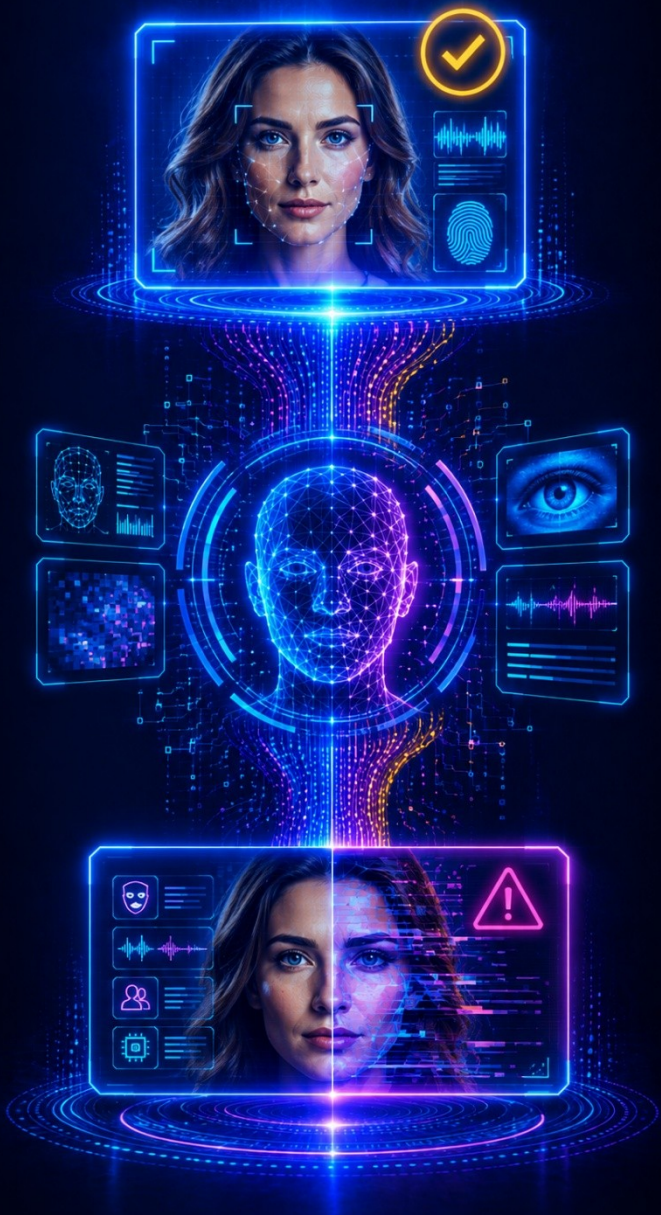


HAYSTACK®



VALID™

VERIFICATION AND LEGAL IDENTIFICATION
AUTHENTICATION OF DIGITAL MEDIA

ILTACON

August 23-27, 2026

Meet Your Presenter



John Wilson

*Chief Information Security Officer and President of Forensics,
HaystackID*

As Chief Information Security Officer and President of Forensics at HaystackID, John Wilson provides consulting and forensic services to help companies address various matters related to electronic discovery and computer forensics, including leading forensic investigations, cryptocurrency investigations, and ensuring proper preservation of evidence items and the chain of custody. He regularly develops forensic workflows and processes for clients ranging from major financial institutions to governmental departments, including Fortune 500 companies and Am Law 100 law firms.

Why Now?

THE COST OF FAKING EVIDENCE HAS COLLAPSED.

- ✓ A convincing deepfake video, a cloned voice, or an AI-generated document now takes minutes and almost no skill.
- ✓ “Is this real?” is now a question that courts, regulators, and insurers must answer.
- ✓ Most teams answer it ad hoc, with no replicable, court-defensible methodology.



Image and Video



Audio



Documents



AI-Generated Content

The Question Every Matter Now Asks

IS THIS REAL, AND CAN YOU PROVE IT?

- ✓ Deepfake-enabled wire fraud, cloned-voice business email compromise, and AI-generated content are already in live matters.
- ✓ A bare probability score does not survive cross-examination. A documented finding does.



Disputed Media



Authenticated



Documented Finding

“

Authentication is not a model output. It is a finding an examiner will defend under oath. VALID is where that discipline meets the tooling. Human Intelligence plus AI equals the truth.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

What VALID Is

MEDIA AUTHENTICATION, BUILT FOR THE COURTROOM.

