THE DIGITAL FORENSICS BRIEF

Phone Data Extraction, LLC & The PowellPath Group

WHEN ARTIFICIAL INTELLIGENCE MANUFACTURES EVIDENCE

What lawyers need to know about false digital proof, challenged authenticity, and the forensic work required to sort one from the other

AUTHOR Taylor J. Black

DATE May 12, 2026

FALSE DIGITAL PROOF | CHALLENGED AUTHENTICITY | NATIVE SOURCE DATA | FORENSIC EXAMINATION

EDITOR'S NOTE

The authentication problem has changed

Artificial intelligence has changed the proof problems that lawyers face in both civil and criminal matters. A digital exhibit can now be fabricated, altered, stripped of context, or challenged as fake with far less effort than most courts and counsel would have expected even a short time ago. That shift affects how lawyers should think about screenshots, exported documents, social-media records, video clips, audio files, and phone extractions.

This issue of The Digital Forensics Brief is not an advertisement and is not meant to stir panic. It is meant to describe the problem plainly. The legal system is entering a period in which digital evidence can no longer be treated as self-proving merely because it appears familiar on a screen or in a PDF. Native source data, provenance, metadata, chain of custody, and disciplined technical examination matter more now than they did before the rise of generative systems.

What follows is a short paper for lawyers who need to understand where the risk lies, how fabricated evidence is likely to appear in litigation and investigation, and what digital forensics experts actually do when authenticity is in doubt.

AT A GLANCE

- False digital proof and unsupported claims that real evidence is fake now create paired risks.
- Forensic work focuses on provenance, metadata, device and account artifacts, logs, and chain of custody.
- Screenshots, forwarded PDFs, and short clips are presentations of evidence, not the native source.
- Early preservation often determines whether authenticity can be tested or merely debated.

Prepared for lawyers evaluating digital communications, recordings, photographs, video, account records, exported documents, and phone data extractions.

FEATURE ARTICLE

When Artificial Intelligence Manufactures Evidence

What lawyers need to know about false digital proof, challenged authenticity, and the forensic work required to sort one from the other

Artificial intelligence has altered the economics of fabrication. What once required time, technical competence, and a workable cover story can now be produced in minutes: a text exchange that never occurred, a voice recording of words never spoken, a photograph of an event that never happened, a PDF that appears ordinary until someone examines the underlying file structure, or a video clip that borrows enough real detail to make the false portion difficult to spot on casual review.

The legal problem is not limited to fabricated evidence offered as genuine. There is a second problem, and it is just as serious. Authentic evidence can now be attacked as fake with more surface plausibility than before. In practical terms, lawyers and courts are now dealing with two threats at once: false digital proof dressed as real evidence, and real digital proof treated as suspicious merely because modern tools have made fabrication easier.

This is no longer a theoretical concern. Federal authorities have publicly warned that criminals are using voice clones, fake identification documents, and convincing video in fraud schemes. NIST is now conducting formal work on media forensics and deepfake evaluation because synthetic media has become a real evidentiary problem rather than an academic one. And the federal judiciary is actively studying whether the Federal Rules of Evidence should address deepfake challenges more directly. As of May 7, 2026, the Advisory Committee on Evidence Rules was still considering, but had not adopted, a possible Rule 901(c) directed to evidence alleged to have been fabricated in whole or in part by generative artificial intelligence.

That development should get the attention of every litigator and every criminal defense lawyer. Courts do not revise the authentication rules because of a passing technology fad. They do so because the ordinary assumptions behind authentication are under strain.

> *The danger now is not just that a false exhibit can be made quickly. It is that the false exhibit can begin to drive the case before anyone has tested the native source.*

In civil cases, AI-assisted fabrication can appear in places counsel already see every week. A screenshot offered to prove notice. A cropped email thread offered to prove knowledge or consent. A photograph offered to prove location, condition, injury, or property damage. A social-media post used to show bias, motive, harassment, or reputation. A spreadsheet or invoice used to support damages. A business record exported into a form that looks polished enough to avoid early scrutiny.

