Techno Security & Digital Forensics Conference

May 31 – June 3, 2020| Myrtle Beach, SC USA
SNEAK PEEK of CONFIRMED SESSIONS

(As of March 4, 2020 – All sessions and full details including times, dates, and speaker bios will be available March 31)

"Alexa, Lawyer Up": Digital Crime Scene Safety
Officer safety is paramount, and we consider safety before we visit a suspect's residence to execute a search warrant or conduct an interview. But do we consider how we could be injured by electronic devices or how they could be used maliciously to destroy evidence? Many officers may not have thought about this growing threat. During this session, attendees will learn how electronic devices could potentially injure police officers or cause evidence to be destroyed. A demonstration will be conducted to show how this might work.

A Statistical Examination of the Temporal Discrepancies in DVR Recordings
DVRs are typically suitable for measuring time periods of minutes or even a few seconds, but are they accurate enough to measure to sub-second accuracy? There are two potential sources for error; the input from the camera and output to the drive. There are strong reasons to believe that cameras themselves do not introduce significant error, but there the suggestion that DVRs don't is largely anecdotal. This session will discuss an ongoing study that aims to examine a variety of DVRs, isolated from cameras, to provide an answer with a statistical basis.

A Synergistic Approach to Information Security and Technology Audits
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.

A Unique Internet of Things (IoT) Forensic Analysis: Increasing Our Knowledge of the MyQ App on Our Mobile Devices
Inspired by the rising adoption of IoT technologies amongst the general population, this session offers a methodology for the effective forensic examination of two IoT devices that have independent and cooperative capabilities - the "MyQ" series of network-enabled garage door openers and the "Nest" series of indoor surveillance cameras. By conducting tests with a variety of forensic tools and identifying the local and remote-storage characteristics of both IoT devices, this session's contribution to the digital forensic community is two-fold: 1) increase the collective knowledge regarding the digital

artifacts associated with two popular IoT devices; and, 2) provide a methodology for conducting a comprehensive IoT-related mobile forensic investigation.

Active Directory: Negating Insider Attacks in Real-Time
Organizations have to be keenly aware of their own employees due to the advanced computer knowledge that most employees have today. If an employee becomes disgruntled, bored, challenged, etc., might give the employee reason to find holes in the computer network security. This combination of knowledge and reason has led to many organizations losing critical data, experiencing prolonged downtime, and loss of millions of dollars. Being able to track the different aspects of in insider attack can give administrators time to negate these attacks. This session will discuss the various ways that insiders attack Windows networks and how you can setup tracking to discover malicious behavior before it is too late.

An Unparalleled Method to Extract Evidence from Deleted/Damaged Virtual Machines
The latest reports predict that the coming years will see a significant growth of the data virtualization market. This indicates that digital forensics experts will have to answer an increase in demand for extracting evidence from virtual drives. That would not be a problem, per se. But only if the virtual disk allocation is available. So how do you recover data when this information gets damaged or overwritten? The attendees of the session will discover a surprisingly easy and unique solution to this seemingly difficult task.

APFS Imaging Considerations for Forensic Examiners
This session will discuss best practices for triaging Mac computers. As the security on Macs continues to increase the need to triage live in the field becomes more of a necessity. The presenter will explore the different options for triage based on the type of Mac encountered and look at the different scenarios involved including T2 chipset vs. Non-T2 chipset, APFS, target disk mode, volatile data and the newest challenges from Catalina the latest Mac operating system. In addition, the session will cover the importance of collecting passwords on the scene and some tactics for acquiring them.

Architecting for Incident Response in the Cloud
This session will look at how systems can be designed or re-architected to take advantage of cloud-based technologies not just to prevent incidents but prepare for and respond to, incidents. The presenter will share ideas and technologies that are applicable across cloud providers will be discussed. Additionally, it will look at some specific examples related to incident response in a few of the larger cloud provides will be touched upon.

