Techno Security & Digital Forensics Conference

June 2-4, 2026 – Myrtle Beach, SC

SNEAK PEEK

Confirmed Conference Sessions

(as of February 11, 2026)

Full Conference Program will be available mid-March

A Tale of 2 Outputs: Man vs the Machine

It is a head-to-head battle of man vs machine. This session will discuss the outcomes of a ground-breaking research study looking at the ability of human examiners and AI to understand and interpret complex digital forensics results. Who will come out on top? What can be learned for future use of AI in digital forensic examinations? Will AI ever replace human examiners? This session will explore these topics using industry-first empirical data and have a look into the future of AI within digital forensics.

Achieving Operational Excellence: A Framework for Readiness, Execution, and Situational Awareness for Investigative Teams

Achieving mission requires preparedness, insight, and agility in decision-making—no small feat given today's complexities: heightened workforce skills, overwhelming information streams, and stringent stakeholder expectations. This session introduces a practical framework for leaders to effectively oversee investigative operations by integrating three critical dimensions that transform oversight into proactive leadership.

Agentic AI - Coordinated AI Agents Helping Solve Cases

Agentic AI represents a shift from models that merely generate text to systems capable of autonomous, goal-directed action. This session examines how early AI coding agents, such as Claude Code, can be adapted into DFIR agents. The session will share how agents can collaborate within an agentic architecture to accelerate casework and reduce manual work.

The talk introduces “Vibe DFIR,” applying Vibe Coding’s conversational workflow to investigations, where agents create and execute disposable forensic micro-tools as needed, interpret results and refine actions based on its goal.

The session concludes with Poirot, a prototype agentic DFIR system.

Analyzing SQLite Write-Ahead Logs and Transaction History
Navigating SQLite Write-Ahead Logs is essential for digital forensic investigators, particularly when examining unsupported or partially supported applications. This session guides you through the manual analysis of SQLite WAL files, breaking down how transactions are recorded, committed, and preserved outside the main database.

Artificial Threats: How Cybercriminals Are Turning AI Against Us
As AI technologies become increasingly accessible, cybercriminals are rapidly integrating their capabilities into their attack methodologies. This session examines the emerging threat landscape where adversaries leverage AI to enhance the scale, sophistication, and evasiveness of attacks. The session will review cases of AI-enabled threats, including the use of LLMs to craft convincing phishing campaigns, AI-generated deepfakes for social engineering and executive impersonation, and machine learning algorithms that adapt malware behavior to evade signature-based defenses.

Augmented OSINT: Leveraging Python and AI for High-Integrity Intelligence at Scale

Investigators rely on global information streams including multilingual news sources, government alert channels, social media, and specialized technical blogs. This session presents an open-source Python and AI approach to extract high-value, actionable intelligence from these diverse sources. Attendees will learn how to ingest and normalize heterogeneous feeds, detect and translate multilingual content, extract key entities, perform sentiment and behavioral analysis, and identify indicators of emerging threats. The session demonstrates how Python, AI, along with engineered prompts can augment and enhance traditional OSINT tradecraft.

Authentication and Admissibility of AI and GenAI Evidence: What Rules Apply and How Might That Evidence be Admitted
Proposed exhibits can be enhanced or created by Artificial Intelligence and generative AI. To be admitted into evidence, such exhibits must be authenticated by the party offering the exhibits and meeting standards for admissibility established by rules of evidence. This session will examine the rules that govern authentication and admissibility, address what

must be shown to meet those standards, and consider defenses to admissibility. The session will also explore the role of experts in the enhancement or creation of exhibits and judicial responses to "hallucinations" in expert reports.

Avatars of Exploitation: Child Exploitation & CSAM within Online Gaming
Online gaming platforms, including mainstream titles and child exploitation themed games, are increasingly leveraged to groom children, produce CSAM, and facilitate sexual abuse. This session examines how gaming features are weaponized, explores links between gaming spaces and dark web networks, and presents investigative findings and response strategies to address vulnerabilities and support prevention, investigations and prosecution.