In many matters, the falsity is not complete invention from a blank page. The more common risk is selective alteration of genuine material. One message is inserted into an authentic thread. A timestamp is changed. A sender name is swapped. An image is re-rendered with false context. A page is replaced in a multi-page document. A recording is clipped to remove the material that gives the disputed statement its meaning. An export is made in a way that strips metadata and leaves only presentation. These are not dramatic movie tricks. They are practical manipulations that can influence settlement positions, motion practice, and credibility findings long before a case reaches trial.

Criminal cases raise the stakes further. A false message thread can be offered to show intent, conspiracy, coercion, or knowledge. A synthetic voice recording can be cast as an admission. A manufactured image can be used to place a defendant in a location or to suggest possession or contact. Surveillance footage can be slowed, sharpened, enlarged, excerpted, or combined with synthetic elements in ways that are misleading even if the whole file is not invented from scratch. If that material is accepted too quickly, the damage is not confined to the evidentiary phase at trial. It can shape charging decisions, probable cause arguments, detention decisions, plea leverage, and sentencing narratives.

The first practical mistake lawyers make in this environment is treating a screenshot as if it were the evidence itself. A screenshot is not the message database. A forwarded PDF is not the native email. A short clip is not the original recording environment, not the application in which edits may have occurred, not the cloud account from which the file was drawn, and not the device that created it. Once that distinction is understood, the right questions become clearer. What is the native source? Where did it live? Who controlled it? What software created it? What logs, metadata, account records, device artifacts, or carrier records surround it? Can the item be tied to an actual source through preserved technical evidence, or is the case being built on a visual presentation alone?

That is where digital forensics experts become necessary. Their work is not based on hunches. A qualified examiner does not simply look at a printout and say that something feels wrong. The process starts with preservation and provenance. The examiner identifies the source device, account, application, server record, or cloud repository that may contain the native evidence. He acquires data in a defensible manner, documents the process, preserves chain of custody, calculates and records hash values where appropriate, and examines the technical environment in which the evidence existed.

> *A polished exhibit is not the same thing as a trustworthy exhibit.*

The examiner then compares the offered exhibit to the underlying technical record. That may include message databases, file system artifacts, email headers, application logs, export history, account activity, embedded metadata, thumbnail caches, synchronized cloud copies, system timestamps, carrier records, or related device artifacts. The point is not merely to inspect what appears on the face of the exhibit. The point is to determine whether the exhibit can be traced to a genuine origin, whether its history is consistent with the story attached to it, and whether the surrounding technical evidence supports or contradicts the claim of authenticity.

This work serves several functions. Sometimes it exposes fabrication directly. Sometimes it shows re-export, recompression, transcoding, clipping, or other changes inconsistent with the way the exhibit has been described. Sometimes it shows that part of a thread is missing, that a file was created later than claimed, or that the offered item has no reliable tie to the device or account said to be its source. In other cases, the forensic work confirms that the evidence is genuine, which is just as important. Lawyers do not need experts only to attack digital proof. They need experts to test it, preserve what is real, isolate what is false, and narrow disputes to what can actually be shown.

Just as important, a serious examiner understands limits. Not every suspicious-looking item is fake. Not every anomaly proves alteration. Not every AI detection tool performs reliably under real-world conditions. NIST's recent work in this area is useful precisely because it recognizes that deepfake detection systems must be evaluated under demanding operational conditions rather than trusted on reputation alone. A responsible expert therefore does more than run software and produce a score. He asks whether the source material was sufficient, whether the native file was available, whether the methodology is appropriate, and whether the evidence supports a conclusion strong enough to survive legal scrutiny.

This is one reason timing matters so much. Once digital material has been flattened into screenshots, copied into declarations, excerpted into motion papers, or passed around in informal correspondence, the chance to test it properly may already be slipping away. Early preservation is not procedural fussiness. It is often the difference between examining the evidence and arguing over a presentation of the evidence. Where authenticity, authorship, timing, manipulation, deletion, or selective omission may matter, lawyers should think early about preserving source devices, cloud accounts, exports, account logs, application data, and server-side records before routine use, syncing, deletion, or overwriting changes the evidentiary landscape.