1

Determines whether an image, video, audio file, or document is authentic, manipulated, or AI-generated.

2

Covers traditional tampering and forgery and generative-AI fakes, in one methodology.

3

Produces court-ready documentation that backs the finding.

How VALID Works

FROM INTAKE TO A DEFENSIBLE FINDING.



INTAKE

Secure intake and cryptographic hashing, integrity preserved from first touch.



TRIAGE

AI-assisted analysis with reliability scoring and anomaly detection.



PROVENANCE

Metadata, source, and container analysis to trace how the artifact was made.



ENHANCE

Scientific enhancement of low-quality media without altering probative value.



REPORT

A litigation-grade report with explicit confidence levels and a replicable method.

The Difference That Holds Up

A DOCUMENTED OPINION, NOT A BLACK BOX.

BLACK-BOX SCORE

0.87

FAKE?

No method. No error rate.
Nothing to reproduce or cross-examine.

VS



DOCUMENTED, REPRODUCIBLE FINDING



Named, versioned detection methods with disclosed error rates.



A reasoned opinion an examiner will defend under oath, not a bare probability score.



The methodology is replicable, so an independent expert can reproduce it.

Built for the Proposed Rule 707

READY FOR THE STANDARD THAT IS COMING.

Proposed Federal Rule of Evidence 707 sets a reliability standard for AI and machine-generated evidence in federal court. It expects documented provenance, a replicable process, transparent methodology, and a chain of custody.

VALID is built to align with it, so the authentication holds up when the standard applies.

RULE 707

- Documented provenance
- Replicable process
- Transparent methodology
- Chain of custody

Rule 707 is proposed, not in force. Earliest effective date: December 1, 2027.

VALID and TRACE™ Suite

TWO HALVES OF THE AI-EVIDENCE QUESTION.

Prove what your AI did, and prove whether the evidence is real. One forensic bench.

PRESERVE · UPSTREAM

TRACE Suite

Preserves the AI interaction, upstream, as it happens.



AUTHENTICATE · DOWNSTREAM

VALID

Authenticates the disputed artifact downstream.

ONE FORENSIC BENCH

TRACE Suite is named here as the upstream half of the bench; it is not represented as generally available.

Right-Sized to the Matter

ONE METHODOLOGY, THREE TIERS.

VALID Assess™

A fast first-pass authentication with reliability scoring.

VALID Verify™

Deep forensic authentication with a written expert opinion.

VALID Expert™

Full testimony-track authentication for a trial-bound matter.

One chain of custody. Escalate without re-collecting or re-documenting.

Who It Is For

BUILT FOR THE TEAMS THAT HAVE TO PROVE IT.



Litigation Counsel

With a video, image, audio recording, or document in dispute.



General Counsel and CISO Teams

Facing deepfake fraud, voice-clone compromise, or AI-generated content.



Insurers, Media, and Regulated Industries

Where an AI artifact enters a matter.

A Proven Forensic Bench

A DEFENSIBLE FINDING FROM AN ESTABLISHED BENCH.

A published, generally available authentication suite, with a decade-mature forensic practice behind it.

Recognized globally by industry leaders, including Chambers, Gartner, IDC, and Legaltech News.

A 2026 Cyber Insurance Awards USA finalist for VALID.

Named recognitions are stated as text only; the Cyber Insurance Awards status is a finalist, not a win.

What This Looks Like for You

HOW WE SCOPE VALID FOR YOUR MATTER.

THE ARTIFACT

We start with the artifact and the stakes:
what is disputed and where it has to hold up.

1

THE TIER

We map the right tier, from a fast
assessment to a full expert testimony track.

2

THE METHOD

We define the method and the chain
of custody, documented from intake.

3

Next Steps

A SHORT PATH TO A DEFENSIBLE FINDING.

STEP 1

A scoping conversation about your matter and your exposure.

STEP 2

A sized engagement at the tier that fits.

THE ASK

A follow-up working session with your team.

VALID. Human Intelligence + AI = The Truth.

OPEN FLOOR

VALID. Human Intelligence + AI = The Truth.

PRESENTER

John Wilson

ROLE

Chief Information Security Officer and
President of Forensics, HaystackID

EMAIL

JWilson@HaystackID.com