody/User-Activity

Chain of Custody/User-Activity.html

The text file is a plain chain-of-custody log. The HTML file is a more review-friendly representation. These logs are valuable because they show the procedural sequence: application startup, version, investigator identity, navigation, page load, screenshot, source capture, download, report creation, timestamping, recording events, and session closure. The browser profile directory may contain cache, cookies, persistent storage, and other browser state:

Browser-Profile/

The browser profile is highly sensitive. It can help explain how content was accessed, especially in authenticated sessions, but it may contain session tokens or personal data. Do not distribute browser profile material casually. If legal disclosure does not require it, follow counsel or organizational policy before sharing it. The pages source directory may contain source files that were saved outside a finalized evidence item:

Pages-Source-Code/

These files can help reconstruct browsing or analysis activity, but the strongest evidence source files are normally those packaged into evidence items with summaries and hash records. The network artifacts directory may contain:

Artifacts-Network/Browser-NetLogs.json
 Artifacts-Network/<acquisition-id>.PCAPNG-TLSKeys.log
 Artifacts-Network/Local-TShark/<acquisition-id>.PCAPNG
 Artifacts-Network/Local-TShark/<acquisition-id>.log

Browser-NetLogs.json is the browser network log. It can contain browser-level network activity, including requests, redirects, timing, errors, and other diagnostic data. The PCAPNG file is the packet capture. The TShark log records the packet capture tool's behavior. The TLS key log can support decryption of browser TLS traffic in compatible tools and should be treated as highly sensitive. The acquisition may include video artifacts:

<acquisition-id>-Video001.mp4
 <acquisition-id>-Video.log
 <acquisition-id>-Video-Device.mp4

Exact names can vary. Video artifacts document the acquisition session visually. They are particularly useful for explaining how the investigator interacted with a dynamic page, selected content, initiated downloads, or ended the session. Video should be reviewed for accidental exposure of sensitive material before disclosure. The acquisition may include environment files:

systeminfo.txt
 certificates.txt

systeminfo.txt documents the acquisition workstation. **certificates.txt** documents certificate trust information. These files help establish the technical environment in which evidence was collected. The acquisition report files are normally named:

<acquisition-id>-report.pdf
 <acquisition-id>-report.json

These reports summarize the session. They should describe acquisition identity, type, investigator, timing, duration, settings, evidence items, archive information, and integrity metadata. The acquisition summary JSON is normally named:

<acquisition-id>-summary.json

This summary records file information and hashes for the acquisition archive and report. It is timestamped and may be blockchain anchored. Because it summarizes the acquisition archive, it is the primary acquisition-level integrity statement. The acquisition hash list is normally named:

<acquisition-id>-hashlist.txt

This file records the acquisition file tree, file creation times, modification times, sizes, and hashes. It is useful for technical review of the acquisition archive contents. The acquisition package therefore preserves not only individual evidence items, but also the operational context that produced them.

I.3 Acquisition Page Interpretation

The acquisition page in the application is a review interface over acquisition metadata and package records. It should be read as a structured summary of the session. Common acquisition page fields include acquisition ID, acquisition name, acquisition type, investigator, IP/country, Tor state, start time, end time, user agent, DNS-over-HTTPS mode, device ID, mail type, mail server, mail user, archive file name, archive SHA2-256, summary file name, summary SHA2-256, blockchain transactions, and enabled collection options. When reviewing the acquisition page, investigators should confirm:

- The acquisition ID matches the package and folder names.
- The acquisition type matches the intended workflow.
- The investigator name is correct.
- Start and end times are plausible and in UTC or clearly labeled.
- User agent and routing settings are expected.
- Network capture state matches expected artifacts.
- Video state matches expected artifacts.
- WHOIS, system info, certificates, and deep collection states match expected artifacts.
- Archive and summary hashes are present.
- Evidence list is complete.
- Corruption flags or error messages are absent or documented.

The acquisition page is not the evidence itself. It is a navigational and review layer. The authoritative artifacts remain the package files, reports, summaries, logs, database, and hashes.

