Techno Security & Digital Forensics Conference

October 20-22, 2026, San Diego, CA

SNEAK PEEK

(Confirmed sessions as of July 20, 2026)

Full Conference Program will be available beginning of August

Agentic AI: Unlocking a Competitive Edge in Digital Investigations

Investigators are required to process vast amounts of data including forensic artifacts, logs, open-source intelligence, multimedia content, and other data sources. Agentic AI introduces a new paradigm enabling investigators to define curated objective statements and then launch them to discover accurate critical evidence without bias. This session demonstrates how to design and develop these curated objective statements that guide agentic AI systems in digital investigations. It will explore why objective-driven agentic AI provides a decisive competitive advantage, along with the risks of failing to adopt Agentic AI methods.

AI Can Write the Report. But Can It Validate the Evidence?

This session shares observations from an experiment using agentic AI in a mobile forensic case involving a timestamp interpretation issue. It examined whether an AI agent would simply trust parsed forensic tool results or perform a more comprehensive review. Rather than making broad claims about AI capability, the session focuses on what happened when an AI agent was used for context-building, artifact review, and validation. Attendees will learn about potential risks in AI-assisted analysis, ways to use agents more effectively, and why human analyst oversight remains critical.

AI Crime - The Future Is Now

This session will cover emerging criminal trends effectuated and enabled by artificial intelligence. Attendees will learn about the latest AI crimes; how to protect against these crimes and evidentiary issues that may arise when litigating these types of cases.

Anatomy of a Digital Forensic Investigation - From Authorization and Scoping through Analysis and Testimony

This session walks through the lifecycle of a digital forensic investigation from authorization and scoping through analysis, reporting, presentation, and testimony using the Digital Forensics Reference Model (DFRM) as a guide. Rather than focusing on specific tools or artifacts, the session examines investigative planning, documentation, communication, legal awareness, and forensic defensibility using real-world examples and case studies. Attendees will learn structured investigative methodology, reporting considerations, and operational concepts that impact forensic credibility.

Beyond the Skid Marks: Unlocking and Using Digital Evidence in Vehicle-Related Crimes

Vehicles play a role in many investigations, from homicides to narcotics and traffic crimes, yet their digital evidence is often underused. This session will fill that gap shows how data from vehicle systems can reconstruct movements, reveal interactions, and show intent. Through real cases, we'll demonstrate linking subjects to locations and analyzing driver behavior. Attendees will leave with practical approaches for integrating vehicle-based digital evidence into everyday casework across the full spectrum of criminal investigations.

Building Practical Cryptocurrency Investigation Capabilities for Under-Resourced Law Enforcement Agencies

This session directly addresses one of the most critical challenges in the field - the significant disparity between investigative needs and available resources. The session will discuss how research shows that over 40% of law enforcement cases already involve cryptocurrency, with expectations to surpass 50% by 2027, yet agencies face major obstacles, including a lack of trained investigators, insufficient tools and funding, and a persistent technology gap.

Can You Trust the Narrative? Using ChatGPT for a framework of verification

This session demonstrates how investigators can leverage Open-Source Intelligence (OSINT) methodologies, combined with generative AI tools such as ChatGPT, to build a structured investigative framework for conducting comprehensive background investigations. Using publicly available records and a real-world individual, attendees will learn how to transform scattered data into a chronological, evidence-based investigative framework while maintaining the standards expected in private-sector, government, and law enforcement investigations. Additionally, discussion on ChatGPT's limitations.

CASE STUDY: TD Bank Investigation
This session takes an in-depth look into the investigation of TD Bank. Agents will discuss where it started, typologies the bank failed to catch, and AML areas that were the bank was criminally non-compliant. The session will give attendees an upfront look into the importance of a strong AML program as well as tips to strengthen their own.

Closing the Signal Trust Gap: Physical-Layer Authenticity for AI, Cybersecurity, and Digital Forensics
As AI-generated content, synthetic media, and sensor spoofing become increasingly sophisticated, determining whether information is authentic has become a growing challenge. This session explores the emerging "Signal Trust Gap"-the difference between authenticated information and authentic information-and examines how acquisition-derived authenticity assessment may provide additional trust indicators beyond traditional authentication, integrity, and provenance mechanisms.

CASE STUDY: Defensible AI-Assisted DFIR: Evidence Grounding, Triage, and Timeline Reconstruction Without Vendor Lock-In
Modern intrusions leverage automation and adaptive tactics that challenge traditional DFIR. This session presents a case study demonstrating an AI-assisted investigation workflow for evidence-grounded analysis and defensible reporting. Attendees will learn: (1) how to validate AI outputs against raw artefacts (logs, processes, network traces), (2) how to triage and correlate multi-source evidence, and (3) how to reconstruct verifiable timelines while preserving chain of custody and auditability.