There is another mistake that deserves equal attention. Because generative tools are now widely available, some litigants will respond to authentic digital evidence by calling it fake in a vague and unsupported way. That approach is no better than blind trust in a polished exhibit. Courts will need help distinguishing grounded authenticity challenges from speculation. Digital forensics experts help in that setting as well. Their role is not to encourage reflexive distrust. It is to test the item, evaluate the provenance, identify what is technically supportable, and explain where the evidence ends and conjecture begins.

This is not a small professional adjustment. It is a structural one. Generative systems have made it easier to manufacture false proof and easier to cast suspicion on real proof. The burden of creating a deceptive exhibit has dropped sharply. The burden of disproving one has not dropped at the same pace. That imbalance is where the current risk lies.

For lawyers, the practical rule should now be simple. When a case turns on digital communications, recordings, photographs, videos, account records, or exported documents, appearance alone is no longer enough. Ask for the native source. Preserve the technical environment. Examine provenance, not just content. And bring in a qualified digital forensics expert early enough that the material can still be tested before it hardens into the case as accepted truth.

PRESERVATION CHECKLIST

What To Preserve Immediately

When there is reason to suspect fabricated, altered, incomplete, or falsely contextualized digital evidence, counsel should move quickly. Delay changes the data.

1

Preserve the source device

If the evidence is said to come from a phone, computer, tablet, DVR, camera, or external storage device, preserve the actual device before further routine use changes logs, caches, message stores, or timestamps.

2

Preserve the native file

Ask for the original file, not a screenshot, not a printout, not a pasted image in a PDF, and not a forwarded copy stripped of embedded information.

3

Preserve the account environment

Where the evidence may be tied to cloud storage, email, messaging platforms, or social-media systems, preserve the associated accounts and account activity records, including login history, export history, synchronization history, and security logs where available.

4

Preserve message databases and application data

Text messages, encrypted chats, call logs, notes, photos, and attachments usually exist inside application databases or system containers that carry more information than what appears on the face of a screenshot.

5

Preserve metadata and headers

For emails, obtain full headers. For documents, images, audio, and video, preserve metadata in native form. For PDFs, preserve the original file rather than a re-scanned image of the file.

6

Preserve chain of custody

Document who had the item, where it was stored, what was done to it, what software touched it, what exports were made, and who received the resulting copies.

7

Preserve cloud and service-provider records

Some of the most important authenticity evidence may exist outside the device itself: server logs, carrier records, platform records, download logs, or account-change histories.

8

Stop informal editing and forwarding

Well-meaning people damage evidence constantly by forwarding files, renaming exports, taking screenshots of screenshots, printing and rescanning, or saving over originals.

9

Identify the claimed origin story early

Ask at once: who created this item, on what device, in what application, at what time, through what export process, and with what subsequent handling?

10

Bring in a forensic examiner before the data is flattened

The sooner a qualified examiner can identify and preserve the right source, the greater the chance that the authenticity question can be answered with technical discipline instead of guesswork.

REFERENCE MATERIALS

Selected Sources

The sources below were supplied for this issue and are preserved as live links in the PDF.

NIST, Digital Investigation Techniques: A NIST Scientific Foundation Review
https://www.nist.gov/publications/digital-investigation-techniques-nist-scientific-foundation-review

NIST, Digital and Multimedia Evidence
https://www.nist.gov/forensic-science/digital-and-multimedia-evidence

NIST, Guardians of Forensic Evidence: Evaluating Analytic Systems Against AI-Generated Deepfakes
https://www.nist.gov/publications/guardians-forensic-evidence-evaluating-analytic-systems-against-ai-generated-deepfakes

NIST, Open Media Forensics Challenge (OpenMFC)
https://www.nist.gov/publications/nist-open-media-forensics-challenge-openmfc-briefing-iird

FBI, Artificial Intelligence
https://www.fbi.gov/investigate/counterintelligence/emerging-and-advanced-technology/artificial-intelligence

FBI, Oversight of the FBI Cyber Division
https://www.fbi.gov/news/speeches-and-testimony/oversight-of-the-fbi-cyber-division-032922

FBI, Cryptocurrency and AI Scams Bilk Americans of Billions
https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

U.S. Courts, Advisory Committee on Evidence Rules - May 2026
https://www.uscourts.gov/sites/default/files/document/2026-05-evidence-rules-agenda-book.pdf