Beyond Screenshots: Modernizing Public-Web Evidence for Forensics, eDiscovery & Investigations
Public-web and social media content are core inputs to OSINT-driven investigations, yet screenshots and consumer capture tools often fail under legal and forensic scrutiny. This session explores why traditional web-collection methods fall short and how evidentiary standards affect the use of OSINT in legal and investigative contexts. Attendees will learn how to (1) assess risk in common OSINT capture techniques, (2) preserve public-web intelligence with context and metadata intact, and (3) apply defensible collection workflows that withstand technical review, audits, and cross-examination.

Beyond the Console: What DFIR Can Learn from Journalists and Intelligence Analysis from an OSINT Expert
This session will explore how Digital Forensics and Incident Response teams can significantly strengthen their investigative capabilities by adopting OSINT methodologies pioneered outside the cybersecurity domain. Attendees will learn how cross-disciplinary OSINT provides actionable situational awareness, enriches digital evidence, helps build timelines, and transforms technical indicators into meaningful narratives. This is an inspirational, practitioner-focused session designed to show how DFIR investigations can advance by integrating investigative OSINT techniques honed well beyond the traditional cybersecurity toolkit.

CASE STUDY: Behind the Decentralized Shadow: CSAM, Human Trafficking, & Crypto
This session will cover human trafficking trends in crypto, highlighting the forced labor behind many crypto scams, covering a case study of CSAM and live streaming abuse in the Philippines, and highlighting some recent alarming trends of cryptocurrency being involved

in sex trafficking both in the US and abroad. Come pull back the curtain on some of the most pressing modern slavery issues with a nexus to cryptocurrency.

CASE STUDY: From Cell Phone to Courtroom: The Digital Evidence that Led to a 22.5-year Federal Conviction

This case study shows how rapid patrol response and mobile device forensics turned a local complaint into a federal child-exploitation conviction. It covers key decisions, digital grooming analysis, multi-agency collaboration (ICAC, CDI, HSI, BACA), and trauma-informed interviewing.

CASE STUDY: From Fragmented Signals to Convictions: Solving a Cross-Border Murder Through Fused Digital Evidence

Attendees will learn how cloud-based criminal analytics enabled investigators to correlate communications, movements, and digital identities; reconstruct timelines across borders; and expose hidden command-and-control relationships behind the crime. The session will walk through lawful ingestion, automated filtering, link analysis, and geospatial anomaly detection - demonstrating how weeks of manual analysis were compressed into hours without compromising privacy, auditability, or prosecutorial integrity.

CASE STUDY: From Tipline to Courtroom: Mobile Forensics in CSAM Investigations

This case highlights mobile forensics in CSAM investigations, from tipline reports to courtroom prosecution. Investigators extract and analyze data from devices while preserving evidence integrity. Extreme sensitivity is maintained to protect minor victims, limit exposure to exploitative material, and follow victim-centered protocols. Clear forensic reporting ensures legal admissibility and supports justice without compromising the dignity of children.

CASE STUDY: Husband & Wife CSAM Investigation

Case study involving a husband and wife, Alexandria Stevens and Michael Taylor, who produced CSAM with the wife's 7-year-old sister, attempted with her minor brother as well, and solicited children on Omegle for sexual acts.

Beginning with a NCMEC cybertip from Playstation, images of CSAM were sent between Stevens and Taylor. A search warrant executed at their residence in New Jersey lead to the discovery of in person live CSAM production and internet based CSAM production by both Stevens and Taylor with a minor victim. The case study will go through the investigation, lessons learned, and the sentence.

CASE STUDY: Operation Winter Guardian
In 2024 the NC SBI Computer Crimes Unit along with more than 40 local, county and federal law enforcement agencies conducted a multi-agency operation known as "Operation Winter Guardian". This operation utilized various components such as undercover techniques, and techniques used to locate offenders sharing CSAM over popular file sharing networks. This operation yielded numerous subjects who were arrested for either wanting to meet child for the purpose of sexual activity or were found in possession of child sexual abuse material. This session will show the audience the preparation, logistics, execution and the results of this operation.

CASE STUDY: Searching for Nothing: When Silence Becomes Forensic Proof
Digital forensic investigations often assume evidence will surface through artifact recovery. This session examines a serial homicide case where repeated extractions produced nothing—and that absence became the evidence. By shifting from artifact categories to system behavior & iOS system logs, incl. fseventsd, periods of iDevice silence were identified, coinciding with homicide events. Attendees will learn how silence is forensic proof.