Digital Forensic Artifact Research - Verifying Results for Courtroom Testimony
The days of "Trust me, I'm an expert" are long gone and digital forensic artifacts are being challenged in the courtroom. Verifying artifacts are an essential part of the investigative and courtroom process and has become a hot topic in recent years. This session will provide guidelines and resources for digital forensic examiners to verify digital forensic artifacts through research and present those findings in the courtroom.

Digital Intelligence Team Overview
The session focuses on the development of an all-civilian digital evidence team within the police department to support investigations. Attendees will understand how social media platforms, mobile devices, vehicle data, and geolocation data from various sources can be used to support criminal investigations and increase success rates as civilians pull data and conduct analysis while sworn personnel have more time available for other tasks. Attendees will understand the best practices and potential issues

related to digital evidence collection, as well as the importance of drafting appropriate search warrants for digital evidence.

Digital Witness - How the Denver District Attorney's Office uses Digital Evidence to Support Prosecutions

For over a generation, our lives have become increasingly digitized. While corporations' information to drive revenue, the same digital trail provides law enforcement and prosecutors with new forms of evidence - what we refer to as "digital witnesses."

This session explores how the Denver District Attorney's Office Digital Evidence Unit uses digital witnesses to transform raw data into forensic reports used in criminal trials. The session will define "digital witness", explain how this evidence is evaluated and presented in court, and provide a case study from the prosecution of Steven Matthews - a multiyear serial sex-assault investigation.

Don't Be That Guy - Best Practices in Collecting and Processing Media and Device Evidence

Too often, digital evidence is compromised because of improper collection, preservation, management, or analysis. In many cases, the first personnel to respond to an incident lack the training needed to properly identify, handle, and protect critical digital evidence.

This session will provide attendees with the core principles needed to collect and preserve digital evidence in accordance with the standards and best practices in digital forensics. Attendees will learn methods for collecting and preserving surveillance videos, images, audio recordings, and cell phone data as well as tips in analyzing and presenting this digital evidence.

Elevating Actionable Intelligence in a Noisy AI World

When it comes to child safety, accessing pertinent information quickly is of paramount importance. However we are in an era of information overload and thanks to AI, it is only expected to increase here on. This session aims to prompt a discussion around valuable data points for agents pursuing child sexual exploitation cases, and opportunities for data connectivity to help the most vulnerable.

Attendees will learn:

- Tools/resources available to those who serve on the front lines.
- Workflow/process trends impacting agents working in child safety units.
- The role AI could play in accelerating child safety.

Fighting Elder Fraud & Transnational Crime

This session will share how San Diego's Elder Justice Task Force (EJTF) is leading the nation in the fight against elder scams by arresting and prosecuting members of money laundering organizations operating here in the United States. The session will share techniques used to successfully pull back money for victim.

Following DPRK's Revenue Trail: A DFIR Playbook for Remote-Work Fraud, Crypto Theft, and Laundering

North Korea-linked financial cybercrime is now a revenue operation, not a single hack. Drawing on sanitized 2024-2025 cases and Korean-language human intelligence, this session follows the trail from crypto theft and remote-work fraud to scam infrastructure and laundering. Attendees will learn to; Spot worker-fraud and laundering signals; Collect evidence from identity, endpoint, cloud apps, human resources, payroll, messaging, and financial records; and Coordinate security, fraud, legal, compliance, and law enforcement response.

Forensic Best Practices for Radio Frequency Propagation Surveys and Multi-Source Evidence Fusion

Phone records and mobile device extractions provide valuable investigative data, but they cannot pinpoint a user's exact location. This session explores how Forensic Radio Frequency Propagation Surveys (RFPS) help validate and interpret location evidence by documenting real-world cellular signal coverage and the environmental factors that affect it.

This session will share different methodologies for critical scenario, route surveys for travel paths, location surveys for crime scenes, and vertical surveys to analyze coverage changes at height. Attendees will learn how to merge field scans with mobile extractions and phone records to provide the solid facts and certainty required for irrefutable results in court.

CASE STUDY: From Cell Phone to Courtroom: The Digital Evidence that Led to a 22 year Federal Conviction

The case study follows a child exploitation investigation from a mother's discovery of explicit messages to a 22.5-year federal conviction. Attendees will learn how digital forensics, mobile device extraction, federal collaboration, and trauma-informed practices strengthened the case while keeping the victim central.

From Towers to Testimony: Using Cellular Records in Investigations and Court
Cellular records are a cornerstone of modern investigations, but their value depends on proper use, analysis, and clear presentation. This session covers how call detail records and cell site data should be used from investigation through prosecution. It also addresses how overcomplicating or overstating analysis creates challenges in court, and discusses who is best suited to interpret and testify to this data.

