PROGRAM MATERIALS
Program #35161
July 21, 2025

AI Forensics: Investigating AI Systems in Litigation

- Joe Sremack - CBIZ, Inc

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

AI Forensics: Examining AI Systems in Litigation

Joe Sremack

CBIZ, Managing Director

Agenda

1. What AI Forensics is and key terminology
2. Types of cases involving AI Forensics
3. How AI Forensics works
4. Challenges and limitations to AI Forensics
5. Current state of AI-specific litigation

Presenter's Bio

Joe Sremack, CFE, CISA, CIPP/US

Managing Director, Head of Forensic Data and Technology Services

Joe Sremack is a forensic data and software analyst with over 20 years of experience examining technology and business operations. He has conducted analysis in numerous high-profile cases and investigations, including the Bernie Madoff and Allen Stanford Ponzi schemes. Mr. Sremack applies his expertise to address complex issues involving the collection, analysis, and reporting of large, complex data and the design and use of software.

Mr. Sremack performs complex data analysis, system and business process analysis, complex data identification and management, data-intensive business process failure and underperformance issues, internal and government investigations, litigation, and regulatory compliance implementation and response. He develops software and assesses source code in numerous programming languages and performs data extraction and analysis involving virtually every major enterprise data system, including various ERPs and cloud-based data services.

His analysis of data and software is applicable to issues found in:

- Class action certification
- Software intellectual property disputes
- Labor and employment litigation
- Consumer privacy litigation relating to online tracking and PII/PHI issues
- Artificial intelligence design and use
- Commercial litigation involving large sets of data for fact development
- Electronic discovery where large, complex data systems are potentially responsive
- Neutral expert roles where questions are present relating to system operations and/or data accessibility

Mr. Sremack holds a master of science degree in computer science from North Carolina State University and is the author of Big Data Forensics and a frequent contributor to professional and academic organizations. He is an active member of the Association of Certified Fraud Examiners (ACFE), IEEE, International Association of Privacy Professionals, and Information Systems Audit and Control Association (ISACA).

CBIZ

AI Forensics and Key Terminology

AI Prevalence

- Algorithm-related litigation has increased by 300% in the past five year.
- Only 17% of organizations have a formal process for auditing AI systems.
- The average large company uses over 35 different AI systems across their organizations.
- More than 75% of commercial enterprise apps are predicted to use AI by the end of 2025.

Understanding Artificial Intelligence: The Basics

What is Artificial Intelligence?

AI refers to computer systems designed to perform tasks that typically require human intelligence. These systems can **learn** from data, **recognize** patterns, and **make decisions** with varying degrees of autonomy.