Cloudy with a Chance of Exfil: Obscure Cyber Threat Actor Persistence and Exfiltration Mechanisms
Prolific threat actors have thrived on double-extortion; proving the ransomware economy remains strong. To hold organizations hostage, identity is now the target of adversary tactics, techniques, and procedures. As a blue teamer sifting through noise, how do you defend against a threat actor with extensive resources? This session will present real-world observations and highlight obscure tradecraft where the cloud, for persistence and exfiltration, has proven successful. To mitigate these TTPs, log sources and countermeasures will be presented to bolster defensive posture and ensure the proper instrumentation of Azure workloads.

Cutting Through the Deepfake Hype: What You Need to Know
Deepfakes are everywhere in today's headlines, fueling fear and driving a surge of "AI vs. AI" detection tools. But here's the truth: recent research shows these solutions often fall short of their promises—and create challenges for admissibility in investigations and legal proceedings. Join us for a candid discussion that slices through the noise. We'll explore: The real state of deepfake detection today; Why current tools struggle to deliver on their claims; and Practical strategies to preserve trust and ensure your media evidence stands up in court.

CyberTheft of Trade Secrets, and Legal Considerations During Data Breaches

Trade secrets make up the majority of value of U.S. companies' portfolios. Not surprisingly, such secrets are high value theft targets for domestic and foreign competitors. In one survey, half of the respondents admitted to taking corporate data when they left their employer and almost two-thirds transferred corporate data to personal devices and never deleted the same. This session explores the world of trade secrets, how trade secrets differ from other intellectual properties, the legal aspects of trade secrets, some recent case law and legislation, and general discovery/attorney-client privileges considerations during such theft/beaches.

Dealing with the Always Evolving Insider Cybersecurity Threat…Shadow IT

It began in the late 1980's with the emergence of personal computers using spreadsheet software to build huge end-user ad hoc desktop applications without the involvement or approval of the Information Technology department… but today, it's high connectivity, high risk Shadow IT and includes: BYOD, rogue wireless, low-code development, content management systems, SaaS applications, and Shadow AI. In this eye-opening and practical session, we will: Assess each notable category of Shadow IT; Identify how each expands your attack surface and cybersecurity risks; and determine how each can be detected and better controlled.

Decrypting AI Apps: Forensic Insights into the New Frontier of Digital Intelligence

AI applications are now widely used by both everyday users and criminals. This session explores how offenders misuse AI to automate tasks, enhance deception, and hide digital traces. This session will cover key forensic artifacts left on devices, including logs, caches, metadata, and tokens, and show how to identify and analyze them. Attendees will gain practical methods for examining AI-related evidence in modern investigations.

Digital Chain of Custody: Defensible Practices for Managing Devices and Media Across the Evidence Lifecycle

As investigations span physical devices, removable media, and legacy data, maintaining a defensible digital chain of custody is increasingly complex. This session examines practical, process-driven best practices for managing custody across the evidence lifecycle. Attendees will explore common breakdowns in visibility & handoffs, learn how consistent documentation, accountability, & cross-functional alignment reduce risk, improve audit readiness, and support defensible discovery outcomes.

End-to-End Investigation Management: Creating a Single Source of Truth in DFIR
DFIR investigations often span multiple tools, teams, and timelines, making it difficult to maintain clarity, consistency, and trust. This session examines the practical principles and best practices of end-to-end case management, showing how a structured approach can reduce complexity, preserve evidence integrity, support chain of custody, and provide a single source of truth. Attendees will gain actionable insights to improve efficiency, accountability, and confidence across the full lifecycle of a DFIR investigation.

Fake It ‘til You Fool Them
This session explores how AI-powered deepfakes can alter faces, voices, and messages, featuring real demo of what current tools can create. This session will share how deepfakes can be used to deliver misleading messages, and discuss the laws, detection methods, and best practices surrounding synthetic media. Attendees will learn how deepfakes are made, how they can be identified, and why understanding them is essential in today's digital landscapes.

Financial Technology in Human Trafficking Investigations
This session will cover the use of fintech applications in Human Trafficking Investigations, primarily the use of CashApp. It will describe its use as a source of intelligence driven investigation and prosecution for sex trafficking cases. The discussions will focus on means of identifying and obtaining records, the basics of the platform, and identifying useful intelligence leads. The session will also cover analysis of the financial records and how to use them in court proceedings.