Ghost Machines
What if an attacker could deploy an entire operating environment instead of relying solely on malware or remote access tools? This session explores "Ghost Machines" lightweight, disposable virtual machines that provide isolated workspaces for browsing, reconnaissance, remote access, tooling, and command execution. This session will examine how AI and large language models could further enhance these environments, enabling autonomous task execution and decision support. Attendees will learn the forensic artifacts, visibility gaps, and detection opportunities associated with this emerging tradecraft.

Incident Response: Living off the Land, Investigating Attacks that Leave No Malware Behind
Modern attackers often hide in plain sight by abusing trusted tools already on compromised systems, including PowerShell, WMI, scheduled tasks, RDP, and other built-in utilities. This session breaks down the LOLBin problem through detection baselines and scoped alerts, separation of legitimate from malicious activity using parent process, arguments, and behavior, and forensic reconstruction from surviving host artifacts, including ScriptBlock logs, WMI subscriptions, task XML, Shimcache, Amcache, prefetch, and RDP/SMB lateral movement.

Integrating OSINT, Cyber Evidence, and Legal Process in Modern Criminal Investigations
Law enforcement investigations increasingly rely on digital and open-source evidence, yet many cases fail when OSINT, cyber evidence, and legal process remain disconnected. This session provides a practical framework for integrating digital evidence, investigative tradecraft, and legal considerations into a defensible workflow. Using real investigative scenarios, attendees will learn how to align platform records, OSINT, and digital artifacts to strengthen attribution, corroborate timelines, and support prosecutorial outcomes.

macOS Acquisitions with an Open-Source Tool
This session will be an overview of acquiring data from macOS devices with Fuji a free, open-source program. Attendees will learn a brief overview of why macOS acquisitions are different and how to use this open-source tool.

Real Systems Engineering for Agentic AI in eDiscovery and Digital Forensics: Beyond Demos to Production Pipelines
Digital forensics, incident response, and eDiscovery teams need reliable agentic AI beyond hype and demos.

This session explores real-world systems engineering approaches for production AI pipelines. Attendees will learn how to design multi-agent workflows for evidence processing, compliance, and risk assessment with human oversight. The session will also share patterns for determinism, auditability, and evidentiary integrity in AI workflows and practical deployment strategies. Real-world examples from eDiscovery and DFIR will be shared for adaptable technical blueprints.

CASE STUDY: Red Room Exchange: A Case Study in Digital Patterns, ICAC, Child Exploitation, Leaked Data, and Cryptocurrency
Red Room Exchange examines a case study involving a dark marketplace used as a human exploitation brokerage site. This session shows how digital patterns, usernames, emails, phone numbers, leaked data, online activity, and cryptocurrency indicators can connect across platforms to strengthen ICAC and child exploitation investigations. Attendees will learn how fragmented data can expose offender networks, reveal missed warning signs, and support stronger investigative leads.

Securing AI Agents: Architecture and Governance
As enterprise cloud infrastructure transitions from chatbots to agentic AI, the security perimeter has to change. And the architectural shift moves the focus from text filtering to system boundary governance. This session will walk through a conceptual AI interaction chain to show how inputs and system instructions move from the orchestrator down to tool boundaries where data crosses into execution zones.

The $5 Bottleneck: How Poor Cables Are Slowing Your Mobile Extractions
Investigators often focus on workflows and extraction tools, but cable quality and USB infrastructure can heavily influence acquisition speed and reliability. This session shows how cables, standards, adapters, and hubs affect performance through real-world testing. It clarifies misconceptions about USB-C, Lightning, and data transfer issues, and offers guidance for selecting and managing hardware to improve efficiency and reduce failed or slow extractions.

The Digital Crime Scene: Investigating Child Exploitation Beyond the Phone
Child exploitation investigations no longer begin and end with a smartphone. Evidence now exists across cloud accounts, messaging platforms, gaming services, wearables, smart devices, and connected ecosystems. This session teaches investigators how to identify, preserve, and leverage overlooked digital evidence while improving search warrant planning, forensic collaboration, and victim-centered investigations.

GenAI from the Trigger to the Courtroom
This session explores how Generative AI is transforming legal work from early case assessment and investigations to depositions, hearings, arbitrations, and trial preparation. Discover how AI can accelerate fact-finding, uncover key players and timelines, and help legal teams build stronger case strategies. The session will highlight practical use cases, lessons learned, and emerging best practices for secure, defensible AI adoption. Attendees will leave with actionable insights for leveraging GenAI while managing risk, governance, and compliance requirements.

The Extract Everything Problem: Why Mobile Device Triage Matters More Than Ever
Mobile device triage offers a sustainable alternative to full extraction as encrypted devices, rising data volumes, and limited staffing strain investigations. This session shows how targeted assessments reveal early investigative value, prioritize devices, ease forensic backlogs, and deliver timely intelligence while maintaining proportionality and defensibility. The session will also cover limits, legal factors, and best practices for integrating triage into workflows.