Auditing and Securing Your Web-enabled Applications
This session will define a technical audit program covering key web application building blocks and significant risks, and systematically sort through the available cyber security safeguards in today's complex Web-enabled applications. Topics covered include: How to identify and assess cyber security control points and software building blocks in a multi-tiered web application; Understand the risks and causes associated with different types of cyber-attacks on web applications; and Gain familiarity with industry best practices for secure web application design and operation

Auditing Cyber Risks in Robotic Process Automation (RPA)
Robotic Process Automation (RPA) promises to revolutionize business processes, cutting cycle times from days down to minutes, practically eliminating manual errors, improving audit trails; the dawning of a new age. But within this dawn are emerging shadows. Is RPA yet another tool in the arsenal of the

control professional, or is it in fact the hacker's best friend? This session will separate hype from reality and examine what auditors really need to know when it comes to RPA, the good, the bad, and the ugly.

Beyond Chip Off: IPhone/Samsung Board-level Hardware Troubleshooting for Encrypted Devices
This session will showcase some of the common "signature faults" that occur in iPhones and modern encrypted android devices. We will show you what diagnosis and repair of these faults looks like by troubleshooting live cases during this session with audience participation. Attendees will also learn what a typical microsoldering setup looks like, including the relative costs of common equipment, and what type of training/experience would be required to safely and efficiently perform logic board repairs through microsoldering.

Best Practice for Drone Extraction and Analysis
Drones are exploding in popularity and their operational capabilities are advancing rapidly as well. Corrections agencies, police and military organizations around the globe are actively developing methods to counter this growing threat. This session n will focus on introducing best practice for drone extraction and analysis. The audience will get a broad understanding about the best way to extract, decode and view the data quickly when a drone is recovered.

Breaking Health Clouds. Fitbit and Other Health Trackers: Obtaining Vital Evidence for Your Investigation
The amount of data collected by health trackers is amazing: from step count and heart rate to running and walking distances with exact timestamps and lots of geolocation data. Some of it goes directly to Apple Health and then to Apple iCloud, while other manufacturers (Samsung or FitBit) keep data in their own clouds. Something goes to Google Fit. Apart from privacy issues, think of how much data can serve as essential evidence during investigations.

Broken Arrow
During this session, attendees are provided a framework to assist domestic abuse victims with detaching their abuser/stalker from their real and digital life. The framework provided to the audience is identical to what is taught to NATO and CIA officers to eliminate counterintelligence risks.
Attendees will learn how to: Control the digital and physical environment; Identify Identity theft and report it; Understand data availability.

Cloudy with a Chance Of?
This session will discuss: Cloud Security Considerations; Shared Responsibility and Contract Language; Cloud Security Requirements; Education and development of effective processes and Governance; and Security Controls Validation

Cyber Smash and Grab? Cleaning up After Digital Crimes
In a cyber smash and grab, the attacker gains access to an organization to facilitate a quick financial gain. The victim organization often suffers damage beyond simple financial loss. Damage occurs through regulatory penalties, shareholder lawsuits, loss of reputation, and uncertainty of the integrity of remaining data. Recent incident response experience underscores the role of preventative steps and incident response methods. This session will share a broader understanding of this complex risk environment and provide illustrations from actual incidents worked by the presenters within the last year. Client experiences include: Ransomware attacks requiring regulatory disclosure; Compromise of E-mail accounts to direct fraudulent transactions; and Business continuity and IT operations during cyber incidents.

Cyberinsurance: When the Cyber Claim Comes In
Ransomware, business interruption, compromised vendors, nation-state attacks – cyber claims run the gamut of risks. Are cyber policies meeting the expectations of insureds when it comes to claims? How can the cyber insurance industry better communicate the value of the coverage in advance of a claim? The session will feature research from Thomson Reuters & SANS Institute based on a wide-ranging discussion with insurance carriers and cybersecurity experts on determining the financial impact of cyber claims, the difficulties inherent in attack attribution, as well as misconceptions about cyber coverage.

Cybersecurity Frameworks and Assurance Services
This session is an introduction to cybersecurity frameworks and will cover a handful of the more popular frameworks, comparing and contrasting each, showing the pros and cons of implementation and certification. It is designed to be at a high enough level, that it wouldn't interfere with anyone else's presentation who has selected a single framework or assurance service to drill down on. Frameworks include are: NIST, ISO, COBIT, SOC, HIPAA, HITRUST and PCI.

