Techno Security & Digital Forensics Conference

June 3-5, 2025 – Wilmington, NC

SNEAK PEEK

Confirmed Conference Sessions

(as on February 17, 2025)

Full Conference Program will be available mid-March

A Beacon in the Darkness: Navigating Cryptocurrency Investigations

A session for law enforcement and private sector investigations professionals to gain a base level knowledge on industry terminology, best practices, and a look into how to investigate cryptocurrency using publicly available information as opposed to paid blockchain analytics services.

Addressing Insider Risk: A Psychological Approach to Proactive Risk Management

Insider threats are a growing challenge as more individuals gain access to sensitive information amid global instability and economic competition. While traditional defenses like access controls and cybersecurity are essential, they often overlook human vulnerabilities like stress, workplace dissatisfaction, and ethical adaptability. This session will highlight key behavioral, psychological, and personality-driven vulnerabilities that contribute to insider risk. It will offer a proactive, individual-centered approach to risk management along with practical intervention strategies.

Adversary or Ally? The Two Sides of the AI Cybersecurity Coin

Artificial Intelligence (AI) has become one of the fastest adopted technologies ever, out pacing cell phones, personal computers and the internet. By design or accident AI brings many possibilities as both an ally and adversary, creating unique and complex security challenges. During the session we will explore many of these possibilities and break down what considerations security professionals need to look at as organizations adopt and adapt to the ever-changing AI landscape. Including how to prepare for and respond to incidents involving AI, implementing responsible AI, defending from AI threats, and how AI can be used as a force multiplier.

AI Hype or Helper in Remediating Security Issues: A Case Study

When AI started to be the technology du jour, many companies decided to integrate it into their own products. The same cybersec teams that worried about potential cybercriminal uses of AI, also tested its ability to protect their data. In this session, a CTO will share a candid glimpse behind the curtain of his company's decision whether to integrate AI into their product pipeline. He will review the steps he took to develop the idea, take it to market, gain feedback and launch it successfully. Hear best practices in both technology adoption and AI's ability to help security teams.

AI in Digital Forensics: Hype, Hope, and Hard Truths

Artificial Intelligence is revolutionizing every industry, and digital forensics is no exception. But with great power comes great responsibility—and even greater scrutiny. This session will explore how AI can and must be safely integrated into forensic workflows, ensuring accuracy, reliability, and accountability. We'll discuss the potential pitfalls of AI-driven analysis, from bias and automation errors to legal admissibility challenges. Through real-world examples, we'll separate the hype from reality, demonstrating where AI truly enhances forensic investigations and where human expertise remains irreplaceable. Join us as we navigate the intersection of technology, ethics, and the law, ensuring AI serves justice rather than distorting it.

AI is Not Enough to Beat AI: Pragmatic Deepfake Detection

This session will explore a holistic approach to discriminating deepfakes from authentic images and videos, including:

- Limitations of automated deepfake detection: why relying solely on automated tools or the analysis of file structure and metadata is not robust enough for forensics.
- Techniques for authenticity evaluation: an overview of methods for analyzing media based on format, artifacts, scene geometry analysis, context, compression artifacts, frequency domain, and AI-based approaches.
- Looking forward: insights into when each technique is most effective and a discussion on the emerging challenges.

An Employee Stole Millions of Dollars' Worth of Company Data… or Did They?

This session will walk through the forensics of a case related to the alleged theft of high value company data. This case is a real whodunit - a riddle, wrapped in a mystery inside an enigma, and stuffed into a paradox. If you want to deep dive into disk, file system, and operating system forensics with a side of good old fashioned detective work - this is the talk for you.

An Overview of AI-generated Results in DFIR Exams

As Artificial Intelligence (AI) evolves, so does the desire to use its great power in forensic tools and examinations. This session will introduce the audience to probabilistic outputs from AI algorithms where results are not presented with absolute certainty. It will discuss what a probabilistic output really is, appropriate uses within examinations, introduction/admissibility in legal proceedings, and practical applications of probabilistic outputs in media authenticity.

Are You on the Blockchain Train?

Join us for this session where we discover the fundamentals of blockchain technology and its integration into mobile application development. Explore how blockchain extends beyond cryptocurrency, powering non-crypto applications, and examine the unique security challenges it introduces for forensic analysis in mobile apps.

