

YOUR SCREENSHOT IS NOT SELF-AUTHENTICATING

A screenshot can faithfully show what was visible and still leave the reviewer unable to identify the subject, population, source, method, time, or claim.

PRACTITIONER POSITION

PCI DSS assessment work examines evidence that is appropriate to the requirement and the entity's implementation. PCI SSC FAQ 1566 reinforces that a QSA remains responsible for determining whether collected evidence is specific to the assessment scope, directly related to the requirement, within the applicable timeframe and testing-procedure conditions, and sufficient to support an opinion about whether controls are in place. FAQ 1567 preserves the same independent-review boundary when underlying evidence comes from another attestation engagement. Neither FAQ prescribes a screenshot template. My practitioner position is that a screenshot becomes assessment-usable only as part of a capture package: the request or claim, exact subject, authoritative source location, visible state, population and filters, observation time and timezone, collector and method, transformation and sensitivity treatment, corroborating evidence, limitations, and custody record travel together. A screenshot may be excellent evidence of a point-in-time configuration. It usually cannot, by itself, establish completeness, historical operation, recurring performance, effectiveness, or a compliance conclusion. Capture enough context to make the observation attributable; preserve enough surrounding evidence to make the claim testable.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A control owner submits a tightly cropped image showing 'Enabled.' The interface logo is absent. The tenant, environment, resource, policy state, exclusions, browser path, page count, filters, observation time, timezone, collector, and requested testing objective are unknown. The image may be genuine. It may even show the right setting. The assessor still cannot determine which system it describes, whether the displayed object is active, whether the visible rows are the full population, whether the capture falls within the assessment period, or what conclusion the image is supposed to support. The team responds with four more screenshots, each cropped differently. Volume increases; attribution does not.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The capture shows a value but not the setting name, resource, tenant, account, environment, or policy state.
- The filename or upload date is treated as proof of when the underlying condition was observed.
- A table screenshot omits filters, total count, pagination, exclusions, export logic, or the source used to establish completeness.

- A dashboard total is offered without the population, query, time window, failed items, or drill-down record.
- A terminal image hides the command, host identity, execution context, timezone, or whether output continued below the viewport.
- A browser address bar exposes a secret, session value, customer identifier, or sensitive path merely to prove navigation context.
- A crop, annotation, blur, redaction, or conversion replaces the original capture without a parent record.
- Several images are submitted with no sequence, overlap, stable capture ID, or explanation of how they form one observation.
- A point-in-time setting is used to claim that a recurring control operated throughout a period.
- The screenshot is attached before anyone writes the exact claim, testing objective, non-claim, or reopening trigger.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Write the evidence request and bounded claim before opening the capture tool. Name the requirement or testing objective, subject, environment, observation needed, relevant period, and conclusion the capture is not being asked to make. A screenshot without a declared job invites hindsight and overclaiming.

Prefer the authoritative source view. Capture the native administration page, report, command, configuration object, or system-of-record view rather than a summary dashboard or pasted transcription when practical. If a derivative view is necessary, identify its upstream source and preserve the path back to it.

Identify the subject at the same granularity as the claim. Provider logo is not tenant identity. Tenant is not subscription. Subscription is not resource. Hostname is not application instance. Show or record the organization, account, tenant, subscription, project, environment, resource, policy, rule, user, group, scan target, or other object that the setting actually governs.

Preserve navigation context without collecting secrets. Page titles, breadcrumbs, selected tabs, resource names, safe URL portions, command prompts, and object identifiers can establish provenance. Tokens, passwords, PAN, sensitive authentication data, private keys, recovery codes, unrelated personal data, and unnecessary customer information should not enter the capture merely to make it look complete.

Bind list and dashboard captures to their population. Record the query, filters, scope selector, date range, sort, total count, pagination, exclusions, empty-result behavior, and how completeness was evaluated. Visible rows are not automatically the complete population, and a clean summary is not automatically the underlying result set.

Separate the clocks. Preserve the control period, observation or execution time, source-generated time, capture time, and timezone or clock basis. A desktop clock can help orient a live capture, but it does not replace a source timestamp and it does not prove how long the displayed state existed.

For command-line evidence, preserve host or workload identity, effective user or role when relevant, the exact command, material parameters, untruncated output, exit or completion state, and time context. Prefer a retained transcript or native output alongside the screenshot when the command result is too large or too

consequential for one viewport.

