



EVIQUIRE

QUICK START GUIDE

Your first forensic web evidence acquisition

CREATE → CAPTURE → REVIEW → VERIFY → EXPORT

Designed for investigators who need to preserve online evidence with documented collection steps, integrity information and a structured case package.

01

CREATE A CASE

02

START ACQUISITION

03

CAPTURE EVIDENCE

04

REVIEW

05

VERIFY

06

CLOSE & EXPORT

DESKTOP EDITION • v6.0.6110.18 • 17 October 2026

Interface screenshots: build D6.0.6110.16. Appearance and available options may vary by operating system, build and license.



A product of Ricta Technologies Srl

www.ricta.io | support@ricta.io

BEFORE YOU START

Prepare the workstation

A short preparation check helps preserve the acquisition context and prevents avoidable capture failures.

Install or launch Eviquire

- 01 Obtain the approved package from www.eviquire.com: Windows installer or portable ZIP; compatible Ubuntu AppImage; or an authorized macOS beta build.
- 02 Install the application, or extract and run the portable package. Launch Eviquire and sign in using your registered credentials or organization-approved activation method.
- 03 Confirm the correct investigator profile, application version, writable evidence-storage location, available disk space and system time.

NETWORK CAPTURE NOTE PCAPNG capture requires supported host packet-capture components and permissions (for example TShark/dumpcap). A portable Eviquire package does not install host capture permissions.

Understand the evidence structure

CASE	ACQUISITION	EVIDENCE
The investigation container. A case can contain multiple acquisition sessions.	One recorded collection session, with its options, logs and artifacts.	An individual screenshot, pageshot, source capture, download or other captured item.

First-run checklist

- Confirm you are authorized to access and collect the target web content.
- Use a stable connection and adequate writable storage; avoid unrelated browsing or applications.
- Set a clear case reference and meaningful acquisition name.
- Decide in advance whether you need video, PCAPNG/HAR, cookie collection or other sensitive artifacts.

START SIMPLE For your first practice case, capture a page you are authorized to use. A screenshot plus a local report and acquisition Chain of Custody demonstrates the basic workflow without requiring every advanced option.

Time stamps and admissibility

Eviquire records acquisition activity and integrity metadata. A recorded hash or timestamp supports evidence preservation; it does not independently establish the truth, authorship or legal admissibility of web content.

STEP 01 / CASE MANAGER

Create your first case

The case is the outer container for all evidence collected for the same investigation.

- 01 Select Case Manager in the left navigation, then choose New Case.
- 02 In NEW CASE CREATION, review the generated Internal Case ID and enter a descriptive Internal Case Name and a short, factual Description.
- 03 Add External Case ID / External Case Name if your organization uses an incident or matter reference. Leave Advanced bulk options off for a standard first case.
- 04 Select CREATE NEW CASE. Confirm the new record appears in the CASES LIST.

NEW CASE CREATION

Internal Information:

Internal Case ID: C-20261017-165454608UTC

Internal Case Name: C-20261017-165454608UTC

Case Owner: eqcom-demo001@riccardotani.com

Description: type in Comment

External Information:

External Case ID: type in External Case ID

External Case Name: C-20261017-165454608UTC

Advanced

☐ Bulk Pageshot Acquisition ☐ Dump Images ☐ Download Video

type in URL's

CANCEL CREATE NEW CASE

Figure 1 • New Case Creation: enter investigative context, then create the case.

What you should see

Internal Case ID	External Case ID	Status	Date	No. Acq.	Desc
C-20261013-141230099UTC		Open	13 Oct 2026 - 18:12:30	4	
C-20261013-034241855UTC		Closed	13 Oct 2026 - 07:42:41	1	
C-20261013-034021515UTC		Open	13 Oct 2026 - 07:40:21	3	
C-20261013-031930393UTC		Open	13 Oct 2026 - 07:19:30	40	
C-20261012-162457697UTC		Open	12 Oct 2026 - 20:24:57	3	
C-20261012-142639164UTC		Closed	12 Oct 2026 - 18:26:39	1	
C-20261012-132041735UTC		Open	12 Oct 2026 - 17:20:41	12	
C-20261012-024850163UTC		Open	12 Oct 2026 - 06:48:50	1	
C-20261012-024538887UTC		Closed	12 Oct 2026 - 06:45:38	1	

ID	Type	Name	Date	Duration	Size	Version
A-20261012-204240897UTC	Web Acquisition		13 Oct 2026 - 00:42:40	00:00:17	22.68 MB	D6.0.6110.15
A-20261012-202253636UTC	Web Acquisition		13 Oct 2026 - 00:22:53	00:00:21	21.62 MB	D6.0.6110.15
A-20261012-162459455UTC	Web Acquisition		12 Oct 2026 - 20:24:59	00:00:32	32.53 MB	D6.0.6110.15

Figure 2 • The Case Manager shows the case list and the acquisitions belonging to the selected case.