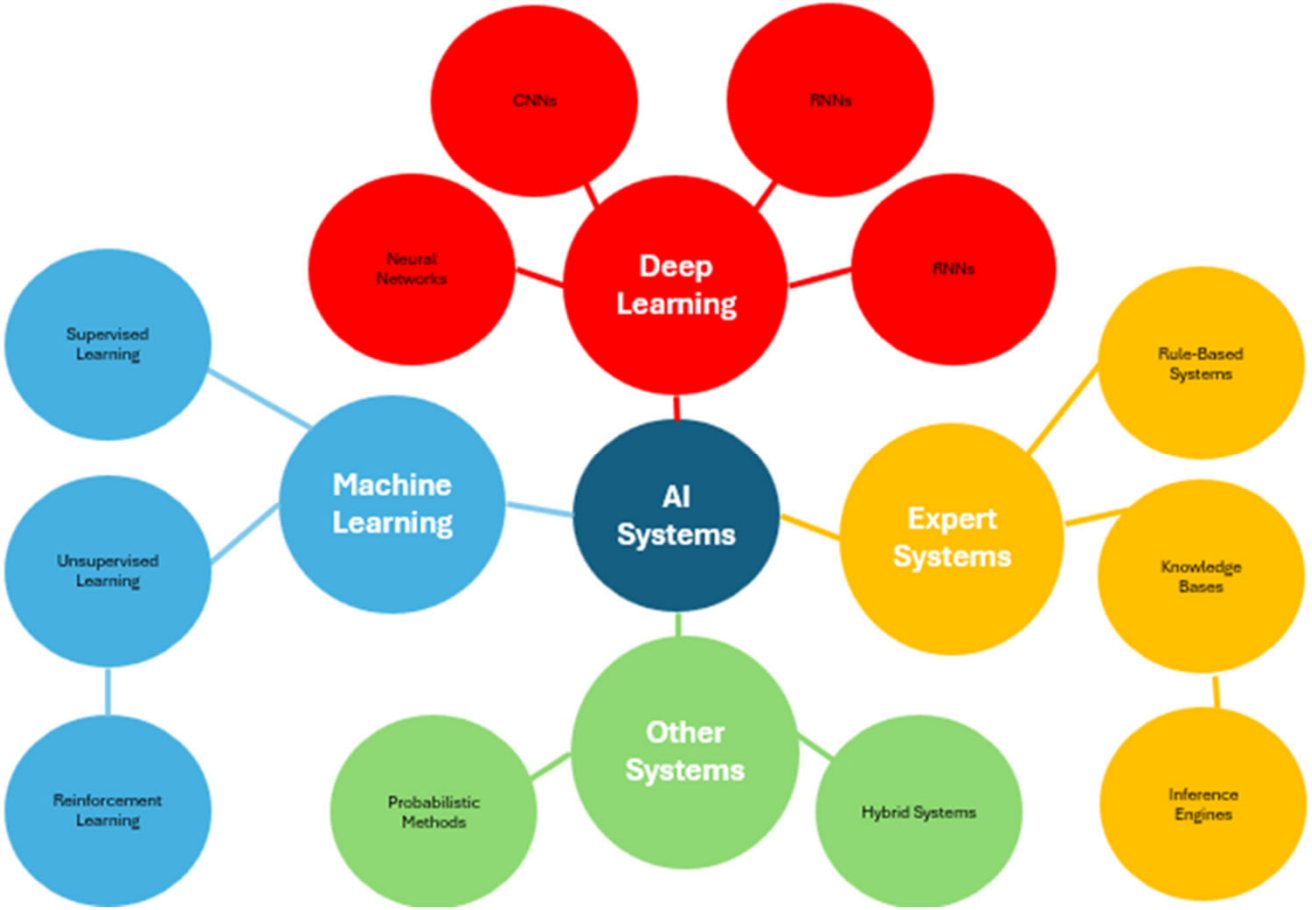
Think of AI as:

- Computer programs that can improve with experience
- Systems that can analyze large amounts of data to find patterns humans might miss
- Technology that can make predictions or recommendations based on past data
- Software that can adapt to new information without being explicitly programmed

How AI Works: Simplified

1. **Data Collection**
   AI systems learn from vast amounts of data. The quality and diversity of this data significantly impacts the system's performance and quality.
2. **Training & Learning**
   The system analyzes this data to identify patterns and relationships, adjusting internal parameters to improve accuracy over time.
3. **Prediction & Decision-Making**
   The AI can make predictions or decisions when presented with new data, applying what it learned during training and learning.
4. **Feedback & Refinement**
   Many AI systems continue to learn and improve based on feedback about their performance, adapting to new information over time.

AI System Taxonomy



Key takeaway: The corpus of AI system types is large and complex—and growing.

CBIZ

AI Systems and Sample Use Cases

PREDICTIVE SYSTEMS

AI systems that analyze data to predict future outcomes or make recommendations

- Financial Services (credit scoring)
- Healthcare (disease prediction)
- Risk Assessment (insurance underwriting)

COMPUTER VISION

AI systems that process, analyze, and understand visual information in the world

- Surveillance
- Medical Imaging
- Autonomous Vehicles

LANGUAGE PROCESSING

AI systems that analyze, understand, and generate human language

- Legal Tech
- Customer Service
- Content Generation

GENERATIVE AI

AI systems that create new content across various mediums

- Creative Content
- Software Development
- Synthetic Media

AUTONOMOUS SYSTEMS

AI systems that operate with limited or no human intervention

- Transportation
- Manufacturing
- Security Systems

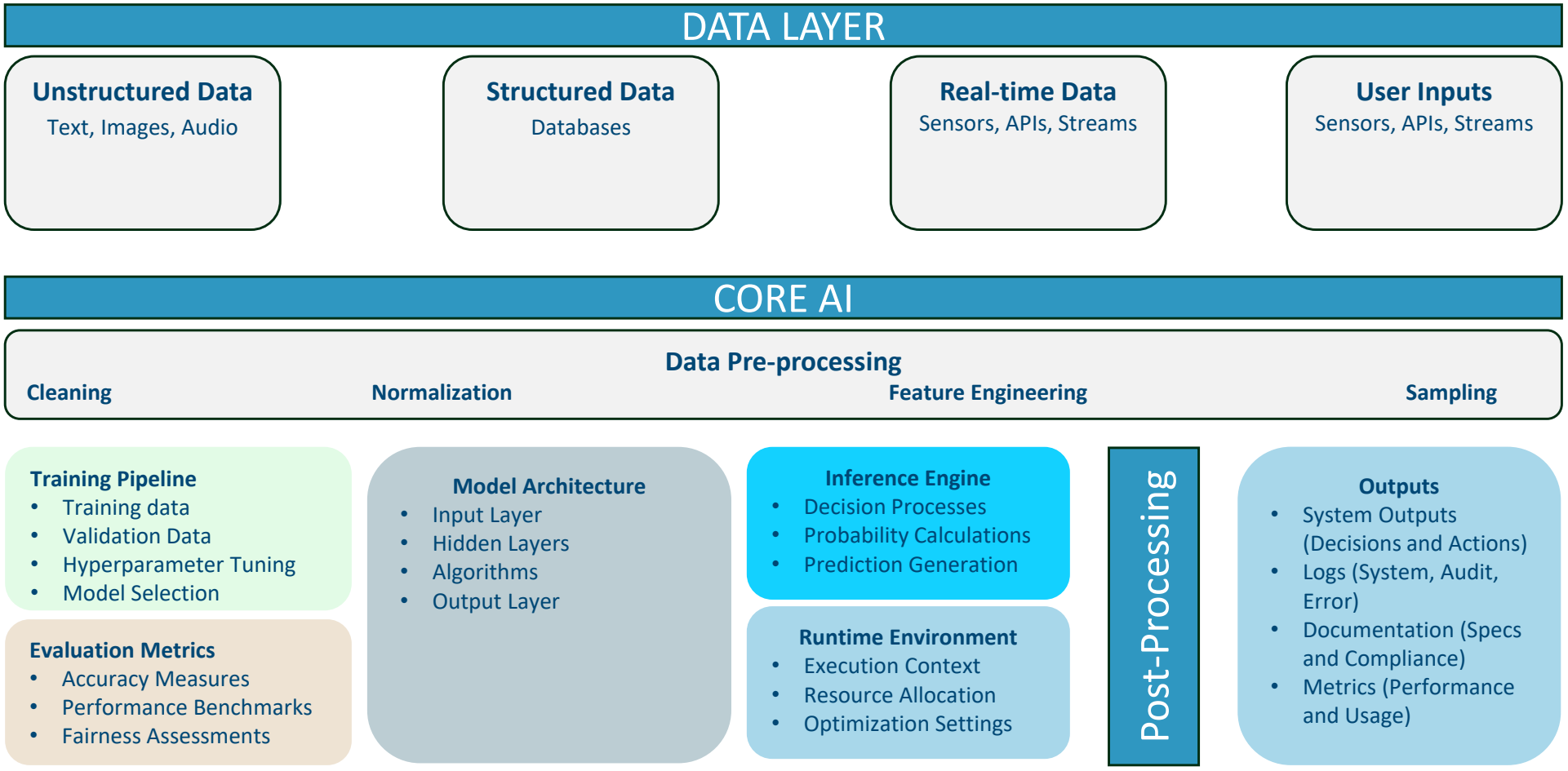
DECISION SUPPORT

AI systems that assist humans in making complex decisions

- Healthcare Diagnostics
- Judicial
- Financial Market Analysis

CBIZ

Anatomy of an AI System



Defining AI Forensics

What is AI Forensics?

The specialized scientific discipline focused on the investigation, analysis, and documentation of artificial intelligence systems for legal proceedings and regulatory compliance.