Forgery Factory: How Dark Web Criminals Are Leveraging AI to Draft and Submit Fraudulent Legal Process Requests
Dark web activity shows threat actors using compromised law enforcement email credentials to train AI models that generate realistic subpoena forgeries at scale. This session explains attack methods and how government email compromise undermines traditional verification of subpoenas and emergency requests. Attendees will learn best practices to protect customer data, and; How these tactics work and how traditional methods of verifying investigators/documents/agencies are already failing; How to design identity-first verification workflow; and How to apply risk-based controls (intake method, compromise tracking, pattern detection

From Early Case Assessment to the Hot Seat: Secure, Defensible GenAI Workflows for Investigations, Litigation, and Beyond

Generative AI goes beyond document review, transforming early case assessment, investigations, and preparation for depositions, hearings, arbitrations, and trials. This panel brings together legal tech and eDiscovery experts to examine how AI can be applied securely and defensibly across the matter lifecycle—accelerating fact-finding, identifying key players and timelines, informing strategy, and supporting deposition and trial preparation while addressing risk, security, and compliance.

From Passwords to Persistence: How BEC Tradecraft Has Outpaced Traditional Investigations

Business Email Compromise (BEC) has evolved from simple credential theft into a persistent, cloud-native threat that bypasses traditional investigative assumptions. Modern attackers abuse trusted services, identity platforms, and legitimate application workflows to evade detection. This session examines emerging BEC tradecraft—including IPv6 adoption, VPN usage, abuse of SaaS platforms, SPF/DKIM/DMARC bypass, API and OAuth persistence, EWS exploitation, and AI-driven scale—and defines the investigative pivot required to move beyond mailbox-centric analysis and identify attacker intent, persistence, and impact.

HANDS ON LAB: Digital Forensics with Open-Source Tools: Solving Crimes at Retail Prices

This hands-on lab provides hands-on instruction in using open-source tools for mobile and digital forensics. Attendees will gain practical experience acquiring, parsing, and analyzing data from both Android and Apple devices using tools such as LEAPPs, UFADE, and ALEX.
**Pre-registration required. BYOD*

HANDS ON LAB: NetFlow Analysis

With the advent of encryption, NetFlow has become the standard for what we have available to analyze network traffic. In this hands-on lab, participants will learn what NetFlow is composed of and, using Excel, be able to analyze the NetFlow session data.
**Pre-registration required. BYOD*

Incident Response and AI: Leaving the Spreadsheet of Doom Behind

The spreadsheet of doom—that sprawling tracker of timelines, observables, and case notes—remains the backbone of incident response at top firms. AI should help here. Often it doesn't.

This session shares practical approaches. Attendees will learn: What the spreadsheet reveals about the comprehension problem AI must solve; Techniques for managing context limits and hallucination risk, and How to design AI that augments analysts instead of replacing them.

Integrating OSINT and Cyber Investigative Tradecraft in Complex Investigations

Cyber investigations increasingly require integrating OSINT with legal and cyber investigative processes. This session presents a structured, practitioner-focused approach to aligning OSINT, platform data, and forensic artifacts to strengthen attribution, timelines, and evidentiary reliability. Using investigative scenarios rather than tools, the session emphasizes defensible methodology and documentation.

LE ONLY: Roblox: Overview for Law Enforcement

This session provides law enforcement with an overview of the Roblox platform, its safety and parental control features, and how to work effectively with Roblox to obtain timely responses to lawful requests. Attendees receive a guided walkthrough of the Roblox Law Enforcement Portal, including request best practices, available data types, retention timelines, required identifiers, and a brief end-to-end case study, followed by Q&A.

LE ONLY: Snapchat Safety Operations 101

The goal of this session is to educate law enforcement about the Snapchat application and ways to work with the Snapchat Law Enforcement Operations team. This session will cover what data might be available pursuant to legal process, how to request voluntary disclosure of data in imminent threat to life situations, and lastly a brief introduction to safety on Snapchat and current initiatives.

LE ONLY: Unlocking the Secrets of Mobile RAM Forensics: Cracking Encrypted Android App Databases

This session will demonstrate how RAM analysis enables the decryption of unsupported encrypted Android app databases—revealing evidence that was once considered inaccessible. Attendees will learn how keys can be extracted from RAM and applied to decrypt thousands of encrypted databases, opening new investigative pathways and expanding the scope of recoverable evidence.