Cybersecurity Merger and Acquisition Due Diligence
During a merger or acquisition, you get all the assets of the acquired organization, but you also take on all their liabilities. That's why due diligence has been so important for M&A. Cybersecurity posture is often not considered during M&A due diligence checks, but it absolutely should be. With minimal changes to standard threat hunting methodologies, M&A cybersecurity due diligence is relatively easy to perform. In this session, the presenter will explain the principles of general threat hunting and then show what changes are required to maximize value for M&A due diligence assessments.

CyberTheft of Trade Secrets and an Attorney's Ethical Obligations During a Breach
From the solo entrepreneurs to Fortune 100 companies, trade secrets may be a most valuable asset to any company, large or small. It is difficult to overestimate their importance in the global economy: According to the U.S. Chamber of Commerce, trade secrets make up 70% of the value of U.S. public companies' portfolios. Not surprisingly, such secrets are high-value theft targets for domestic and foreign thieves. A report from the Commission on the Theft of American Intellectual Property estimates that the domestic economic damage attributed to trade secret theft exceeds $300 billion annually. This session explores the diverse world of trade secrets, how trade secrets differ from other forms of intellectual properties, the legal aspects of trade secrets, some recent case law and legislation, and general ethical and discovery considerations of attorneys responding to a security breach.

DarkWeb fundamentals and Investigation Techniques
The Dark Web has become a household term synonymous with criminal activity targeting both public and private sectors. Even the most careful user utilizing the Dark Web will slip up and eventually reveal their identity, location and other pointers about their systems. While accessing the Dark Web is straightforward, safely finding the intelligence you need is the challenge. This session will explore techniques that can be used to exploit information leaked through the system to expose the person behind the mask. Using best techniques to conceal your identity this session will describe how a TOR browser functions and methods for safe anonymous usage throughout an investigation. We will discuss how the clear web can reveal clues to a user's activity on the Dark Web and explore popular markets where contraband and information is sold.

Data Breach Investigations: The Good, the Bad and the Ugly

This is an action-packed lesson learned session for public and private sector IT, InfoSec, and executives. Learn from other organization's mistakes and improve your organizations' incident response capability at all levels. This is not an industry recap of data breaches, but a chance to obtain insights from an incident response team to experience what works and what doesn't. While frequently much focus provided on preventing incidents, often too little is emphasized on handling data breaches effectively once they do occur. This session will help attendees learn where they are excelling, areas where incident response capability needs to be improved, and learn of issues you haven't considered yet. Get exposed to the Good, the Bad, and the Ugly of Data Breach Investigations.

Department of Homeland Security: CISA Cyber Threat Update
Current trends and threats in cyber security and the evolving DISA no cost services to combat them.

Digital Analysis of Audio & Video Recordings
Forensic analysis of datasets is continuing to grow more complex and include audio and video files with greater frequency. Typical investigations in both the public and private sector involve audio and video recordings. Forensic analysis of multi-media files has not evolved with the speed of other data.
This session will demonstrate workflow that will enable examiners to automatically identify audio files and process those files, transcribe the words spoken, identify gender, emotion and transcription confidence and render the recordings keyword searchable. Additionally, the results of keyword searches will point to the time in the recording where the keyword was identified enabling analysts to go directly to the responsive part of the audio file instead of listening to the entire recording. This workflow can also be used on the audio track of a video recording.

Digital and Multimedia Forensics from Crimes Committed on the Dark Net - Capability Gaps and Current Research Needs for State and Local Law Enforcement
Law enforcement is faced with a multitude of challenges in acquiring digital evidence from crimes committed on the dark net: TOR's built-in encryption, the use of crypto currency, and the obfuscation of the ownership of that medium of exchange through tumblers. The National Institute of Justice, working with federal, State, and local law enforcement, industry, and academia have identified the capability gaps in the acquisition, analysis, and reporting of digital evidence from crimes committed on the dark net, and areas of research that could be pursued. This session will highlight those capability gaps and clarify the practitioner community's research needs in this area.

