Techno Security & Digital Forensics Conference

OCTOBER 10-12, 2022 | SAN DIEGO, CA USA

SNEAK PEEK of CONFIRMED SESSIONS

(As of June 29, 2022– All sessions and full details including times, dates, and speaker bios will be available at the end of July)

[Air]Tag You're It

With Apple's joining of the Bluetooth tracker market with the AirTag, their worldwide device network means that it's easier than ever to track our items. However, what happens when someone slips an AirTag into an unsuspecting user's bag? How can you find not only unauthorized devices, but also find out how long they've been close? In addition to tracking AirTags, Apple's FindMy service opens the potential to additional digital evidence. This session will explore artifacts relating to both AirTag tracking and the FindMy services.

Actively Engaging the Business in Security Initiatives

A challenge for Security professionals is getting management "on board" with security initiatives. Business managers and executives are hired for business expertise, not security expertise. However, with the assistance of security and audit professionals, they can participate in implementing security controls. This session will present real-life examples of how businesses can work with security and audit to help the business implement and document security controls. Attendees will walk away from this session empowered with real-life tools to make security an easier and more transparent process for their business.

Artificial Intelligence: Use Cases, Discovery & Admissibility

Artificial intelligence (AI), however we define it, has arrived in civil and criminal litigation. AI can be used for various purposes, including proof of claims or defenses. AI can also be the subject of litigation. This session will examine the nature of AI, how it might be relevant, how discovery of AI might be conducted, and whether the fruits of AI can be admitted into evidence.

Breaches Are Everywhere. What's a Good Security Leader to Do?
Breaches are on the news seemingly weekly, as organizations are struggling to secure their data. Phishing attacks are proliferating & compromising our workforce. Ransomware has taken several victims and payment demands are escalating. All organizations have become prime targets. This session will share strategies to combat the rise of cybercrime, and how to make your networks more secure.

Building a Pattern of Life. Leveraging Location and Health Data
Location data is crucial in most investigations. However, while it's important to understand where someone was, it is potentially more important to understand what they were doing at the location in that exact moment. This session will be a deep dive into physical movement as it correlates to health and locations.

Cameras, CACs & Clocks: Enterprise IoT Security Sucks - A Story of Two Million Interrogated Devices
During this session the speaker will share how across two million IOT devices he identified threats and trends, compiled statistics, summarized compelling cases, and evaluated common offenders. This session will share tactics that organizations can employ to recognize value from their IoT devices while minimizing risk and ensuring that devices that are secure today will stay secure tomorrow.

Conducting Forensic Investigations in a Zero-Trust Environment
Corporations are faced every day by insider and outsider threats and the Zero-Trust security approach is quickly becoming the standard for both corporations and federal agencies. While Zero Trust Network Access solutions are helping these corporations and agencies enhance control over their security infrastructure, it poses some challenges to internal DFIR and security teams This session will discuss: Best Practices for completing forensic investigations in a Zero-Trust environment and how Zero-Trust may impact the legitimate forensic work being carried out by agencies and organizations.

Conducting Investigations on Social Media: Collection and Review of Social Media Data at Scale
Drawing from high-profile examples in the private and public sectors, this session will examine how investigators can streamline social media investigations. It will discuss how they can work with social media evidence at scale and offer practical tips and strategies for transforming live social posts into evidentiary-quality records.

Cyber Warfare 2022 and Next Level $#@! You Need to Know for Today's Cyber Battleground
During this session, attendees will learn how Nation States, Non-Nation State Actors, Hacktivists, enterprise cyber criminals, shadow government agencies, terrorist organizations, loosely affiliated groups are using this next level $#@! as we speak to conduct cyber warfare to manipulate and influence public opinion, foment criminal violence; infiltrate organizations to conduct fraud, scam, and harass; and highjack legitimate real human accounts for impersonation, and to distribute malware.

Dark Web Fundamentals and Investigation Techniques
This session will explore the different Darknets commonly used for criminal activity and how data is transferred across these networks. The presenter will describe how these networks are accessed and actions criminals use to ensure anonymous usage for their activity. The session will also discuss how the clear web can reveal clues to a user's activity on the Dark Web and explore traces of artifacts found on a host system.

Digital Evidence from Social Networking Sites & Smartphone Apps
According to Statista.com in 2020, the global social penetration rate reached 49 percent. Many technology thought leaders believe social networking will displace traditional email as the leading communication medium. This session will provide a practical walkthrough of preservation of top social media sites and how to effectively utilize tools for evidentiary collection across the Web, PCs/desktops and smart devices. The session will look at social media apps on smartphones and what digital evidence exists compared to what can be found on the cloud., as well as explore innovations in emoji/avatar Apps such as Bitmoji.

