

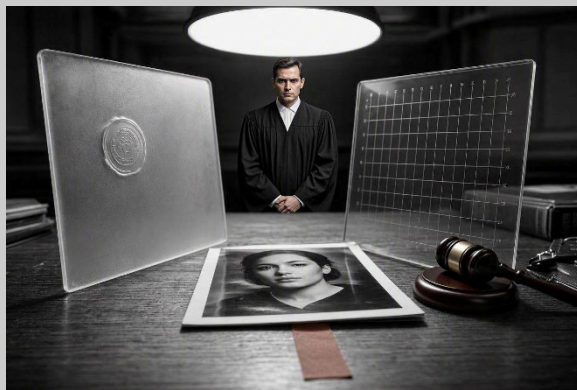


SUMMER 2026 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss how AI technology is pitting the forger and the authenticator in the battle over digital media in the legal arena.

When the Evidence Is the Question: AI Authentication in the Courtroom

In early 2024, when a Hong Kong-based finance employee at the British engineering firm Arup joined what looked like a routine video call with his company's CFO and several colleagues, every face on that call was AI-generated. Unfortunately duped, the employee authorized fifteen wire transfers totaling roughly \$25 million before anyone realized the meeting itself had been fabricated ([CNN story](#)). No court ever heard that case; Arup's money was simply gone. But that chain of events foreshadowed what would follow, and it wasn't just a furious uptick in cybersecurity training. Courts were about to face the same problem Arup's employee faced, suspicious image, video, and audio evidence, except with a judge's obligation to get it right in the face of rapidly evolving technology. Three recent rulings show what "getting it right" now requires, and they point to the same underlying question: does AI-touched evidence belong in the record at all?



Deeply flawed deepfakes. In [Mendones v. Cushman & Wakefield, Inc.](#) (No. 23CV028772, Cal. Super. Ct., Alameda County, Sept. 9, 2025), plaintiffs Ariel and Maridol Mendones submitted video testimony from a witness named Geri Haas in support of their motion for summary judgment. Judge Victoria Kolakowski noticed the witness's face was oddly motionless and her expressions repeated in a loop. On review, [the court found the exhibits were products of Generative AI](#) which did not capture the actual speech or image of the person they claimed to depict, clearly defining them as deepfakes. Metadata was decisive. The video's embedded data showed it was captured on an iPhone 6, a device that lacked the capabilities the plaintiffs' underlying story required. The court found the plaintiffs had submitted fabricated evidence and issued terminating sanctions, dismissing the case with prejudice.

Unreliable enhancement. In [State v. Puloka](#) (No. 21-1-04851-2, Wash. Super. Ct., King County, 2025), a murder defendant sought to admit an AI-enhanced version of a bystander's smartphone video, arguing the original, which was low-resolution and motion-blurred, needed clarifying before

the jury could evaluate it. There was no dispute over the source video's authenticity. The fight was over whether an AI tool's improved version could augment the original. Judge Leroy McCullough excluded it under Washington's Frye standard. Frye requires that novel scientific techniques must be generally accepted in the relevant field before a court will admit them, and Judge McCullough found the "forensic video analysis community" had not accepted AI video enhancement as reliable. The defense's own expert didn't know what data the tool had been trained on or whether it used generative methods at all and couldn't say the algorithm was anything but proprietary and opaque. McCullough wrote that admitting the enhanced footage risked "confusion of the issues" and a trial-within-a-trial over an unreviewable process. The court also found it failed Washington Rules of Evidence 702 (reliability) and 403 (unfair prejudice outweighing probative value).

Human intelligence. Not every AI-fabrication case hinges on the AI. In [*Adams v. Anderson*](#), No. 2025-CA-1309-MR, 2026 WL 1501021 (Ky. Ct. App. May 29, 2026) (unpublished), an otherwise ordinary custody-modification hearing turned on a single photograph. A mother testified she'd taken her child to urgent care and offered a picture of the prescription bottle as proof. The father didn't need a forensic tool to unravel it; he called the urgent care center and the pharmacy directly, and both confirmed no record of the visit existed. Confronted with the facts and warned by the court that falsified evidence meant jail, the mother's own counsel conceded the testimony and the photo were false or AI-altered. She pleaded guilty to contempt and was sentenced to 45 days, upheld on appeal. No metadata analysis, no expert witness, no spectral fingerprinting: the fabrication came apart under the oldest verification method there is, a phone call to the source. It's a useful reminder that as detection tools get more sophisticated, the fastest way to catch a fake is sometimes still following your gut instinct.

Mendones, Puloka, and Adams didn't need a new rule of evidence to reach their results. Existing standards for authentication, reliability, and fabrication sanctions did the work. What's changing is what it now takes to get that evidence into court. Digital forensics experts who can build a metadata trail that holds up under scrutiny, explaining both that a file is authentic and how that conclusion was reached, are crucial to winning a case.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ILTACON 2026

Nashville, TN: August 23-27, 2026

AI TECHWORLD 2026

Santa Clara, CA: September 1-3, 2026

NATIONAL EDISCOVERY LEADERSHIP INSTITUTE CONFERENCE 2026

Kansas City, MO: September 24-25, 2026

RELATIVITY FEST 2026

Chicago, IL: September 29, 2026 - October 1, 2026

THE AI CONFERENCE 2026

San Francisco, CA: September 29, 2026 - October 1, 2026

[Click here to see more upcoming events and links.](#)



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

[Contact us today!](#)

FOLLOW US AT:

