Techno Security & Digital Forensics Conference

June 4-6, 2024| Wilmington, NC, USA
SNEAK PEEK of CONFIRMED SESSIONS

(As of February 13, 2024. All sessions and full details including times, dates, and speaker bios will be available early March)

A Process for Identifying USB Storage Device Activity in Windows 11
This session outlines a process for identifying USB storage device activities on Windows 11. Leveraging Sysinternals Procmon, we monitor registry changes related to USB insertions, removals, and persistent connections. As Windows evolves, adapting investigation methods becomes crucial. Objectives include interpreting registry key changes, associating timestamps with USB activities, and mastering Procmon for real-time monitoring. Vital for forensic professionals, this session addresses the absence of public documentation on these registry keys in the latest Windows release, providing a documented approach applicable to newer OS versions.

AI and the Impact it Will Have on Children, Digital Forensics, Regulation and Legislation.
Artificial intelligence has garnered significant interest in the United States Congress, impacting investigators and potential victims. This session will address what is coming from an A.I. legislative and policy perspective. The presenter will discuss how policy and legislation impact digital forensics and cyber investigators. The session will also share how to avoid pitfalls in utilizing A.I. and how to position you and your organization with minimal impact. Finally, the presenter will illustrate AI's impact on victims and what is being done to address that from a policy perspective.

AI in Digital Forensics: Navigating Tools, Crime, and Courtrooms
Explore the convergence of Artificial Intelligence (AI) and Digital Forensics in this dynamic panel discussion. Uncover AI's impact on forensic tools, crime detection, and its admissibility in court. Industry experts will address legal challenges, ensuring AI-driven evidence meets scrutiny while envisioning the future of AI in digital investigations.

An E-Discovery Conundrum: The Disappearance of Ephemeral Data
Ephemeral data presents a real conundrum for everyone who works in the legal business. Lawyers have legal and ethical obligations to preserve, collect, review, and produce relevant electronically stored information. Law enforcement and government regulators seek relevant ESI in almost all investigations. But what happens if the data disappears? In this panel session, attendees will learn more about common sources of ephemeral messaging data and its impact on litigation, investigations, and regulatory inquiries.

Applied Use of AI Computer Vision for Forensic Data Analysis

OSINT is a great mechanism for the collection of data, but what do you do with all of it once it's collected? For the last 5 years we've been exploring Azure and AWS for computer vision to rapidly process large sets of image and video data forensic evidence; and perform object detection, facial recognition, OCR, voice to text, etc. This session will explore the use of AI to exponentially improve your analysis.

Architecting for Cybersecurity

The cloud has created opportunities for adoption of emergent technologies, e.g., Artificial Intelligence (AI), that many would have considered out of reach a few years ago. Additionally, data is spanning geographic zones in ways that can redefine both organizational & legal boundaries. This creates not only new opportunities, but many new complexities cybersecurity experts must account for. This session will look at how systems can be designed or rearchitected to take advantage of cloud technologies to improve cybersecurity postures around threat/risk management, vulnerability mitigation, & how we prepare for & respond to incidents.

Are We Prisoners of Convenience?

In 2023, we have seen very serious data breaches of Manage File Transfer products by ransomware gangs. Analysis shows that the attacks came through the web browser. MFT vendors provide a browser interface for transferring files, claiming it is "too hard" to use FileZilla using more secure methods like FileZilla for SFTP.

This is a tale as old as time. Software is supposed to be easy to use, but companies have tipped the scales too far in favor of convenience, at the expense of security. During this session, the presenter will speak about striking the right balance and staying secure.

Bad Moon Arising Out Your Back Door - Securing and Auditing Remote User Network Access

Use of remote user access to enterprise networks has exploded dramatically since the start of the recent COVID pandemic...but due to its often-careless management and use, it has become a dangerous backdoor conduit for ransomware and other cyber-attacks. Compromised remote access credentials have become a hot item on the Dark Web. In this highly practical session, you will learn how to detect, test, and mitigate serious vulnerabilities associated with remote access technologies including: remote desktop services and VPNs. Session material will include IT audit/security assessment checklists and sources of useful cyber tools and references.