*AI Forensics applies scientific methods to **identify**, **preserve**, **extract**, **analyze**, and **document** evidence from AI systems to establish facts.*

Purpose of AI Forensics

- Establish facts about the AI system's behavior and decision-making
- Determine compliance with legal and regulatory requirements
- Identify potential bias or malfunctions
- Support expert testimony and analysis in litigation

Key Characteristics

Scientific Methodology: Application of systematic, repeatable processes with verifiable results that meet evidentiary standards

Multidisciplinary Approach: Integration of computer science, data analysis, statistics, law, and domain-specific expertise relevant to the AI system

Documentation: Detailed recording of all examination procedures, findings, and methodologies

Technical Depth: Examination of algorithms, training data, model parameters, and inputs/outputs and architecture

Legal Context: Consideration of legal and regulatory factors

Key Terminology in AI Forensics

AI-Specific Terms

Machine Learning: Systems that improve performance through experience with or without explicit programming, using patterns identified in training data.

Training Data: The dataset used to develop AI capabilities and shape system behavior.

Model Architecture: The structural design of an AI system, including layers, connections, and components.

Algorithm: A defined sequence of computation steps, such as transforming an input into an output.

Forensic Method Terms

Chain of Custody: Documentation showing chronological possession, control, and handling of evidence.

System Provenance: The documented history of a system, including development, modifications, deployments, and version control records.

Model Interrogation: Systematic testing of an AI system with varying inputs to understand behavior, decision boundaries, and potential vulnerabilities.

Documentation Standard: Protocols for recording examination procedures, findings, and methodologies to ensure admissibility and withstand scrutiny.

Technical Analysis Terms

Explainability: The degree to which an AI system's decisions can be understood by humans.

Bias Detection: Methods to identify systematic errors or unfair disparities in AI system behavior.

Adversarial Testing: Examination technique to intentionally attempt to manipulate inputs to identify deficiencies.

Model Performance Metrics: Quantitative measurements to evaluate AI system accuracy, reliability, and consistency.

Legal Terms

Daubert Standard: Legal criteria for admitting expert testimony, requiring scientific validity, peer review, error rates, and general acceptance of methods.

Algorithmic Transparency: How well AI decision-making processes can be inspected and understood by non-experts.

Spoliation: The destruction, alteration, or failure to preserve evidence relevant to litigation.

System Certification: Validation that a system meets certain standards for its intended use.

Types of cases involving AI Forensics

Types of Cases Involving AI Forensics: Intellectual Property

Copyright Infringement in Training Data

Cases involving unauthorized use of copyrighted materials (images, text, code, …) to train AI models, where forensic examination focuses on identifying source materials within training datasets.

Forensic Methods: Identify specific training data sources, determining substantiality of use, tracing transformative processes between source materials and model outputs.

Notable Case

Getty Images v. Stability AI
Case No. 1:23-cv-00135 (D. Del. 2023)
Getty Images alleged that Stability AI copied and processed millions of protected images without permission to train its image generation AI model.

Key Issues: Whether training data extraction constitutes fair use, proof of specific images in training data, transformative nature of AI processing.

Types of Cases Involving AI Forensics: Intellectual Property

Trade Secret Misappropriation

Cases where proprietary algorithms, unique datasets, or specialized model architectures are allegedly stolen or improperly accessed, requiring forensic analysis to prove similarity or derivation.

Forensic Methods: Comparing algorithmic implementations, distinguishing common techniques from proprietary methods, establishing access to protected information.

Notable Case

WeRide v. Huang
Case No. 5:18-cv-07233 (N.D. Cal. 2019)
WeRide alleged that former employees took proprietary autonomous vehicle AI technology to a competitor.

Key Issues: Distinguishing proprietary elements from standard industry techniques, establishing unauthorized access, and demonstrating uniqueness of algorithms.

Types of Cases Involving AI Forensics: Algorithmic Bias & Discrimination

Criminal Justice Applications

Cases challenging AI systems used in bail, sentencing, or recidivism prediction, where forensic analysis examines potential racial or socioeconomic bias in risk assessments.

Forensic Methods: Assessing false positive/negative rates across demographics, examining historical data biases, evaluating procedural fairness and due process concerns.

Notable Case

State v. Loomis
881 N.W.2d 749 (Wis. 2016)
Defendant challenged the use of the COMPAS risk assessment algorithm in his sentencing, arguing it violated due process.