Digital Forensics and E-Discovery: How use your Forensics Expertise to Get Food at E-Discovery
Digital forensic examiners often dive deep into the evidence to find all the details necessary to prove or disprove a theory. They are often asked to support E-Discovery cases but either do not want to get involved with that type of work or provide too much information to attorneys. This session is designed to overcome these two obstacles. Attendees of this presentation will learn: Where Forensics and E-Discovery processes cross paths; Why Forensics expertise is so valuable in the E-Discovery process; and How to tailor their Forensics processes so they can add value to any E-Discovery case

Encrypted Messenger Forensics (Signal, Wickr, Telegram, & More): on Mobile and Computer Platform
Digital forensic investigators generally struggle with the extraction of evidence from mobile devices when it comes to encrypted, third-party applications such as Signal, Wickr, and Telegram. These applications are meant to be tough to crack, with their end-to-end encryption and inability to recover from a mobile device backup or computer acquisition. This session will

cover the decryption of these applications for proper acquisition and analysis as well as how to report our findings."

Everything You Need to Know About Imaging Apple Silicon Macs

Every forensic examination starts with getting the right image. In the Mac Forensics world, understanding what to image and how to properly acquire an image has never been more complicated. For the time being, new startup securities have placed restrictions on creating boot environments. In addition, the removal of Target Disk Mode has changed the way we look at acquiring a Mac. Join the presenter to learn all you need to know about imaging Apple Silicon Macs.

Get Live & Historical Data from Twitter for FREE!

Collecting data across social media platforms can be complicated and expensive. Well, it doesn't have to be! You will get free ways to pull data from Twitter. Not just random tweets, but refined searches that include geo-data, images, videos, friends associations, and more! You will learn the easy way and a more advanced way to pull data directly from Twitter's own API or a free desktop application. Want to watch a location for any tweets containing threats or that might contain evidence? This session will show you how... Did I say FREE? Yup!

Hacking the Supply Chain

Every company in the world has been negatively impacted one way or another by a cyber security breach that has occurred within their supply chain. Organizations have started spending more time and resources on Cyber Security which has forced the criminals to adjust their game plan. Criminals have figured out it’s easier to exploit a single supplier which results in hundreds of companies being attacked in a supply chain than it is to attack one large organization. During this session attendees can expect to learn: How to build redundancy into your supply chain; How to identify and remediate weaknesses within your supply chain; and the Important benefits of cyber insurance.

How to Leverage Best Practices and Automation to Put Victims First in Examinations of Child Sexual Abuse Material

This session will help you improve your workflow in today’s demanding child sexual abuse investigations. Caseloads of indecent images of children keep soaring; hence, investigators often lose sight of victims, and focus instead on grading images or videos, to secure a conviction. This session will discuss new thinking and solutions; enabling you to rebalance priorities and quickly uncover victims.

Internet Browser Artifacts
This session will l examine the most common browser artifacts that can be examined to support an investigation. History, Cookies, Cache files and other stored items, such as personal user information and recovered passwords, will be discussed from the most popular internet browsers such as MS Edge, Google Chrome and Firefox.

Interoperability for Facial Recognition and Person-Centric OSINT for Intelligent Investigations
Law enforcement information systems are rapidly developing, but investigators face challenges solving crimes and revealing victims' and suspects' identities. Some of the reasons are the systems are implemented in silos and contain sensitive data & strict data ownership rules. Furthermore, when the investigators use methods of OSINT "Open Source Intelligence" to investigate terrorism & serious crime, it is very difficult to match the identity-related data and facial images of the suspects stored in the Law Enforcement systems with the data from open sources. This session will share methods and mechanisms for achieving intelligent investigations.

Investigating Docker - The New Virtual Machine
Docker is the latest in virtual machine technology and is being implemented worldwide by millions of companies to run various parts of their infrastructure. Docker is an OS-level virtualization platform that allows the deployment of services within "containers". Typically, each Docker container runs as an isolated Linux system and can function as literally anything including web servers, databases, Python services, or full app platforms like an ELK stack. This session will provide insight to Docker and its use cases, and dive into collection and analysis techniques to be aware of.

Pay Up or Else: Critical Knowledge Necessary to Respond to a Ransomware Detonation
Ransomware attacks haven’t subsided despite efforts to shutdown major operational organizations. Defending against them in case an attack gets through your defenses require preparation – both technical and operationally. This session will provide critical first steps and understanding of things to do and things not to do based on lessons learned in the field.