Balancing Privacy and Effective Investigation with Team-Based Review

Whether working a HIPPA case, client-attorney privilege, or just a system with mixed file and data ownership can raise privacy concerns and without a proper methodology hinder the investigation. This session will discuss some case-law history, MLB legend Barry Bonds, and key considerations investigators should apply when investigating mixed ownership cases. The presenter will cover collection and review methodologies and technologies (including cloud solutions and offline Portable Case) that make team-based review easier and more approachable without sacrificing quality.

Big Data - Big (Addressable) Challenges
The number of data sources continues to grow. Leading organizations now have Chief Data Officers to lead the governance and set the direction in dealing with the data sets. Reports are dynamically generated at time of need and decisions happen based on the most accurate data. At least theoretically. This session looks at pitfalls like delays in data feeds or failures to capture decision points from data. Attendees will learn how to identify gaps in the governance and supporting technology to avoid surprises during discovery.

Building a Resilient Future: Security Risk Management in the World of eDiscovery
In today's digital landscape, data is curial to business and legal processes. Managing eDiscovery security risks is vital. This session will enhance your grasp of international standards, introducing a security risk framework tailored for legal and eDiscovery professionals, transitioning from a requirements-centric to a reference-based approach.

Case Study: Todd Engles- Construction Superintendent During the Day and Producer of Child Sexual Abuse Material (CSAM) at Night
This case study shares how a construction superintendent Todd Engles, who produced CSAM with multiple 9–12-year-old girls on multiple social media platforms to include Discord, TikTok and Instagram. The case study will begin with the NCMEC Cybertip and continue through the investigation and details of the communication with the victims and will end with sentencing information.

Chromebook Investigations: Unveiling Digital Artifacts and User Activity
This session offers a focused exploration into Chromebook forensics, navigating Chrome OS to unveil essential digital artifacts and user activities. Delving into the unique features of Chromebooks, including the file system and cloud integration, attendees will gain insights into key artifacts like photos, calls, browser history, and system logs. The session covers extracting evidence by scanning and imaging Chrome OS devices. This session will provide a concise yet comprehensive guide to Chromebook forensics, equipping attendees to efficiently uncover and interpret critical digital evidence in their investigations.

Cracking the Code: 5 Essential Secrets to Becoming a Cybersecurity Pro
This session provides a roadmap for cybersecurity professionals to become "Hacker Minded." Today, cyber career discussions are boxed into certifications and education. The presenter will share the "5 Essential Secrets" that transitions career development beyond both, provides transparency, and addresses technical approaches, security basics, and typical gaps associated with becoming a cybersecurity pro.

Creating and Leveraging GPTs for OSINT Investigations
This session will explore the revolutionary potential of Generative Pre-trained Transformers (GPTs) in Open-Source Intelligence (OSINT). Attendees will learn to harness Chat GPT for insightful OSINT investigations, enhancing data analysis and decision-making. Discover how to apply GPTs for in-depth investigative research and uncover hidden data patterns. Key takeaways include: 1) Strategic integration

of GPTs in OSINT workflows, 2) Advanced techniques for data extraction and analysis using Chat GPT, and 3) Customizing GPT models to meet specific investigative needs, ensuring tailored solutions for diverse investigative challenges.

Cryptocurrency Investigation: A Brave New World
Join us for an in-depth exploration of cryptocurrency and its impact on law enforcement investigations. Discover the hardware, software, and exchanges that underpin this digital currency, and gain insights into the tools and techniques used to trace transactions, identify assets, and preserve evidence. This session will equip attendees with the knowledge to effectively navigate the complexities of digital forensics and cybersecurity forensics investigations involving cryptocurrency.

Cyber Incident Response and Root Cause vs. Sufficient Cause vs. Likely Cause
When the event has been resolved & the threat has been mitigated the client, CISO, CEO & BoD will want to know root cause, a resource consuming and costly project. Investigation into sufficient or likely cause may reveal the root cause, but more importantly reveal vulnerabilities, gaps, APT and malware or exploits that could be leveraged to compromise the network and prevent them from being leveraged in the future. This session will identify the investigative processes & procedures to identify the cause of the cyber incident as well as other compromise assessments & considerations to thwart future compromise.