I.4 Case Package Internals

A case package is designed to answer the broadest question: what is the complete preserved investigative matter, including all acquisitions and their supporting reports and integrity records? The case archive is normally named:

<case-id>-archive.zip

This archive contains the case directory and acquisition material. During case closure, Eviquire creates a case-level hash list, compresses the case, generates reports, creates a summary JSON, timestamps the summary, and optionally includes a viewer package in the final case ZIP. The final case package is normally named:

<case-id>.zip

The final case ZIP may contain:

```
<case-id>-archive.zip
<case-id>-report.pdf
<case-id>-report.json
<case-id>-summary.json
<case-id>-summary.json.tsq
<case-id>-summary.json.tsr
<case-id>-summary.json.tsq_text
<case-id><blockchain raw suffix>
viewer files, when included
```

The case archive contains the acquisition archives and case-level data. The case PDF report is the human-readable summary of the matter. The case JSON report is the structured equivalent. The case summary JSON is the integrity statement for the case archive and report. The timestamp files and blockchain metadata provide external verification layers for the case

summary. The case package is appropriate for long-term archive and formal transfer. It should usually be treated as the master deliverable. If a case package is password-protected, preserve the password separately using approved key management procedures.

I.5 How Reviewers Should Interpret Package Layers

When reviewing Eviquire exports, use a layered interpretation model. At evidence level, ask:

- What single item was captured?
- Which raw files represent the item?
- What URL, domain, device, or mail context is recorded?
- What hashes verify the item?
- Was the evidence summary timestamped?
- Is there a report explaining the item?

At acquisition level, ask:

- What session produced the evidence?
- Which investigator performed it?
- Which options were active?
- What routing, DNS, user-agent, video, and network conditions applied?
- Which evidence items were created?
- Was the entire session video recorded properly?
- Are chain-of-custody logs complete?
- Did the acquisition finalize normally?

At case level, ask:

- What investigation does this represent?
- Which acquisitions belong to it?
- Was the case closed?
- What is the final case package hash?
- Are case reports and summaries present?
- Are timestamp and blockchain records present?
- Has transfer or disclosure been documented?

This model helps avoid a common review mistake: treating a screenshot as if it were the entire evidence record. In Eviquire, the screenshot is only one artifact. The stronger forensic object is the evidence package, and the stronger session object is the acquisition package.

I.6 Package Handling Rules

Use these rules when handling Eviquire package files:

1. Preserve original packages unchanged.
2. Compute and record hashes before extraction.
3. Extract only into controlled review folders.
4. Use copies for analysis.
5. Do not rename internal files unless creating a separate working copy.
6. Do not remove timestamp or blockchain metadata.
7. Do not discard JSON reports.
8. Do not disclose browser profile, PCAP, TLS key logs, or mail artifacts without scope review.
9. Record every transfer.
10. Keep passwords separate from packages.

The most defensible workflow is to preserve the original export, create a working copy, verify the working copy hash, extract and review the copy, and document all findings separately.

Appendix J: Publication Notes

This manual describes Eviquire workflows and artifacts from the perspective of investigators and reviewers. Specific options may vary by edition, license, operating system, and deployment configuration. Organizations should supplement this manual with local standard operating procedures, legal authority requirements, retention rules, and security controls.

Appendix K: Courtroom And Audit Preparation Guide

Eviquire packages are designed to support later explanation, but the software does not replace the investigator's responsibility to prepare a clear narrative. Before presenting or disclosing Eviquire evidence, the investigator should be able to explain the collection process in ordinary language and then support that explanation with technical artifacts.

K.1 Preparing The Evidence Narrative

A strong evidence narrative answers five questions:

1. What was the investigative objective?
2. What source was accessed?
3. What tool and version were used?
4. What was collected?
5. How was integrity preserved after collection?

For example, an investigator might explain that they opened a specific case, started a web acquisition, navigated to a target URL, captured a screenshot and page source, allowed Eviquire to create an evidence package, and then closed the acquisition so that reports, hash lists, timestamps, and archives were generated. The supporting package then demonstrates the details: timestamps, URLs, hashes, reports, and chain-of-custody entries. Avoid overstating what the evidence proves. A screenshot can show that certain content was displayed to the forensic browser during the acquisition. It does not automatically prove authorship, intent, identity, or truthfulness. Those conclusions usually require additional investigation.

K.2 Preparing Technical Verification

For technical review, prepare a verification worksheet containing:

- Package name.
- Package type: evidence, acquisition, or case.
- Export date.
- Export location.
- SHA2-256 hash of the delivered ZIP.
- Summary JSON name.
- Archive hash from summary JSON.
- Report hash from summary JSON.
- Timestamp validation result.
- Blockchain reference, if available.
- Name and version of verification tools used.
- Reviewer name and date.

This worksheet can be maintained outside Eviquire as part of the case file. It helps a later reviewer reproduce the verification procedure without guessing which files were checked.