Many Hands

The era of “many hands” in digital forensics has arrived, with investigations spanning multiple agencies, devices, and stakeholders. Live collaboration is now essential—but true collaboration requires more than shared data. It demands clear workflows, defined roles, controlled permissions, and preserved evidentiary integrity to support parallel work. Without structure, teams risk version conflicts, duplicated effort, inconsistent tagging, and communication breakdowns that slow cases instead of advancing them.

This session explores what makes collaborative forensic work succeed — and where it commonly fails. We’ll look at practical considerations such as maintaining data provenance, structuring review processes, preventing context loss between teams, and designing workflows that scale without compromising defensibility.

Myanmar Scam Compounds: A Cyber Approach to Investigating Coups, War Crimes, Human Trafficking and Sanctions

This session examines blockchain forensic techniques used to investigate crypto money laundering, including practical tactics for tracing illicit digital asset transactions. Attendees will learn how to apply OFAC sanctions—specifically those targeting the Karen National Army and affiliates—to compliance screening and investigations. The session will also highlight how financial intelligence, OSINT, and geospatial analysis can be integrated to support complex investigations and victim rescue efforts.

Offline Localized AI: A World Without Rules

This session explores the growing ecosystem of home-built AI such as Ollama, Stable Diffusion, Open WebUI, N8N, and more; showing how offenders are leveraging them to operate without guardrails. This session provides practical guidance on what artifacts these tools create and how they can be examined forensically."

Pinpoint Accuracy: Mastering Mobile Forensics for Location Evidence

Geolocation data is often pivotal in criminal investigations, but building a reliable location timeline from mobile devices is challenging. This session for forensic examiners, investigators, and prosecutors covers key location artifacts -- how to extract, correlate, and overlay them into a cohesive, court-ready narrative.

Rapid Triage Workflow: Tactics, Techniques, and Procedures for Incident-Response Endpoint Investigations

You've had a ""true positive” security event on a Windows or Linux endpoint (or more than one)! Now what!?

Combining investigative methodology with creative utilization of some free tools and custom scripts, this session will discuss “tactical forensics"" and rapid triage workflow for Windows and Linux, including investigative priorities; the most important Windows and Linux forensic artifacts; and outline technical workflow for artifact selection, acquisition and analysis.

Reviewing Video as Evidence: When the Camera Doesn't Tell the Full Story
Seeing is not always believing. We know that intuitively when you witness a magician on the street, but it's harder to remember when a video is sent to us as proof of an incident. We take at face value what we see from phone videos or social media and may miss crucial clues or a fuller perspective of the situation. This session will look at how to get the complete picture from your video evidence, how to see what is there, what isn't, and how tools that "enhance" or authenticate videos become vital in interrogating your digital witness.

Sunlight on the Shadow Workers: Hunting State Sponsored Corporate Financial Espionage
Learn how North Korean IT workers infiltrate enterprises using stolen identities, contractor loopholes, & remote-work obfuscation. This session teaches practical OSINT, remote digital forensics, UBEA telemetry analysis, and AI-driven techniques to detect fraudulent applicants, spot identity-spoofing, correlate 2FA/device anomalies, & prevent foreign actors from gaining access to your organization.

Test Points in Mobile Forensics: Principles, Practice, and Pitfalls
Test points have long been used in mobile forensics to place devices into specific operational modes for acquisition and analysis. This session will provide a deep dive into test points, focusing on how and why they work, not just where they are located. Attendees will learn how test points are used to influence boot behavior, access modes, and communication states across a wide range of mobile devices. Rather than presenting a device “cookbook,” the session emphasizes transferable knowledge that enables practitioners to approach unsupported or unfamiliar devices with confidence.

The 5 Stages of Cyber Grief

In today's digital age, the impact of cybersecurity breaches on organizations can mirror the profound effects of personal loss, leading to what can be described as 'cyber grief.' This session explores the psychological journey organizations undergo following a cybersecurity incident. This journey mirrors the well-known framework of the five stages of grief: denial, anger, bargaining, depression, and acceptance.

The Modern Analyst's Toolkit: Why Non-Traditional Tools Matter

Digital investigations are evolving faster than most traditional forensic tooling can adapt. In this session, we'll 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.