The First 60 Minutes of Digital Evidence: The Investigator Advantage
The critical initial hour at a search and seizure scene involving digital devices in ICAC and human trafficking investigations. Focus is on the identification, preservation, and rapid triage of digital evidence from mobile devices and computers to support timely decisions. During this session attendees will learn: How to apply the order of volatility in the first 60 minutes to preserve critical evidence frequently lost, the key digital artifacts are on mobile devices and computers to prioritize during triage and the approaches for using on-scene triage findings to support immediate investigative decisions.

The Human Factor in DFIR: Reducing Investigator Strain in an Era of Data Overload
Digital investigators face unprecedented volumes of data, increasing case complexity, and growing pressure to deliver timely results. While advances in forensic technology continue to improve data collection and analysis, the human challenge of reviewing, interpreting, and managing evidence remains significant. This session explores the

causes and impact of investigator strain, including information overload, repetitive workflows, and investigative backlogs. Attendees will gain practical strategies for improving efficiency, reducing cognitive burden, and helping investigators focus on the evidence that matters most.

The Modern Analyst's Toolkit: Why Non-Traditional Tools Matter
Digital investigations are evolving faster than most traditional forensic tooling can adapt. This session will explore why modern investigators benefit from adopting developer-style tools-including SQL databases (MySQL and SQLite), Python, REST APIs, and emerging AI/LLM systems as practical extensions of their forensic toolkit. This session focuses on practical concepts and workflows, not deep programming expertise. Attendees will leave with a clear understanding of when these tools add value, how they fit into existing investigations, and why embracing them is becoming a necessary skill for modern investigative professionals.

Traveling Organized Burglary Crews – From TDAS to Arrest
This session will through a combination of complex investigations involving organized burglary crews. The session will highlight some of the technological investigative techniques, including Tower Dump Area Searches (TDAS), social media, surveillance and real-time phone pings, and pattern of life analysis.

Trust but Verify: Artificial Intelligence in Forensic Video Redaction and Reliability
Artificial intelligence is rapidly changing how digital evidence is analyzed but how should it be used responsibly within the forensic video analysis community? This session examines when analysts can incorporate it into the workflow, when it introduces risk, and how to maintain transparency and defensibility. Through real-world examples, this session will review tool types, the Scientific Method, and ethical and legal considerations, including reliability, reproducibility, and courtroom readiness.

Uncovering the Truth: What Really Happens During an Onsite Collection?
Most people think once a device is collected, the evidence is immediately available. That is not always the case. Collection and processing are two very different phases of forensic investigation and understanding that distinction could have a significant impact on legal strategy, timelines, and investigation. This session will discuss what really happens during an onsite collection, including: What data is available during a collection; How long collections really take; and Common misconceptions about digital evidence availability.

Using and Preserving Prompts in Digital Investigations
As users increasingly turn to AI platforms such as ChatGPT, Gemini, Claude, and Llama instead of traditional search engines, prompt-driven interactions are becoming a valuable source of digital evidence. This session explores where AI-related artifacts can be found across cloud services, computers, and mobile devices, and discusses best practices for identifying, preserving, processing, reviewing, and producing this emerging data source in digital investigations and legal matters.

Vehicle System Forensics - When Cars Talk
Vehicle data has become valuable evidence in nearly every type of investigation. Vehicle data can provide investigators evidence of where the vehicle has been, how it was driven, how fast it was going, and who was in it. This session will include an overview of vehicle data, including information/evidence commonly available from vehicles, and the various techniques for acquiring vehicle data. It will also share the analysis and validation of vehicle data and examples of when vehicle data has been effectively used in real-world cases and admitted as evidence in court.

Where Did That Come From? Verifying AI in Digital Forensics
AI can surface a lead in seconds, but a fast answer you can't adequately verify is not a finding. It's a lead at best. This session covers how to verify AI-assisted forensic work responsibly: connecting a conclusion to its evidence and tracing it back to source, with a live look at verification in action. Attendees will learn how to: Distinguish a verified finding from an unverified AI guess; Trace an AI result back to its source for independent confirmation; and Apply practical frameworks for verifying AI-assisted work responsibly.

Your Compliance Program Is Not Investigation-Ready: The Hidden Gap Between Compliance Investigations, eDiscovery, and Digital Evidence
Organizations remain investigation-unready because Compliance, Legal, IT, Forensics, and eDiscovery work in fragments, treating chain of custody as a technical task instead of a shared investigative discipline. This session shows how an end-to-end model reduces information loss, accelerates analysis, and improves evidentiary defensibility. Attendees will learn how to: Map evidence ownership across functions; Embed chain-of-custody practices throughout the investigation; and Convert digital evidence into actionable legal and compliance decisions.