Key Issues: Transparency of proprietary algorithms in government contexts disparate impact across demographic groups, and validation of risk scores vs. outcomes.

Types of Cases Involving AI Forensics: Algorithmic Bias & Discrimination

Employment Discrimination & Civil Rights

Cases involving AI-supported hiring, promotion, or compensation systems that allegedly discriminate against protected classes, requiring forensic analysis of model inputs, weights, and decisions.

Forensic Methods: Identify proxy variables for protected characteristics, measuring disparate impacts across groups.

Notable Case

Carpenter v. McDonald's Corp.
Case No. 1:21-cv-02906 (N.D. Ill. 2021)
Lawsuit alleging that McDonald's AI-driven voice recognition technology discriminates against customers with accents or speech impediments, violating the ADA and civil rights laws.

Key Issues: Whether the system performs differently for protected groups; intentionality vs. disparate impact.

Types of Cases Involving AI Forensics: Liability & Product Failure

Autonomous Vehicle Accidents

Cases involving crashes or safety incidents with autonomous or semi-autonomous vehicles, where forensic examination focuses on perception systems, decision logic, and operational parameters.

Forensic Methods: Reconstructing sensor data inputs, analyzing decision trees, determining human-AI interactions.

Notable Case

Nilsson v. General Motors LLC
Case No. 4:18-cv-00471 (N.D. Cal. 2018)
Motorcyclist sued GM after a collision with a Cruise autonomous vehicle, alleging the AI system failed to properly detect and respond to his presence in adjacent lane during a lane-change maneuver.

Key Issues: Analysis of sensor data logs, computer vision performance, and testing motorcycle detection.

Types of Cases Involving AI Forensics: Liability & Product Failure

Healthcare AI Failures

Cases involving medical diagnostic or treatment recommendation systems that allegedly contributed to patient harm, where forensic analysis examines clinical decision support logic and data handling.

Forensic Methods: Evaluating diagnostic accuracy, analyzing confidence thresholds, determining appropriateness of model for specific medical contexts.

Notable Case

Medicare Advantage Beneficiaries v. UnitedHealth Group

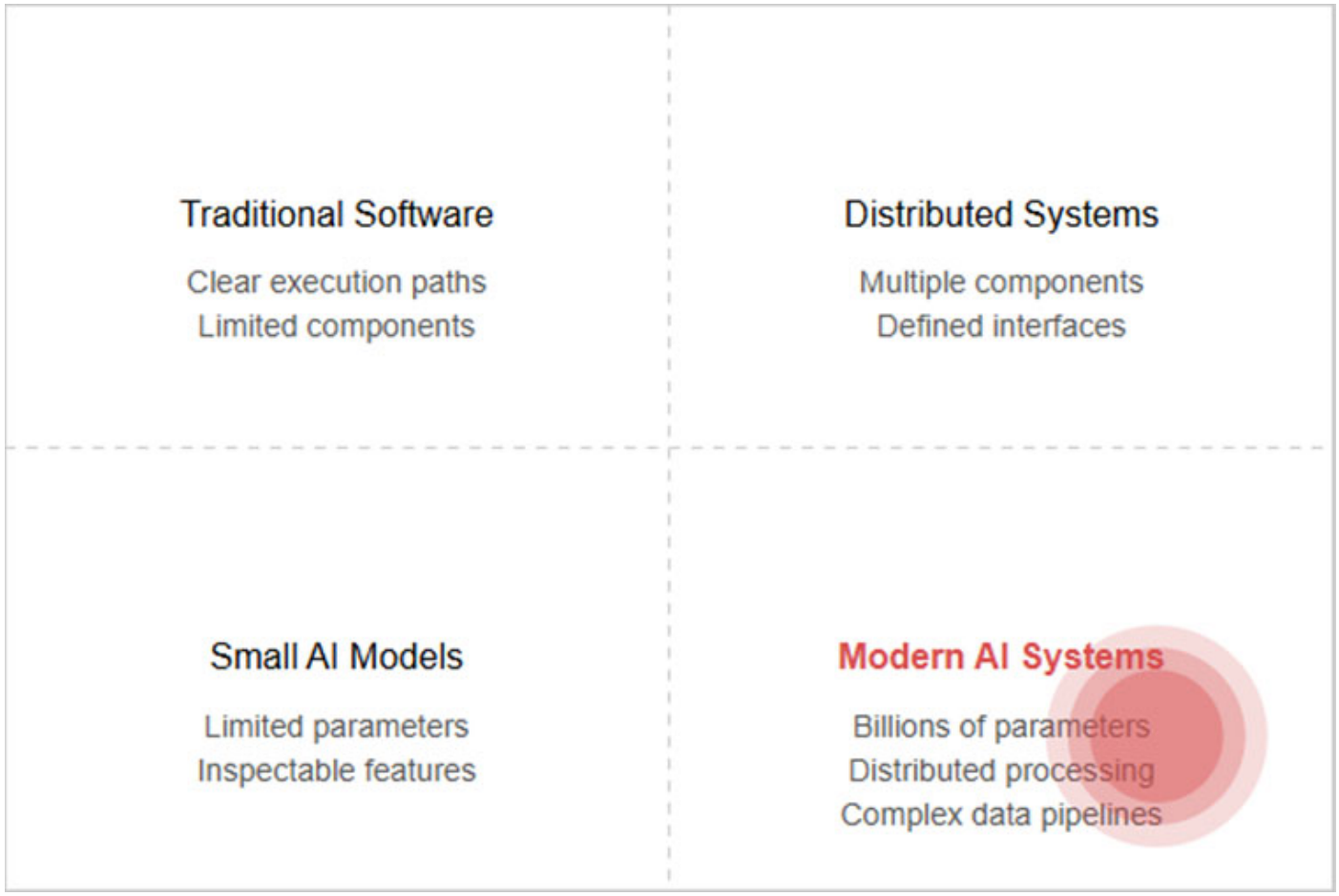
Class Action Filed November 2023 (D. Minn.)