Artificial Intelligence and Generative AI: Causes of Action and Defenses and Discovery

Artificial Intelligence and, more specifically, Generative AI (""GenAI"") has taken the world be storm. It has led to government investigations, state and local regulation, and civil actions arising out of its “products." This session will address:

- Overview of artificial intelligence (“AI) and generative artificial intelligence (“GAI”)
- Benefits and risks of AI and GAI known and foreseeable
- Causes of action arising out of AI and GAI use
- Defenses to liability

Auditing Generative AI Cyber Risks: A Case Study

Generative Artificial Intelligence (GenAI) is revolutionizing our lives. When controlled and used ethically it can automate tasks, increase productivity, solve complex problems, improve our health, and provide many more benefits. However, if left uncontrolled or used by nefarious parties, such as cybercriminals, it will lead to harmful outcomes. GenAI is here to stay. It is critical that the risks associated with it are mitigated before it is too late.

This session will provide an overview of the challenges we are facing, governance frameworks and suggested actions for controlling GenAI, and best practices and practitioner tips for auditing GenAI.

Big Data Investigation within the Dutch Police

This session will discuss collecting large amounts of digital evidence and how to combine all the traces from the digital evidence with other traces that we have at our disposal. It will

include a walkthrough of how the Dutch police work and share a case study of a major investigation that combines large amounts of digital evidence.

Black Box Investigations: Navigating the Risks of Automated Data Collection

This session explores the challenges and risks of relying on black box technologies in OSINT investigations, using a shooting investigation as a case study. Attendees will gain insights into the pitfalls of automated tools, including validation gaps, algorithmic bias, and legal concerns. The session will also highlight how unverified outputs can undermine justice and trust in investigations. Key takeaways include understanding the limitations of black box systems, strategies to balance automation with manual oversight, and best practices for ensuring transparency, accountability, and accuracy in high-profile investigations.

Calling All Digital Forensics Examiners: Outsmarting Anti-Forensics

This session will share practical insights and creative techniques used in real law enforcement cases to tackle anti-forensic methods, uncover hidden evidence, and piece together a complete picture of the investigation. Learn how to outsmart obfuscation tactics and piece together critical data to solve complex cases.

Can a Single Rotten Plank Sink the Ship of Evidentiary Integrity?

The computer evidence cracks the case. But is the computer evidence cracked? During the analysis, malware was identified and dismissed. It was dismissed because it couldn't have been malware…right?

This session will break down a process of how to scan digital evidence for indicators of compromise, how to identify potential malware and how to investigate its potential impact of evidentiary integrity.

Context Matters - Practical Approaches to Turning Data into Actionable Intelligence

This session will spend very little time discussing definitions of terms, basic concepts, etc., and instead will focus on the very real need to create context around so much data coming into organizations. The aim will be to create intelligence, using simple scenarios and use cases, that is both meaningful AND actionable - as well as how to make use of that intelligence - which is something that is often missing from many wide-audience intelligence reports and briefs.

Cracking Cases: Digital Forensics, OSINT, Wiretaps, and Beyond

In modern investigations, successfully integrating digital forensics, OSINT, wiretaps, and beyond is essential for uncovering hidden connections and tracking criminal behavior. This

session will explore how these diverse data sources can be combined to gain new insights, identify criminal suspects, and build stronger cases. The session will discuss merging your location data across sources to trace digital footprints and map locations; how to associate anonymized data with real-world identities; and, how to leverage digital forensics and wiretap data for a more comprehensive and accurate investigation.

CryptOSINT: OSINT Your Crypto Cases… and Not Just on the Blockchain
This session will explore the power of OSINT to conduct your cryptocurrency investigations. It will hop off the Blockchain to try some attribution techniques on breadcrumbs left behind on social media, websites, forums and more. The session will delve into a case that starts abroad but trails into radicalized US citizens and explore the digital exhaust and connections left through transactions that can help identify nefarious threat networks and their sponsors. The marriage of multiple technologies will also be highlighted to show the power of 2 + 2 =5 when applied correctly.

Deep Space - Private Space in Android 15
Android version 15 introduced the Private Space feature that allows users to hide sensitive items natively. This session will discuss the nature of this new feature and how it can affect mobile device investigations.