Cybertheft of Trade Secrets, and Legal Considerations during Data Breaches
Trade secrets make up majority of value of U.S. public companies' portfolios. Not surprisingly, such secrets are high value targets for domestic and foreign theft. Domestic economic damage attributed to Intellectual Property theft exceeds $600 billion annually. Attendees will be exposed to the legal world of trade secrets, some infamous trade secret theft cases, how they compare to other forms of intellectual property, discuss some important cases and federal laws, and learn some of what attorneys, as integral parts of the breach-investigative team, should ethically and strategically consider while responding to a data breach.

Data Sanitization and Validation
This session will teach attendees about sanitizing/wiping data storage devices, the standards that govern data sanitization, and tools that can be used to wipe data storage devices. The discussion will also cover methods for verifying that data has been removed properly.

Decode, Detect, Resolve: AI Applications in Digital Investigations
This session examines real-world applications of AI to expedite digital investigations. It explores machine learning, natural language processing and computer vision techniques that enable investigators to quickly analyze vast evidence, expose connections, and reduce bias.

In addition to addressing AI pitfalls around transparency and security, this session will provide attendees with insights into a range AI-powered processes for parsing keywords, flagging illegal content, reconstructing shredded documents and automating tedious tasks for accelerated case resolution.

DevOps for Red Team Initial Access Operations
This session describes some of the challenges of malware development for Red Team initial access operations, and how continuous integration/continuous development (CICD) pipelines can be employed to assist in solving the challenges. The session will start by introducing some of the known techniques employed by modern endpoint defense software, and then describe how a CICD approach can be used to enable unique malware artifact production for bypass and initial access operational success.

Digital Evidence related to Gangs and Prisons
As digital evidence becomes more prevalent throughout the world this trend also includes the prison system. This case study will follow the Tennessee Department of Correction's first major digital evidence investigation that encompasses the prison system, street gangs, Mexican cartels, drugs, self-mutilation, and homicide. The session will l cover the TDOC's focus on the newest criminal trend, digital evidence, the work with outside partners to bring closure to this investigation.

Domestic Hackers, SIM Swapping, and Cryptocurrency: A Case Study
This case study walks through an investigation beginning with a substantial cash out of Bitcoin and the investigation leading into the dark web of hackers and the uncovering of a prolific SIM swapper.
This session will cover the importance of tracing skills and identifying who controls which cryptocurrency addresses and will address mixers and token swapping. Agents and Analyst will discuss technical capabilities and what to do when you uncover systems utilized and how OSINT plays a substantial role in the case. An Assistant United States Attorney will discuss the judicial abilities and challenges faced with cases such as these.

Drone Above the Bay: A Case Study in Drone Forensics
This session focuses on the investigation and forensic analysis of a drone which was recovered from a criminal incident. Discussion will cover the capabilities of drones, unique forensic artifacts, the role of counter unmanned systems and the legal system.

eDiscovery & Investigations in Focus: A Panel on Privacy, Challenges, and Future Trends in a Modern World
This panel discussion will delve into pressing issues surrounding privacy concerns, as well as the collection and review hurdles confronting eDiscovery professionals across various industries. The conversation will explore real-world applications, policy implications, the role of artificial intelligence (AI), and the evolving landscape of eDiscovery litigation and investigations.

Effectively Navigating the eDiscovery Tools in Microsoft/Office 365 from Collection to Production
Many companies and organizations have rolled out Microsoft/Office 365 in their computing environments, but few have taken advantage of the search and investigatory tools built into Microsoft Purview. That's a shame because there is a lot that IT and legal departments can utilize to streamline the identification and collection of relevant data for investigations and litigation matters. This session will walk through the different levels of tools available and explain how each of them can be used effectively.

End-to-End Encrypted Messaging and Crypto: The New Even Darker Web
This session will share three developments not well known among cybercrime investigators. The session walks through the E2EE apps which are available to anyone with an Internet connection and a mobile

device. Each of the apps puts its own spin on the encryption method utilized. The result is that decryption becomes increasingly difficult for investigators who must find ways to reveal obfuscated information. Like the early days of the Dark Web, knowledge of the super apps and the tools needed to pry open their secrets is limited.

eSIM and Mobile Forensics, the Good, the Bad and the Ugly

This session will explore the impact of eSIM technology, how it has exploded in the world of IoT devices and how this has transitioned to be the solution of choice for smartphones and other mobile devices. This session will cover how to understand eSIM technology and briefly explore methods available to remotely provision this SIM service. It will also examine some of the security measures implemented with eSIMs and the potential problems they can introduce to mobile device forensics.

