Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/authenticating-questioned-media/

MEDIA AUTHENTICATION

Authenticating Questioned Photographs, Audio and Video in the Age of Deepfakes and Generative AI

A questioned photograph, recording or video is now met on both sides with the same claim, that it is fabricated or that it is real, and a documented examination of the file and its history is how the examiner addresses it. Preserve the original file and the device that made it, then call (800) 868-8189 at any hour.

Published September 3, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why Media Authentication Calls for a Documented Method

As generative AI tools and effortless editing apps proliferate, trial attorneys and corporate boards are increasingly confronted with disputed photographs, audio recordings and video clips whose authenticity is challenged. At the same time, parties caught on genuine recordings increasingly raise the deepfake defense, claiming that authentic incriminating media was fabricated. Settling these disputes in court calls for a method the examiner can explain, test and defend. Federal Rule of Evidence 702 asks about a method's reliability and its known error rate, and a documented examination answers those questions with disclosed methods applied to the actual file, including recompressed social media copies.

How Container, Pixel and Sensor Forensics Examine a File

Global Digital Forensics conducts scientific media authentication engagements for retained counsel, internal auditors and insurers using our Forensic Media Analyzer workbench and laboratory examination protocols. Our examiners analyze four distinct technical layers. First, we inspect the binary container structure, MP4 and MOV atom trees and EXIF and XMP metadata tags to determine whether the file matches the exact structural signature of the claimed recording device or bears traces of editing software like Adobe Premiere or FFmpeg. Second, we examine compression history, quantization matrices, error level analysis and packet timestamps to detect splicing, frame drops or localized manipulation. Third, we analyze photo response non uniformity sensor noise and audio electrical network frequency consistency. Fourth, we correlate the file against the original recording handset or cloud backup whenever available.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What a Media Examination Can Conclude

Authentication examinations reach conclusions about consistency. The findings state whether the file's container structure, metadata, compression history, sensor noise and signal characteristics are consistent with the claimed capture device and history, or inconsistent with them in ways that indicate editing, synthesis or transcoding. An inconsistency can be localized to a region of an image, a span of audio or a range of frames, and the report says what the inconsistency is and what processes could produce it. A finding of consistency covers the aspects tested, which showed no indication of manipulation, and the report names those aspects so the court weighs the finding on that basis.

The file's history shapes what each layer can address. A video that passed through a messaging application has been recompressed and stripped of most metadata, which smooths the traces of editing and the signatures that tie the file to its camera alike. The examiner works such a file through frame level consistency, audio continuity and lighting and geometry, and turns to the sender's original and the capture device for the question of device origin. A clean result on a camera original carries more weight than the same result on a heavily recompressed copy, and the report weighs each finding accordingly.

The examination speaks to the file and to what its pixels and samples record. Meaning is weighed with context: an authentic recording can be misleadingly framed, and a real conversation can be cut at its start or end, where the cut sits outside the file, so the examiner reads the file alongside other copies and the account of how it was made. Our opinions address the file and its history, and counsel and the trier of fact draw the inferences about meaning. Our audio, video and image authentication page describes the scope of the examinations we perform and the kinds of questions they answer. Keeping the opinion focused on the file is what makes it useful to the court.

Rule 901, Rule 702 and the Arrival of Content Credentials

Media is authenticated under the same rule as any other evidence. Rule 901(a) asks for evidence sufficient to support a finding that the item is what its proponent claims, and 901(b)(9) permits authentication by “evidence describing a process or system and showing that it produces an accurate result” (Federal Rule of Evidence 901). A witness with knowledge may testify that a recording fairly depicts what they saw, and a forensic examiner may testify to the file's consistency with its claimed origin. Where the two conflict, the court weighs them, and the examiner's testimony must meet Rule 702, which asks for a disclosed method and a known error rate, the two things a documented examination supplies.

Content credentials are changing part of this picture. The C2PA specification defines a manifest that a capture device or editing application can cryptographically bind to a media file, recording the device, the actions taken and the identity of the signer. Where a file carries a valid manifest, the examiner can verify the signature and read the recorded history, which is strong evidence of provenance for the steps the manifest covers. Where a file carries no manifest, the examination proceeds through the other layers, since most cameras and applications are only beginning to produce manifests and a stripped manifest leaves no trace. A file without credentials is evaluated on its structure and history like any other.

Counsel can anticipate the deepfake defense against genuine recordings and meet it with the same examination used to detect fabrication. The strongest answer to a claim that a recording is synthetic is the camera original with its metadata and sensor noise intact, the device that produced it, and the account or

© 2026 Global Digital Forensics, Inc. All rights reserved.

cloud backup that received it, examined together. Our guide to Rule 702 and Frye scrutiny explains why novel detection techniques invite a hearing and how validation answers it. The party that preserved its original holds the strongest answer to the defense.

