Techno Security & Digital Forensics Conference

September 30 – October 2, 2019 | San Antonio, TX USA

SNEAK PEEK of CONFIRMED SESSIONS

(As of June 10, 2019 – All sessions and full details including times, dates, and speaker bios will be available in early July)

A Synergistic Approach to Information Security and Technology Audit

The disciplines of Information Security and IT Audit are quite different and require different skill sets. However, they have many common goals and objectives. This session will explore what these disciplines have in common, and attendees will learn how practitioners of each discipline can jointly leverage the other's unique skill sets and techniques. Real-world examples of success will be presented, and attendees will explore how they can utilize the unique skill sets and techniques of each discipline. Attendees will leave with an understanding of how, together, Information Security and IT Audit professionals can better achieve their common goals and objectives.

APFS Imaging Considerations for Forensic Examiners

This session will address Apple File System (APFS) unique characteristics, forensic imaging methods of APFS Macs, and items of consideration for APFS analysis on different forensic platforms.

Attorneys, Cybersecurity, and Technology: Perfect Together?

This session will examine new technologies such as autonomous vehicles and the challenges that these technologies will pose for attorneys and investigators, cybersecurity issues for business and government entities arising out of new technologies, and ethical issues for attorneys arising out of new technologies.

Blockchain and eDiscovery: The Legal Impact of Blockchain Technology

With the increasing usage of cryptocurrencies and blockchains in today's world, eDiscovery professionals need to understand how these emerging technologies should be considered and investigated as part of data discovery and legal discovery processes. This session will highlight both cryptocurrencies and blockchains and provide attendees with fundamental information that will help attendees understand how to examine and investigate these technologies and the electronically stored information that results from their usage.

Breaking into Your Building: A Hacker's Guide to Unauthorized Access

This session will discuss proven methods of bypassing popular physical security controls and employees, using only publicly available tools and social engineering. You'll hear war stories from assessments that we have performed, and the frightening simplicity of gaining unauthorized physical access to many things from server rooms to Top Secret Ops rooms. These assessments will be broken down to discuss the various social engineering and physical security bypass methods and tools used, as well as remediation recommendations.

Bringing Data Analytics into Your Investigations

In this day and age, no matter where an individual goes, new raw data is being created and collected. A cell phone can be tracked through its Wi-Fi connection as one walks through the mall to alert stores of their shopping patterns. When using a badge to enter a secured building, a transaction is recorded as to the time and location an individual entered. From accounting and fulfillment systems to web logs and access monitors, the use of databases have become pervasive throughout corporations and our everyday life. In this session, the presenter will explore the complexities surrounding the collection and analysis of "Big Data" and how it applies to corporate investigations and litigation.

CCleaner© – Is This Tool the End of Forensic Investigations As We Know it?

The CCleaner website targets users wanting to "Speed up and Optimize" their PCs. CCleaner can delete internet history, cookies, caches, and temporary files. Among the destruction of Internet artifacts, it also can delete valuable forensic artifacts which are commonly used in digital investigations. CCleaner is able to delete Windows event logs, registry files, old prefetch data, shell items, and custom files and folders. Starting to be more commonly seen in cases for the purpose of data destruction, the use of CCleaner can have quite an impact on a forensic investigation. This session will help you determine if CCleaner was executed on a computer and what data you will see once these important artifacts have been deleted.

Concept Searching: Reveal Possible Issues and Risks that Keywords Miss

Data volumes are exploding as are potential data sources requiring analysis for investigations. Wading through such volumes can take time that corporations don't have and have unnecessarily high costs. For corporate compliance and governance officers, growing data volumes creates a pressing need for methods, technologies and processes which can be used to quickly analyze massive amounts of communications and information. Keyword searches can be very useful when you know exactly what it is that you are looking for, but no one calls a bribe a bribe. Shifting our approach toward analytics allows us to describe the ideas and activities at issue within a collection of exemplar paragraphs, and then let the analytics engine find and report the correlations and connections. Organizations facing investigations, or simply developing compliance assurance protocols, can include analytics in their initiatives to prioritize collection efforts, proactively audit corporate document populations, and identify priorities in the areas of training, monitoring and policy development. In this session, the presenter will discuss the foundations of analytics, and explore exciting new developments in workflows, methods, and applications - all of which can be leveraged in compliance initiatives and investigations of all kinds.

Crawl, Monitor, Walk, Detect, Run like Heck- Stages of Building and Executing a Threat Hunting Program

This session will highlight important strategies, tools, techniques and planning to consider for your hunting engagements. The presenters will highlight realities of the relationship between incident response, cyber threat intelligence and threat hunting, as well as provide real world examples of identifying attacker methodologies. As organizations are forced to combat threats in numerous vectors, it has forced defenders to rethink their tactics. Technology such as firewall, SIEMS, and DLP are all but standard, but meant to aid in detecting attacks. Once attacks occur and have slipped past the radar it's time to enter the world of threat hunting to discover attacker motives. Let us discuss how to leverage attacker techniques coupled with threat intelligence and incident response to foster active threat hunting engagements. This session will foster examples of tracing attacker movements, edging attackers out of your network, and creating proactive countermeasures.

Creating VM's from Forensic Images for Courtroom Presentation

One of the biggest hurdles in computer forensic testimony, is figuring out how best to approach all the technical terms, procedures and evidence that needs to be explained and presented to a "non-technical" courtroom. One of the best ways to overcome this hurdle is by providing the judge and jury with a "virtual tour" of the evidence. By harnessing forensic and VM technology, you can virtually "boot" a suspect's computer by creating a virtual machine from your forensic

image file (e.g., .E01, .DD, etc.), and viewing the system just as if you had physically brought the computer into the courtroom and powered it on. Attendees will learn the process of creating and booting a VM of a forensic image, and how they can also use this process to locate additional evidence that's not typically viewable via traditional forensic tools. Attendees will also learn useful tips and tricks on how to successfully introduce this in a courtroom setting.

Cyber Security Threat and Forensic Intelligence

Cyber threat intelligence and analytic is among one of the fastest growing interdisciplinary fields of research. It brings together researchers from different fields such as digital forensics, political and security studies, criminology, etc. to detect, contain and mitigate advanced persistent threats and fight against organized cybercrimes. In this session, the presenter will discuss some of the challenges underpinning this inter- / trans- /multi-disciplinary field as well as research opportunities.

Cybersecurity Risk Management - Aligning Contracts with Reality

In this session the presenter will review data breach and cybersecurity essentials with a focus on risk management in contracts and vendor collaboration. The session will share the current threat landscape, the key elements of cybersecurity preparedness, the pitfalls and promises of using insurance to mitigate risk, and the hidden tricks in common cybersecurity related contract provisions including incident response and notification, security practices and addenda, and meaningful risk allocation. The presenter will also review how to effectively utilize privilege to protect forensic investigations when a breach occurs.

Dark Web, Version 2: The New Challenge for LE

The Dark Web has changed dramatically in the past 18 months with the number of sites and services decreasing significantly. But illegal activity via Internet connected systems continues to rise. This session reviews the new methods that bad actors are using to locate fellow travelers, communicate, exchange data and media, and pay for contraband like stolen financial information (FULLZ). In this session, the presenter will illustrate the shift to end-to-end encrypted messaging, the use of Surface Web discussion groups and services like pastesites, and alternative obfuscation tools like TAILS, QUBES, and similar systems. Attendees will learn how to keep pace with the innovations the erosion of the Dark Web is encouraging with information about new tools designed for LE and intel professionals.

Deep in the Heart of Windows Memory Analysis

In many cases, memory analysis can provide access to evidence you can't obtain through "dead-box" forensics alone. Decrypted data, network activity, chat records, carved files, usernames and passwords, these are just some examples of evidence that may only be found in volatile memory. During this session, attendees will learn how to incorporate memory artifacts into their investigations and see what critical evidence they may be missing.

Digital Forensics in the Era of Fake News

Jurors are becoming more skeptical of forensic evidence and the authenticity of what is being presented in court. In the era of cyber warfare and technical innovation, digital media can be easily manipulated to sway opinions and jurors know it. Public awareness of digital tools, such as Photoshop, is high, and other digital manipulation techniques have gone viral on the web. This session will show how digital photographs, video, and voice recordings can be altered convincingly to fool even the most critical thinker.

Examining Security Threat Avoidance Theories

Between October 2009 through the end of 2017, 164 million patient records were affected in 1,138 health data breaches. The highest data breach resolution costs often occur in healthcare where recovery costs average $408 per record. This session will share the results of a research study conducted to determine which constructs influence one's intent to protect their personal computing device by testing the Technology Threat Avoidance Theory, the Protection Motivation Theory, and the Fear Appeals Model. This session will identify the one that best identifies one's intent so that organizations can strategize security training.

Fakes, Frauds and Forgeries a "Forensicator's" Guide to Questioned Digital Document Examination

This session discusses and demonstrates how to discover signs of forged/faked digital documents – specifically Microsoft office documents and PDFs. Using only free tools, techniques, and novel approaches, a forensic investigator will gain an understanding of actionable methods to uncover fraudulent documents and assist in questioned digital document examinations.

Forensic Analysis of the Windows 10 Activity Timeline

The Activity Timeline feature was released in Windows 10 version 1803. It tracks many types of activity including websites accessed, documents opened and edited, applications executed, and even details when a user was actively engaged in a specific activity. Its purpose is to remind users of past activities and allow them to continue activities at a later time, including across devices. Fortunately, it is also a gold mine for investigators. This session will present an examination of the timeline from the perspective of its usefulness to digital forensics investigations.

How the GDPR will Improve Your Bottom Line, Culture and IT Processes

While both the GDPR and the CaCPA have caused panic and fear in most corporate circles with rigorous rules and serious consequences, an in-depth review of all aspects of an organization will create an opportunity to improve the efficiency of the organization and must include every aspect of the business. This session will share why including all stakeholders in the review will give everyone ownership of changes and improvements, reducing costs, increasing efficiencies, and building camaraderie.

Investigations-Legal-Forensic "Statements of Work" - Don't Get Caught Without It

The best investigations, legal support tasks and forensic work have a strategy, plan and delivery outcomes and expectations. What's the scope of the work? Who's authorizing the work? What report work product is needed? This session will discuss why establishing a Statement of Work (SOW) to manage the engagement and delivery outcomes is non-negotiable. Attendees will learn the fundamental (and often neglected) art and value of: Using a SOW to initial scope and manage various aspects of the investigation; Effectively manage and document "authorization" to conduct the investigation; Manage and document scope creep; Effectively communicate time, effort and billing; and Provide the mutual agreement on the scope, type and intended purpose of the investigative work product.

Love to Work Out, but Who’s Watching?

Fitbit, Apple Watch, and Samsung devices not only track the heart rate, but also the location, payment information, messages, and more. This session will share how can this data be extracted; What is stored on the device; What’s is in the cloud; and How to get this data.

macOS: Forensic Artifacts and Techniques that are Essential for Mac Investigations

Mac investigations can be challenging for a number of reasons. Learn about the Apple File System (APFS) and the changes made as part of the update from HFS+, while discussing the best techniques for successfully completing macOS investigations. In this session we will also investigate APFS Operating System artifacts and files such as: KnowledgeC.db, FSEvents, Volume Mount Points, Quarantined Files, and bash history, providing context on how these artifacts will help connect the dots in your investigations.