Extracting Actionable Intelligence from RSS Feeds

Global news sources provide a vast sea of data for investigators. This session explores a new approach that combines Python, Natural Language Processing (NLP), and ChatGPT, to transform the way we harvest RSS feeds for actionable insights.

RSS feeds have long been a valuable source of information, providing updates from a multitude of websites and blogs. However, the sheer volume of data and the varying formats have made manual analysis impractical. This session discloses an approach that combines Python, NLP, and ChatGPT to automate intelligence extraction. All attendees will receive the source code demonstrated during this session.

Forensic Analysis of Docker and Containerized Systems

Containerized systems are becoming widely used throughout the tech industry and is changing how we use virtualized systems. This session will introduce the concept of containerized systems and how they work, then conduct a deep dive into the forensic analysis of these systems and the type of data that can be revealed. The session will also cover how containers and container management applications like Docker can be used as a forensic tool in the lab.

From Theory to Practice: Enhancing DFIR Skills through Threat Simulation Scenarios

Threat simulations involving malware and C2 frameworks are crucial in Cybersecurity training and readiness. They provide a realistic environment for Cybersecurity professionals to understand and counteract cyber threats. By replicating the TTPs of real threat actors, these exercises offer invaluable hands-on experience in identifying, mitigating, and responding to cyber incidents. Threat simulations allow professionals to experience the nuances of APTs and learn how to detect them effectively. This session will focus on emerging threats like malware and C2 frameworks to help professionals effectively combat cyber threats.

How Artificial Intelligence Will Change the Future of Investigations

During this session, the presenter will discuss the current and future role artificial intelligence plays in augmenting both traditional and digital investigations. The session will speak about how artificial intelligence can be combined with automation and case management to transform investigations.

How to Identify and Mitigate Hacker Obfuscation Techniques

Discover three of the key obfuscation techniques attackers use to break down defenses and exploit systems through undetectable means, including impersonation, trusted site, and human ingenuity techniques. During this session, the presenter will share a bird's eye view of how attackers are trying to bypass controls to gain access to large websites across several industries. At the end of the session, attendees will understand the various approaches toward trusted site obfuscation and find out why you understand attacker techniques to know which security controls will protect your data without effecting user experiences or business practices.

How to Talk About Cyber Security Risk to Senior Leaders without Tech Mumbo Jumbo

This interactive session will present three distinct views from cyber security veterans including real life scenarios each of us has experienced talking about cyber risk with senior leaders. In 2024 we will see corporate boards needing clearer roles and responsibilities around ensuring adequate controls around cybersecurity.

iOS Live: Working with Live Data from iOS

Important device information can be identified through the monitoring of raw data sent via USB protocol. iOS devices present sensitive information in the back end even when this information is not seen by iTunes and third-party software. This session will demonstrate a freeware toolkit that both gathers and parses live data from iOS devices.

Leveraging eDiscovery with Forensics to Put out the Fires of Internal Investigations

A panel of industry practitioners will discuss the role of eDiscovery and Forensics within internal investigations. The panel will explore workflows, tools, processes, best practices, and other related topics. Attendees will walk away with an understanding of when, how, and why internal investigations take place along with who is involved and what tools can be used. Participants will also gain insight into how to mitigate risks that ultimately result in an investigation. Finally, attendees will learn practical ways eDiscovery processes and forensic analysis work together to create efficient and accurate outcomes.

Leveraging GenAI to Enhance DFIR Capabilities

GenAI is here, but are we ready to embrace what has become increasingly accessible to both defensive teams and malicious actors? This session will cover how to find success in implementing GenAI in DFIR, tools and techniques that can help us implement it, valuable insights to enhance its execution – but most importantly, what is needed to address before we can get buy in from our organization to support its use. Attendees will gain perspective on how you can leverage this technology for DFIR and learn how to address the likely organizational barriers to adoption.