Detecting Deep Fake Digital Photographs: Utilizing Python and AI to Analyze and Detect Anomalies in Digital Images
Deep fake digital photographs are becoming increasingly sophisticated, posing significant risks to personal, corporate, and national security. This session explores advanced techniques for detecting deep fake images using Python and AI-driven anomaly analysis. Drawing from extensive research in image-based steganography detection, these methodologies are now applied to uncover hidden patterns and inconsistencies that differentiate authentic photographs from manipulated ones. The session will demonstrate the application of Python and AI to identify these fraudulent images.

Determining Reality: Defensive Techniques to Combat Advanced Synthetic Identities
This session will focus on combatting advanced synthetic identities through a multi-layered, technology-driven approach including: Implementing machine learning, applying multi-source verifications and integrating biometric and behavioral analytics.

Discord OSINT Demystified: Tools, Tips, and Best Practices

Despite being overshadowed by social media giants, Discord is an underrated gem in the OSINT realm. With over 150 million monthly users, it hosts diverse communities ranging from gaming and tech to education, hobbies, and activism.

Public servers and channels on Discord offer opportunities to uncover connections, group dynamics, and potential evidence, making it a valuable platform for OSINT investigations.

This session will explore practical tips and tricks for conducting OSINT on Discord, including: Effectively navigating Discord communities; Identifying servers and channels of interest; and Gathering details about users.

Essential Early Case Assessment for Mobile Device Extractions

The session will cover key topics such as case context, evidence identification, prioritization techniques, and case examples. By understanding the nature of the case, investigators can identify key data points and anticipate potential challenges. Through effective prioritization, they can streamline their analysis and focus on the most relevant information.

Fire in the Sky: Drone Threats to Critical Infrastructure and the Digital Forensic Examiners Response

In 2024 an alarming new threat began to emerge, cheap commercially available drones used to threaten critical infrastructure. During this session, forensic examiners will walk through a drone forensic investigation from start to finish, uncovering critical evidence to trace the origins of the attack and the perpetrators behind it. Attendees will gain insights into the step-by-step process and understand the challenges and importance of securing critical infrastructure.

Forensic Analyses of Audio and Video Evidence

Audio, acoustic and video evidence are common and critical in civil and criminal litigation. Often such evidence is from a computer or mobile device. This session will discuss why proponents and opponents of such evidence must at least be familiar with what can (and cannot) be done forensically and legally including: Content-based authenticity analyses forensically determine if the evidence is trustworthy (admissible), or has been tampered with in any way (inadmissible) and digital signal processing (enhancement) makes the audio or video more audible or clearer. Actual cases with audio and video evidence as received will be discussed.

From Factory to Forensics: Configuring Your Mac for Digital Investigations

Transform your Mac into a forensic workhorse with this practical, step-by-step guide. In this session, you'll learn how to configure your Mac from day one to handle forensic investigations, no matter what tools you use—native macOS applications, open-source utilities, or commercial solutions. This session will share where to find and how to install hundreds of free, open-source forensic tools, covering everything from imaging and analysis to triage. Save yourself time, stress, and mistakes—join this session to set up your Mac for forensics the right way!

Going on a Cyber Attack Surface Treasure Hunt

As information technology progresses and expands, its Cyber-attack surface expands dramatically. Everywhere you look there's more "Smart"..(or in some cases, Not SO Smart technology!) being connected to the Internet. Many organizations haven't a clue what their attack surface really looks like. This session will provide a practical, low-cost methodology to detect, assess, and exploit numerous cybersecurity vulnerabilities that stem from improper software configuration, software/firmware inconsistencies, and design flaws within an overall network infrastructure and applications. This session will also identify sources of useful info and tools.

HANDS ON LAB: Encryption Nuts and Bolts

We all use encryption with AES and RSA algorithms ubiquitous, but how do these algorithms actually work and why is this important? As digital forensic examiners and analysts you may be required to explain how this stuff works. This hands-on workshop will go into detail on the workings of encryption and use Python and Excel to demonstrate the inner working of these algorithms. Emphasis will be on RSA and some AES given the time constraints.

***BYOD*

HANDS ON LAB: LEAPP Forward: Unlocking the Power of Open-Source Forensic Analysis

The LEAPP suite is a collection of open-source forensic tools designed to empower investigators with efficient methods for parsing and analyzing data across multiple platforms, including iOS, Android, Windows, and vehicle infotainment systems.
Key takeaways will include:

- An overview of each tool within the LEAPP suite and its specialized focus.
- Practical examples of artifact extraction and analysis.
- Guidance on implementing these tools in everyday forensic investigations.