Class action lawsuit filed on behalf of Medicare Advantage beneficiaries alleging UnitedHealth used an AI algorithm (nH Predict) to deny medically necessary care.

Key Issues: Analysis of algorithm validation methods, historical appeal outcomes, and Medicare compliance.

How AI Forensics Works

Types of Forensic Systems Analysis



AI Forensics vs. Traditional Digital Forensics

Dimension	Traditional Digital Forensics	AI Forensics
Primary Focus	• Static data and files; recovering, preserving, and analyzing digital artifacts	System behavior, decision processes, and algorithmic operations; analyzing what it “does” vs. what it “contains”
Examination Objects	• Model architecture • Training methodology • Hyperparameter tuning	• Validation methodology • Model validation reports • Performance benchmarks
Key Techniques	• Hash verification • Timeline analysis • Metadata analysis • Deleted file recovery	• Bias detection • Input variation analysis • Training data auditing • Model testing and explainability
Unique Challenges	• Encryption • Data volume • Anti-forensic techniques • Volatile data	• “Black box” systems • Probabilistic vs. deterministic • Proprietary algorithms • Continuous learning and system evolution

Shared Foundation

- Scientific Methodology
- Chain of Custody Requirements
- Documentation Standards
- Expert Witness Testimony

CBIZ

AI Forensics Framework

How AI Forensics Works

1. **Preservation & Collection**
   Securing AI system components, data, and operational environment
2. **System Identification & Analysis**
   Examining architecture, algorithms, data flows, and decision processes
3. **Testing & Validation**
   Evaluating system behavior, performance metrics, and error patterns
4. **Documentation & Reporting**
   Creating defensible documentation of steps performed and findings and testimony

This framework is based on traditional digital forensics standards. Each step, however, differs from the traditional approach based on requirements and the unique considerations required for AI systems.

Why AI Forensics is Uniquely Challenging

1. **The Black Box Problem**
   Many AI systems function as black boxes, where internal operations are not transparent or readily explainable
2. **Probabilistic Nature**
   AI produces probabilistic—not deterministic—outputs, complicating causation-type analyses
3. **Evolving, Ephemeral System States**
   Many AI systems continuously learn and change, creating challenges for point-in-time analysis
4. **Proprietary Technology**
   Trade secrets and intellectual property concerns can limit access to crucial components
5. **Undefined Recordkeeping Standards**
   Lack of recordkeeping standards may result in the unavailability of key documentation, such as logs and training data