Linkage Investigations: Cryptocurrency, Dark Web & OSINT

With the development of the internet came a new tool for criminals to conduct illegal activity. With the emergence of the dark web and cryptocurrency, criminals gained anonymity for their illicit transactions, making it more challenging for law enforcement agencies to detect them. However, there are OSINT tools that collect, analyze, and disseminate publicly available and legally accessible information assisting in uncovering identities and building cases. A review of the use of cyber technology, looking at cryptocurrency, surface and dark web data, and OSINT (open-source intelligence) will be discussed.

Litigating Generative AI: What Issues Should Be Expected?
Generative artificial intelligence is a new technology that has seen phenomenal growth since late 2022. GAI platforms have proliferated even as uses have multiplied in private and public sectors. Development of databases as what may be generated -- carry benefits and risks that have led to laws and regulations as well as investigations and litigation. Discovery and admissibility of GAI may be problematic as well its impact on access to justice. This session will show attendees how to: Examine the nature of GAI and its uses and abuses; Understand actions that might arise; and Prepare for discovery and admissibility

Locating Criminal Suspects by Tracking NFTs
A detailed and step-by-step account of how a team of investigators was able to locate a criminal suspect by using blockchain forensic tools, metadata from NFTs, and traditional OSINT methods. Combined and utilized, the identity of an anonymous suspect slowly came to light. With these efforts, law enforcement was able to connect the dots to a larger and more sophisticated operation involving traditional fiat.

macOS Advanced File System Artifacts
This session is designed to shed light on the critical yet often overlooked aspects of macOS forensic analysis. The session will explore a variety of advanced artifacts, including File System Events (FSEvents), Local Time Machine Snapshots, Quarantine Events, Apple Extended Attributes, and Find My Artifacts, among others. The focus will be on the practical application of these artifacts in forensic investigations. Attend this talk to master the intricacies of macOS forensic artifacts, elevating your investigative skills with cutting-edge techniques and knowledge.

Maturing from Legacy Vulnerability Management to Modern Exposure Management
Vulnerability management solutions just don't secure an enterprise from the attacks that are occurring daily against organizations of every size. Attackers are using various tactics to expose and exploit assets and the myriad of security issues that each one possesses. However, Continuous Threat Exposure Management (CTEM) is the modern and improved approach to defending against attackers and their tactics. This session will decrypt why vulnerability management is no longer enough, while building up the different pillars around CTEM. Attendees will see what a solid CTEM solution looks like to secure your enterprise.

Meeting the New SEC Cybersecurity Requirements: A Case Study
The SEC issued new Cybersecurity requirements that went into effect December 2023. Will your Incident Response program pass muster? This session will take a deep dive into the SEC's new cybersecurity disclosure requirements, what this means for your organization, what others are encountering, and how to make sure you meet these important requirements.

Microsoft 365 Data Extraction
This session provides a practical walkthrough of extracting employee data from Microsoft 365 using an admin account. Attendees will understand how to identify and export data, investigate user logs, and comprehend the dynamics of data deletion and default retention settings in Microsoft 365.

Mobile Analysis Methodology and 3rd Party App Analysis

Hands-on Workshop (Pre-registration is required, seats are limited. Included with paid registration)

This hands-on workshop teaches a methodology for mobile forensic analysis of unsupported applications and artifacts. The workshop will share a 5-part methodology; Discover, Test, Parse, Find, and Script, which are necessary skills to parse 3rd party applications.

Myth-Busting: eDiscovery Costs and Complexities

In this session, audience members will learn the truth behind common misconceptions about the eDiscovery process. Myths such as "its complicated," "it's expensive," or "manual document review is the gold standard" are debunked by experts, who will walk through key eDiscovery concepts, pitfalls, and best practices to put audience members in control of a critical phase of the litigation process.

Navigating the Certification Labyrinth: AI-Enhanced Strategies for CISA, CISM, CISSP and CCSP Success

In this session, attendees will explore key certifications: CISA, CISM, CISSP, and CCSP, pivotal for career advancement. The journey to certification, enriched by AI-enhanced tools, will be demonstrated. Attendees will learn effective preparation strategies, experience free AI tools for tailored learning, and understand the value of community in this journey.