HANDS ON LAB: Sysdiagnose Logs 101

Sysdiagnose Logs – What are they? This hands-on workshop will answer that question and more! Sysdianose Logs have a plethora of details examiners may be missing. This session will explore how to generate these logs and how to examine the data within them. As with any analysis in forensics, it's important to know what the data is and isn't telling us. After this workshop, examiners will understand what these logs are and what they aren't!

**Limited seats: Pre-registration required*

***BYOD*

How Ransomware Attacks Work, How Cyber Insurance Works, and How You Can Get Work

A ransomware attack is an economic attack against a victim organization by a criminal enterprise. Cyber insurance is most closely associated with this type of attack, but there is another way to understand the attack: business disruption. As civilian and public sector forensic analysts move to the cyber security departments and service providers, understanding the perspective of the organization defending against such attacks provides you with a differentiator to others with a technical skill set. This session concludes with the perspective of two practitioners who made the jump to civilian cyber security leadership.

How to Align Compliance Activities

Chances are your organization is responsible for complying with multiple regulations and frameworks. How do you accomplish this without wasting time, money, and personnel resources? More importantly, how do you get the necessary buy-in from the CISO?
The answer: Proper Security Focus and Execution

This session will discuss FedRAMP, CMMC, NIST 171, SOC2, HIPAA, HITRUST, StateRAMP, TXRAMP, and FISMA and share how reducing redundancies and maximizing your use of internal experts will allow you to successfully comply without breaking the bank and help the CISO approval process.

Incident Response Preparedness

Effective preparation is the bedrock of a successful incident response strategy, as underscored by both the NIST and SANS frameworks. In this session, we will delve into the critical steps necessary to build a robust incident response plan. Attendees will learn how to minimize financial losses and prevent reputational damage through rapid and well-coordinated responses to cybersecurity incidents. Join this session to ensure your organization is equipped to handle cybersecurity threats with agility and confidence.

Just the "Just the Arti-facts, Ma'am"
Traditional workflows of collecting & examining full disk images is no longer a viable Cyber Incident Response option with the larger drives, cloud and network storage & the timeframe customers and CISOs want answers to the Who, What, When, Where, & Why questions in a Cyber Security Incident.

The efficient workflow is collection and analysis of artifacts to find the answers and secure the network. Join Joe Friday and Bill Gannon (aka Robert O'Leary & Dr. Kall Loper) in the pilot episode of Cyber Dragnet! Learn how to make your Cyber IR teams better prepared to get to the Arti-Facts! faster."

LE ONLY: Unmanned System Forensics: How One Drone Can Change the Course of Your Investigation
U.S. Customs and Border Protection's Center for Air and Marine Drone Exploitation (CAMDEx) will highlight the latest techniques involving Unmanned System (UxS) forensics. As this genre of digital forensics is largely under-researched, CAMDEx will offer up the path forward in acquiring, parsing and analyzing the highly unique data found within these systems. Attendees will walk away with insights and methods on how best to examine a variety of drones including the latest encrypted models

Linkage Investigations: Cryptocurrency, Dark Web & OSINT
With the rise of the internet, criminals have found new ways to engage in illegal activities like human trafficking and child exploitation. The dark web and cryptocurrency have allowed criminals to conduct transactions anonymously, making it difficult for law enforcement to track them. However, there are OSINT tools available to collect, analyze, and share publicly available information that can help uncover identities and build cases. This session will review the use of cyber technology, focusing on cryptocurrency, clear and dark web data, and OSINT (open-source intelligence), with a special emphasis on child exploitation on the dark web.

Living Off the Land and Emerging Threats
This session provides a concise yet comprehensive overview of the methodologies employed by nation-state threat actors to infiltrate, persist, and operate within targeted environments undetected. Leveraging the concept of Advanced Persistent Threats (APTs), these actors employ sophisticated strategies to exploit native tools and sessions, blending seamlessly into legitimate operations.