STEP 02 / WEB ACQUISITION

Configure an acquisition

Each acquisition is a separate, time-bounded collection session within the selected case.

- 01 Select your case. In ACQUISITIONS CONTAINED IN THE SELECTED CASE, choose New Web Acquisition.
- 02 Enter an Acquisition Name, verify the Investigator and add a factual Description. Check Browser user agent, Proxy, TOR Proxy, Content Language and DoH Settings only as needed for the investigation.
- 03 Review the Acquisition options on the right. Enable only collection methods your case requires; then choose START NEW ACQUISITION.

NEW ACQUISITION

Acquisition ID

A-20261017-113645660UTC

Investigator

Eviquire Demo

Acquisition Name

type in Acquisition Name

Description

type in Comment

Browser user agent

Proxy

No proxy

☐ TOR Proxy

Content Language

en-US

DoH Settings

Acquisition options:

Core options:

☒ Video Recording

☒ Network Traffic

☐ Application Network Acquisition (HAR)

☐ Chromium Network Audit (NetLog)

Evidence options:

☒ Realtime Evidence Timestamp

☐ Save Evidence Report Online

Domain & System Artifacts collection:

☐ Automatic Tests

☐ Fetch WHOIS Data

☐ Save System Info

☐ Save Certificates

Browser & Web Artifacts

☒ Advanced Resources Collection

☐ Advanced Cookies Collection

☐ Automatic Cookie Consent

Reject all

CANCEL

START NEW ACQUISITION

Figure 3 • Web acquisition configuration: settings become part of the recorded collection context.

Settings you are most likely to use

Video Recording	Records session actions; generates a larger and potentially sensitive acquisition package.
Network Traffic / HAR	PCAPNG captures host packets when configured. HAR captures browser-observed HTTP activity; they are different artifacts.
Realtime Evidence Timestamp	Requests external timestamps for eligible finalized evidence integrity records when enabled.
Automatic Cookie Consent	Optional; select Reject all or Accept all when applicable. Only actual interactions are reflected in Chain of Custody.

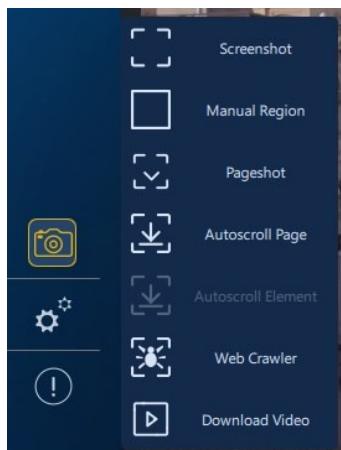
IMPORTANT Local PDF/JSON evidence reports can be created even when “Save Evidence Report Online” is not selected. Online reporting is a separate choice.

STEP 03 / FORENSIC BROWSER

Capture your first screenshot

Use the forensic browser rather than an external browser so the image is linked to the acquisition records.

- 01 Wait for the Eviquire forensic browser to launch, then navigate to the target URL.
- 02 Allow the page to load and verify the page, URL and visible content. If relevant, document any login, consent or other interaction.
- 03 Select the camera icon in the left toolbar to open the capture menu. Choose Screenshot to preserve the current visible state.
- 04 Wait for confirmation that the screenshot was saved. Repeat for any additional relevant on-screen state.



CAPTURE MENU

- Screenshot — visible browser state.
- Manual Region — selected portion of the page.
- Pageshot — extended page capture.
- Autoscroll Page — guided page traversal.
- Autoscroll Element — a detected scrollable region, when available.
- Web Crawler / Download Video — supported advanced workflows.

Figure 4 • Capture menu accessed from the camera icon in the browser.

What gets preserved?

A screenshot evidence item may include a PNG, supporting page/source context, report and summary JSON, relevant hashes and Chain-of-Custody entries when finalized. The exact package contents depend on enabled options and collection results.