AI Forensics Methodology: Initial Phases

Phase 1: Preservation & Collection

What the Expert Does:

- Forensic copies of system components (code, models, databases)
- Captures system logs, input/output data, and operational data
- Documents system architecture and data flows
- Preserves training data and model parameters
- Secures access credentials and authentication records
- Establishes proper chain of custody documentation

What Attorneys Need to Know:

Timing is Critical: AI systems continuously update; delays in preservation can lose evidence

Scope Negotiations: Know which components are essential vs. nice-to-haves

Preservation Orders: Consider seeking specific preservation orders for AI components

Phase 2: System Identification & Analysis

What the Expert Does:

- Identifies AI model architecture and components
- Analyzes training data and evaluates for potential biases
- Examines decision-making algorithms and parameters
- Reviews system documentation and development history
- Determines update history and version control practices
- Identifies human oversight mechanisms and intervention records

What Attorneys Need to Know:

Black Box Challenge: Understand testing for detailing internal operations

Explainability Matters: Expert should translate complex AI concepts to general audience

Training Data Focus: System behavior is often shaped by training data; data analysis is vital

AI Forensics Methodology: Later Phases

Phase 3: Testing & Validation

What the Expert Does:

- Conducts controlled testing with known inputs and expected outputs
- Performs statistical analysis of system performance
- Tests for bias across different demographic groups
- Examines error rates and failure modes
- Validates system against industry standards and best practices
- Performs adversarial testing to identify vulnerabilities

What Attorneys Need to Know:

Methodology Matters: Review expert's testing plan before commencing

Error Rates are Critical: Understanding system error rates and confidence intervals = reliability

Benchmark Comparisons: Compare to industry standards and reasonable alternatives

Phase 4: Documentation & Reporting

What the Expert Does:

- Creates comprehensive technical documentation of findings
- Develops visual aids to explain complex AI concepts
- Prepares expert reports with conclusions and supporting evidence
- Translates technical findings into legally relevant analysis
- Develops analogies and explanations for judges and juries
- Prepares for cross-examination on technical methodologies

What Attorneys Need to Know:

Qualification Strategy: Technical credentials and demonstrated forensic experience/knowledge

Simplified Explanations: Work with expert to develop intuitive analogies and visual aids

Documentation Thoroughness: Include all testing methodologies, tools used, and limitations

Case Strategy for Attorneys

Early Case Assessment

Identify the AI system(s) involved and their role.

Ask these questions:

- What type of AI system is involved?
- What was its role in the events at issue?
- Who developed and who operated the system?
- What data was used to train and operate it?

Build Your Expert Team Strategically

Consider:

- AI/Machine learning specialist
- Digital forensics expert
- Domain expert in the field where AI was applied
- Data scientist to analyze training data
- Human-computer interaction expert

Discovery Planning

Craft AI-Specific Discovery Requests

Sample requests:

- Documentation of algorithm selection
- Details of training data sources and preparation
- Testing protocols and validation results
- Error rates and performance metrics
- Audit logs re: system updates and errors

Prepare for Trade Secret Objections

Effective approaches:

- Propose protective orders with tiered access
- Request high-level data without algorithm details
- Seek black-box testing when white-box is denied
- Focus on outputs rather than internal code

Case Strategy for Attorneys

Evidence Presentation

Develop Effective Visual Aids

Effective Approaches:

- Interactive demonstrations showing inputs/outputs
- Flowcharts of decision points
- Visual comparison of system performance
- Before/after comparisons of system evolution

Frame Technical Issues in Human Terms

Narrative Elements:

- Who made key design decisions
- What known risks were accepted or ignored
- How system limitations were disclosed
- Why alternative approaches were not chosen

Challenging AI Evidence

Focus on Training Data Issues

Sample requests:

- Unrepresentative or biased training samples
- Data quality issues
- Improper data cleaning or normalization
- Inadequate validation datasets
- Copyright or privacy issues in training data

Challenge Testing Adequacy

Areas to Investigate:

- Inadequate real-world testing before deployment
- Failure to test with diverse user population
- Missing test cases
- Insufficient monitoring after deployment
- Poor documentation of test procedures

Closing Remarks

Thank You

Joe Sremack

Managing Director, Forensic Consulting Group

joe.sremack@cbiz.com

202.423.9803