Digital Document Archaeology: Excavation into .PDF and .DOCX Files to Unearth Information
Forensic examiners and investigators may only look at visible document metadata. Still, there may potentially be much more information available "buried" internally within a file if we conduct a bit of straightforward document "archaeology." This session is about "excavating" into PDF and DOCX documents and examining the internal contents and structures to unearth details, which may provide the additional evidence needed in an investigation. Attendees will see clear examples and forensic analysis using freely available tools to identify potential evidence such as document creation, alteration/modification, origins, authorship, dates/timelines.

Dude, Where's My (encryption) Keys?! a Reverse Engineer's Take on Secure Messaging for Mobile
Would you consider buying a new car that had no keys, completely invisible locks and a written commitment from the dealership stating the car has the best security in the industry, can only respond to you, and won't be stolen by any random person walking by? In the world of secure messaging, this proposition plays out regularly-- the general public are expected to make informed decisions on which apps they should trust their private message data with. They make this decision based on marketing

jargon, download counts, customer reviews, word of mouth, and the media. Security, and by extension secure messaging, are more commonly at the forefront of our minds more than any time in history. This presentation will cover a real-world example where reverse engineering proved indispensable in refuting an alibi for a homicide investigation. This session explores just how reliable these sources are, from the perspective of a reverse engineer. This session will delve into reverse engineering methods that can be used not just by those developing forensic tools, by forensic examiners in the trenches looking to validate or identify data from unknown sources Frida, a free toolkit for dynamic binary instrumentation (DBI), can be used by forensic examiners to incredible effect when static analysis fails.

Enterprise Ransomware: The Boogieman of Governments and Corporations Alike
Enterprise ransomware has undoubtedly garnered the most news coverage of information security threats in the past few years. Unlike complex or esoteric threats, enterprise ransomware is readily understandable to C-level executives and government leaders: it stops their organization from functioning and brings unwanted public and media attention. This session will discuss four of the more common along with their respective threat actor Tactics, Techniques, and Procedures. Attendees will take away how to approach these enterprise-wide incidents to quickly identify the initial infection vector threat actor actions on the objective, lateral movement, and method of ransomware deployment.

Enterprise Social Media Investigations
Current threat vectors show targeted attacks on social media accounts owned by enterprises and their employees. Most organizations lack a defense-in-depth strategy to address the evolving social media threat landscape. The attacks are outside their network, commonly occur through their employee's personal accounts, and circumvent existing detection technologies. This session will explore the taxonomy of social media impersonation attacks, phishing scams, information leakage, fake news, espionage, and more. In addition, it will provide a method to categorize these threats and enhance DFIR strategies. Real world examples will be demonstrated providing deep and tangible insights into this systemic problem.

Forensics in the Cloud
This session will discuss and demonstrate the process of forensics in the cloud. We will look at both AWS and Azure and will address secure communications, encryption, authentication, dynamic provisioning, evidence handling, and processing evidence in the cloud.

How Artificial Intelligence Is Revolutionizing Investigation for Law Enforcement
Artificial intelligence (AI)-backed technologies are helping law enforcement overcome challenges of resource and manpower shortages, while optimizing investigation productivity and performance. This session will explore how AI can be used to process and analyze digital data sources, such as video surveillance footage, to advance investigations and bolster intelligence. Attendees will understand how digital data can be made searchable, quantifiable and actionable, exploring real use cases from police departments in New Orleans, LA, Hartford, CT and Dearborn, MI, that demonstrate how AI is revolutionizing investigation efficiency and effectiveness.

How Do You Solve a Problem Like Deepfakes?
This session will begin with an overview of the state-of-the-art of the technology which creates deepfakes, and (more importantly) of the technology which can be deployed to detect deepfakes. Thereafter, the presenter will analyze the technological challenges which are hampering the realization of effective and efficient solutions for use in the real world, towards combating deepfakes. The presenter will share insights into new advances and tools, and their implications for digital forensics

practice. Attendees can expect to: Gain a good appreciation of deep learning, including its strengths and weaknesses; Acquire a good awareness of the technology for detecting deepfakes, and the challenges that the detection technology faces; and Gather some background knowledge and thus gain some ability to manage the expectations of oneself or others, regarding the autonomy of deepfakes detection tools when deployed in digital forensics.