FORENSIC PRACTICE Capture surrounding context before taking a narrow region screenshot. Avoid editing the original files, and do not treat an image alone as the complete forensic record.

OPTIONAL / PAGESHOT

Preserve a long or dynamic page

Use Pageshot or Autoscroll when the relevant material extends beyond one visible screen.

- 01 Navigate to the target page and wait for it to stabilize. Open the camera menu and choose Pageshot or an applicable Autoscroll command.
- 02 In Page Shot Options, choose Page Shots for visual frames and Source Code for associated page source, where appropriate.
- 03 For supported social platforms, Expand comment/replies may collect additional visible discussion context. Select Smart scroll direction unless a specific direction is required.
- 04 Confirm with OK. Avoid changing tabs or interacting with the page while automatic scrolling and capture are in progress.

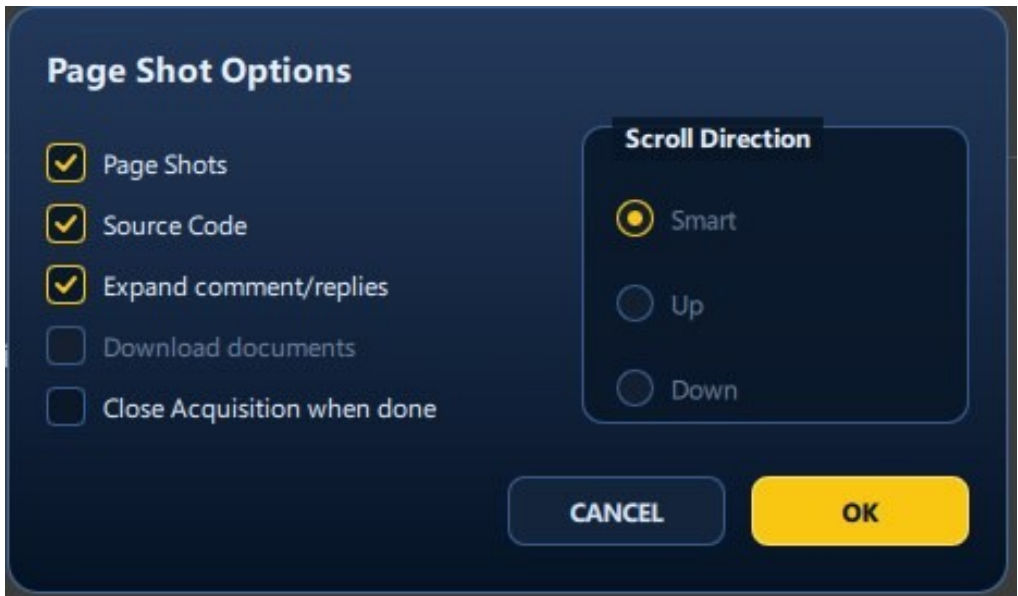


Figure 5 • Page Shot Options: choose outputs, optional reply expansion and scroll behavior.

Which capture is right for the task?

SCREENSHOT	A fast record of the visible page state at a particular moment.
PAGESHOT	A sequence of frames preserving a long page beyond the current viewport.
AUTOSCROLL ELEMENT	Capture a detected scrollable panel, such as a comments list, when available.

Understand the limitations

On dynamic sites, content can move, disappear or load during scrolling. Automatic comment expansion and consent handling depend on supported website structures; neither guarantees a complete copy of all available content. Consult the acquisition logs when describing what was actually captured.

QUICK CHECK If you are testing your first acquisition, capturing one screenshot is sufficient to proceed to review. Pageshot and comment expansion are optional additions, not prerequisites.

STEP 04 / REVIEW

Inspect your acquisition

After collection, end the acquisition through the application and wait for finalization before inspecting its records.

- 01** End the browser acquisition using the application's normal close/finish workflow. Allow media, reports, hashes and archives to finish writing.
- 02** In Case Manager, select the case and acquisition. Check the acquisitions table for the session and the evidence table for captured items.
- 03** Open Acquisition Review for the selected session. Choose EVIDENCES to select an evidence item and preview its files; use SCREENSHOTS for rapid visual review.

