



## WINTER 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 our predictions for 2026's most impactful trends on eDiscovery and cybersecurity. We address AI technology innovation, security risks and AI lawsuits coming online.

### AI-Driven eDiscovery and Digital Forensics Predictions for 2026

As we move rapidly into 2026, AI tools continue to gain traction for organizations. Legal teams who assumed AI was a distant concern now face an immediate reality: the tools their employees use daily are fundamentally reshaping the eDiscovery landscape. Four interconnected predictions are creating what may be the most significant shift in eDiscovery and Digital Forensics in a decade. This year, we're preparing to face some new challenges head on, and sharing our predictions.

#### **Prediction #1: Multimodal AI Will Explode Increasing Stored Data Sizes**

Modern AI tools don't just generate written responses—they create images, audio clips, videos, code, and mixed-format outputs. An employee might ask an AI to visualize quarterly sales data, generate a presentation with custom graphics, or create a video summary of a project timeline. Each of these outputs carries files that are dramatically larger than traditional text documents. When multiplied across thousands of employees using AI tools daily, storage requirements become staggering. Storage infrastructure must scale to handle dramatically increased evidence volumes without compromising integrity or accessibility.

This data explosion also changes storage, processing, hosted review, and analysis requirements for eDiscovery and digital forensics, creating an acquisition, analysis, and review crisis. Traditional eDiscovery and digital forensics tools built for keyword searching and hash matching struggle with multimodal content. How do you analyze audio artifacts for evidence of manipulation? Traditional keyword search is useless against an AI-generated image, video, or audio file. More intelligent tools will be on everyone's wish list as multimodal outputs become an increasing sector of digital evidence. Tackling the digital issues of multimodal output data explosion and multimodal output acquisition, analysis and review will be hot topics as 2026 progresses.



### **Prediction #2: AI Prompts and Responses are Definitely Discoverable**

It's looking more like every conversation an employee has with an AI tool potentially contains discoverable material. Prompts reveal intent, strategy, and decision-making processes. Responses may constitute work product or contain confidential or privileged analysis. Yet most AI platforms don't preserve these conversations by default. Users can delete histories with a click (but may be recoverable). Cloud-based tools operate outside traditional IT infrastructure, making collection difficult even when data exists.

The forensic implications are significant. Investigators must identify which AI platforms were accessed, determine what data can be recovered, and establish authentication for AI-generated evidence. RAM artifacts, browser cache, and API logs may be the only evidence that critical AI interactions occurred. Timestamp correlation becomes complex when AI tools operate across multiple cloud services with varying clock synchronization. However, legal holds that fail to capture AI interactions risk spoliation claims. Organizations face hard questions about whether employee prompts to AI tools are personal or business records, and how to authenticate AI-generated content when it becomes evidence. The chain of custody for data that lives in proprietary AI systems is murky at best. Our prediction for 2026 is that the discoverability of AI prompts and responses won't be merely confirmed, the process of collection and analysis will present some major challenges.

### **Prediction #3: Agentic AI Creates Collection and Analysis Chaos**

The newest frontier in AI isn't just answering questions—it's taking action. Agentic AI systems can schedule meetings, draft and send emails, update databases, and coordinate across multiple platforms autonomously. When an AI agent handles a complex task, its actions fragment across systems: calendar entries here, email threads there, document edits somewhere else. Reconstructing what happened, why it happened, and who (or what) was responsible becomes genuinely difficult.

This creates unprecedented challenges for eDiscovery. How do you establish a complete audit trail when actions are distributed across platforms? How do you prove an AI agent took a specific action? What even constitutes a "record" when an AI autonomously executes a multi-step workflow? Reconstructing agentic AI activity requires correlating data creation across diverse sources. Determining authorship requires examining metadata that may not clearly distinguish human from AI actions. File system timestamps might show modifications, but establishing the complete chain of automated actions demands understanding the AI's decision-making process—information often locked in proprietary systems or ephemeral runtime states.

Examinations must now include questions like: What AI tools had access? What permissions did they have? Can we reconstruct the complete sequence of automated actions? These capabilities don't exist in standard forensic and review tools, yet. And these aren't hypothetical questions—they're issues legal teams will face as agentic AI deployments accelerate through 2026.

### **Prediction #4: AI Identity Takeover Causes eDiscovery and Digital Forensics Headaches**

The identity authentication crisis is here. AI tools now act under employee credentials, scheduling meetings, drafting emails, creating documents, and executing tasks that appear to come from humans but originate from algorithms. When an email arrives from john.smith@company.com, was it written by John Smith or by his AI assistant operating under his identity? The metadata looks identical. The sender field is the same. Traditional authentication methods that rely on these

markers become unreliable in a world where AI routinely operates as humans, leaving us not knowing who, if anyone, is behind the keyboard.

In 2026, we predict increasing challenges to the authenticity of evidence, arguing that AI-generated content lacks the credibility and reliability of human-created material. Deepfakes and synthetic content add another layer, making it possible to fabricate convincing audio, video, and documentary evidence that appears genuine. We're caught in a world where nothing is as it seems, and where digital evidence isn't what it used to be.

The authentication burden will shift from presumption to proof as AI identity takeover increases. Legal teams should prepare for discovery disputes where authenticity becomes the central issue. The question "How do you know a person created this?" will become commonplace in the near future.

### **Challenges Converge**

These four predictions aren't isolated trends—they're interconnected stages of AI transformation. More data becomes harder to search, which becomes difficult to reconstruct when AI agents are involved. 2026 won't be the year these problems get solved; it will be the year they become unavoidable. Organizations that recognize this reality and prepare now will have significant advantages over those caught unprepared and scrambling to react. The future of eDiscovery and digital forensics isn't just coming—it's what we're already preparing for at Digital Mountain.

**Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to [info@digitalmountain.com](mailto:info@digitalmountain.com).**

## **UPCOMING INDUSTRY EVENTS**

**NETDILIGENCE CYBER RISK SUMMIT**  
Miami Beach, FL: February 9-11, 2026

**PLANET CYBER SEC CONFERENCE**  
Orange County, CA: February 11, 2026

**MAGNET VIRTUAL SUMMIT 2026**  
February 23-27, 2026

**13TH ANNUAL UF LAW E-DISCOVERY CONFERENCE**  
Gainesville, FL: February 24-26, 2026

**THE SEDONA CONFERENCE WORKING GROUP 6 ANNUAL MEETING 2026**  
Atlanta, GA: November 13, 2025

*[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](mailto:marketing@digitalmountain.com).*

## **DIGITAL MOUNTAIN, INC.**

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

[www.digitalmountain.com](http://www.digitalmountain.com)

*Contact us today!*

**FOLLOW US AT:**