Mastering Attack Surface Management: Reducing Risk in a Complex Cyber Landscape
In the face of a rapidly expanding attack surface driven by cloud services, IoT devices, and remote work, organizations should include effective Attack Surface Management (ASM) strategies. This session offers an in-depth exploration of ASM, covering key concepts like asset discovery, continuous monitoring, and risk prioritization. Attendees will learn about the tools and technologies available for managing vulnerabilities, the challenges of scaling ASM, and best practices for integrating it into broader security programs. This session provides actionable insights for minimizing cyber threats and securing complex IT environments.

Mastering Microsoft OneDrive Forensics: Navigating Cloud-Based Challenges
Explore the challenges of cloud-based forensics in Microsoft OneDrive environments. This session equips attendees with strategies to analyze OneDrive artifacts, interpret unique digital footprints, and examine locally stored items. Learn to extract critical data from synchronization logs to reconstruct timelines and investigate user activity. Enhance your expertise in navigating the complexities of cloud-integrated ecosystems and uncover actionable insights for modern forensic investigations.

Obfuscation in Digital Forensics: Joseph Andes Case Study
A case study related to the conviction of Joseph Andes. Joseph Andes had identified on grand jury for a CSAM case and used knowledge of LE forensic capabilities to hide his own crimes. This session will review the original case report and the indicators of forensic obfuscation originally found. The session will share the novel motion his lawyer attempted and go over the more in-depth examination done on the obfuscation in preparation for the motion to dismiss hearing. Attendees will learn on how to better investigate obfuscation in our examinations and reports.

Quantum Computing and Its Impact on INFOSEC
AI is the new "big thing," while quantum computing advances out of the public view. However, quantum computing will have an impact on information security, especially with respect to cryptography. This session will discuss what quantum computing is, why it offers significant improvement over traditional computing in specific use cases, what those cases are, and what you and your organization should be doing to prepare for it. The session will also look at proposed timelines for when particular milestones in quantum computer are predicted to be reached.

Redefining Insider Threat Management: A Human-Centric Approach

As organizations continue to invest in advanced security technologies, we often overlook the essential human element at the heart of the problem. This session challenges the status quo, advocating for a proactive approach that prioritizes understanding and addressing the motivations driving insiders to compromise security. By reframing the problem, we aim to foster environments that reduce the likelihood of insider threats, ultimately diminishing the need for additional security tools. Join us to explore innovative solutions that go beyond technology and embrace a human-centric strategy to safeguard your organization from insider threats

Secure Element Enabled Android Phones, What is it and How Does it Affect my Work?
Secure Element phones come in many flavors, eSE, SPU and SE. This session will share how these were previously used in high-end models, they are now also found in mid-range volume phones, making the forensic examiners and investigators' work challenging. The session will discuss how moving the encryption components away from the operating system, into dedicated chips designed to resist exploits and attacks. And share how in some cases, data can be recovered from these devices, even when the suspect is not cooperating by giving up their passcode.

Securing Resources and Funding for Mobile Device Forensics and Training
This session will guide law enforcement practitioners and leaders through strategies to build a compelling case for resource allocation. Attendees will learn how to demonstrate the value of mobile forensics tools, gather and present impactful data, and address concerns from decision-makers, procurement teams, and grant committees. From identifying agency-specific needs to comparing solutions and strengthening funding proposals, this session equips agencies with practical steps to secure essential resources for effective investigations.

Self-healing and Cross-architecture Code Similarity: Two DARPA Funded Research Projects with Impacts on Cybersecurity and Digital Forensics

This session will share and discuss two rather exotic capabilities that are being developed under a DARPA contract including:

- Cross-architecture code similarity where the system can identify similar functions at the binary level, even if they've been compiled for different architectures.
- A self-healing bus environment where isolated systems can detect anomalous behavior, identify the code region, propose a patch, and apply the patch, all without human intervention.

The session will walk attendees through the “how"" of both processes and then explore with the audience possible applications that would make their lives easier, more effective, or less stressful.

Staying Ahead of Cybercriminals: Generative AI and the New Era of Financial Fraud
This session will help attendees understand the threat landscape and gain insights into how cybercriminals are leveraging Generative AI, including deepfakes, to execute sophisticated financial fraud such as CEO/CFO impersonation and electronic fund transfer schemes. Attendees will learn about the latest tactics in reputation manipulation and automated phishing campaigns powered by Generative AI, and how these exploit trust within organizations. Lastly, attendees will discover proactive measures and technologies to detect and counteract AI-enabled threats, empowering your organization to stay ahead of evolving cybercrime tactics.