Navigating the Cloud: Trends in Innovation, Multi-cloud, and Kubernetes

Many modern businesses rely on a cloud environment (if not multiple) to store and host valuable employees, customers, and proprietary data. But cloud security is constantly evolving, emphasizing the need for orgs to fully understand the potential impact of their cloud security strategies on their overall business success. Attendees will come away with an understanding of the trends and challenges decision makers are facing now, what the landscape could look like in the future if these emerging trends continue, and actionable takeaways to drive security-enabled success for their own businesses.

Navigating the Shadows: Linux Tails Examinations for the Digital Forensic Examiner

Digital forensics professionals are increasingly encountering privacy-focused tools like Linux Tails, which present unique challenges when conducting investigations. This session will guide attendees through the intricacies of Linux Tails examinations. By the end of this session, attendees will be better equipped to tackle Linux Tails examinations with confidence, enabling you to uncover critical evidence."

Peeling the Onion – Additional Layers of Device Security

Filesystem or full disk encryption on Android and iOS devices is an accepted and well understood norm nowadays. However, there are almost invariably additional layers of security on these devices now, that may mean important data is not extracted or remains encrypted, even with a 'decrypted' full filesystem or physical extraction. This session will explore what they are, where they exist, how they work, and some of the ways they can be overcome.

Pixelated Laundering: Exploring the Nexus of Closed Virtual Assets, Video Game Economics, and Cybercrime

This session explores the confluence of virtual economies, cybercrime, and money laundering within video gaming. It aims to understand the dynamics of closed virtual currencies and in-game economics. The research will investigate the susceptibility of gaming platforms to cybercrime, especially regarding

the grooming of under-aged users. A detailed study of money laundering practices using games as conduits will be presented. The session proposes proactive strategies for prevention and law enforcement and evaluates potential future scenarios as digital economies evolve.

Preparing for Trial: What to Expect as a Forensic Examiner when the Prosecution Calls You to the Witness Stand

Almost all serious crimes nowadays contain a digital footprint, and the effective session of this digital evidence to juries is essential for successful prosecutions. In this session attendees will learn what to expect when subpoenaed to testify in a criminal case. Topics include working with prosecutors to prepare for direct testimony, creating court exhibits from your work product, what to expect during cross-examination and more.

Prove It! The Future of Synthetic Media (AI) Detection in Justice and Public Safety

Tom Cruise performing magic tricks on TikTok, foreign leaders declaring acts of war…the prevalence of high-quality synthetic media online has brought a new age of disinformation and distrust to society. How does this relate to evidence admissibility in criminal investigations and legal proceedings? What is the true threat to public safety?

This session will address the real concerns with synthetic media as it pertains to law enforcement and forensic examiners who have to authenticate evidence for court. Reliable, explainable, and repeatable techniques for the examination and authentication of video evidence will be introduced.

Publicly Available System Hardening Tools Discussion and Demonstration

NIST, DoD, NSA, DHS CISA, and other organizations have publicly available tools to help all types of organizations harden their systems. This session will explore how these tools can help you do your job. Join this session for a review, discussion, and demonstration of some publicly available resources for assisting system administrators in performing their cybersecurity job.

Python - A Crash Course for DFE's

Hands-on Workshop (Pre-registration is required, seats are limited. Included with paid registration)

Does this sound familiar? “I’m a digital forensics examiner (DFE), and I know that I need some scripting skills, but I don’t want to be a full-time programmer.” If so, this workshop is for you.

Python has become the scripting language de jure for digital forensics for many reasons: It runs on all platforms although it is not native to Windows; Python code is readily available on the Internet on sites like Stack Overflow and GitHub; and Last, but not least, the wealth of modules available make what would be complicated programing in other languages covering hundreds of lines of code a short exercise.

This is a crash course in Python programming. Students should have a solid understanding of the command line in the Windows environment, but programming expertise per se is welcome but not needed. We will be looking at Python from a digital forensics’ perspective. The class is completely hands-on. Students will need to bring their own laptops and download the community version of PyCharm.