Hundreds of Apps and Not Enough Time? There's a Solution for That

With the pace of change in mobile apps, including highly encrypted apps, law enforcement agencies and vendors are playing catch up when it comes to reverse engineering the structure of apps and recovering digital evidence quickly and in a forensically sound manner. In this session, we will review several new methods to acquire and analyze data from both native and third-party apps, including using Python scripting, app downgrades and others. The presenter will review best practices on how to parse through vast quantities of data to get straight to the information you need for your investigations.

Industrial Control System Security: Protecting the Systems That Control Our World

Industrial Control Systems (ICS) control the world we live in. The power grid, our water supply, sewage treatment, petrochemical refineries, mass transit, and manufacturing centers are just a few examples of critical infrastructure that depend on ICS. This session will discuss the history of cyberattacks on ICS, the current ICS threat landscape, how ICS cybersecurity differs from traditional IT cybersecurity, and what common security controls would have prevented or largely mitigated previous cyberattacks on ICS.

Internet Crimes Against Children Investigative Techniques

This session provides you with an understanding of investigative techniques associated with reports of Internet crimes, focusing on child exploitation and the CyberTipline reports investigated by members of the Internet Crimes Against Children (ICAC) task force. Attendees will receive an overview of the topic, as well as learn techniques that will assist you identifying the suspect source, how to preserve data, legal process, interviewing techniques, and the effective apprehension of predators who use technology to exploit children.

Internet of Things: The Latest Security Risks Posed by Convenience

The Internet of Things has been evolving for years - and 2020 presents many of the most exciting developments in Internet-connected devices ever. Consumers seeking convenience, healthcare providers seeking more advanced solutions, and corporations seeking better connectivity are banking on IoT progress. However, the privacy and security communities are throwing down yellow caution tape as, unsurprisingly, the technology is moving by leaps and bounds, and relevant regulation and security considerations are left in the dust. This session reviews the latest Internet of Things offerings, the unparalleled benefits many provide, and the slightly less rosy picture colored by the relevant security and privacy risks.

Intro to Blockchain & Crypto Currency Investigations (Lab)

With the increasing importance of privacy and security in today's business world coupled with the advancement and acceptance of cryptocurrencies such as Bitcoin and Ethereum, today's digital forensic professional is behind the proverbial power curve if they do not have a basic understanding of emerging blockchain and cryptocurrency technologies. During this session we will have a hands-on experience cover the following topics: Understand blockchain and transaction technologies; Examine raw data on blockchain ledgers; Research information about specific addresses and transactions; Follow the cryptocurrency trail Note: This lab is BYOL (Bring your own laptop) however any basic laptop that can browse the internet will suffice.

Is Your Database Leaking Encrypted Data?
Forensic tools often operate in non-ideal conditions (e.g., damaged devices or corrupted files) or in adversarial conditions (e.g., user purposely deleted files). These tools reconstruct data independently (at the byte-level) from an untrusted environment. Existing data encryption research considers disk encryption, file encryption, and client-side encryption. However, such work does not consider data that is stored and managed by a database management system (DBMS). DBMSes support their own native encryption mechanisms, managed independently from file-based or client-side encryption. This session will provide attendees with an understanding of: The role of different memory structures in DBMS data processing flow; A survey of built-in encryption mechanisms supported by different DBMS vendors; and the scope of data exposed by different categories of common SQL operations.

Leveraging PowerShell and Python for Incident Response and Forensics
Bring together Microsoft's PowerShell and Python to address digital investigations and create state-of-the-art solutions for incident response teams, and forensic investigators. Attendees will learn how to join PowerShell's robust set of CmdLets and access to the internals of both the MS Windows desktop and enterprise devices and Python's rich scripting environment allowing for the rapid development of new tools for investigation, automation, and deep analysis. This session will deliver a practical approach that provides an entry point and level playing field for a wide range of attendees; investigators, incident response teams, researchers, students and academics to participate.