For recurring controls, pair the frame with operating evidence. A screenshot can show that a feature is enabled now; occurrence records, logs, tickets, approvals, exception history, monitoring, or native reports may be needed to show that the process ran for the required population and period. One frame is not an occurrence history.

Treat multi-image captures as a sequence. Give the package a stable ID; number each frame; preserve intentional overlap; state what changed between frames; and record whether scrolling, expansion, filtering, impersonation, or navigation occurred. A reviewer should not have to infer order from filenames.

Preserve the original before cropping, annotation, redaction, conversion, or compression. Create a derivative record that identifies the parent, operator, time, reason, redacted field class, and digest where proportionate. Redact the sensitive value-not the source, subject, setting, or time context needed to understand the observation.

Finish with an admission decision that is not a compliance result. A capture may be usable, usable with corroboration, or require recapture because attribution is missing. After admission, the assessor still evaluates relevance, scope, timeframe, testing procedure, population, contradictions, and sufficiency. A beautiful screenshot can pass the capture check and fail the assessment question.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 What exact claim or testing objective is this capture intended to support, and what is it explicitly not being asked to prove?
- 02 Which organization, account, tenant, environment, system, resource, policy, rule, identity, target, or occurrence is visible or recorded?
- 03 Is this the authoritative source view, a summary, a derivative, or a manually assembled representation?
- 04 Which query, filters, time window, scope selector, count, pages, exclusions, and empty-result behavior define the displayed population?
- 05 Which clocks describe control operation, source generation, observation, capture, and upload, and what timezone makes them comparable?
- 06 Who or what collected the evidence, using which role, navigation path, command, parameters, and capture method?
- 07 What relevant state lies outside the frame: hidden tabs, continued output, collapsed sections, failed items, exceptions, alternate environments, or historical records?
- 08 Does the capture contain cardholder data, sensitive authentication data, secrets, unrelated personal data, or identifiers that should be omitted or redacted?
- 09 Is the file an original or derivative, and can every crop, annotation, redaction, conversion, and sequence step be traced to its parent?

10 What corroborating export, log, configuration file, ticket, interview, observation, or occurrence record is needed before the claim can be evaluated?

11 Can a cold reader reconstruct the capture package without calling the collector, and can the assessor still see exactly where the conclusion must stop?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Start with one evidence request and identify the exact claim, subject, source view, population, period, sensitivity boundary, and likely corroboration before capturing anything.

02 / MAP

Assign a stable capture-package ID and connect request, subject, source locator, navigation or command path, filters, clocks, collector, frames, original, derivatives, corroboration, claim, and custody.

03 / EXPLAIN

Describe what each frame directly shows, what source context establishes attribution, what population and period it represents, and which conclusions remain outside the frame.

04 / REDUCE

Remove secrets and unrelated data, replace decorative dashboard shots with authoritative views, eliminate redundant frames, and recapture any image whose provenance or subject was cropped away.

05 / PROVE

Run the cold-reader and evidence-admission checks, preserve the original and transformation chain, then evaluate the admitted package against the applicable testing objective without promoting capture quality into a compliance result.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A SCREENSHOT RECORDS A FRAME. A DEFENSIBLE CAPTURE PACKAGE RECORDS WHY THAT FRAME DESERVES TO BE BELIEVED-AND WHERE BELIEF MUST STOP.

Download the Screenshot Evidence Capture Record. Build one package from request through cold-reader check before uploading another anonymous green setting.

TECHNICAL GROUNDING

START WITH THE SOURCE MATERIAL

These references ground the practitioner interpretation. They do not turn the metaphor or method into official PCI DSS terminology.

- WACK-SOURCE-0001 / PCI DSS v4.0.1 / PCI Security Standards Council / [Open source](#)

- WACK-SOURCE-0080 / FAQ 1566: Can a QSA ask an auditor from the same company to collect evidence for a PCI DSS assessment? / PCI Security Standards Council / [Open source](#)

- WACK-SOURCE-0081 / FAQ 1567: Can a QSA rely on results from a non-PCI DSS assessment? / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / ASSESSOR_JUDGMENT / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-16 against canonical digest

c701d6a76b48617c89d51dfe0e55d89afbefd52344f9563f97106a0e5170671. Educational content, not a compliance determination.

Independent practitioner resource; not affiliated with or endorsed by PCI SSC. Authorship and authority classification do not determine legal intellectual-property ownership.