Telegram & its 2025 Crypto Initiatives
Telegram is the fifth largest instant messaging service in the US. The organization has identified the US as the target number one for expansion in 2025. This lecture provides basic information and practical tips for making sense of Telegram information about users, discussion groups, and cyber fraud.

The Artificial Witness - Forensic Implications of an Onboard Artificial Intelligence
Artificial Intelligence has come to devices in the form of operating system level enhancements to instantly turn our thoughts into actions. This session will explore the impact this observer could have on your digital forensic investigations.

The Challenge of Hyperlinked Documents in E-Discovery
Hyperlinked files, sometimes referred to as “modern attachments,” are turning up in legal and technical environments and they are causing headaches for e-discovery, information governance, and forensics professionals. Links sent in emails and messaging platforms to documents that are stored in platforms like OneDrive, Google Docs, and others, present a real challenge to legal and forensics professionals, particularly as relates to legal discovery and the process of collecting electronically stored information for legal matters. This panel discussion will explore the challenges and potential solutions related to hyperlinked documents.

The Critical Role of Metadata in Solving a Complex Child Exploitation Case
This case study highlights the pivotal role of metadata when no other evidence appears to exist. Through a meticulous analysis of both deleted and hidden metadata, investigators uncovered key evidence that directly linked a found flash drive to a suspect and his

personal laptop. These metadata artifacts were instrumental in building an irrefutable case, ultimately leading to the arrest and conviction of a future pediatrician. This case exemplifies the crucial importance of metadata in forensic investigations and demonstrates how a single, deleted digital artifact can be the breakthrough needed to bring justice and prevent future harm to children.

The Future of Network Security: Trends and Predictions

This session will explore the current and emerging technologies shaping network security, from AI-powered threat detection to the convergence of wired, Wi-Fi, and cloud-native security. The presenter will dive into trends like SASE, Zero Trust, and quantum-resilient encryption, offering insights into how to secure networks today while preparing for tomorrow's challenges. Learn actionable strategies to future-proof your infrastructure against advanced threats. This ain't your grandma's NAC and firewall tools.

The Intersection of AI, Forensic Readiness, and eDiscovery: Preparing for the Future of Litigation

As artificial intelligence continues to transform the legal landscape, the intersection of AI, forensic readiness, and eDiscovery has emerged as a critical area of focus for legal professionals and forensic practitioners. This session will explore how organizations can integrate AI tools into their forensic and eDiscovery workflows to streamline processes, enhance efficiency, and uncover deeper insights—all while maintaining compliance and defensibility in legal proceedings.

Attendees will leave with actionable insights and readiness strategies to adapt to the evolving landscape of litigation, leveraging AI to stay ahead in an increasingly complex digital evidence environment.

The Nation-State as Cybercriminal

When cybersecurity professionals think about cybercrime, the usual threat actors who engage in data theft, extortion, and other financially motivated attacks for personal gain usually come to mind. The threat landscape is constantly evolving, and one recent development has been increased cybercriminal activity by nation-states, which is both troubling and challenging because of the resources that nation-states can muster for their attacks. This growing threat is one that most organizations will find difficult to combat. This session will discuss nation-state motivations, tactics, possible defense strategies and the challenges of each.

The Safe Use of AI: Strategies to Ensure Data Integrity and Evidence Admissibility

Artificial Intelligence (AI) is increasingly embedded in every aspect of our lives, and its role

in digital investigations is no exception. This session explores strategies for the safe and responsible use of AI, tackling potential oversight, bias, and ethical challenges while ensuring evidence admissibility, robust chain of custody, and the highest standards of data security and integrity. Attendees will gain insights into practical applications, industry best practices, and actionable approaches to integrating AI into investigative processes while maintaining legal defensibility and ethical accountability.

Tower Dumps and Area Searches

In the realm of investigation, the utilization of tower dumps and area searches has become increasingly pivotal. This session delves into the methodologies and applications of these techniques. This session will cover the technical aspects of the search, including acquisition and analysis, and a case study. It will also address the legal considerations around a geolocation-based search. Attendees will gain a comprehensive understanding of how tower dumps and area searches can be effectively employed in modern investigations, ultimately contributing to more efficient and successful outcomes.