New Tools, Techniques, and Emerging Challenges in macOS Forensics
This session will discuss recent advancements in macOS forensics as well as emerging challenges. This will include new tools and techniques as well as a discussion of changes in macOS Catalina that are relevant to forensic analysis.

New Ways to Commit Crimes... and New Ways to Solve Them (with Cars)
Modern vehicles pack increasing amounts of connected sensors and features… which can be exploited by criminals to commit all sorts of old crimes in new ways. It is already happening, and law enforcement often don't know what to look for, and where, to solve those crimes. In this session, attendees will learn how criminals can easily steal cars, commit fraud and identity theft, stalk, use the cars of unsuspecting citizens as escape vehicles, and even commit murders and terrorist attacks leveraging new car technologies. Most importantly, attendees will learn how to go beyond traditional vehicle forensics and know where to look and what questions to ask to solve these crimes.

Reinventing the SOP for Corporate Investigations
When completing a digital forensics investigation in a corporate setting, you're often working against the clock to deliver results to your executive stakeholders. Although hard work is important, there are a number of tips and tricks that can help you work smarter to save time and find the relevant results that you're seeking. In this session the presenter will share a number of innovative methodologies that help teams meet the demands of their customers while competing investigations as efficiently as possible.

Securing Microsoft Azure
You're either about to stand up resources in Microsoft Azure or you're already there but unsure of your security configuration in Microsoft's cloud. What should you have configured? What additional resources do you need? What small tweaks could you do to get better reporting, better alerting, and a tighter overall security posture? In this session, we'll look at the bare minimums everyone should have in their Azure environment. The presenter will discuss both what should be configured on the security

side, but also what you need to plan for to avoid single points of failure and easier recovery. From there, the presenter will look at typical deployment scenarios and what you should add to deal with your increased risk. Finally, we'll talk about what on-premises resources you can leverage to reduce your overall Azure bill.

Selecting Security & Privacy Controls Using NIST SP 800-53
This session will cover how your team can use the NIST Security and Privacy Control Catalog in NIST SP 800-53 to identify and select IT security controls, identify common controls, and tailor a security control baseline. This session maps to the Select step in the NIST Risk Management Framework and will cover the guidance outlined in SP 800-53.

Slacking on Insider Threats? Investigative and Monitoring Approaches to Use Within Slack to Locate Bad Actors
It's no secret that Slack's popularity has exploded in recent years- once dubbed "the email killer", organizations have implemented Slack as an efficient collaboration environment either alongside email, or in some instances, replacing email as their primary internal communication mechanism. Although a large portion of communication and file transfers are taking place within Slack, often organizations are missing this crucial evidence during an investigation, either due to a lack of understanding or improper retention. Furthermore, organizations should be taking a proactive investigative approach and onboarding Slack as part of their insider threat program. This session will review a case study where Slack data was crucial to the investigation. Additionally, the presenter will review current investigative approaches, both reactive and proactive, as well as mechanisms for conducting insider threat investigations in Slack.

Smartphones and Social Media
Smartphones are the most common connection to the internet and can contain a wealth of information when it comes to an investigation. Over 396 million downloads of social media Apps occur in one quarter, and this number is growing exponentially. This session will share how attendees can find this data to capitalize on the value it can add to their investigation.

Social Media and Open Source Intelligence (Lab)
As criminal use of the Internet becomes more and more sophisticated, law enforcement's ability to locate and act on publicly available information is more crucial than ever. Investigators must be able to turn information from varied sources into actionable intelligence as quickly and efficiently as possible. This session covers mainstream social media sites as well as third-party websites that can allow for quicker identification of potentially relevant information.

Stomping the Puddles: An Investigators Look at the Exploits Furthering Our Access to iOS Devices
Most are aware that Checkm8 and checkra1n provide unique access to iOS devices that those outside of Law Enforcement previously weren't able to leverage. What do these exploits offer that set them apart from current ubiquitous methods of gathering iOS data? How big is the footprint left behind and will it impact your investigation? It is likely examiners will employ the use of the Checkm8 exploit, whether consciously deciding to do so or because a commercial vendor will implement it into their process. We will discuss how much access you are getting and how it compares to the solutions that already exist. This session will discuss the perpetuity of the exploit and project how long it will remain relevant. Not only will we stomp around in the puddles, we will take a deeper look at the differences in using these exploits versus using traditional acquisition methods for mobile forensics.