K.3 Explaining Hashes To Non-Technical Reviewers

When explaining hashes to attorneys, managers, or court personnel, use precise but simple language. A hash is a calculated fingerprint of a file. If the file changes, the fingerprint changes. Eviquire records hashes when evidence is captured and packaged. A reviewer can calculate the hash again later and compare it to the recorded value. Matching values support the

conclusion that the file being reviewed is the same as the file described in the package metadata. Do not describe a hash as encryption. A hash does not hide the file. It verifies the file.

K.4 Explaining Timestamping

Timestamping can be explained as an external time proof over the summary JSON. The summary JSON contains hashes of important package files. Eviquire sends a timestamp request and stores the timestamp response. If validated, the response supports the conclusion that the summary existed in that form at the timestamp time. This does not mean every raw file was individually submitted to the timestamp authority. Instead, the summary acts as the integrity statement for the package. Because the summary records the archive and report hashes, timestamping the summary helps timestamp the package integrity record.

K.5 Explaining Chain Of Custody

Eviquire's chain-of-custody logs document tool actions during acquisition. They show when the browser navigated, when pages loaded, when screenshots or sources were saved, when downloads occurred, when reports were generated, and when the session closed. The logs should be used together with investigator notes and organizational evidence-handling records. If asked whether the logs prove that no human error occurred, answer carefully. Logs document recorded application events. They do not replace investigator testimony, case notes, or independent validation. Their value is that they provide a contemporaneous technical record of the session.

K.6 Disclosure And Redaction Considerations

Before disclosing Eviquire packages, review whether the package contains sensitive artifacts beyond the visible evidence. Browser profiles, cookies, PCAP files, TLS key logs, mailboxes, downloaded files, and video recordings may contain private, privileged, or out-of-scope information. Legal teams should decide whether complete packages, filtered exports, reports only, or specific evidence packages are appropriate for disclosure. Never alter the original package to perform redaction. If redaction is required, create a derivative disclosure set, document the redaction process, preserve the original, and record hashes for both the original and derivative materials.

21. Version 6 Interface Reference

This section is a quick-reference map of the principal controls shown in the current desktop screens. It complements the procedural chapters; the legal and technical requirements for each operation still apply.

21.1 Case Manager: Work Areas

UI area	What it shows	Typical operation
Left navigation rail	Case Manager, About, Settings, Support, Close	Move between the primary application functions.
Cases List	Case identity, external reference, open/closed status, date, acquisition count, description	Select a case; create or import cases.
Acquisitions in Selected Case	Each acquisition's ID, type, name, date, duration, size, version, description	Start web/mobile/mail acquisition; select a session to inspect.
Evidence in Selected Acquisition	Each item's ID, type, time, investigator, domain, URL	Select a capture item and review the snapshot and hash data.
Right Details Panel	Context for current case, acquisition, or evidence selection	Review record metadata, attachments, hash and blockchain references.

21.2 Case Details: File Handling and Timestamp Fields

When **CASE DETAILS** is active, the **Attached Files** section lists supporting case documents separately from collected evidence. For attachments, the panel can display a submitted **Summary SHA-256** hash and a **Celo** transaction identifier. A copy control

and a link control appear beside the transaction in the example. Inspect the complete case package when validating both the attached document and its corresponding integrity record.

The **EDIT CASE → FILES** view includes the columns **FILE**, **COMMENT**, **SIZE**, and **ADDED**, plus **ADD FILES** and per-file operations. File changes are saved immediately, and all attached files are accessible to whoever receives an exported case. This is especially relevant when attachments contain warrants, internal notes, privileged legal material, or identifiers.

21.3 Acquisition Details: Recorded Options

The acquisition details list is the post-acquisition record of which technical options were active. The illustrated example reports **True** and **False** for each enabled feature, including **Video Recording**, **System Network Traffic Dump (PCAP)**, **Application Network Traffic Dump (HAR)**, **Chromium Network Audit (NetLog)**, **Realtime Evidence Timestamp**, **Advanced Resources Collection**, **Advanced Cookies Collection**, and several domain/system options. It also records **Automatic Cookie Consent** and **Content Language**.

Compare this record to the original collection plan. If expected data such as a HAR or packet capture was not enabled, document that limitation rather than implying the artifact should exist.

21.4 Evidence Details: Snapshot and Package Records

For the selected screenshot, the interface displays **Package File Name** and **SHA2_256 File Hash**, **Summary File Name** and **SHA2_256 File Hash**, a blockchain **Submitted Hash** and transaction reference where available, and a visual **Evidence Snapshot**. The same evidence ID appears in the evidence list and in filenames. This allows reviewers to cross-reference one visible capture with its packaged forensic records.