Mobile Device Acquisition Approaches

This session will cover the most popular software methods of modern mobile device acquisition. The presenter will discuss the capabilities and limitations of each extraction method. The session will share: How to navigate through the file system of obtained dumps; What types of evidence could be found inside; and What mobile app artifacts can help in a course of a forensic investigation or an incident response case. In addition, the presenter will share tips on which methods are suitable for which devices.

Proving a Negative: Case Studies Illustrating Methods to Safeguard the Organization from Something That Didn't Happen

Organizations face growing scrutiny and uncertainty over breach and cyber incident response. Regulators and public perception demand that corporations disclose before even understanding the issue. This session will share three recent responses that are provided as case studies to illustrate both technical and strategic innovations required to protect the good name of good organizations. The case studies present distinct, fact-based solutions to the no-win situation of proving a negative.

Really Bad SysAdmin Confessions

It's a common belief that SysAdmins make great Infosec professionals. Many believe this is due to their wide knowledge of software and technologies. In reality, it's because THEY KNOW WHERE THE DEAD BODIES ARE! That's right. Learn from the mistakes of real sysadmins. During this session, attendees will witness and learn the mistakes of current and former Systems Admins so this doesn't happen to you!

Social Media, Digital Evidence and What Lurks in the Cloud

Today's online investigative research is more than a simple Google search, or a profile check on social media. We have an extraordinary amount of information floating throughout the internet and lingering on your digital devices. According to Statista.com in 2018, 2.26 billion of Internet users worldwide were social network users and these figures are expected to grow. When you combined what you can extract from the internet, add some information recovered from devices, you have a great combination of intelligences. This session will explore best practices for understanding the intelligence you can recover from social media, digital evidence and the cloud, which equals to a great combination of intelligence for your investigation.

The 007 Spy Games of the Bits, Bytes and Nibbles

Cyberattacks against our public and private institutions from nation-state and cyber-criminal threat actors are on the rise at alarming rates. With the ever-evolving threat landscape and the growing sophistication of threat vectors, the line between espionage and cyber war is blurred. The consequences to our political, military and economic well-being are significant and requires leveraging a degree of counterintelligence-like disciplines in cyberspace to prevent catastrophic results. This session will share why both private and public sectors must unite forces and leverage each other's capabilities on the front lines by launching counterintelligence-like operations in cyberspace in response to our adversaries' provocative actions.

UAS Forensics - Visualizing the Data

This updated session is designed to help investigators understand what data may be available from UAVs and what types of questions the data can answer. Then, using data from real world events, the presenter will guide attendees through the process of selecting and visualizing the data to answer specific questions in a vendor agnostic approach.

UAV (Drone) Forensic Analysis

The use of drones is rapidly growing and expanding into criminal enterprises and terrorist organizations. Correctional Facilities and deployed militaries are now dealing with UAV's on a regular basis and creating a new branch of digital forensics. This session is designed to introduce the investigator into the world of Drone Forensics and gain insight into the types of evidence the examiner is likely to encounter.

US Data Protection Law: Past, Present, and Future

This session will discuss the present state of US Data Protection including how and why our current system of data protection is highly fragmented by industry and jurisdiction. It will highlight some of the challenges this presents to business in terms of compliance, from both an operational perspective and a legal/regulatory perspective. In addition, there will be a brief overview of the EU's General Data Protection Regulation to contrast to the present state of US law. Finally, the session will gaze into the future, summarizing various state data protection laws that are under consideration.

When the Cyber Intrusion Alarm Rings, Will You Know?

Like the business environment, cybersecurity risk management is complicated. There are multiple variables changing subtly throughout the year. Similarly, expenditures on security skilled people, security related processes, and security technologies are subject to entropy and may lose potency as your company's cybersecurity risk profile changes. Legacy security activities can lose focus of adapting to emerging security risks in favor of automating routine security activities. This session will share why it may be time to rebalance risk controls and risk finance to strengthen Detection & Response capabilities!