Taking a Byte out of Chromebook Analysis

A new challenge of forensics is upon us as Chromebooks become more and more popular. One of the challenges is understanding the difference obtained from different types of acquisitions as well as the cloud. Due to this challenge, a group of 30 forensic examiners came together to workshop the problem at a Brews and Bytes event in Denver, Colorado. From that perch in the mile-high city, we assessed the data in the cloud, as well as more terrestrial images from Chromium VM and data from Chromebook acquisitions. The analysis team looked at different locations where data can reside and compared the different types of acquisitions. The team then worked to develop the comparative analysis we will present of the types of data that can be recovered from different sources associated with Chromebooks and where it resides.

The Butterfly Effect Theory: Web Intelligence and the Lone Wolf Shooter Syndrome

In the last few years, mass casualty shootings have posed increasing threats and are rapidly becoming a global epidemic. With each attack inspiring other terrorists, or domestic extremists, these events can leave digital traces across the internet that can identify some clear and visible links to seemingly unconnected events. This session will discuss how Law Enforcement and Intelligence Agencies can stay one step ahead with the power of Artificial Intelligence-enabled web investigations. The presenter will discuss how AI-enhanced investigation platforms overcome human limitations, helping pinpoint and predict early warning signs, alerting us to concerns for optimal response times.

The Cat and Mouse Game with iOS Forensics

iOS forensics has been a hot topic over the last few years. Apple is constantly strengthening its security measures on their devices such as iPhones, iPADs, Apple TV, Apple Watch etc. This was is designed to prevent hackers and by doing so law enforcement investigators access to its devices, Things like remote phone wiping, not allowing the passing of data through lightning cable, requests to enter a PIN after potentially suspicious actions (like changing a SIM card), 6-digit PIN by default etc., make digital investigations much more difficult. There are, however, some breakthrough advances in the field of Apple device forensics, such as checkm8 and checkra1n jailbreak. This session will discuss latest advances in iOS forensics and about proper process of analyzing iDevices.

The Challenges of Cloud Data Collection - Why Making Assumptions Can Be Dangerous

In this session, attendees will learn How to identify collection challenges for cloud data and ways to avoid costly pitfalls; Ways to effectively apply search terms and achieve verified results; and Methods to authenticate cloud created documents.

The Dangers of Frameworks, a False Sense of Security

Implementing Regulation & Frameworks with No Context Leaves Perception of Security. the Key to Security Is a Well Thought Implementation of the Framework by a Common-sense Approach
You've implemented security exactly according to regulation and in accordance to the framework. You've implemented the controls, deployed the tools and followed the procedures. Now, your enterprise must be secure, or is it? Virtually every framework today uses the same risk rating methodology, yet the losses are up instead of down. This session will cover why unfortunately, organizations that implement blindly without applying the regulations and frameworks to its specific organizational context, have a false sense of security. Whether it's NIST, PCI, ISO, SOX, HIPPA, etc., the key to compliance and security is a well thought out plan, implementing the framework by a common-sense approach.

The Future of Inter-Tool Functionality and Informational Resources

Digital investigations are complex undertakings collecting and analyzing information from a diverse range of sources and in this complexity, defensible findings are often-times hard to create. As a community, we use various tools and information sources that offer different and overlapping capabilities, and we manually combine findings from these tools and sources in an effort to develop a full understanding of the digital evidence at hand. Our community needs a standard way to achieve integrated information interoperability regardless of the type of investigation, authority of the investigator, the tool or source used, or the location of the investigator's jurisdiction. To achieve this, a cross-section of leaders in our community established the Cyber-investigation Analysis Standard Expression (CASE) and Unified Cyber Ontology (UCO) communities to create this standard approach. This presentation will share coordinated projects and applicable use cases that will help all of us interoperate better in the future to allow our tools to work together and incorporate additional sources of information.