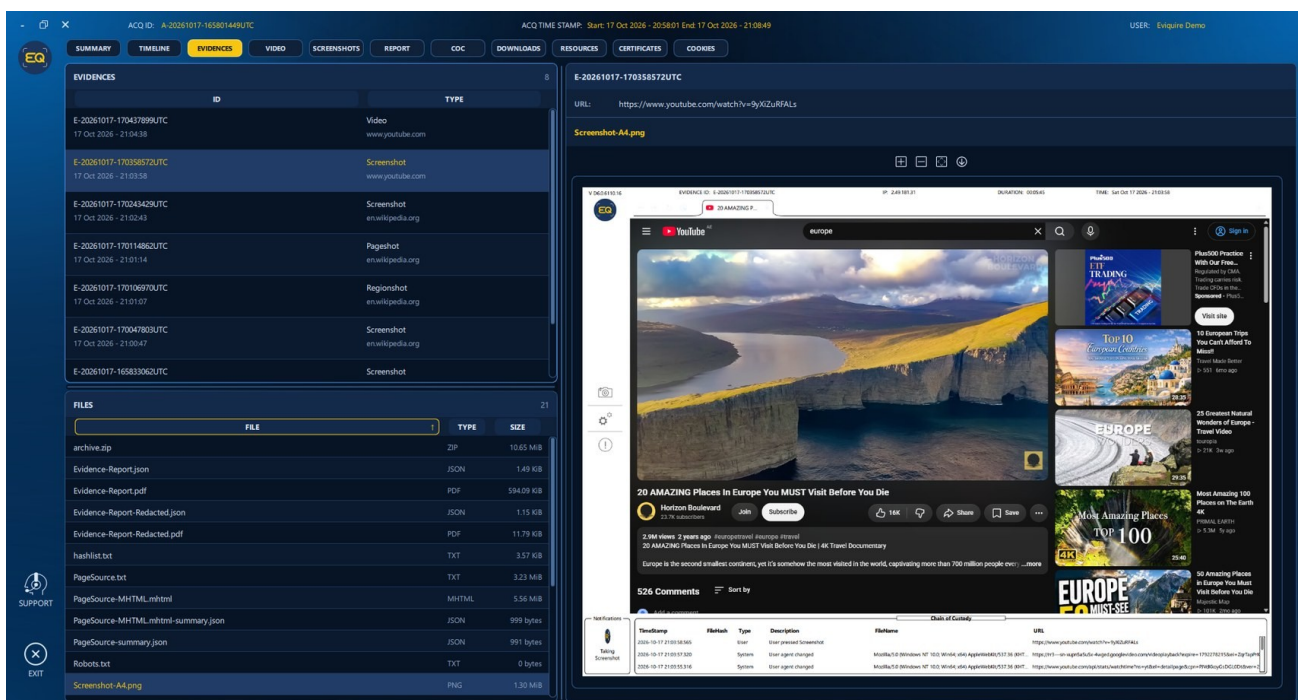


Figure 6 • Acquisition Review: the EVIDENCES tab pairs the captured item with its file inventory and preview.

Where to look next

SUMMARY

Browse the acquisition archive, including reports, source files, hashes and network artifacts.

COC / TIMELINE

Inspect timestamped user/system actions and the sequence of selected evidence, video, cookie and TLS events.

REPORT

Read the acquisition PDF, including case linkage, investigator, acquisition settings and package integrity fields.

REMEMBER The viewer shows read-only previews. Original evidence packages, summaries and recorded hashes remain the primary forensic deliverables.

STEP 05 / INTEGRITY

Verify before delivery

Use the built-in integrity checks to identify missing or changed files before closing the case.

- 01 In Case Manager, right-click the case row and select Verify all acquisitions.
- 02 Wait for checks to finish. Review acquisition statuses and use the information button to inspect the detailed file findings for each session.
- 03 If a result indicates a mismatch or missing file, preserve the original material, review the record and investigate before relying on the package.