The Examination From Original Capture to Report

The engagement begins with provenance collection. We ask for the earliest available copy of the file, the device that produced it, the application through which it was shared, the accounts that stored it and the names of everyone who handled it. Where the device is available we acquire the file directly from it along with the device's own records of the capture, and where a cloud backup exists we export from the account under counsel's direction. Every copy is hashed and its history documented, because the comparison between copies is often where editing is first visible.

Analysis proceeds through the four layers the earlier sections of this guide describe, with the methods documented and the tools validated. Container and metadata analysis compares the file's structure to reference files from the same device model and software version. Compression and signal analysis examines quantization, encoding history, frame timing, audio spectral continuity and electrical network frequency where a mains signal is present. Sensor and content analysis examines photo response non uniformity against exemplar images from the claimed device, lighting and geometry, and the physical plausibility of motion and shadows. Each finding is recorded with the method and the exemplar used.

The report states the conclusions as consistency findings with the reach of each, explains the methods in terms a court can follow and attaches the data that supports each finding. Where testimony is needed, the examiner presents the same material with demonstratives drawn from the actual file. Our Forensic Media Analyzer is the workbench we use for much of this analysis, and the photo forensics (evestigate.com/tools/photo-forensics/) and video forensics (evestigate.com/tools/video-forensics/) tools let counsel look at a file locally before the engagement begins. Those tools run entirely in the browser and keep the evidence on your computer, so a local look leaves the file as it was.

Handling Steps That Protect the Record

The first step is keeping the questioned file in its original form. Messaging applications and email clients recompress what they carry, so the file moves by direct copy and the original stays in place, which lets the examination work from the original rather than a transcoded copy. The second is keeping the file out of editors, because saving it in an editor, even with no changes, rewrites the container and metadata. The third is copying the file itself rather than capturing a screenshot or screen recording, since a capture is a new file with its own structure and the examiner compares the original's structure to the device.

The fourth step is securing the device. The camera or phone that produced a recording holds the strongest evidence of its origin, including the device's own capture records and the sensor pattern that can be compared to the file, so it is kept in its current state and held back from reset or reissue. The fifth is preserving the account. Cloud photo libraries and messaging backups often hold a copy closer to the original than anything on a device, and their retention follows settings and provider policy, so counsel directs their preservation early.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Who acts before the first call: whoever holds the file copies it unopened, records where it came from and when, and holds further circulation. Whoever holds the device isolates it and keeps it in its current state. Counsel directs the preservation of accounts and requests originals from the other parties who hold copies. Our common digital evidence mistakes resource covers the general preservation pattern, and the examiner can walk through the specifics of a media file on the first call. The earlier the original is secured, the more the examination can say about it.

Inspect Your Questioned Media Locally Right Now

Preserve the original file bytes of a questioned image or video first, because messaging apps strip metadata and recompress pixels the moment a file is re saved, texted or emailed inline. You can run an initial, zero upload inspection in your browser right now using our 18 view Photo Forensics (evestigate.com/tools/photo-forensics/) workbench or our Video Forensics (evestigate.com/tools/video-forensics/) analyzer, or call Global Digital Forensics at (800) 868-8189 to engage a senior media authentication examiner. The initial consultation is free.

The Four Layers of a Media Examination

The examination works through layers of technical analysis, each with a disclosed method. This table names each layer, the question it asks, what a finding at that layer can state and what the examiner relies on to reach it. Read the last column against how the questioned file reached you, because a video that passed through a messaging application has been recompressed, and the examiner then reaches for the original and the device. A finding of consistency covers the aspects tested, and the report names them so the court weighs it on that basis.

The four analytical layers of media authentication, what each can conclude and what each relies on.

Layer	Question it asks	What a finding can state	What the examiner relies on
Container and metadata	Does the structure match the claimed device and software	Consistency with a camera original or traces of editing software	The earliest available copy, since recompression strips metadata
Compression and encoding history	Does the quantization and packet timing show reprocessing	Splicing, frame drops or localized change	The least transcoded copy available
Sensor and signal analysis	Does the sensor noise or mains frequency stay consistent	A match or mismatch against exemplars from the device	Exemplars from the claimed device
Comparison to the original	Does a claimed original or backup agree with the file	Where editing first becomes visible between copies	An earlier copy or backup to compare
Content credentials	Does a C2PA manifest verify and read	Verified provenance for the steps the manifest covers	The manifest where one is attached, with the other layers carrying the work where none is

© 2026 Global Digital Forensics, Inc. All rights reserved.

In COMLAB v. Kal Tire, metadata analysis showing a last modified time that post dated the date last saved supported the court's finding of fabrication, the layered examination this guide describes applied to documents.