Ukraine/Russia - Lessons Relearned for Critical Infrastructure Operations

The hybrid nature of modern conflicts show the importance of defending and attacking critical infrastructure. This session will discuss the present situation in attacks against critical installations and installations and derive a set of principles for future threats

Unlocking Hidden Data: Mastering SQLite Forensics

Navigating SQLite Databases is essential for digital forensic investigators, especially when dealing with unsupported applications. This session will guide you through the manual analysis of SQLite databases, showing how to extract and interpret critical user data like messages and contacts. Understanding these databases is key to uncovering hidden evidence, and SQLite Viewers provide the tools needed for thorough analysis, ensuring no vital information is overlooked.

USB Flash Drive Artifact Hunt

Forensic examination of USB device activity is crucial for many different types of investigations. Findings of connections are useful for proof of data exfiltration and/or identifying further evidence to recover. USB device activity can help place the suspect at the keyboard or show knowledge of possession and/or indicate contraband distribution. When an external device is connected, many artifacts of interest are created. This session will cover the methodology of chaining these artifacts together as we pursue them across a Windows system, discover acts perpetrated during and around connection times, and report findings in a meaningful way.

Using AI Computer Vision in Your OSINT Data Analysis

This session will share how AI-infused computer vision can rapidly increase your image and video OSINT data analysis processing time, accuracy, and comprehensiveness. It will share how to use computer vision in your OSINT investigation to uncover artifacts and objects in images and video commonly overlooked by the human eye. Attendees will walk away with new insights in how to approach your OSINT processes, especially image and video forensic evidence and create a much stronger narrative surrounding the results.

Utilizing ETW for Ransomware Threat Detection

Windows Event Tracing for Windows (ETW) offers a powerful, native telemetry framework that provides deep insights into system and application behavior. Despite its potential, ETW remains underutilized in many investigation and threat-hunting scenarios.
This session explores the critical role of ETW in identifying ransomware attacks, showcasing how it can monitor key activities like rapid file modifications, anomalous file access patterns, and encryption behaviors. This session will demonstrate how ETW enables the detection of ransomware tactics at various stages, from initial execution to file encryption attempts.

Vehicle Forensics: Data Extraction from the Memory Chips of Telematic and Wireless Modules

This session will take a closer look at the telematics systems and wireless modules found in vehicles. The session will explore the types of memory chips they use, the file systems they rely on, and the valuable data that can be recovered from them. Most importantly, the presenter will show how this data can play a key role in solving cases in digital forensics

What Happens Next? Using eDiscovery Tools and AI to Tell the Rest of the Story

This panel of eDiscovery experts will explore the AI and eDiscovery tools and processes that are used to analyze forensic data and reporting. Attendees will learn about eDiscovery methodologies in collecting data, the pros and cons of using AI tools, and how it impacts the "ROI." The panel will explore the defensibility and admissibility of investigative findings revealed in this analysis.

Why CTEM Can Help You Secure Your Enterprise

Continuous threat exposure management is one of the hottest trending topics and for good reason. It takes the concepts of vulnerability management, which is vital, and adds to the other key security components that every organization needs to be truly secure. This session will break down CTEM into its core components, then build them back up so you

have a clear understanding of what each component is, why it is important, and what you need to look for to have a comprehensive CTEM solution for your environment.

Why Your Threat Modeling Program Doesn't Work and What You Can Do About It.
Organizations say they want more 'shift-left' to reduce vulnerabilities but don't understand how to execute effective solutions that reduce the risk causing senior leadership to become less supportive of the initiative. This session will outline some common gaps often seen in threat modeling programs, demonstrate why most programs fail to show value and provide actionable insights to boost effectiveness.

Wireless Witness: Uncovering Digital Evidence from Android WiFi & Bluetooth
Every connection tells a story. Android devices constantly interact with WiFi networks and Bluetooth devices, leaving behind a trail of digital breadcrumbs that can be invaluable in forensic investigations. This session will dive into how forensic examiners can extract, analyze, and interpret WiFi and Bluetooth artifacts from Android devices. We'll explore the forensic significance of connection histories, MAC addresses, and geolocation data, demonstrating how these records can establish movements, associations, and alibis. Through real-world case studies, we'll highlight best practices, challenges, and legal considerations when leveraging wireless evidence. Whether you're tracking a suspect's movements or verifying an alibi, understanding Android's wireless footprint can make the difference between speculation and solid evidence.