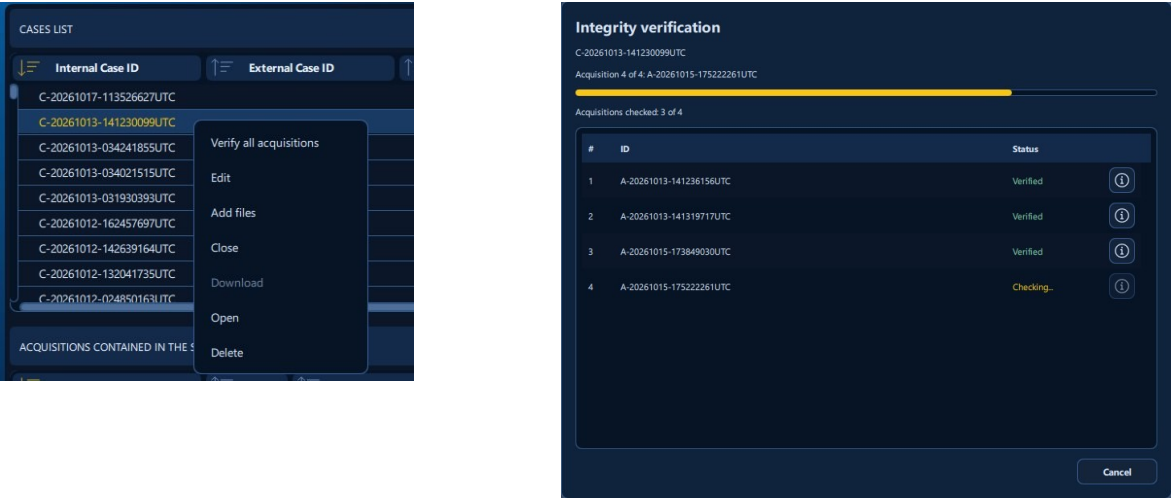


Figure 7 • Case context menu and verification progress, with an entry for each acquisition.

Reading a verification result

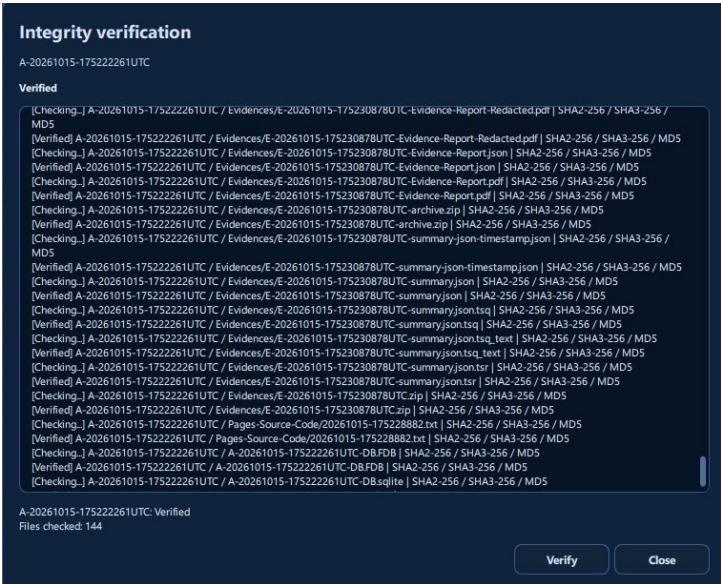


Figure 8 • Detailed findings show individual file checks and the verification result.

WHAT VERIFICATION MEANS A successful built-in hash check supports file integrity; it does not prove the truth of the source content or independently validate every external timestamp or blockchain receipt.

STEP 06 / FINALIZE

Close, export and preserve

Complete the case only after all intended acquisitions and evidence have been reviewed.

- 01 Confirm the case includes all intended acquisitions. In Case Manager, right-click the case and select Close.
- 02 In CLOSE THE CASE, choose an export Password if required by your workflow. Select Save Report Online or Add Viewer only when needed and authorized.
- 03 Select CLOSE THE CASE. Wait for compression, reports, hashes and final packaging to complete; do not interrupt storage or shut down the workstation.
- 04 Locate the exported case ZIP and record its SHA-256 using an approved verification tool. Transfer a copy using an approved secure method; deliver any password separately.

Figure 9 • CLOSE THE CASE provides password and optional reporting/viewer selections.

IMPORTANT Closed Eviquire cases cannot be reopened for editing. Preserve the closed original and create a separate supplemental case if further collection is required.

First acquisition — completion check

- ✓ Case ID, acquisition ID and investigator are correct.
- ✓ The intended screenshot or other evidence appears in the evidence list.
- ✓ The acquisition report and Chain of Custody are available.
- ✓ Integrity verification was completed and exceptions were documented.
- ✓ The final ZIP was preserved, its export hash was recorded, and access is controlled.

Need assistance?

Ricta Technologies Srl • Product: Eviquire

Technical support: support@ricta.io | Help Center: help.eviquire.com

Product website: www.eviquire.com | Developer: www.ricta.io

When contacting support, provide the application version, operating system, affected workflow and relevant error details. Do not send original evidence, credentials, cookies or TLS secrets unless explicitly authorized and securely transferred.