Post-Quantum Computing Cryptography Is Now Real - What Is It and How Does It Affect Us
Quantum Computing (QC) is not yet a reality, but advanced preparation is imperative to properly protect sensitive information because the world's Cryptography standards are challenged by QC. While post-quantum crypto standards are still being developed, some are taking the first steps now. Microsoft has a post-quantum crypto project ongoing, and OpenSSH 9.0, release April 2022, includes the NTRU Prime key exchange algorithm, believed to be safe against QC threats. What do these post-quantum computer cryptography developments mean

for information security? During this session, our presenter will discuss these developments and learn what it means to all of us.

Where Should I start with the NIST Cyber Security Framework and the NIST Privacy Framework?

There are a number of frameworks available to base your organizations' cybersecurity and privacy programs on but the latest of these has been provided to us by the US Government. Attendees will learn: Why is it important to use a framework?; Which of the different levels of NIST 800-53 should I map to NIST CSF?; and Where should to begin a cybersecurity and privacy program for the organization?

Rogue Warrior: The Privatization of Cyber War and the Erosion of Government Control

Our world has entered into a new era where a large army of rogue cyber warriors have turned their skills sets and tools at Russia and its allies. This new era has exposed failures and shortcomings of bloated governments to respond rapidly enough to a 21st Century battle ground. New issues are exposed as individuals wage war and governments debate policy. This session will detail the privatization of cyberwar, review case studies, and explore the future of cyberwar.

Strengthening Phishing Awareness Training Using NIST Phish Scale

Phishing is a common technique that is used by adversaries to gain access to information and cause loss to the organization. Phishing has evolved and new tactics are emerging including replicating websites, and cloud provider notifications asking for credentials. This session will discuss: Do lower click rates for simulated phishing emails reflect an effective security awareness training program?; How can you use the NIST phish scale to tailor your training program?; and How to benchmark your organization's users' ability to identify difficult to easy phishing emails.

The Evolving Role of Emojis in eDiscovery

We are all familiar with emojis. They are present in emails, text messages, social media, and virtually every online modality. According to emojipedia.com, over one in five tweets includes an emoji (21.54%) and five billion emojis/day on Facebook Messenger. This session will discuss: Do emojis provide probative value during eDiscovery?; Can we translate these quirky images into meaningful text equivalents?; Can we track, correlate, connect suspects or accomplices through their use of emojis?" and more.

Walk through of a Business Email Compromise Investigation
This session will walk the participants through business email investigations and give attendees a high-level understanding of how to work this type of investigation.

What to Expect When You Are Expecting (to testify)
Most examiners, no matter how skilled, dread testifying. Nonetheless, it is a necessary evil and the final work product for many cases. This session will cover how to properly prepare for and execute testimony, from examination to reporting to being on the stand or in the deposition. This session will share how to prepare a report that will withstand later attack, preparing for testimony, how to be an effective listener when being examined, recognizing strategies to lead you astray in court and being an effective communicator while testifying.

When the Phone is All You Have
Pick the scenario … you have to prove or disprove something, and your proof is locked away in a phone. The phone is encrypted and locked when you power it on. What to do? Try an exploit? Brute force the lock? Gather good intel about the owner. Maybe create a custom dictionary attack profile with which to attack that lock? This session will share how to leverage multiple technologies and attack vectors against locked devices.

When You Need to Get it Right: Understanding Video Playback, Interpolation, and Timing Data
As recent cases have shown, video evidence is becoming more prevalent. As such, understanding what is happening, the timing of events, and even the speed of a vehicle have increasingly relied upon video evidence. This session will discuss some common issues every examiner needs to understand and how to find that information within a file. Special emphasis will be on file creation, decoding and playback issues, video and frame timing, and their relationship to speed.

Why Threats to Critical Infrastructure, like the Industroyer2 Attack on the Ukraine Power Grid, are Creating a Cyber Deterrent
When Russia attacked Ukraine, it started a series of alerts from government agencies warning of the possibility for devastating cyberattacks. When aimed at critical infrastructure these attacks have the potential to cause uncertainty and chaos, as witnessed when Colonial Pipeline suffered a ransomware attack. Hear from the company that discovered Industroyer2 malware targeting Ukraine's energy sector and delve into past and present cyberattacks against critical infrastructure. In an age where all sides possess the ability to launch a cyberattack of untold potential, join the presenter in a discussion on the potential of a 'cyber-deterrent'.

Windows 11 Updates: What's New in Windows OS Forensics

With the release of Windows 11 examiners are bracing themselves for the analysis new artifacts within the Operating System and possible file system changes which have not yet been encountered on previous versions of Windows systems. This session will provide the audience an overview of what is new, old, and depreciated on the latest version of Windows 11. In addition, this session will examine local artifacts vs. online data and the challenges of log file analysis. Further discussion will focus on Microsoft's virtualized apps in Windows 11.