Try the Tool Before You Call

Open the Photo Forensics workbench (evestigate.com/tools/photo-forensics/) and load the questioned photograph as it was received, before anyone resaves it. Work through the views in order: the file structure and embedded text views tell you whether the container matches a camera or an editor, the recompression view shows regions saved at a different quality from the rest of the image, the noise views show whether the sensor pattern is consistent across the frame, and the metadata view records the hash of the file you examined. The branded report downloads to your computer and nothing is uploaded. Treat a clean result as a first look that a laboratory examination builds on. When the views disagree, or the matter turns on the image, call so provenance can be tested against the device or cloud backup.

Load the questioned clip into the Video Forensics analyzer (evestigate.com/tools/video-forensics/) and start with the container and timing views, because a clip that was exported from an editor or a generator carries a different structure and frame cadence from a phone recording. Step to the frames that matter and examine each in detail, then add a reference recording from the same device or scene when you have one so the two can be compared. The optional model results run on your device and are read as the page describes. Keep the file as received. When the timing, structure and frame evidence point in different directions, call for a laboratory examination under the direction of counsel.

How to Begin and What Happens on the First Call

Bring the questioned file in its earliest available form, a note of where it came from and who has handled it, the device that produced it if known, the accounts and applications through which it passed, and the proposition the file is offered to prove or disprove. The examiner asks how the file was received, whether the original device or account is reachable, whether other copies exist, what the opposing party claims about it and whether a declaration or testimony will be needed. The conversation produces a written proposal naming the copies to be collected, the device and account acquisitions, the analyses to be performed, the deliverable and the timing drivers such as the availability of exemplars. The initial consultation is free. Call (800) 868-8189 at any hour.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: C2PA technical specification and Guardians of Forensic Evidence report.

Authorities cited in this guide: Federal Rule of Evidence 901. Supplies the authentication standard and the process or system illustration quoted in the guide, current text at Cornell LII. Federal Rule of Evidence 702. Sets the reliability standard a media examiner's disclosed method and known error rate are built to meet, current text at Cornell LII. C2PA technical specifications. Defines the content credential manifest that binds provenance data to a media file, current published specification consulted October 2026. NIST, Guardians of

© 2026 Global Digital Forensics, Inc. All rights reserved.

Forensic Evidence: Evaluating Analytic Systems Against AI Generated Deepfakes. Reports NIST evaluation of automated deepfake analytic systems and their performance, as published by NIST and cited on the existing page.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Media Authentication

Can you tell whether a video is a deepfake?

We can examine a video for indications that it was synthesized or manipulated, including container and encoding inconsistencies, frame timing anomalies, lighting and geometry errors, audio discontinuities and sensor pattern mismatches, and we can state whether the file is consistent with the claimed capture. Our conclusions rest on the file's own structure and recorded history, examined with disclosed methods and known error rates, which is what a court weighs. The report describes what was found and how far each finding reaches.

Can a recording that came through WhatsApp or iMessage be authenticated?

Yes, it can be examined. Messaging applications recompress media and strip most metadata, which smooths both the traces of editing and the signatures that tie the file to a device, so the examination works through frame level and audio analysis of the transmitted copy. For device origin, the examiner turns to the sender's original file and device, which counsel can request, and compares the two. The report explains which conclusions the available copy supports.

Do you need the original device to authenticate a photo or video?

The device strengthens the examination considerably, and the examination also proceeds from the file itself. The device provides exemplar images for sensor pattern comparison, its own records of the capture and reference files that show how that device and software version structure their output. When the device is unavailable, the examination draws on the file's internal consistency and on reference data from the same device model, which serves findings of inconsistency well, and the device itself adds the strongest support for origin. We advise counsel on the value of obtaining the device in each matter.

What does a media authentication report say?

It identifies the file examined and its provenance, describes each method applied and the tools and exemplars used, and states findings as consistency or inconsistency with the claimed origin and history, localized to regions, time spans or frames where applicable. It explains what each finding shows, accounts for recompression and for which originals were available, and attaches the supporting data. It is written so the examiner can present the same material in a declaration or at trial.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Can you determine whether an audio recording was edited or spliced?

Often. Audio analysis examines spectral continuity, background noise consistency, the electrical network frequency signature where mains hum is present, encoding history and container structure for indications of cuts, insertions or transcoding. Carefully made edits in heavily compressed files call for closer work, and the report states the weight each finding carries. We also compare the questioned recording to the recording device and to other copies where they exist, which is frequently where an edit first becomes visible.

Web Addresses for the Sources Cited

1. Federal Rule of Evidence 901: https://www.law.cornell.edu/rules/fre/rule_901
2. Rule 702: https://www.law.cornell.edu/rules/fre/rule_702
3. C2PA specification: https://spec.c2pa.org/specifications/
4. Guardians of Forensic Evidence report: https://www.nist.gov/publications/guardians-forensic-evidence-evaluating-analytic-systems-against-ai-generated-deepfakes

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.