Restoring Trust in Multimedia Evidence: A Framework for Content Authentication of Image and Video Evidence

Video and image evidence is vital to all aspects of investigations as well as security. Trusting evidence that is submitted has increasingly been challenged, particularly related to "deepfake" video. A recent identity fraud report reveals that there has been a more than 1500% increase in deepfakes reported cases. This session will discuss the current state of video manipulation, as well as propose a workflow to authenticate video or image evidence. This workflow will discuss techniques related to metadata, file structure, and content authentication.

Revolutionizing Crime Scene Collection: Embracing the Digital DNA

In the digital age, crime scenes are rich with untapped information—digital footprints left by Wi-Fi, Bluetooth, & cellular devices. This session will explore the critical evolution of crime scene collection. This session delves into the indispensable role of digital footprints as the DNA of contemporary crime scenes, providing a deep dive into extraction, interpretation & application methods.

Safeguarding Controlled Unclassified Information (CUI)

This session examines the current state of the computer security requirements that have been imposed on defense contractors to protect Controlled Unclassified Information. In the process it examines what constitutes a cyber incident, a contractor's duties for forensically analyzing and reporting a cyber incident, and finally, it examines the flaws that will keep the rules from preserving the defense industrial base and really protecting America's secrets from cyber theft, particularly by nation states employing Advanced Persistent Threats

Same Data, Different Story: Law Enforcement vs Independent Experts

The public-private sector relationship can be a veritable minefield of relational issues. Law enforcement examiners can often find themselves at odds with policy, procedure, supervisors and/or prosecuting attorneys, which can lead to miscommunication and delays. This session will explore the issues from both perspectives in a practical manner and discuss approaches that government/LE examiners can undertake for optimal success when dealing with opposing experts and shed light on what opposing experts are seeking from these interactions while working a case.

Security is as Security Does. Law Enforcement's Great Migration to Operating Securely in the Cloud

The Cloud has been thought of as a frontier which only the bold few Law Enforcement agencies have entered. Cloud services have arrived and understanding their implementation within your digital investigative workflow is the key to scaling available resources, churning through case backlogs, and providing skilled examiners an opportunity to do what they do best. For law enforcement, migrating to the Cloud is no longer a question of if, but when. This panel, comprised of local, state, and federal legal and law enforcement experts will examine law enforcement use of cloud-hosted service offerings.

That's How We've Always Done Things: An Enterprise Investigations Team Breaking Away Story

You've been hired to build a team from the ground up, now what? In this session, you will be presented with the scenarios and questions inherent in developing an Enterprise forensics and eDiscovery team. The presenter will share his 'breaking away' story from a large conglomerate to a new, separate corporate entity. Topics to be covered include: Where do I hire to have global coverage? What tools and technology do I implement that are legally defensible and capable? What previous investigative efforts can I do differently as a newly formed team? Please bring your questions to this interactive session.

The Evidence Isn't Speaking to You: Investigating a Digitally Diligent Subject
As examiners, we learn to listen to the who, what, where, when, and must understand the why. What happens when the evidence is silent? What happens when the storyline doesn't make sense? What if the absence of data helps you as an examiner? Will it be hard work? Yes! Will you grow as an examiner? Yes! Sometime the "dark periods" in the digital timeline are the evidence. We often hunt for the thread that can unravel the truth. This session will share how to think differently and take a deeper look on why the evidence can't speak for itself.

The Future of Law: Integrating AI, Digital Forensics, and eDiscovery into Tomorrow's Legal Practice
The legal sector is on the cusp of a technological revolution, propelled by AI, digital forensics, and eDiscovery. This session explores their integration in legal practice, focusing on AI's impact on research, digital forensics' role in litigation, and eDiscovery's relevance in data management. It addresses ethical challenges, future skill needs, and the transformative potential of these technologies in law. The aim is to motivate legal professionals to embrace these changes for a redefined legal future.

The Trouble with Torrents: Criminal Defense Issues in Digital Forensics
Digital forensic evidence can convict the guilty or exonerate the innocent. Justice requires transparency in pretrial discovery & scrupulous ethics by all investigators. During this session, attendees will learn how to educate typically untrained lawyers & judges about the methods & underpinnings of the evidence & search tools employed. Attendees will be encouraged to prepare reports which fairly present the results of their examination, including possible limitations on their conclusions, how to assist the lawyers with pretrial discovery & how to confront possible ethical dilemmas they may encounter.