The Multi-Billion Architecture of Deception: Mapping Illicit Flows in the Crypto Industry

As the crypto industry strives for legitimacy, a shadow economy persists. This session uses blockchain data to uncover how criminal syndicates obfuscate capital flows. We reveal over 32,000 annual "trust-building" micro-deposits that moved approximately $27.8 billion annually into suspicious accounts between 2021 and 2023. Attendees will gain an understanding of the crypto industry and its role in sustaining global criminal flows.

The Nexus of Tech and Trafficking: A Multi-Disciplinary Response

Traffickers increasingly exploit technology to groom, recruit, and control victims. This session highlights how multidisciplinary teams—analysts, prosecutors, and social workers—collaborate throughout investigations to improve outcomes. Using real cases, we'll explore identifying online platforms used in human trafficking, detailed steps for building a strong digital investigation & prosecution, and how integrating trauma-informed, person-centered social service support throughout the process builds victim trust and significantly increases the likelihood of successful case resolution.

The Rise of IoT in Digital Investigations

IoT devices are everywhere and causing potential chaos with the data they collect and store. With risks to digital security and information sharing they are becoming a prime suspect in digital evidence. Learn the new process for seizure and capture of the data associated with these digital devices. Discover the untapped information that can be discovered from them from security risks and leaks to digital evidence.

The Security Blind Spot: Why Airspace Intelligence + Drone Forensics Are Now Imperative

Despite heavy investments in cyber and physical security, low-altitude airspace remains a critical blind spot as drone threats grow. This session explores how airspace intelligence and drone forensics close this gap. This session will detail how the drone forensic lifecycle—from detection to operator identification—turns aerial data into actionable evidence.

To Cull or Not to Cull: Why Early Data Volume Assessment Matters

In this session, legal and forensic experts will break down practical strategies for culling and filtering electronically stored information (ESI) during and after collection in an e-discovery project. Attendees will learn how to gain early insight into their data, streamline review workflows, and reduce the costs and risks associated with large-scale data collections—empowering legal teams and law enforcement to work more efficiently and defensibly from the outset.

Turning Big Discovery into Clear Strategy With AI

In this session, experts will discuss how modern AI empowers legal teams to make sense of large datasets and move efficiently from documents to actionable insights. Attendees will learn how AI can surface priority documents for faster case understanding, connect facts to themes and timelines to support early case development, identify patterns and inconsistencies within productions, and strengthen deposition preparation by quickly linking documents, key issues, and potential lines of questioning.

Unmasking the Hidden: Dark Web Monitoring Meets Crypto-Asset Analytics

As anonymization tools and cryptocurrency adoption expand, criminals increasingly exploit anonymous networks and digital assets to conceal identities, launder funds, and coordinate illicit activity. In this joint session, using real-world cases, Todd Shipley and Mark van Staalduinen will present a practical, investigative-focused overview of the Dark Web and its intersection with cryptocurrency ecosystems, demonstrating how Dark Web

Monitor and Crypto-Asset Analytics work together to expose criminal infrastructure, financial flows, and operational missteps that lead to deanonymization.

When AI Meets the Witness Stand: Examiner Readiness and Legal Risk
This two-hour panel prepares digital forensic examiners for AI related challenges in court. It will feature two seasoned digital forensic examiners and two attorneys fluent in the current AI world, that will discuss how AI is currently changing digital forensics, the risks it introduces, and how it affects testimony. The session will introduce the concepts of defending AI's use in testimony through a live mock cross examination to demonstrate responding clearly and defensibly when examiners are questioned about AI.

When Monitoring Fails: Digital Tradecraft Gaps in Exploitation and Trafficking Investigations
This session examines how digital exploitation and trafficking investigations are shaped by investigative tradecraft influenced by registry-based and monitoring systems. The session explores how reliance on static systems and incomplete data creates investigative blind spots, even when relevant digital evidence exists. The session highlights how offenders exploit gaps between physical monitoring and digital behavior across online platforms, encrypted communications, gaming environments, and cross-jurisdictional networks, and how system-driven assumptions and workflow constraints limit effective interpretation of digital artifacts. Attendees will gain practical tradecraft strategies to recognize false signals of safety, strengthen reassessment practices, and identify and escalate digital indicators of exploitation and trafficking that forensic tools often overlook.

"