The Video Narrative: Harness the Power of Condensed Videos for Suspect Identification

Once investigators have completed the sometimes-troublesome tasks of video evidence recovery and footage playback, how do organizations identify suspects? How many people actually view footage of the incident instead of some still images on a bulletin? Attendees will learn how Police Agencies are using condensed videos on internal and external platforms (Social Media, YouTube), for suspect identification, sometimes with amazing results. The session will share a brief overview about how law enforcement agencies around the world have been using social media and video hosting platforms for suspect identification.

Testifying in Court - A Guide for First Timers and Pros

In this session the presenters will take an informative and sometimes lighthearted look at what it means to testify in court, what to expect, how to prepare, what to do and more importantly not do. Attendees will understand what it means to be subpoenaed, learn what Voir Dire means and who Duabert was. The session will discuss body language and eye contact, working with juries and how not to get cross under cross.

Uber Resources for Law Enforcement Investigations

With an average of 18 million trips a day and growing, Uber is one of the most widely used transportation companies in the world. While critical incidents and criminal activity involving Uber are a fractional percentage of overall trip volume, the billions of trips executed a year allow this comparable lightning strike to happen enough that law enforcement needs to understand the tools and support that Uber can provide to their investigations. Uber's Law Enforcement Operations Team is dedicated to providing law enforcement training and education that will prepare them for the changing transportation landscape in their cities and jurisdictions. This session will impart insight into how Uber can assist them in their investigations.

Using Drone Forensics in Criminal Investigations

NOTE: This presentation is for Law Enforcement only. Proof of identification will be required to attend.

As technology evolves, so must law enforcement's approach to digital forensics. No longer can an investigator rely solely on what is now considered traditional electronic device extractions to build their case. With the steady increase in small Unmanned Aerial Systems (sUAS) "aka Drones" being used by hobbyists and professionals alike, law enforcement must be prepared to add this expansive dataset to their case package. Agents from U.S. Customs and Border Protection will discuss how a sUAS intercepted along the border near San Ysidro became the first Federal conviction of a narcotics smuggler using the

unmanned delivery platform. The presentation will focus on preservation of the evidence to actual extraction and analysis of the aircraft's flight logs. The Case Agent will discuss how he integrated this unique set of data into the prosecution package and how it affected his investigative methods. The conclusion will cover how this case has since evolved CBP's sUAS data forensic capabilities and how CBP assists agencies around the world grow and develop their own drone forensic capabilities.

Using Wi-Fi to Develop Case Leads and Improve Intelligence
Attendees will learn how free tools can be used to leverage Wi-Fi signals in criminal investigations. Both ends of Wi-Fi communications, the client device and the access point, can be valuable in investigations. Attendees will also be introduced to some important legal considerations when considering Wi-Fi evidence, including the 4th Amendment and Electronic Communications Privacy Act (ECPA), and how the use of some tools likely violate the law.

Video Forensics Casework: Issues, Solutions, Trends
This session will share a case study that will answer the questions: the most common requests for video analysis? What are the most common scenarios and sources of image and video data during investigations?; What are the most problematic video formats?; and more. This session will help stakeholders to better understand scenarios, issues, and chances of success for image and video forensics activities. It will also help the research community to understand today's challenges and, possibly, focus efforts on solving them.

What Could Be Lurking in a Windows Computer
Internet artifacts can be a tremendous treasure trove of investigative data, but that is not all. Windows users utilize desktop messaging apps like Telegram, WhatsApp, Line, and others to communicate. Not to mention the user's passwords and tokens are left, waiting to be discovered. This session will share why using this information investigators can build not only a great case but utilize the uncovered credentials to open the case wide open.

Which Tool Used Doesn't Matter
This session will cover; Why patching is the best method to secure an endpoint; Why the tool used to discover what endpoints are unpatched doesn't matter if you understand how the data is discovered; and Why often what's missing is that while an unpatched system flags in vulnerability scanning tool.

Zipfile Forensics 2
This session will address the date anomalies of decompressed files as well as look at zipfile fragment and why some do not repair with automated tools. Attendees will leave the session with the ability to rebuild a zipfile using a hex editor and dos commands as well as provide the knowledge to support the file efficacy of the rebuilt file in court.