The Urgency of Modern Wi-Fi Security
In the world of network security, the latest Wi-Fi security standard is a "Breaking Bad"" level of intense. Not to be overly dramatic, but 99% of your business networks are using technology that's been hacked for over a decade. This is a hilariously technical treatise on why and how to upgrade to WPA3 security.

Transitioning from Public to Private Sector - All Your Questions Answered
Are you thinking about moving from the public sector into the private sector? Join this panel of industry-leading experts who have successfully made the move. Learn from their experiences and get your questions answered. This is a must for anyone considering the move.

Triage to Control Backlog - Targeting Devices with Evidentiary Value
This session will discuss the vital topic of backlog reduction and how digital forensic triage can improve ICAC/CSAM investigations. Attendees will learn: How to reduce the seizure of unnecessary devices

through new approaches to traditional problems; The tools, technologies, and techniques used to identify CSAM quickly, while also ruling out non-suspect devices; and How to more effectively determine probable cause on scene to facilitate arrests sooner. The presenter will share how all of this can improve case turnover times and reduce: time-on-scene/costs/backlogs, whilst also improving officer wellbeing.

Unleashing the Potential of Reddit and Discord OSINT: Tips and Tricks for Successful Investigation
Despite being overshadowed by social media giants, Reddit and Discord are underrated gems in the realm of OSINT. Reddit stands out for its vast assortment of third-party tools that grant access to previously deleted content. Meanwhile, Discord, has expanded beyond the gaming audience that fueled its initial growth. With millions of daily active users, these platforms provide valuable information for effective OSINT gathering.

In this session, we will explore tips and tricks for Discord and Reddit OSINT, including overviews on: Finding communities of interest; Finding details about users; and Navigating Reddit subreddits or Discord servers' communities.

Unlocking Digital Clues: Enhancing Investigations through Social Media Intelligence
As an investigator, you're constantly searching for ways to close cases faster. One of the most effective ways to do so is by implementing social media data from multiple sources, but how? This session will explain the importance of requesting data from multiple social media companies, show methods for acquiring and processing large returns, and share successes from agencies who've done it.

Unmasking Clouds: The Art of Cloud Forensics
Cloud forensics involves analyzing and collecting digital evidence from various cloud-related sources. This session will discuss how whether data is hosted and offered through the cloud, generated, and stored by cloud applications or by services provided by cloud platforms, you should have the capability to leverage all areas to perform cloud forensics effectively and investigate potential criminal activities or security incidents.

Unveiling the Hidden: Navigating the Maze of AI Artifacts in Windows Forensics
This session focuses on the challenges of finding AI traces in Windows systems from a digital forensics point of view. The presenter will share how AI works with the operating system and the tough job of detecting AI-generated data from normal user-generated data. The session will focus on what this means for legal and DFIR professionals, emphasizing the need for better tools and methods to spot and understand AI's impact in investigations.

Use Cases Using Operating Systems Artifacts and Metadata
The session demonstrates real use cases in Brazilian investigations solved using operating system artifacts, metadata, and data collection from open sources. This educational session will delve into practical applications of operating system artifacts, metadata analysis, and OSINT in the context of solving real investigations in Brazil. Attendees will gain insights into the methodologies employed, evidence discovered, and the formulation of crime typologies.

Vehicle Forensics- Looking Under the Hood

Updated with more video and resources. This session will walk through a case study that used vehicle data to assist in an investigation. In this case, the subject rented a 2016 Lincoln Navigator which had a Sync Gen-3 infotainment module. The data from the module corroborated the investigators findings. The data showed all the connected devices, locations, events, and track logs of the vehicle which assisted in the investigation. The data led to further leads for the investigators on where the vehicle was repaired after the shooting. Ultimately, the investigators were able to gather more information on the subjects which assisted in the investigation.

Who's at Your Table? Why Performing Tabletop Exercises can Prevent Disasters

This session will cover the importance of testing response plans and procedures through performing tabletop exercises focusing specifically on insider threats. The presenter will discuss *the proper preparation and planning to ensure a productive tabletop, including how to get buy-in and attendance from critical departments. With a Forensic focus, this session will provide tips on how to make a tabletop successful and how to implement key takeaways.