21.5 Suggested First Acquisition Checklist

1. Select the correct open case and check the internal/external case references.
 2. Start **New Web Acquisition** from the acquisitions band.
 3. Enter a descriptive acquisition name and objective.
 4. Confirm investigator, user agent, proxy/Tor, content language, and DNS settings.
 5. Enable the intended PCAPNG, HAR, NetLog, and video outputs, considering their privacy and size implications.
 6. Decide whether the target warrants WHOIS, system information, certificates, advanced resources, or cookie collection.
 7. Configure automatic cookie consent only when the protocol requires the interaction.
 8. Enable realtime timestamping where the engagement requires it, then start collection.
 9. After closure, select the acquisition and inspect the settings that were actually recorded.
 10. Inspect evidence snapshots, review reports and logs, validate hashes, and export through a secure handoff process.
-

21.6 Acquisition Review Tool Navigation

The review workspace contains eleven tabs: **SUMMARY**, **TIMELINE**, **EVIDENCES**, **VIDEO**, **SCREENSHOTS**, **REPORT**, **COC**, **DOWNLOADS**, **RESOURCES**, **CERTIFICATES** and **COOKIES**. Chapter 12 provides illustrated workflows for each tab and explains how to distinguish previewed content from the preserved evidence and its integrity records.

22. Release Evolution and Further Help

22.1 From Version 4.8 to the Version 6 Interface

This edition updates the earlier Version 4.8 manual to reflect the three-level Case Manager shown in Version 6 and changes introduced during the 2026 release cycle. The operational procedures in this manual follow the current labels while retaining the established forensic concepts: cases, acquisitions, evidence items, hash lists, timestamps, report packages, and chain-of-custody records.

Release generation	Significant documented changes
Version 4.8 baseline	Core forensic web collection, evidence packaging, hashes and timestamping, case/acquisition/evidence reports.
5.0.6110.2 (10 May 2026)	Modern UI refinements, evidence comments included in acquisition reports, acquisition-review screenshot download, proxy manager and bulk proxy integration, improved capture and chain-of-custody presentation.
5.0.6110.13 (5 Aug 2026)	macOS beta, FFmpeg-based recording redesign, window/audio isolation improvements, modernized mobile/mail interfaces, pageshot and autoscroll enhancements.
6.0.6110.16 / 6.0.6110.18 (Oct 2026 generation)	Illustrated Case Manager interface, expanded New Acquisition option groups, visible HAR and NetLog options, automatic cookie consent controls, and case attachment handling and integrity display.

22.2 Official Release Information

Refer to the vendor's support articles for maintenance-specific installer information, known issues, and release notes:

- [5.0.6110.2 — 10 May 2026](#)
- [5.0.6110.13 — 5 August 2026](#)
- [6.0.6110.18 — 16 October 2026](#)

The Version 6 screens reproduced here come from Version 6.0.6110.16; the release-specific article is the reference for later maintenance-build corrections.

22.2.1 What Version 6.0.6110.18 Adds to This Manual

This revision incorporates the October 2026 **unified timeline, deep cookie and TLS certificate evidence, HAR and NetLog, historical website comparison, local report generation and branding, social metadata, case attachments, individual evidence downloads, integrity verification, cookie-consent automation, portable packages, recording and media review, and acquisition recovery.**

Operational improvements include Windows acquisition protection; FreeTSA and blockchain timestamp concurrency with bounded waits; reuse of acquired WHOIS, robots.txt, and sitemap context within an acquisition; better handling of dynamic social-media interfaces; and more robust Pageshot cancellation, scrolling, and PDF generation.

Known limitations include changing social-media structures, potentially sensitive HAR/NetLog contents, host-side Linux packet-capture prerequisites, compatible X11/XWayland support for the ApplImage, recommended consistent multi-monitor scaling, and macOS beta status.

22.3 Help, Updates, and Training

Product website: <https://eviquire.com/>. Support portal: <https://help.eviquire.com/>. For in-app assistance, select **Support** from the left sidebar. For formal training, consult the [Advanced Web Forensics Course / CWFE](#). Publisher: Ricta Technologies Srl (www.ricta.io). For technical support email support@ricta.io.

Final reminder: Use only the capabilities provided by your installed edition and permitted under the engagement authorization. Evidence protection depends on the full capture and handling workflow, not on any single screenshot, hash, or blockchain entry.

22.4 Publisher, Help and Product Information

Eviquire is developed and published by Ricta Technologies Srl. Product documentation, software updates and support information should be obtained from the official channels below.

Software product	Eviquire Web Forensics Browser
Developer and publisher	Ricta Technologies Srl
Publisher website	www.ricta.io
Technical support	support@ricta.io



Copyright © 2026 Ricta Technologies Srl. All rights reserved.